ISACA®
Trust in, and value from, information systems

ESCENARIOS DE RIESGO

Utilizando COBIT® 5 para Riesgos

COBIT® 5
AN ISACA® FRAMEWORK

Acerca de ISACA®
Con más de 115,000 integrantes en 180 países, ISACA (*www.isaca.org*) ayuda a empresas y líderes de TI a construir confianza en, y maximizar el valor de, la información y los sistemas de información. Fundada en 1969, ISACA es una fuente confiable de conocimiento, normas, comunidad y desarrollo profesional para los profesionales en auditoría de sistemas de información, aseguramiento, seguridad, riesgos, privacidad y gobierno. ISACA ofrece el Cybersecurity Nexus™, un completo conjunto de recursos para los profesionales de ciberseguridad, y COBIT®, un marco de negocio que ayuda a las empresas a gobernar y gestionar su información y su tecnología. ISACA también promueve el avance y valida las habilidades y conocimientos críticos para el negocio, a través de las credenciales globalmente respetadas: Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk e Information Systems Control™ (CRISC™). La asociación tiene más de 200 capítulos en todo el mundo.

Descargo de responsabilidad
ISACA ha diseñado y creado *Escenarios de Riesgo Utilizando COBIT® 5 para Riesgos* (el "Trabajo"), ante todo como un recurso educativo para profesionales en el área de aseguramiento, gobierno, riesgo y seguridad. ISACA no afirma que el uso de cualquier componente del Trabajo asegure un resultado exitoso. El Trabajo no debe ser considerado como inclusivo de toda la información, procedimientos y pruebas apropiadas, ni tampoco como excluyente de otra información, procedimientos y pruebas que se aplican razonablemente para obtener los mismos resultados. Para determinar la conveniencia de cualquier información específica, procedimiento o prueba, los profesionales de aseguramiento, gobierno, riesgo y seguridad deben
aplicar su propio criterio profesional a las circunstancias específicas presentadas por los sistemas específicos o por el entorno de tecnología de la información.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Correo electrónico: *info@isaca.org*
Sitio web: *www.isaca.org*

Envíe sus comentarios a: *www.isaca.org/riskscenarios*
Participe en el Centro de Conocimientos de ISACA: *www.isaca.org/knowledge-center*
Siga a ISACA en Twitter: *https://twitter.com/ISACANews*
Únase a ISACA en LinkedIn: ISACA (Oficial), *http://linkd.in/ISACAOfficial*
Dé un Me gusta a ISACA en Facebook: *www.facebook.com/ISACAHQ*

Escenarios de Riesgo Utilizando COBIT® 5 para Riesgos
ISBN 978-1-60420-632-6

AGRADECIMIENTOS

ISACA desea agradecer a:

Desarrollador líder
Urs Fischer, CISA, CRISC, CIA, CPA (Suiza), Fischer IT GRC Beratung & Schulung, Suiza

Equipo de desarrollo
Evelyn Anton, CISA, CISM, CGEIT, CRISC, UTE, Uruguay
Robert E Stroud, CGEIT, CRISC, CA, EE.UU.
Mike Hughes, CISA, CGEIT, CRISC, 123 Consultants GRC Ltd., Reino Unido
Elza Adams, CISA, CISSP, PMP HP, EE.UU.
Jimmy Heschl, CISA, CISM, CGEIT, Experto ITIL, bwin.party digital entertainment plc, Austria
Eduardo Ritegno, CISA, CRISC, QAR (IIA), Banco de la Nación Argentina, Argentina
Andre Pitkowski, CGEIT, CRISC, APIT Informatica, Brasil

Revisores expertos
Mohamed Tawfik Abul Farag, KPMG, Egipto
Mark Adler, CISA, CISM, CGEIT, CRISC, CCSA, CFE, CFSA, CIA, CISSP, CRMA, CRP, Wal-Mart Stores, Inc., EE.UU.
Gerardo H. Arancibia Vidal, CISM, CRISC, Ernst & Young, Chile
Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, Reino Unido
Vilius Benetis, CISA, CRISC, PhD, NRD CS, Lituania
Jean-Louis Bleicher, CRISC, Francia
Graham Carter, CISA, CGEIT, ABB Limited, Suiza
Richard Cartwright, CGEIT, ISP/ITCP, ITIL, PMP, MZP Solutions, Canadá
Katalina Coronel Hoyos, CISA, SASCURE Cia. Ltda., Ecuador
Gabriel Croci, CISA, CRISC, SOMOS Consultancy Services, Uruguay
Diego Patricio del Hoyo, CISM, CRISC, CISSP, Westpac Banking Corporation, Australia
Leela Ravi Shankar Dhulipalla, CGEIT, Asesor Certificado COBIT, Entrenador Acreditado COBIT 5, PMP, Venlee IT Consultancy LLP, India
Joseph Fodor, CISA, CPA, Ernst & Young, LLP, EE.UU.
Giovanni Guzmán De León, CISM, ITIL, CFC, ISO 9001, Candidato Doctora, Consultor Independiente, Guatemala
Jason Hageman, CISA, ITIL V3, MGM Resorts International, EE.UU.
Tomas Hellum, LinkGRC, Dinamarca
Sharon Jones, CISA, MGM Resorts International, EE.UU.
Masatoshi Kajimoto, CISA, CRISC, Consultor Independiente, Japón
Satish Kini, CRISC, CISSP, Asesor Certificado COBIT 5, Firstbest Consultants Pvt Ltd., India
Vaman Amarjeet Gokuldas Kini, CISA, CISM, CEH, CISSP, LPT, 27KLA, The World Bank Group, India
Shruti Shrikant Kulkarni, CISA, CRISC, CISSP, CPISI, CCSK, ITIL V3 Expert, Infosys Technologies Limited, India
John W. Lainhart, CISA, CISM, CGEIT, CRISC, CIPP/G, CIPP/U, IBM Global Business Services, EE.UU.
Michel Lambert, CISA, CISM, CGEIT, CRISC, Ministere de l'Agriculture, des Pecheries et de l'Alimentation du Quebec, Canadá
Romualdas Lecickis, CISA, CISM, CGEIT, CRISC, NRD CS, Lituania
Debbie A. Lew, CISA, CRISC, Ernst & Young LLP, EE.UU.
Sebastian Marondo, CISA, CISM, NRD-EA, National Audit Office- Tanzania, Tanzania
John Simiyu Masika, CISA, CISM, Kenya Airways Ltd., Kenia
Radmila Mihajlovic, CISA, Consultor, Canadá
Lucio Augusto Molina Focazzio, CISA, CISM, CRISC, ITIL, GovernaTI, Colombia
Oscar Moreno Mulas, CISA, OKY Consulting/Zelaya Rivas Asociados, El Salvador
Raphael Otieno Onyango, CISA, BCOM, CPA (K), Ecumenical Church Loan Fund – Kenia, Kenia
Abdul Rafeq, Wincer Infotech Limited, India
Vittal R. Raj, CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA, Kumar & Raj, India
Franco Rigante, CISA, CRISC, PMP, Grant Thornton Argentina, Argentina
Salomon Rico, CISA, CISM, CGEIT, Deloitte México, México
Eddy J. Schuermans, CGEIT, ESRAS bvba, Bélgica
Paras K. Shah, CISA, CGEIT, CRISC, CA, Vital Interacts, Australia
David Sheidlower, CISM, Health Quest, EE.UU.
Emil David Skrdla, CISA, CISM, CGEIT, CRISC, ITIL V3, PCI ISA, PCIP, The University of Oklahoma, EE.UU.
Gustavo A. Solís, Grupo Cynthus, S.A. de C.V., México
Mark Stacey, CISA, FCA, BG Group, EE.UU.

AGRADECIMIENTOS *(CONT.)*

Revisores expertos*(cont.)*
Donald T. Steane, CIA, CMA, CPA, CRMA, DTS Consulting Services, Canadá
Dirk Steuperaert, CISA, CGEIT, CRISC, ITIL, IT In Balance BVBA, Bélgica
Louis C. Tinto, CISA, CRISC, CFE, CIA, Omnicom Media Group, EE.UU.
Alok Tuteja, CGEIT, CRISC, CIA, CISSP, Mazrui Holdings LLC, E.A.U.
Orlando Tuzzolo, CISM, CGEIT, CRISC, World Pass IT Solutions, Brasil

Consejo de Dirección de ISACA
Robert E Stroud, CGEIT, CRISC, CA, EE.UU., Presidente Internacional
Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, Reino Unido, Vicepresidente
Garry J. Barnes, CISA, CISM, CGEIT, CRISC, BAE Systems Detica, Australia, Vicepresidente
Robert A. Clyde, CISM, Adaptive Computing, EE.UU., Vicepresidente
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, España, Vicepresidente
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, Cámara de Representantes de EE.UU., EE.UU., Vicepresidente
Vittal R. Raj, CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA, Kumar & Raj, India, Vicepresidente
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Gobierno de Queensland, Australia, Ex presidente Internacional
Gregory T. Grocholski, CISA, The Dow Chemical Co. (retirado), EE.UU., Ex presidente Internacional
Debbie A. Lew, CISA, CRISC, Ernst & Young LLP, EE.UU., Director
Frank K.M. Yam, CISA, CIA, FHKCS, FHKIoD, Focus Strategic Group Inc., Hong Kong, Director
Alexander Zapata Lenis, CISA, CGEIT, CRISC, ITIL, PMP, Grupo Cynthus S.A. de C.V., México, Director

Comité de Conocimiento
Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, Reino Unido, Presidente
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., Holanda
Neil Patrick Barlow, CISA, CISM, CRISC, CISSP, IntercontinentalExchange, Inc. NYSE, Reino Unido
Charlie Blanchard, CISA, CISM, CRISC, ACA, CIPP/E, CIPP/US, CISSP, FBCS, Amgen Inc., EE.UU.
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapur
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, EE.UU.
Anthony P. Noble, CISA, Viacom, EE.UU.
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, Reino Unido
Ivan Sanchez Lopez, CISA, CISM, CISSP, ISO 27001 LA, DHL Global Forwarding & Freight, Alemania

Comité de Orientación y Prácticas
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, EE.UU., Presidente
John Jasinski, CISA, CGEIT, ISO20K, ITIL Exp, SSBB, ITSMBP, EE.UU.
Yves Marcel Le Roux, CISM, CISSP, CA Technologies, Francia
Aureo Monteiro Tavares Da Silva, CISM, CGEIT, Brasil
Jotham Nyamari, CISA, CISSP, Deloitte, EE.UU.
James Seaman, CISM, CRISC, A. Inst. IISP, CCP, QSA, RandomStorm Ltd., Reino Unido
Gurvinder Singh, CISA, CISM, CRISC, Australia
Siang Jun Julia Yeo, CISA, CRISC, CPA (Australia), MasterCard Asia/Pacific Pte. Ltd., Singapur
Nikolaos Zacharopoulos, CISA, CRISC, CISSP, Merck, Alemania

Reconocimiento especial por apoyo financiero:
Capítulo de Nueva Jersey

ÍNDICE

LISTA DE FIGURAS

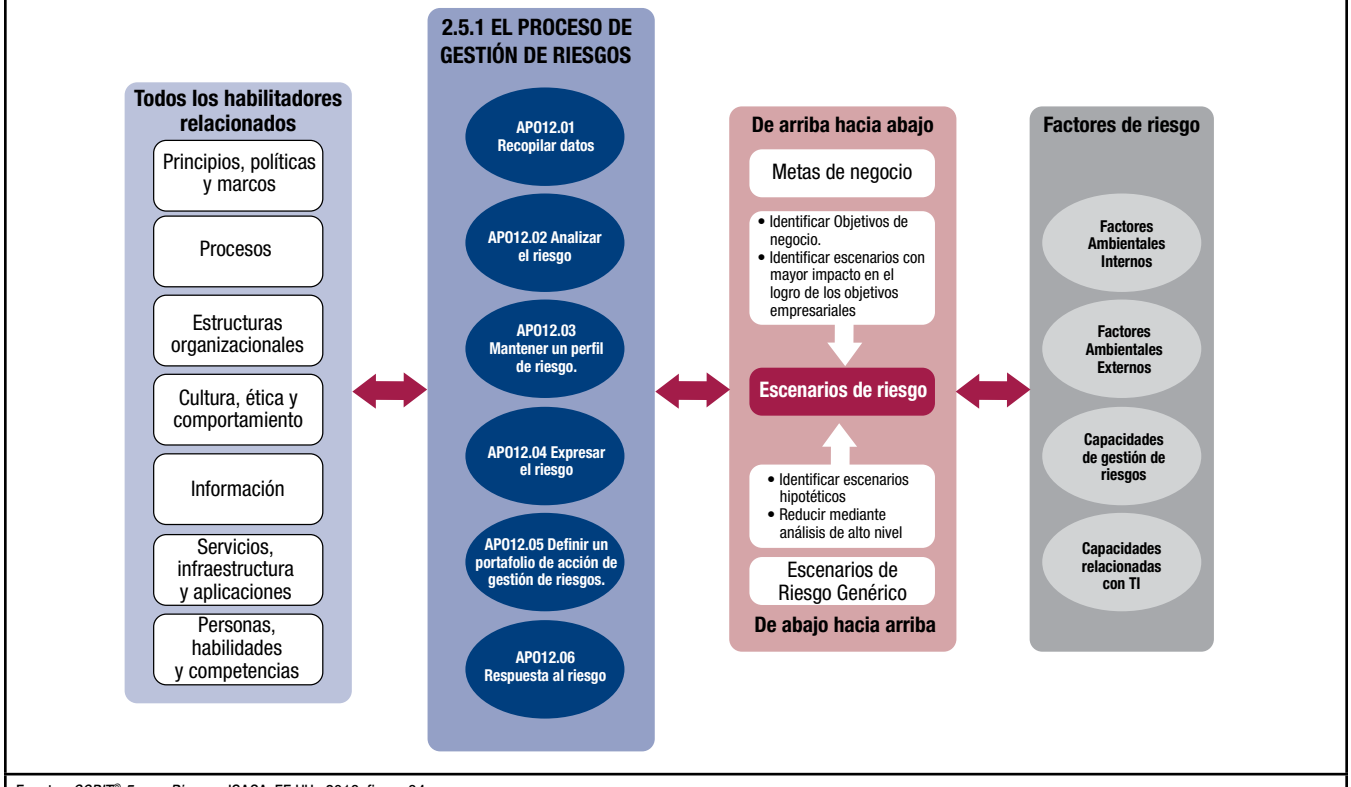
Página intencionalmente en blanco

CAPÍTULO 1
INTRODUCCIÓN

Antecedentes

El análisis del escenario de riesgo es un componente importante de la Gestión del Riesgo Empresarial (ERM) (**figura 1**). Esta técnica es una herramienta poderosa porque ayuda a describir el riesgo en términos que son más fáciles de entender para los líderes empresariales. ISACA ha emitido los *Escenarios de Riesgo Utilizando COBIT 5 para Riesgos* para proporcionar orientación a los profesionales que son responsables de ayudar a sus empresas a gestionar sus carteras de riesgo.

Figura 1: Visión general del escenario de riesgo



Fuente: *COBIT® 5 para Riesgos*, ISACA, EE.UU., 2013, figura 34

Los Escenarios de Riesgo Utilizando COBIT 5 para Riesgos es una guía práctica sobre cómo utilizar *COBIT 5 para Riesgos* con el fin de preparar escenarios de riesgo relacionados con TI que se pueden usar para el análisis y la evaluación de riesgos. *Los Escenarios de Riesgo Utilizando COBIT 5 para Riesgos* proporcionan a los lectores posibles escenarios a considerar en sus propias organizaciones, para permitir que los escenarios sean adaptados; esto requerirá que los escenarios sean agregados, removidos y modificados para proporcionar un conjunto enfocado de escenarios relevantes que se ajusten al riesgo específico, apetito de riesgo y necesidades empresariales de las organizaciones.

El **análisis** de riesgo es el proceso utilizado para estimar la frecuencia y la magnitud de los escenarios de riesgo relacionados con TI. La **evaluación** de riesgo es un proceso utilizado para identificar y evaluar el riesgo, sus posibles efectos y la evaluación de las probabilidades de un evento en particular. La evaluación del riesgo es ligeramente más amplia e incluye las actividades preliminares y auxiliares del análisis de riesgos, es decir, la identificación de escenarios de riesgo detallados y la definición de respuestas como planes de mitigación y la descripción de controles existentes. El análisis y la evaluación de riesgos son un enfoque básico para aportar realismo, conocimiento, participación organizacional, análisis mejorado y estructura al complejo tema de riesgo de TI. Los **escenarios de riesgo** son la representación tangible y evaluable del riesgo, y son uno de los elementos de información clave necesarios para identificar, analizar y responder al riesgo (Proceso APO12 de COBIT 5).

Propósito de esta publicación

Escenarios de Riesgo Utilizando COBIT 5 para Riesgos se enfoca en el desarrollo de**escenarios de riesgo relacionados con TI** y se debe leer en el contexto de *COBIT 5 para Riesgos* y el marco COBIT 5. La publicación ofrece una visión general de alto nivel de los conceptos de riesgo, junto con 60 ejemplos de escenarios de riesgo que abarcan las 20 categorías descritas en *COBIT 5 para Riesgos*. Un kit de herramientas complementario está disponible en el sitio web de ISACA y contiene plantillas interactivas de escenarios de riesgo para cada una de las 20 categorías.

El principal propósito de *Escenarios de Riesgo Utilizando COBIT 5 para Riesgos* es proporcionar orientación sobre el desarrollo de escenarios de riesgo relacionados con TI. Estos escenarios se basan en la determinación del valor de un activo o de un proceso de negocio. Se deben considerar las amenazas y vulnerabilidades potenciales que pueden derivar en un evento de pérdida, así como los beneficios potenciales para el logro más eficaz y eficiente de los objetivos del negocio y la protección o el aumento del valor del negocio. El propósito secundario de esta publicación es proporcionar orientación sobre cómo responder a los riesgos que exceden el nivel de tolerancia de la empresa. Se ofrece orientación especial sobre la forma en que los habilitadores de COBIT 5 pueden ayudar en las actividades de gestión de riesgos.

¿Quién debe usar esta guía?

La audiencia prevista para *Escenarios de Riesgo Utilizando COBIT 5 para Riesgos* es amplia, e incluye a cualquier persona responsable de ayudar a la empresa a gestionar el riesgo. Los profesionales de gestión de riesgos, en particular, pueden beneficiarse de esta publicación y de la orientación proporcionada para desarrollar el análisis de escenarios de riesgo para apoyar los esfuerzos ERM. Los profesionales de TI y de negocios, en general, se benefician de los conceptos y las prácticas descritos en esta publicación, y pueden comprender mejor el papel que pueden desempeñar en el proceso ERM.

La adopción del análisis de escenarios de riesgo puede ayudar a satisfacer los requerimientos de múltiples partes interesadas. La **figura 2** describe los beneficios potenciales de las partes interesadas que el análisis de los escenarios de riesgo puede proporcionar.

Figura 2: *Escenarios de Riesgo Utilizando COBIT 5 para Riesgos* Partes interesadas y beneficios

Rol/función	Beneficios de la adopción de *Escenarios de Riesgo Utilizando COBIT 5 para Riesgos*
Consejo y dirección ejecutiva	Mejor comprensión de las implicaciones del riesgo de TI para los objetivos estratégicos empresariales y de cómo utilizar la TI de mejor manera para una ejecución exitosa de la estrategia
Director de Riesgos (CRO) y administradores de riesgos corporativos para la gestión de riesgos empresariales (ERM)	Asistencia con la gestión de riesgos de TI, en línea con los principios ERM generalmente aceptados, e incorporación del riesgo de TI en el riesgo empresarial
Administradores de riesgo operativo	Vincular su marco ERM a *COBIT 5 para Riesgos*; identificación de pérdidas operativas o desarrollo de indicadores clave de riesgo (KRI)
Gerencia de TI	Mejor comprensión de cómo identificar y gestionar el riesgo de TI, y cómo comunicar el riesgo de TI a los tomadores de decisiones empresariales
Gerentes de servicios de TI	Mejora de su visión del riesgo operativo
Seguridad de TI	Posicionamiento del riesgo de seguridad entre otras categorías de riesgo de TI
Seguridad de la información/Director de Seguridad de la Información (CISO)	Posicionamiento del riesgo de TI dentro de la estructura de gestión del riesgo de la información empresarial
Director de Finanzas (CFO)	Obtener una mejor visión del riesgo de TI y sus implicaciones financieras
Área de negocios	Mejor comprensión y gestión del riesgo de TI en línea con los objetivos del negocio
Auditores internos	Mejor análisis del riesgo en apoyo de los planes y reportes de auditoría
Cumplimiento normativo	Asesorar al área de riesgo con respecto a los requerimientos de cumplimiento y su impacto potencial en la empresa
Asesor jurídico	Asesorar al área de riesgo sobre el riesgo relacionado con las regulaciones, y el impacto potencial o las implicaciones legales para la empresa
Reguladores	Apoyar la evaluación del enfoque de gestión de riesgos de TI de las empresas reguladas, y el impacto del riesgo en los requerimientos regulatorios
Auditores externos	Orientación adicional sobre los niveles de exposición al establecer una opinión sobre la calidad del control interno
Aseguradoras	Ayudar a establecer una cobertura adecuada de seguros de TI y obtener un acuerdo sobre los niveles de exposición
Contratistas y subcontratistas de TI	Mejor alineación de la utilidad y garantía de los servicios de TI proporcionados; comprensión de las responsabilidades derivadas de la evaluación de riesgos

Alcance y enfoque

La orientación práctica en esta publicación se dedica específicamente a la preparación de escenarios de riesgo relacionados con TI y análisis de escenarios de riesgo. *Escenarios de Riesgo Utilizando COBIT 5 para Riesgos* describe, a un alto nivel, los conceptos de gestión de riesgos y los diferentes pasos necesarios para preparar un análisis completo de los escenarios de riesgo. La **figura 3** proporciona una breve descripción de cada capítulo y apéndice.

Figura 3: Visión general del documento y orientación sobre su uso	
Capítulo	**Descripción**
Capítulo 1. Introducción	Presenta una visión general sobre quién debe usar esta guía, el alcance y el enfoque, y proporciona orientación sobre los prerrequisitos
Capítulo 2. Descripción de Alto Nivel de Conceptos de Gestión de Riesgos	Describe a un alto nivel los conceptos de gestión de riesgos en los que se basa esta guía
Capítulo 3. Explicación de Escenarios de Riesgo	Proporciona una definición de los escenarios de riesgo; explica cómo se puede desarrollar un flujo de trabajo de escenario de riesgo y cómo se pueden utilizar los factores de riesgo en el contexto de los escenarios de riesgo; proporciona las características de los buenos escenarios
Capítulo 4. Escenarios de Riesgo Genéricos	Contiene ejemplos de categorías de escenarios de riesgo genéricos relacionados con TI y algunos consejos prácticos sobre cómo utilizar mejor estos ejemplos
Capítulo 5. Uso de Habilitadores de COBIT 5 para Mitigar Escenarios de Riesgo de TI	Proporciona ejemplos que muestran cómo usar los habilitadores COBIT 5 para responder a los ejemplos de escenarios de riesgo descritos en el capítulo 4
Capítulo 6. Expresión y Descripción de Riesgos	Describe los componentes adicionales necesarios para preparar un análisis integral de los escenarios de riesgo; describe los procesos que se pueden utilizar para analizar el impacto y la frecuencia del riesgo; y describe posibles opciones de respuesta al riesgo
Capítulo 7. Ejemplo Detallado de Escenarios de Riesgo	Contiene más de 50 análisis de escenarios de riesgo y describe los habilitadores COBIT 5 que pueden utilizarse para responder en cada escenario en particular
Apéndice 1. Plantilla de Análisis de Escenarios de Riesgo	Proporciona una plantilla del análisis integral de escenarios de riesgo
Apéndice 2. Glosario	Define los términos clave que se utilizan en esta guía
Apéndice 3. Procesos para el Gobierno y Gestión de la TI de la Empresa	Muestra los 37 procesos de gobierno y gestión definidos en COBIT 5 y sus respectivas actividades según se definen en *COBIT 5: Procesos Habilitadores*

Conocimiento de prerrequisitos

Escenarios de Riesgo Utilizando COBIT 5 para Riesgos se basa en *COBIT 5 para Riesgos*. Los conceptos clave sobre el uso de escenarios de *COBIT 5 para Riesgos* se repiten en esta guía, por lo que es una guía bastante autónoma; en esencia, no requiere ningún conocimiento previo. Sin embargo, una comprensión de *COBIT 5 para Riesgos* acelerará la comprensión de los contenidos de esta guía. Además, algunos elementos relevantes para el riesgo que se describen en *COBIT 5 para Riesgos* no se repiten en *Escenarios de Riesgo Utilizando COBIT 5 para Riesgos* y pueden requerir el uso de otras guías en la familia de productos COBIT 5.

Para la mitigación del riesgo, *Escenarios de Riesgo Utilizando COBIT 5 para Riesgos* hace referencia principalmente a los habilitadores COBIT 5, al modelo de referencia de proceso y a los procesos COBIT 5 descritos en el mismo. Si los lectores desean saber más acerca de los habilitadores COBIT 5, p. ej., para implementar o mejorar algunos de ellos como parte de una respuesta al riesgo (mitigación), se les remite a las siguientes guías de la familia de productos COBIT 5: el marco COBIT 5, *COBIT 5: Procesos Habilitadores* y *COBIT 5: Información Habilitadora*.

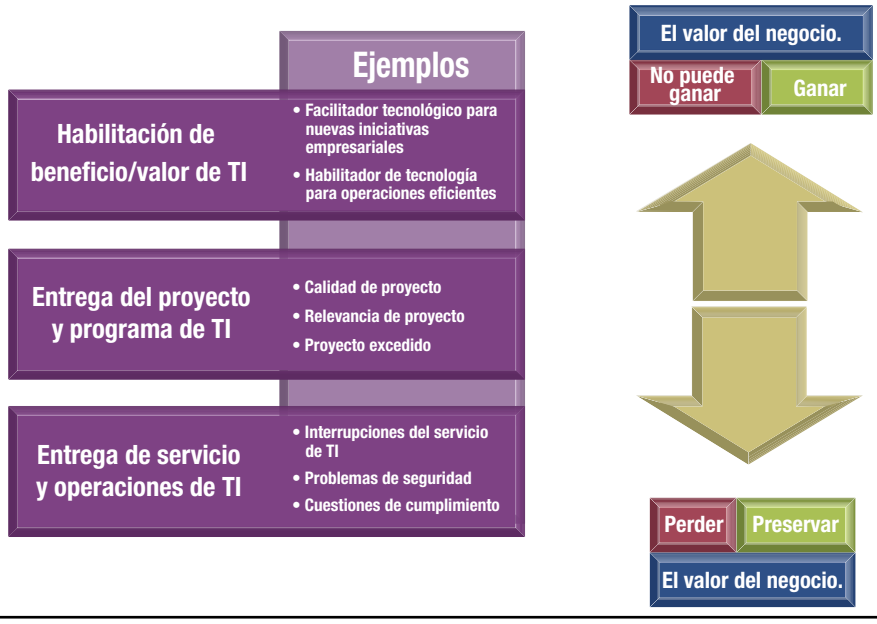
Página intencionalmente en blanco

Capítulo 2
Descripción de Alto Nivel de Conceptos de Gestión de Riesgos[1]

El riesgo se define generalmente como la combinación de la probabilidad de un evento y sus consecuencias (Guía ISO 73). Las consecuencias son que los objetivos de la empresa no se cumplen. *COBIT 5 para el Riesgo* define el riesgo de TI como un riesgo de negocio, específicamente el riesgo de negocio asociado con el uso, propiedad, operación, participación, influencia y adopción de TI dentro de una empresa. Consiste en eventos relacionados con TI que potencialmente podrían impactar al negocio. El riesgo de TI puede ocurrir con frecuencia y magnitud inciertas, y crea desafíos para el cumplimiento de las metas y los objetivos estratégicos.

La **figura 4** muestra que para todas las categorías de riesgo de TI descendente ("no obtener" o "perder" valor comercial) hay un valor ascendente equivalente ("ganar" y "conservar" negocios).

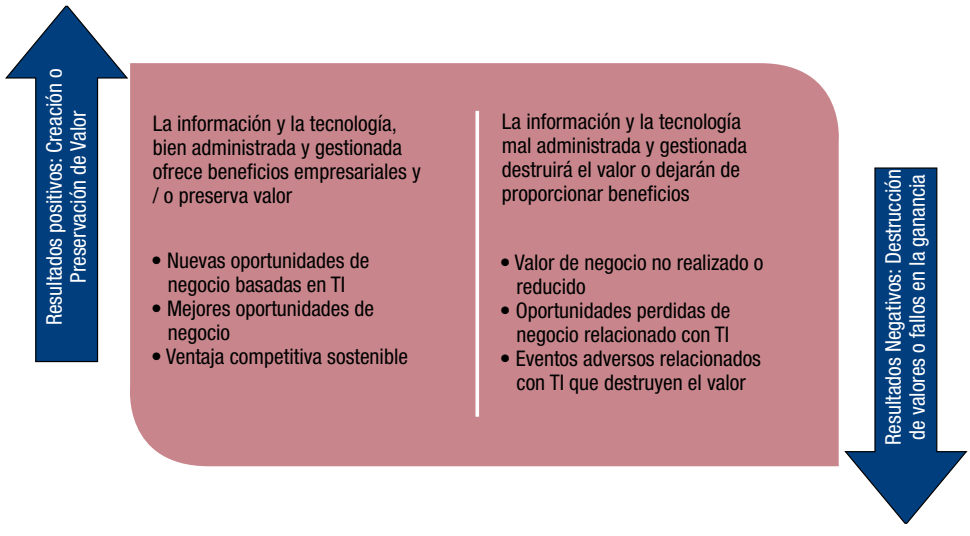
Figura 4: Categorías de riesgo de TI



Fuente: *COBIT® 5 para Riesgos*, ISACA, EE.UU., 2013, figura 5

Es importante mantener esta dualidad de riesgo ascendente/descendente (ver la **figura 5**) durante todas las decisiones relacionadas con el riesgo.

Figura 5: Dualidad del riesgo



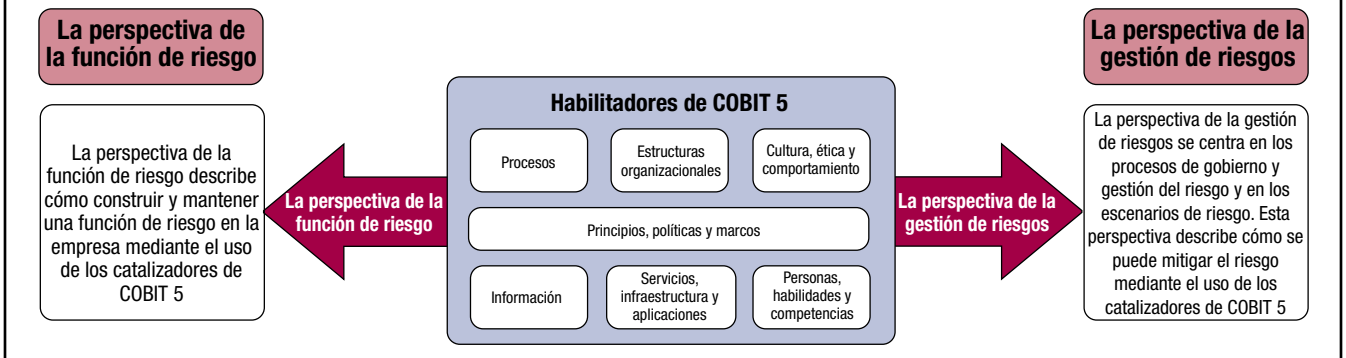
Fuente: *COBIT® 5 riesgos*, ISACA, EE.UU., 2013, figura 6

[1] El contenido de este capítulo se basa en la siguiente publicación: ISACA, *COBIT® 5 para Riesgos*, EE.UU., 2013.

COBIT 5 para Riesgos explica las siguientes dos perspectivas sobre cómo usar COBIT 5 en un contexto de riesgo (**figura 6**):

- **Perspectiva de la función de riesgos**: Describe lo que se necesita en una empresa para construir y sostener actividades centrales eficientes y efectivas de gobierno y gestión del riesgo.
- **Perspectiva de la gestión de riesgos**: Describe cómo el proceso central de gestión del riesgo de identificar, analizar, responder y reportar sobre el riesgo puede ser asistido por los habilitadores de COBIT 5.

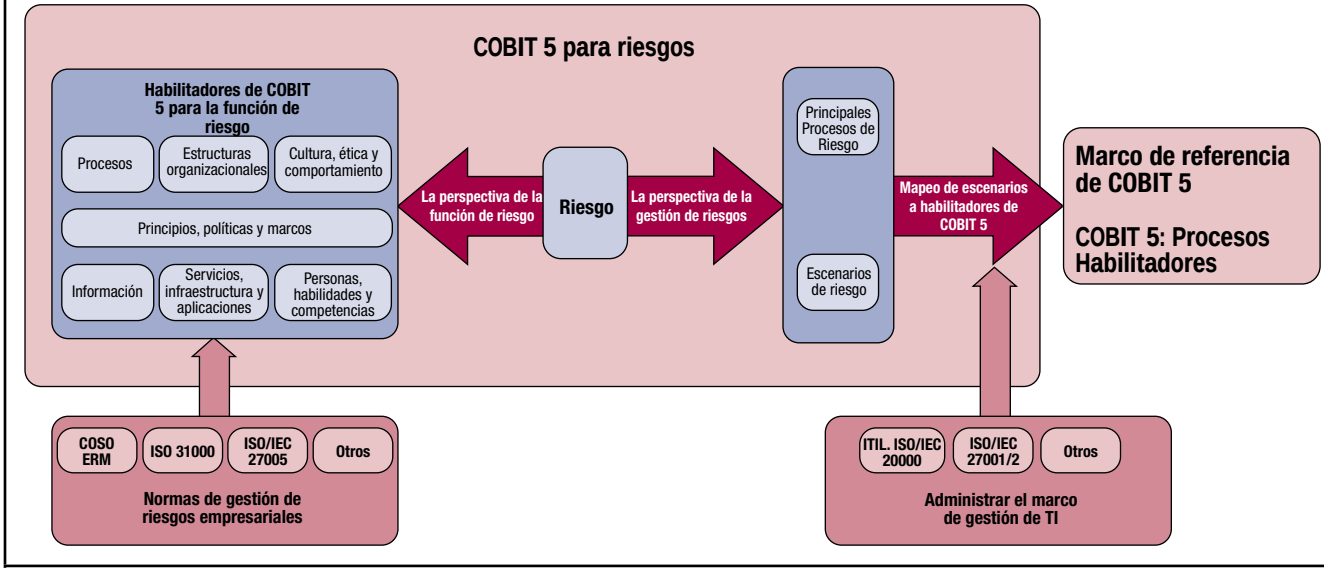
Figura 6: Dos perspectivas sobre el riesgo



Fuente: *COBIT® 5 para Riesgos*, ISACA, EE.UU., 2013, figura 8

La **figura 7** muestra el alcance de *COBIT 5 para el Riesgo* y la relación entre los escenarios de riesgo y la perspectiva de la gestión de riesgos. Los escenarios de riesgo apoyan esta perspectiva al proporcionar un vínculo entre el riesgo identificado y los habilitadores de COBIT 5 que pueden usarse para mitigarlo.

Figura 7: Alcance de *COBIT 5 para Riesgos*

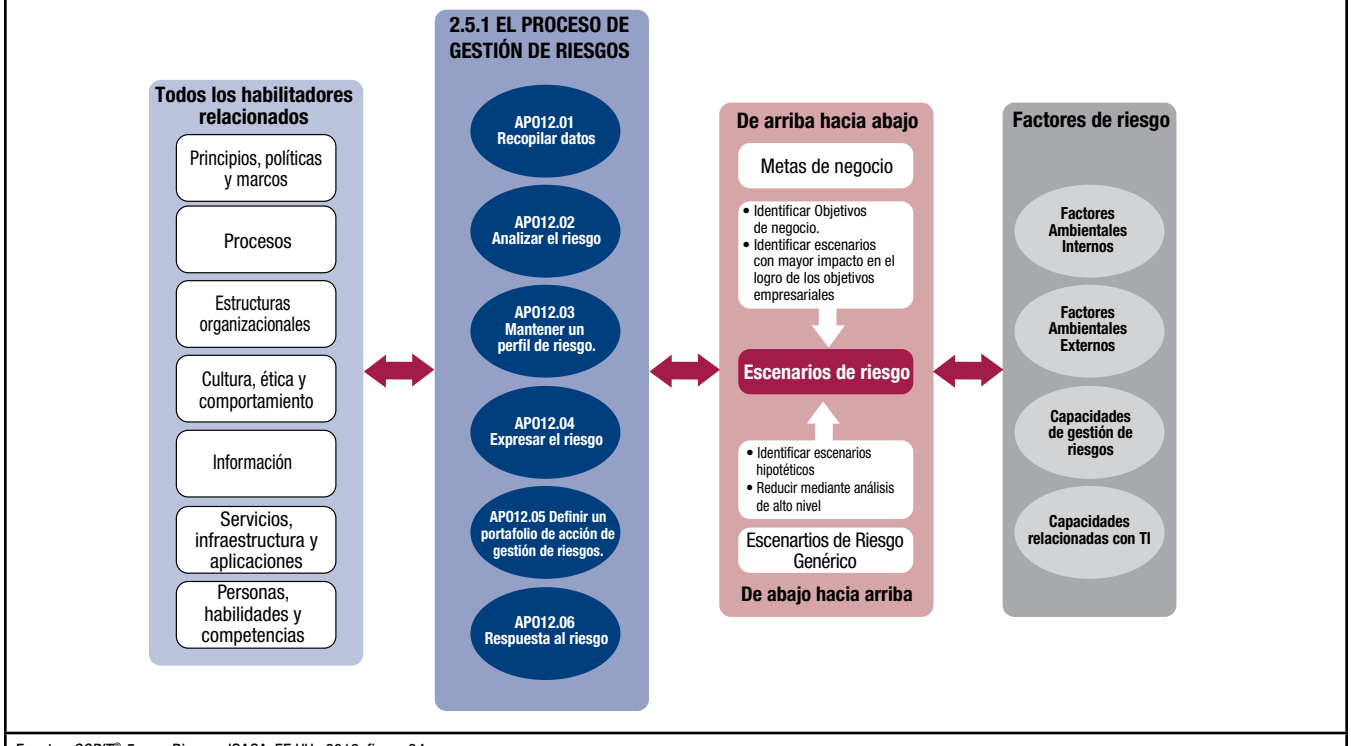


Fuente: *COBIT® 5 para Riesgos*, ISACA, EE.UU., 2013, figura 10

Capítulo 3
Explicación de Escenarios de Riesgo[2]

Un elemento de información clave utilizado en el proceso básico de gestión de riesgos de COBIT 5 APO12 es el escenario de riesgo (**figura 8**).

Figura 8: Visión general del escenario de riesgo



Fuente: *COBIT® 5 para Riesgos*, ISACA, EE.UU., 2013, figura 34

Definición de escenarios de riesgo

Un escenario de riesgo es una descripción de un evento posible que, cuando ocurra, tendrá un impacto incierto en el logro de los objetivos de la empresa. El impacto puede ser positivo o negativo.

El proceso básico de gestión de riesgos requiere que las necesidades del riesgo sean identificadas, analizadas y se actúe sobre ellas. Los escenarios de riesgo bien desarrollados apoyan estas actividades y las hacen realistas y relevantes para la empresa.

La **figura 8** también muestra que los escenarios de riesgo pueden derivarse a través de dos mecanismos diferentes:
- Un **enfoque descendente**, donde uno comienza en los objetivos globales de la empresa y realiza un análisis de los escenarios de riesgo de TI más relevantes y probables que impactan los objetivos empresariales. Si los criterios de impacto utilizados durante el análisis de riesgo están bien alineados con los impulsores de valor real de la empresa, se desarrollarán escenarios de riesgo relevantes.
- Un **enfoque ascendente**, donde se utiliza una lista de escenarios genéricos para definir un conjunto de escenarios más relevantes y personalizados, aplicados a la situación individual de la empresa.

Los enfoques son complementarios y se deben usar simultáneamente. De hecho, los escenarios de riesgo deben ser relevantes y estar vinculados al riesgo empresarial real. Por otra parte, el uso de un conjunto de ejemplos de los escenarios de riesgo genéricos podría ayudar a identificar el riesgo y reducir la posibilidad de pasar por alto los escenarios de riesgo importantes/comunes, y puede proporcionar una referencia completa para el riesgo de TI. Sin embargo, los elementos específicos de riesgo para cada empresa y los requisitos críticos del negocio se deben considerar en los escenarios de riesgo empresariales.

Nota: No confíe demasiado en la lista de ejemplos de escenarios de riesgo genéricos. La lista, aunque bastante completa, amplia y abarca la mayoría de los elementos de riesgo potenciales, debe adaptarse a la situación específica de la empresa. No se pretende que, en el futuro, toda la gestión de riesgos de TI utilice el mismo conjunto de escenarios de riesgo de TI predefinidos. En su lugar, se alienta a que esta lista se utilice como base para el desarrollo de escenarios específicos y relevantes.

[2] El contenido de este capítulo se basa en la siguiente publicación: ISACA, *COBIT® 5 para Riesgos*, EE.UU., 2013.

Desarrollo del flujo de trabajo escenarios de riesgo

En la práctica, se sugiere el siguiente enfoque:
- Utilice la lista de ejemplos de escenarios de riesgo genéricos (consulte la **figura 14** En el Capítulo 4, Escenarios de riesgo genéricos) para definir un conjunto manejable de escenarios de riesgo adaptados a la empresa. Para determinar un conjunto manejable de escenarios, un negocio puede comenzar considerando escenarios comunes en su industria o área de producción, escenarios que representan fuentes de amenaza que aumentan en número o gravedad, y escenarios que involucran requerimientos legales y regulatorios aplicables al negocio. Otro enfoque podría ser el identificar las unidades de negocio de alto riesgo y evaluar uno o dos procesos operativos de alto riesgo dentro de cada una, incluyendo los componentes de TI que habilitan ese proceso. Además, algunas situaciones menos comunes se deben incluir en los escenarios.
- Realice una validación comparando los objetivos del negocio de la entidad. ¿Los escenarios de riesgo seleccionados abordan los impactos potenciales en el logro de los objetivos empresariales de la entidad, en apoyo de los objetivos de negocio generales de la empresa?
- Refine los escenarios seleccionados basándose en esta validación; detállelos a un nivel en línea con la criticidad de la entidad.
- Reduzca el número de escenarios a un **conjunto manejable**. "Manejable" no significa un número fijo, pero debe estar en línea con la importancia general (tamaño) y criticidad de la unidad. No hay una regla general, pero si los escenarios se enfocan de manera razonable y realista, la empresa debe esperar desarrollar al menos una docena de escenarios.
- Mantenga todos los escenarios en una lista para que se puedan reevaluar en la siguiente iteración, e incluirse para un análisis detallado si se han vuelto relevantes en ese momento.
- Incluya en los escenarios un evento no especificado, p. ej., un incidente no cubierto por otros escenarios.

Una vez que se haya definido el conjunto de escenarios de riesgo, se puede usar para el análisis de riesgos, donde se evalúan la frecuencia y el impacto del escenario. Los componentes importantes de esta evaluación son los factores de riesgo.

La empresa también puede considerar la evaluación de escenarios que tienen la posibilidad de ocurrir simultáneamente. Esto se conoce con frecuencia como pruebas de "estrés", y en realidad consiste en la combinación de múltiples escenarios y la comprensión del impacto extra si ocurrieran juntos.

Factores de riesgo

Los factores de riesgo son aquellas condiciones que influyen en la frecuencia y/o impacto en el negocio de los escenarios de riesgo. Pueden ser de diferentes naturalezas y pueden clasificarse en dos categorías principales:
- **Factores contextuales**. Se pueden dividir en factores internos y externos, siendo la diferencia el grado de control que una empresa tiene sobre ellos:
  – Factores contextuales internos: En gran medida, están bajo el control de la empresa, aunque no siempre son fáciles de cambiar.
  – Factores contextuales externos: En gran medida, están fuera del control de la empresa
- **Capacidades**. Cuán eficaz y eficiente es la empresa en una serie de actividades relacionadas con TI. Se pueden distinguir en línea con el marco de COBIT 5:
  – Capacidades de gestión de riesgos de TI. Indique hasta qué punto la empresa tiene la experiencia para realizar los procesos de gestión de riesgos.
  – Capacidades relacionadas con TI. Indique la capacidad de los habilitadores de COBIT 5 relacionados con TI.

La importancia de los factores de riesgo radica en la influencia que tienen en el riesgo. Son grandes influyentes en la frecuencia y el impacto de los escenarios de TI, y se deben considerar durante cada análisis de riesgo.

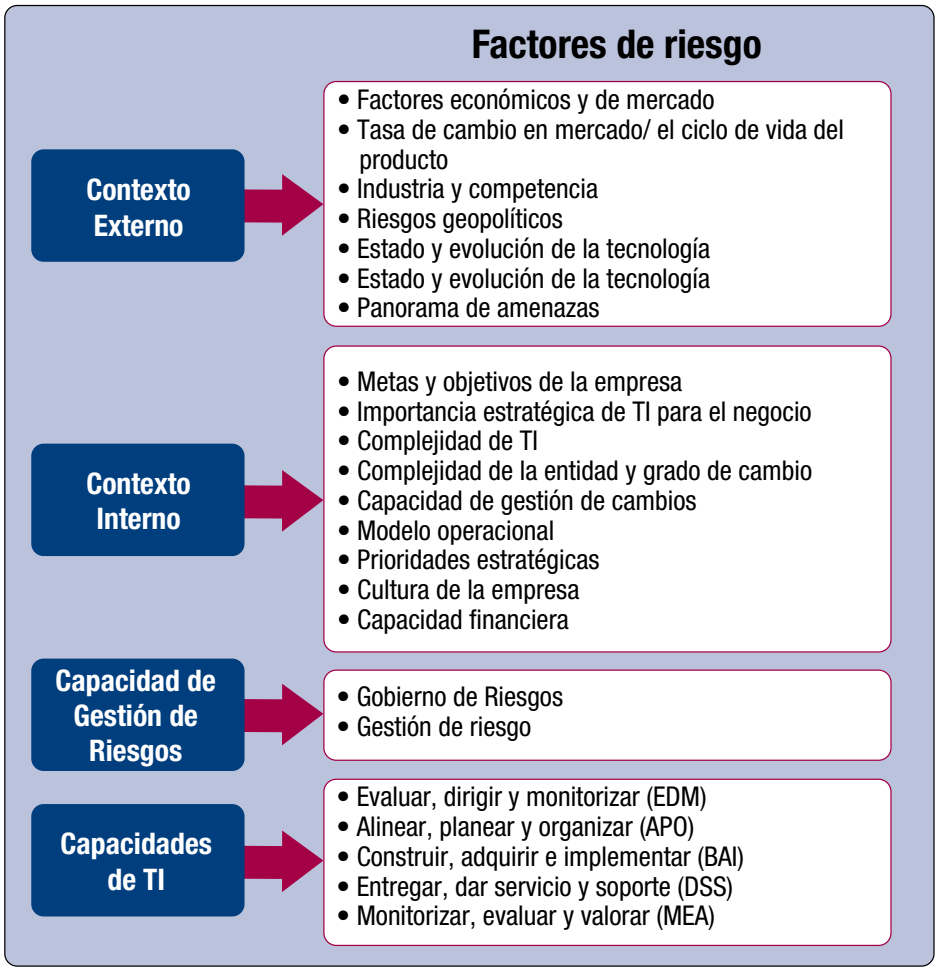
Los factores de riesgo también se pueden interpretar como factores causales del escenario que se está materializando, o como vulnerabilidades o debilidades. Estos son términos utilizados con frecuencia en otros marcos de gestión de riesgos.

El análisis de escenarios no solo debe basarse en la experiencia pasada y en los acontecimientos actuales conocidos, sino también en las circunstancias futuras posibles. El riesgo futuro podría estar relacionado con tecnologías emergentes, nuevas regulaciones, cambios demográficos y nuevas iniciativas del negocio.

Los factores de riesgo cambian con el tiempo; por lo tanto, los escenarios también cambiarán. Este cambio requiere que una empresa realice evaluaciones de riesgos y monitorización de riesgos de manera continua. La evaluación de riesgos que se basa en los escenarios debe realizarse al menos anualmente y cuando ocurre un cambio importante en los factores de riesgo internos o externos.

La **figura 9** describe los factores de riesgo que se analizan con mayor detalle en los siguientes párrafos.

Figura 9: Factores de riesgo



Fuente: *COBIT® 5 para Riesgos*, ISACA, EE.UU., 2013, figura 35

Contexto externo

Factores de riesgo de TI contextuales, es decir, aquellas circunstancias que pueden aumentar la frecuencia o el impacto de un evento y que no siempre son directamente controlables por la empresa, incluyen:

- **Factores de mercado/económicos**: El sector industrial en el que opera la empresa, p. ej., si opera en el sector financiero, requiere diferentes requerimientos de TI y capacidades de TI que si operara en un entorno de fabricación. También se pueden incluir otros factores económicos, p. ej., nacionalización, fusiones y adquisiciones, consolidaciones.
- **Ritmo de cambio en el mercado en el que la empresa opera**: ¿Los modelos empresariales están cambiando fundamentalmente? ¿El producto o servicio está al final de un momento importante del ciclo de vida?
- **Entorno competitivo**: Mercado, industria o región en la que opera la empresa.
- **Situación geopolítica**: ¿La ubicación geográfica está sujeta a frecuentes desastres naturales? ¿El contexto político local y económico general representa un riesgo adicional?
- **Entorno regulatorio**: ¿La empresa está sujeta a nuevas o más estrictas regulaciones relacionadas con TI, o a regulaciones que impactan las TI? ¿Existen otros requerimientos de cumplimiento más allá de la regulación, p. ej., específicos de la industria, contractuales?
- **Estado y evolución de la tecnología**: ¿La empresa emplea tecnología de vanguardia, y más importante aún, qué tan rápido evolucionan las tecnologías relevantes?
- **Panorama de amenazas**: ¿Cómo evolucionan las amenazas relevantes en términos de frecuencia de ocurrencia y nivel de capacidad?

Los factores de riesgo en el contexto externo están fuera del control de una empresa. Por lo tanto, la empresa está limitada en las acciones directas que puede tomar para gestionar dicho riesgo. Sin embargo, la empresa puede abordar el riesgo desarrollando estrategias para prevenir exposiciones, evitar riesgos y responder a un incidente de manera eficiente y efectiva cuando se materializa el riesgo, p ej., construir diques para evitar inundaciones, mudarse a un área no inundable y obtener un seguro pueden usarse para hacer frente a desastres naturales como inundaciones.

Contexto interno

Los factores de riesgo internos incluyen:

- **Metas y objetivos empresariales**: ¿Cuáles son las necesidades de las partes interesadas y cómo podrían ser afectadas por el riesgo?
- **Importancia estratégica de TI en la empresa**. ¿Es un diferenciador estratégico, un habilitador funcional o una función de apoyo?
- **Complejidad de la TI**. ¿Es altamente compleja (p. ej., arquitectura compleja, fusiones recientes) o es simple, estandarizada y simplificada?
- **Complejidad de la empresa**: (incluyendo la cobertura geográfica y la cobertura de la cadena de valor, p. ej., en un entorno de fabricación) ¿La empresa fabrica y distribuye partes y/o está también realizando actividades de ensamblaje?
- **Grado del cambio**: ¿Qué grado de cambio está experimentando la empresa?
- **Capacidad de gestión del cambio**: ¿En qué medida la empresa es capaz de un cambio organizacional?
- **La filosofía de gestión de riesgos**: ¿Cuál es la filosofía de riesgo de la empresa (aversión al riesgo o asunción de riesgos) y, en relación con ello, los valores de la empresa?
- **Modelo operativo**: El grado en que la empresa opera independientemente o está conectada a sus clientes/proveedores, el grado de centralización/descentralización.
- **Prioridades estratégicas**: ¿Cuáles son las prioridades estratégicas de la empresa?
- **Cultura de la empresa**: ¿La cultura existente de la empresa requiere de un cambio para poder adoptar de manera efectiva la gestión de riesgos?
- **Capacidad financiera**: La capacidad de la empresa para proporcionar apoyo financiero con el fin de mejorar y mantener el entorno de TI mientras optimiza el riesgo.

Al considerar los factores de riesgo internos durante el desarrollo y/o refinamiento de los escenarios, se deben tener en cuenta las siguientes consideraciones (**figura 10**):

Figura 10: Consideraciones del factor de riesgo interno

Enfoque/problema	Guía de resumen
Importancia de la Integridad y la ética de la gestión empresarial	La estrategia y los objetivos de una empresa, y la manera en que se implementan, se basan en preferencias, juicios de valor y estilos de gestión. La integridad de la gerencia y el compromiso con los valores éticos influyen en estas preferencias y juicios, que se traducen en estándares de conducta. Debido a que la buena reputación de una empresa es tan valiosa, los estándares de conducta deben ir más allá del simple cumplimiento con la ley. Los valores de gestión deben equilibrar las preocupaciones de la empresa, los empleados, los proveedores, los clientes, los competidores y el público. Los gerentes de las empresas bien administradas han aceptado cada vez más la opinión de que la buena ética vale la pena, y que la conducta ética es buena para el negocio. Una empresa que opera con un alto grado de ética puede tener una menor incidencia de riesgo relacionado con fraude o malversación. La integridad y los valores éticos son elementos esenciales del entorno interno de una empresa, y afectan el diseño, la gestión y la monitorización de otros componentes de la gestión de riesgos empresariales (ERM).
El papel de la gerencia empresarial en la determinación de la cultura empresarial	La alta gerencia, empezando por el director general ejecutivo (CEO), desempeña un papel clave en la determinación de la cultura corporativa (la pauta entre la alta gerencia). Como la personalidad dominante en una empresa, el CEO con frecuencia establece el tono ético. Ciertos factores organizacionales también pueden influir en la probabilidad de contabilidad fraudulenta y creativa. Es probable que estos mismos factores influyan en el comportamiento ético. Las personas pueden participar en actos deshonestos, ilegales o poco éticos simplemente porque la empresa les da fuertes incentivos o tentaciones para hacerlo. Un énfasis indebido en los resultados, especialmente a corto plazo, puede fomentar un entorno interno inadecuado.
Determinación de la gerencia de los niveles de competencia	La competencia refleja el conocimiento y las habilidades necesarias para realizar las tareas asignadas. La gerencia decide cuánto invertir en asegurarse de que las tareas se ejecuten correctamente utilizando recursos calificados, equipos y procesos definidos. Esto requiere ponderar la estrategia y los objetivos de la empresa contra los planes para su implementación y logro. Con frecuencia existe una compensación entre las competencias y los costos. El riesgo de fracaso es mayor con el personal no capacitado, equipo mal mantenido o antiguo, o procedimientos no definidos.
Papel del consejo de dirección en el entorno interno	El consejo de dirección de una empresa es una parte crítica del entorno interno e influye significativamente en sus elementos. El rol del consejo en la gobernanza del riesgo a través de la supervisión independiente de la gerencia, el escrutinio de las actividades, y la adecuación del apetito y la estrategia de riesgo de la empresa juegan un papel. Un consejo de dirección activo e involucrado debe poseer un grado adecuado de experiencia administrativa, financiera, técnica y de otra tipo, junto con la mentalidad necesaria para desempeñar sus responsabilidades de supervisión. Esto es crucial para un ambiente ERM efectivo, ya que el consejo debe estar preparado para cuestionar y escudriñar las actividades de la gerencia, presentar puntos de vista alternativos y actuar frente a la conducta indebida.
Impacto de la estructura organizacional de la empresa	La estructura organizacional de una empresa proporciona el marco para planificar, ejecutar, controlar y monitorizar sus actividades. Cualquiera que sea la estructura, una empresa debe organizarse para permitir un ERM eficaz y para llevar a cabo sus actividades para lograr sus objetivos.

Figura 10: Consideraciones del factor de riesgo interno *(cont.)*	
Enfoque/problema	**Guía de resumen**
Asignación de autoridad y responsabilidad	La asignación de autoridad y responsabilidad implica el grado en que las personas y los equipos están autorizados (y limitados por su autoridad) y se les anima a utilizar la iniciativa para abordar y resolver problemas. Esto también incluye el desarrollo y la aplicación de políticas para las prácticas comerciales apropiadas, el conocimiento del personal clave y los recursos proporcionados para el desempeño de las tareas.
Impacto de la delegación	Junto con mejores decisiones basadas en el mercado, la delegación puede aumentar el número de decisiones indeseables o imprevistas. El ambiente interno está muy influenciado por la medida en que las personas reconocen que serán responsables. Esto es cierto hasta el director general ejecutivo, quien, con la supervisión del consejo, tiene la responsabilidad final de todas las actividades dentro de una empresa.
Impacto de las prácticas de recursos humanos (RR.HH.)	Las prácticas de RR.HH. relacionadas con la contratación, orientación, capacitación, evaluación, asesoramiento, ascensos, compensación y la adopción de acciones correctivas, deben enviar el mensaje a los empleados con respecto a los niveles esperados de integridad, conducta ética y competencia.
Adaptado de: ISACA, Manual de Preparación para el Examen *CRISC™* 2014, EE.UU., 2012, pp. 39-41.	

Capacidad de gestión de riesgos

La capacidad de gestión de riesgos es una indicación de lo bien que la empresa está ejecutando los procesos básicos de gestión de riesgos y los habilitadores relacionados. Esto se puede medir usando una tarjeta de puntaje de riesgo. Cuanto mejor se desempeñen los habilitadores, más capaz será el programa de gestión de riesgos.

Este factor se correlaciona con la capacidad de la empresa para reconocer y detectar riesgos y eventos adversos; por lo tanto, no se debe ignorar.

La capacidad de gestión de riesgos es un elemento muy significativo en la frecuencia y el impacto de los eventos de riesgo en una empresa porque es responsable de las decisiones de riesgo de la gerencia (o la falta de ellas), así como de la presencia, ausencia y/o efectividad de los controles existentes dentro de una empresa.

Capacidad relacionada con TI

Las capacidades relacionadas con TI están asociadas con el nivel de capacidad de los procesos de TI y con todos los otros habilitadores. El modelo de habilitador genérico en COBIT 5 contiene un modelo de rendimiento del habilitador que apoya las evaluaciones de capacidad. Una alta madurez con respecto a los diferentes habilitadores es equivalente a las altas capacidades relacionadas con TI, que pueden tener una influencia positiva para:

- Reducir la frecuencia de los eventos, p. ej., tener buenos procesos de desarrollo de software establecidos para entregar software de alta calidad y estable, o tener buenas medidas de seguridad establecidas para reducir el número de incidentes relacionados con la seguridad
- Reducir el impacto en el negocio cuando ocurren eventos, p. ej., tener un buen plan de continuidad del negocio (BCP)/plan de recuperación de desastres (DRP) establecido cuando ocurre un desastre

Estructura del escenario de riesgo de TI

Un escenario de riesgo de TI es una descripción de un evento relacionado con TI que puede derivar en un impacto en el negocio, cuando y si ocurre. Para que los escenarios de riesgo sean completos y utilizables con fines de análisis de riesgo, deben contener los siguientes componentes, como se muestra en la **figura 11**:

- **Agente**: ¿Quién genera la amenaza que explota una vulnerabilidad? Los agentes pueden ser internos o externos y pueden ser humanos o no humanos:
  – Los agentes internos están dentro de la empresa, p. ej., personal o contratistas.
  – Entre los agentes externos incluyen las personas ajenas a la empresa, los competidores, los reguladores y el mercado.
  No todo tipo de amenaza requiere un agente, p. ej., fallas o causas naturales.
- **Tipo de amenaza** (la naturaleza del evento): ¿Es maliciosa? Si no es así, ¿es accidental o es una falla de un proceso bien definido? ¿Es un evento natural?
- **Evento**: ¿Es la divulgación de información confidencial, la interrupción de un sistema o de un proyecto, robo o destrucción? La acción también incluye el diseño ineficaz de sistemas, procesos, etc., el uso inapropiado, cambios en las reglas y regulaciones que impactarán materialmente en un sistema), o la ejecución ineficaz de procesos, p. ej., procedimientos de gestión de cambios, procedimientos de adquisición o procesos de priorización de proyectos.
- **Activo/recurso**: ¿Dónde se presenta el escenario? Un activo es cualquier elemento de valor para la empresa que puede verse afectado por el evento y dar lugar a un impacto en el negocio. Un recurso es cualquier cosa que ayuda a alcanzar las metas de TI. Los activos y recursos pueden ser idénticos, p. ej., el hardware de TI es un recurso importante porque todas las aplicaciones de TI lo utilizan, y al mismo tiempo, es un activo porque tiene un cierto valor para la empresa. Los activos/recursos incluyen:
  – Personas y habilidades
  – Estructuras organizacionales
  – Procesos de TI, p. ej., modelados como procesos COBIT 5 o procesos de negocio

– Infraestructura física, instalaciones, equipos, etc.
– Infraestructura de TI, incluyendo hardware informático, infraestructura de red, middleware
– Otros componentes de arquitectura empresarial (EA), incluyendo información y aplicaciones

Los activos pueden ser críticos o no, p. ej., un sitio web orientado al cliente de un banco importante en comparación con el sitio web de un estacionamiento local, o la intranet de un grupo de desarrollo de software. Los recursos críticos probablemente atraerán un mayor número de ataques o una mayor atención a las fallas; por lo tanto, la frecuencia de escenarios relacionados probablemente será mayor. Se necesita habilidad, experiencia y comprensión completa de las dependencias para entender la diferencia entre un activo crítico y un activo no crítico.

- **Tiempo**: Dimensión, donde se podría describir lo siguiente, si es relevante para el escenario:
  – La duración del evento, p. ej., interrupción prolongada de un servicio o centro de datos
  – El momento (¿El evento ocurre en un momento crítico?)
  – Detección (¿La detección es inmediata o no?)
  – Tiempo transcurrido entre el evento y la consecuencia (¿Existe una consecuencia inmediata, p. ej., falla de la red, tiempo de inactividad inmediato o una consecuencia retardada, p. ej., una arquitectura de TI incorrecta con altos costos acumulados durante un período de varios años?)

Es importante mantenerse al tanto de las diferencias entre los eventos de pérdida, los eventos de amenaza y los eventos de vulnerabilidad. Cuando se materializa un escenario de riesgo, se produce un evento de pérdida. El evento de pérdida ha sido desencadenado por un evento de amenaza (tipo de amenaza más evento en la **figura 11**). La frecuencia del evento de amenaza que conduce a un evento de pérdida está influenciada por los factores de riesgo o vulnerabilidad. La vulnerabilidad es usualmente un estado y se puede aumentar/disminuir por eventos de vulnerabilidad, p. ej., el debilitamiento de los controles o la fuerza de la amenaza. **Uno no debe mezclar estos tres tipos de eventos en una gran "lista de riesgos"**.

Figura 11: Estructura de escenarios de riesgo

Fuente: *COBIT® 5 para Riesgos*, ISACA, EE.UU., 2013, figura 36

El Capítulo 4, Escenarios de Riesgo Genéricos, y el Capítulo 7, Ejemplo Detallado Escenarios de Riesgo, contienen escenarios de riesgo de TI que se construyen de acuerdo con el modelo descrito en los párrafos anteriores. Los conjuntos de escenarios contienen ejemplos de resultados negativos, pero también ejemplos donde un riesgo, cuando se maneja bien, puede derivar en un resultado positivo.

Principales problemas al desarrollar y usar escenarios de riesgo

El uso de escenarios es clave para la gestión de riesgos, y la técnica es aplicable a cualquier empresa. Cada empresa necesita desarrollar un conjunto de escenarios (que contengan los componentes descritos anteriormente) como punto de partida para realizar su análisis de riesgo.

Desarrollar un conjunto completo de escenarios significa, en teoría, que cada valor posible de cada componente debe ser combinado. Cada combinación debe entonces ser evaluada en cuanto a relevancia y realismo, y si se considera relevante, se ingresa al registro de riesgos. En la práctica, esto no es posible; muy rápidamente, se puede generar un número inviable de diferentes escenarios de riesgo. El número de escenarios a desarrollar y analizar debe mantenerse a un número relativamente pequeño para mantenerse manejable.

La **figura 12** muestra algunas de las principales áreas de enfoque/temas a abordar cuando se utiliza la técnica de escenario de riesgo.

Figura 12: Principales áreas de enfoque de la técnica de escenario de riesgo

Enfoque/problema	Guía de resumen
Mantener actualizados los escenarios de riesgo y los factores de riesgo.	Los factores de riesgo y la empresa cambian con el tiempo; por lo tanto, los escenarios cambiarán con el tiempo, en el transcurso de un proyecto o con la evolución de la tecnología. Por ejemplo, es esencial que la función de riesgo desarrolle un programa de revisiones y que el CIO trabaje con las líneas de negocio para revisar y actualizar los escenarios según su relevancia e importancia. La frecuencia de este ejercicio depende del perfil general de riesgo de la empresa, y se debe hacer por lo menos una vez al año, o cuando se producen cambios importantes.
Utilizar escenarios de riesgo genéricos como punto de partida y desarrollar más detalles dónde y cuándo sea necesario.	Una técnica para mantener el número manejable de escenarios es propagar un conjunto estándar de escenarios genéricos a través de la empresa, y desarrollar escenarios más detallados y relevantes cuando sea necesario y justificado por el perfil de riesgo solo en los niveles más bajos (de entidad). Las suposiciones hechas al agrupar o generalizar deben ser bien entendidas por todos, y estar adecuadamente documentadas ya que pueden ocultar ciertos escenarios o ser confusas cuando se busca respuesta a los riesgos. Por ejemplo, si "amenaza interna" no está bien definida dentro de un escenario, es posible que no sea claro si esta amenaza incluye miembros privilegiados y no privilegiados. Las diferencias entre estos aspectos de un escenario pueden ser críticas cuando uno está tratando de comprender la frecuencia y el impacto de los eventos, así como las oportunidades de mitigación.
El número de escenarios debe ser representativo y reflejar la realidad y complejidad del negocio.	La gestión del riesgo ayuda a hacer frente a la enorme complejidad de los entornos de TI actuales al priorizar la acción potencial de acuerdo con su valor en la reducción de riesgos. La gestión de riesgos consiste en reducir la complejidad, no generarla; por lo tanto, este es otro motivo para trabajar con un número manejable de escenarios de riesgo. Sin embargo, el número de escenarios retenido aún debe reflejar con precisión la realidad y la complejidad del negocio.
La taxonomía de riesgos debe reflejar la realidad y la complejidad del negocio.	Debe haber un número suficiente de escalas de escenarios de riesgo que reflejen la complejidad de la empresa y el grado de exposición a los que la empresa está sujeta. Las escalas potenciales podrían ser de clasificación "baja, media, alta", o una escala numérica que califica la importancia del riesgo de 0 a 5. Las escalas deben estar alineadas en toda la empresa para garantizar una puntuación uniforme.
Utilizar una estructura de escenario de riesgo genérico para simplificar los reportes de riesgo.	Del mismo modo, con el fin de reportar los riesgos, las entidades no deben reportar todos los escenarios específicos y detallados, sino que podrían hacerlo usando la estructura de riesgo genérico. Por ejemplo, una entidad puede haber tomado el escenario genérico 15 (calidad del proyecto), traducirlo a cinco escenarios para sus proyectos principales, y posteriormente, realizar un análisis de riesgo para cada uno de los escenarios, luego sumar o resumir los resultados y reportarlos utilizando el encabezado de escenario genérico "calidad del proyecto".
Garantizar los requerimientos de personas y habilidades adecuados para desarrollar escenarios de riesgo relevantes.	El desarrollo de un conjunto manejable y relevante de escenarios de riesgo requiere: • Pericia y experiencia, no pasar por alto los escenarios relevantes y no verse atraído por escenarios muy poco realistas[3] o irrelevantes. Si bien es importante evitar escenarios irrealistas o irrelevantes para utilizar adecuadamente los recursos limitados, se debe prestar atención a las situaciones que son infrecuentes e impredecibles, pero que podrían tener un impacto catastrófico en la empresa. • Un entendimiento completo del entorno. Esto incluye el entorno de TI (p. ej., infraestructura, las aplicaciones, dependencias entre aplicaciones, componentes de la infraestructura), el entorno empresarial en general, y un entendimiento de cómo y qué entornos de TI respaldan el entorno de negocio para entender el impacto en el negocio. • La intervención y los puntos de vista comunes de todas las partes involucradas: alta gerencia, que tiene el poder de decisión; gerencia de negocios, que cuenta con la mejor vista del impacto en el negocio; TI, que tiene la comprensión de lo que puede ir mal con las TI; y gerencia de riesgos, que puede moderar y estructurar el debate entre las demás partes. • El proceso de desarrollo de escenarios generalmente se beneficia de un enfoque de intercambio de ideas/taller, donde por lo general se requiere una evaluación de alto nivel para reducir el número de escenarios a uno manejable pero relevante y representativo.
Usar el proceso de desarrollo de escenarios de riesgo para obtener la participación de otras partes interesadas.	El análisis de escenarios no es solo un ejercicio analítico que involucra a los "analistas de riesgos". Un beneficio adicional importante del análisis de escenarios es el logro de una participación organizacional por parte de las entidades empresariales y líneas de negocio, la gerencia de riesgos, TI, finanzas, cumplimiento y otras partes. Obtener esta participación es la razón por la cual el análisis de escenarios debe ser un proceso cuidadosamente facilitado.
Involucrar a la primera línea de defensa en el proceso de desarrollo de escenarios.	Además de la coordinación con la gerencia, se recomienda incluir en los debates a miembros selectos del personal que están familiarizados con las operaciones detalladas, cuando se considere apropiado. El personal cuyo trabajo diario es en las operaciones detalladas suele estar más familiarizado con las vulnerabilidades en la tecnología y los procesos que pueden ser explotadas.
No enfocarse solo en escenarios poco comunes y extremos.	Al desarrollar escenarios, uno no debe enfocarse solo en los eventos de los peores casos, ya que rara vez se materializan, mientras que los incidentes menos graves ocurren más a menudo.

[3] No realista o irrealista significa que no está fijado en el tiempo o no es estático. Lo que solía ser impensable, principalmente porque nunca sucedió o porque sucedió hace mucho tiempo, se vuelve realista tan pronto como ocurre nuevamente. Un ejemplo llamativo son los ataques terroristas del 11 de septiembre de 2001 en Estados Unidos. Está en la naturaleza humana pensar que las cosas que aún no han ocurrido, incluso cuando son teóricamente posibles, no son posibles o que son sumamente improbables. Sólo cuando ocurren se toman con seriedad en las evaluaciones de riesgo. Esto puede considerarse como falta de previsión o falta de la debida atención, pero en realidad es la esencia de la gestión de riesgos, intentar moldear y contener el futuro basándose en las experiencias pasadas y las predicciones futuras.

Figura 12: Principales áreas de enfoque de la técnica de escenario de riesgo *(cont.)*	
Enfoque/problema	**Guía de resumen**
Deducir escenarios complejos de escenarios simples al mostrar el impacto y las dependencias.	Los escenarios simples, una vez desarrollados, se deben refinar a escenarios más complejos, mostrando impactos en cascada y/o coincidentes, y reflejando las dependencias. Por ejemplo: • Un escenario con una falla importante de hardware se puede combinar con el escenario de DRP fallido. • Un escenario de una falla importante de software puede desencadenar en la corrupción de la base de datos y, en combinación con respaldos deficientes de gestión de datos, puede derivar en consecuencias graves, o al menos consecuencias de una magnitud diferente a una falla de software por sí sola. • Un escenario de un evento externo importante puede derivar en un escenario de apatía interna.
Considere el riesgo sistémico y contagioso.	Se debe prestar atención a los escenarios de riesgo sistémicos y/o contagiosos: • **Sistémico**: Algo sucede con un socio de negocios importante, que afecta a un gran grupo de empresas dentro de un área o industria. Un ejemplo sería un sistema nacional de control de tráfico aéreo que se cae durante un período de tiempo prolongado, p. ej., seis horas, lo que afecta al tráfico aéreo a gran escala. • **Contagioso**: Eventos que ocurren en varios de los socios comerciales de la empresa en un plazo muy corto. Un ejemplo sería una cámara de compensación que puede estar completamente preparada para cualquier tipo de emergencia al tener medidas de recuperación de desastres muy sofisticadas, pero cuando ocurre una catástrofe, encuentra que ninguna transacción es enviada por sus proveedores, y por lo tanto, está temporalmente sin negocios.
Use el desarrollo de escenarios para aumentar la concientización sobre la detección de riesgos.	El desarrollo de escenarios también ayuda a abordar la cuestión de la detectabilidad, alejándose de una situación en la que una empresa "no sabe lo que no sabe". El enfoque colaborativo para el desarrollo de escenarios ayuda a identificar un riesgo del que la empresa, hasta entonces, no se habría dado cuenta que enfrentaba (y por lo tanto, nunca habría pensado en poner en práctica alguna contramedida). Una vez que el conjunto completo de elementos de riesgo se identifica durante la generación de escenarios, el análisis de riesgos evalúa la frecuencia y el impacto de los escenarios. Las preguntas que se deben hacer incluyen: • ¿La empresa detectará alguna vez que el escenario de riesgo se ha materializado? • ¿La empresa observará que algo ha fallado para que pueda reaccionar adecuadamente? Generar escenarios y pensar creativamente en lo que puede salir mal automáticamente aumentará la detectabilidad, y con suerte, causará una respuesta para éstos. La detectabilidad de escenarios incluye dos pasos: visibilidad y reconocimiento. La empresa debe estar en una posición en la que pueda observar cualquier cosa que va mal, y necesita la capacidad de reconocer un acontecimiento observado como algo incorrecto.
Fuente: *COBIT® 5 para Riesgos*, ISACA, EE.UU., 2013, figura 37	

Características de buenos escenarios

Los escenarios de riesgo deben ser realistas, imparciales y confiables para asegurarse de que la gerencia esté tomando decisiones basadas en información de calidad. Los beneficios del uso de escenarios de riesgo como parte del ERM son significativos, y los profesionales de riesgo deben ser competentes en la preparación de este importante elemento de información para ayudar a la gerencia a identificar, analizar y responder al riesgo.

Los escenarios deben tener las siguientes características (**figura 13**):
Relevancia: Los escenarios deben proporcionar información significativa para apoyar las decisiones. Los escenarios genéricos (de mercado o de la industria) deben personalizarse para reflejar los factores que son relevantes para la empresa.
Consistencia: Cada escenario debe ser convincente por sí mismo. La respuesta adecuada de la gerencia depende de la credibilidad y la integridad de los escenarios utilizados para tomar decisiones.
Plausibilidad: Los escenarios deben ser creíbles y realistas.
Probabilidad: Los escenarios deben, en cierta medida, ser probables de ocurrir.
Oportuno: Los escenarios se deben preparar utilizando los datos más actuales para reflejar el entorno empresarial.

Figura 13: Características de buenos escenarios de riesgo	
Característica	**Explicación**
Relevancia para la decisión	Los escenarios deben proporcionar información significativa para apoyar las decisiones. Los escenarios genéricos (del mercado o de la industria) generalmente no son lo suficientemente adecuados y se deben mejorar.
Consistencia	Cada escenario debe ser convincente por sí mismo. Si no es así, la credibilidad de un escenario puede verse afectada negativamente.
Plausibilidad	Los escenarios deben ser realistas. Deben cumplir con los requerimientos principales de factibilidad básica.
Probabilidad	Cada escenario debe, en cierta medida, ser probable de ocurrir.
Oportuno	Los escenarios deben reflejar eventos y circunstancias actuales.

Capítulo 4
Escenarios de Riesgo Genéricos[4]

Un escenario de riesgo de TI es una descripción de un evento relacionado con TI que puede derivar en un evento de pérdida que tiene un impacto en el negocio, cuando
y si ocurre. Los escenarios genéricos sirven, después de la personalización, como una aportación para las actividades de análisis de riesgo, donde es necesario establecer el impacto final en el negocio (entre otros). Este capítulo contiene un conjunto de escenarios de riesgo de TI genéricos (**figura 14**), desarrollados de acuerdo con el modelo descrito en las secciones anteriores de esta guía. El conjunto de escenarios genéricos contiene ejemplos negativos y positivos.

Una palabra de advertencia: La tabla con escenarios genéricos no reemplaza la fase creativa y reflexiva que cada ejercicio de creación de escenarios debe contener. En otras palabras, no se recomienda que una empresa utilice ciegamente esta lista y asuma que no existen otros escenarios de riesgo posibles, o asuma que cada escenario contenido en la lista es aplicable a la empresa. Se necesitan inteligencia y experiencia para obtener una lista relevante y personalizada de escenarios a partir de esta lista genérica.

Los escenarios de riesgo genéricos en la **figura 14** incluyen la siguiente información:
- **Categoría de escenario de riesgo**: Descripción de alto nivel de la categoría de escenario (p. ej., selección de proyectos de TI). En total, hay 20 categorías.
- **Tipo de riesgo**: El tipo al que encajarán los escenarios derivados de este escenario genérico, utilizando los tres tipos de riesgo explicados anteriormente:
  - Riesgo de la habilitación del beneficio/valor de TI. Asociado con oportunidades (perdidas) de usar la tecnología para mejorar la eficiencia o la efectividad de los procesos de negocio, o como un habilitador para nuevas iniciativas de negocios
  - Riesgo derivado de la ejecución de proyectos y programas de TI. Asociado con la aportación de TI a soluciones empresariales nuevas o mejoradas, usualmente en forma de proyectos y programas
  - Riesgo derivado de operaciones y prestación de servicios de TI. Asociado con la estabilidad operativa, la disponibilidad, la protección y la recuperación de los servicios de TI, que pueden causar destrucción o reducción de valor a la empresa
- **Resultado del escenario de riesgo**: Los resultados positivos son escenarios que pueden derivar en la creación o conservación de valor. Los resultados negativos son escenarios que pueden resultar en la destrucción de valor o en la incapacidad de aumentar valor.

Una "**P**" indica un ajuste primario (grado más alto), y una "**S**" Representa un ajuste secundario (grado inferior). Las celdas en blanco indican que la categoría de riesgo no es relevante para el escenario de riesgo en cuestión.
- **Escenarios de ejemplo**: Para cada categoría de escenario, se muestran uno o varios ejemplos pequeños de escenarios con resultados negativos, indicando si se trata más bien de una destrucción de valor o de la incapacidad de aumentar el valor, y/o un resultado positivo, que indica una ganancia de valor. En total, se incluyen **111 ejemplos de escenarios de riesgo** con posibles resultados negativos y/o positivos.

Figura 14: Ejemplo de escenario de riesgo

Ref.	Categoría del escenario de riesgo	Tipo de riesgo			Escenarios de ejemplo	
		Habilitación del beneficio/valor de TI	Entrega del proyecto y programa de TI	Entrega del servicio y operaciones de TI	Escenarios de ejemplos negativos	Escenarios de ejemplos positivos
0101	Establecimiento y mantenimiento de la cartera	P	P	S	Los programas erróneos son seleccionados para su implementación y están desalineados con la estrategia y las prioridades corporativas.	Los programas conducen a nuevas iniciativas del negocio exitosas seleccionadas para su ejecución.
0102		P	P	S	Hay duplicación entre iniciativas.	Las iniciativas alineadas tienen interfaces simplificadas.
0103		P	P	S	Un nuevo programa importante crea una incompatibilidad a largo plazo con la arquitectura empresarial.	Los programas nuevos se evalúan con respecto a su compatibilidad con la arquitectura existente.
0104		P	P	S	Los recursos en competencia se asignan y gestionan de manera ineficiente y no están alineados con las prioridades del negocio.	

[4] El contenido de este capítulo se basa en la siguiente publicación: ISACA, *COBIT® 5 para Riesgos*, EE.UU., 2013.

Figura 14: Ejemplo de escenario de riesgo *(cont.)*

Ref.	Categoría del escenario de riesgo	Tipo de riesgo			Escenarios de ejemplo	
		Habilitación del beneficio/valor de TI	Entrega del proyecto y programa de TI	Entrega del servicio y operaciones de TI	Escenarios de ejemplos negativos	Escenarios de ejemplos positivos
0201	Gestión del ciclo de vida del programa/proyectos (iniciación de programas/ proyectos, economía, entrega, calidad y terminación)	P	P	S	Los proyectos que fracasan (debido a costos, retrasos, corrupción del alcance, cambios en las prioridades del negocio) no se rescinden.	Los proyectos que fracasan o irrelevantes se detienen oportunamente.
0202		S	P	S	Hay un rebasamiento presupuestario del proyecto de TI.	El proyecto de TI se completa dentro del presupuesto acordado.
0203		S	P		Ocasionalmente, hay una entrega tardía del proyecto de TI por parte de un departamento de desarrollo interno.	La entrega del proyecto se hace a tiempo.
0204		P	P	S	Rutinariamente, hay retrasos importantes en la ejecución de proyectos de TI.	La ruta crítica del proyecto se gestiona en consecuencia y la entrega se hace a tiempo.
0205		P	P	S	Hay retrasos excesivos en proyectos de desarrollo de TI sub-contratados.	La comunicación con terceros garantiza la entrega oportuna dentro del alcance y la calidad acordados.
0206		P	P		Los programas/proyectos fracasan debido a no obtener la participación activa durante todo el ciclo de vida del programa/proyecto de todas las partes interesadas (incluyendo el patrocinador).	La gestión del cambio se lleva a cabo adecuadamente durante todo el ciclo de vida del programa/proyecto para informar a las partes interesadas sobre el avance y capacitar a los usuarios futuros.
0301	Toma de decisiones sobre inversiones en TI	P		S	Los gerentes o representantes de negocios no están involucrados en decisiones de inversión en TI importantes (p. ej., nuevas aplicaciones, priorización, nuevas oportunidades de tecnología).	Hay una toma de decisiones coordinada sobre las inversiones en TI entre el negocio y TI.
0302		P		S	El software incorrecto, en términos de costo, rendimiento, funciones, compatibilidad, etc., se selecciona para su implementación.	Se realiza un análisis inicial y se prepara un caso de negocios para garantizar la selección adecuada de software.
0303		P		P	La infraestructura incorrecta, en términos de costo, rendimiento, funciones, compatibilidad, etc., se selecciona para su implementación.	Se realiza un análisis inicial y se prepara un caso de negocios para garantizar la selección adecuada de infraestructura.
0304		P	P		Se compra software redundante.	
0401	Experiencia y habilidades en TI	P	P	P	Hay una falta o incompatibilidad de habilidades relacionadas con TI dentro del área de TI, p. ej., debido a las nuevas tecnologías.	Atraer al personal adecuado aumenta la prestación de servicios del departamento de TI.
0402		P	P	P	Hay una falta de comprensión del negocio por parte del personal de TI, lo cual afecta la calidad de la prestación de servicios/proyectos.	La combinación correcta de personal y habilidades apoya la entrega del proyecto y la entrega de valor.
0403		P	P	P	No hay habilidades suficientes para cubrir los requerimientos del negocio.	La combinación correcta de habilidades y capacitación garantiza que hay una comprensión completa del negocio por parte del personal, y permite la cobertura total de los requerimientos del negocio.
0404		S	P	P	Hay una incapacidad para contratar personal de TI.	La cantidad correcta de personal de TI, con las habilidades y competencias apropiadas, es atraída para apoyar los objetivos del negocio.
0405		S	P	P	Existe una falta de debida diligencia en el proceso de reclutamiento.	Los candidatos son evaluados para asegurarse de que las habilidades, competencias y actitud apropiadas estén presentes.
0406		S	P	P	Hay una falta de capacitación, lo que deriva en rotación del personal del TI.	Los miembros del personal de TI pueden determinar su propio plan de capacitación basándose en sus aspiraciones y dominios de interés, en colaboración con sus superiores.
0407		S	P	P	No hay retorno en la inversión suficiente en relación con la capacitación debido a la pronta salida del personal capacitado de TI (p. ej., MBA).	El desarrollo profesional se hace de manera formal, y se determinan las trayectorias individuales para asegurarse de que el personal de TI esté motivado para permanecer por una cantidad de tiempo considerable.

Figura 14: Ejemplo de escenario de riesgo *(cont.)*						
		Tipo de riesgo			Escenarios de ejemplo	
Ref.	Categoría del escenario de riesgo	Habilitación del beneficio/valor de TI	Entrega del proyecto y programa de TI	Entrega del servicio y operaciones de TI	Escenarios de ejemplos negativos	Escenarios de ejemplos positivos
0408	**Experiencia y habilidades en TI *(cont.)***	S	P	P	Existe una dependencia excesiva en el personal clave de TI.	La rotación del trabajo garantiza que más de una persona posea todo el conocimiento de la ejecución de una determinada actividad.
0409		S	P	P	Hay una incapacidad para actualizar las habilidades de TI al nivel adecuado a través de la capacitación.	Capacitación, asistencia a seminarios y lectura sobre filosofía de liderazgo garantiza que el personal de TI esté al día con los últimos avances en su área de especialidad.
0501	**Operaciones del personal (error humano e intención maliciosa)**	S	S	P	Se abusan los derechos de acceso de roles anteriores.	La gerencia de RR.HH. y de TI se coordinan con frecuencia para garantizar la eliminación oportuna de los derechos de acceso, evitando la posibilidad de abuso.
0502		S		P	El equipo de TI es dañado accidentalmente por el personal.	
0503		S		P	Hay errores del personal de TI (durante las copias de respaldo, las actualizaciones de sistemas, el mantenimiento de sistemas, etc.).	Se aplica el principio de cuatro ojos, disminuyendo la posibilidad de errores antes de pasar a la producción.
0504		S		P	La información se ingresa incorrectamente por parte del personal de TI o los usuarios del sistema.	Se aplica el principio de cuatro ojos, disminuyendo la posibilidad de ingresar la información incorrecta.
0505		S		P	El centro de datos es destruido (sabotaje, etc.) por el personal.	El centro de datos está protegido debidamente, permitiendo solo el acceso a personal de TI autorizado.
0506		S		P	Hay un robo de un dispositivo con datos sensibles por parte del personal.	Las oficinas están aseguradas y monitoreadas para detectar la actividad irregular.
0507		S		P	Hay un robo de un componente clave de infraestructura por parte del personal.	Los componentes clave de la infraestructura son monitoreados las 24 horas del día para verificar el rendimiento, la disponibilidad, etc. Se levantan alarmas en caso de irregularidades y se actúa inmediatamente.
0508		P	S	P	Los componentes de hardware se configuraron erróneamente.	Se configura un sistema de gestión de la configuración para toda la empresa, lo que garantiza una configuración alineada en toda la empresa.
0509		P	S	P	Se dañaron los servidores críticos en la sala de computadoras (p. ej., un accidente, etc.).	Los componentes clave de la infraestructura son monitoreados las 24 horas del día para verificar el rendimiento, la disponibilidad, etc. Se levantan alarmas en caso de irregularidades y se actúa inmediatamente.
0510		P	S	P	El hardware fue manipulado intencionalmente (dispositivos de seguridad, etc.).	Los componentes clave de la infraestructura son monitoreados las 24 horas del día para verificar el rendimiento, la disponibilidad, etc. Se levantan alarmas en caso de irregularidades y se actúa inmediatamente.

Figura 14: Ejemplo de escenario de riesgo *(cont.)*

Ref.	Categoría del escenario de riesgo	Tipo de riesgo			Escenarios de ejemplo	
		Habilitación del beneficio/valor de TI	Entrega del proyecto y programa de TI	Entrega del servicio y operaciones de TI	Escenarios de ejemplos negativos	Escenarios de ejemplos positivos
0601	Información (filtración de datos: daños, fugas y acceso)	S		P	Se dañan componentes de hardware, lo que lleva a la destrucción (parcial) de datos por el personal interno.	Se establecen procedimientos de copia de seguridad, alineados con la criticidad empresarial de los datos, lo que garantiza que los datos clave del negocio siempre se conserven en una segunda ubicación.
0602		S	S	P	La base de datos está dañada, causando que los datos sean inaccesibles.	
0603		S	S	P	Se pierden/divulgan medios portátiles que contienen datos sensibles (CD, unidades USB, discos portátiles, etc.).	Los medios portátiles están debidamente protegidos y encriptados para garantizar la protección de los datos.
0604		S	S	P	Se pierden/divulgan datos sensibles a través de ataques lógicos.	Los datos sensibles almacenados en las instalaciones de la empresa están protegidos adecuadamente detrás de los cortafuegos (firewalls) y mediante la monitorización continua de la red.
0605		S	S	P	Se pierde el medio de copia de seguridad o no se comprueba la eficacia de las copias de seguridad.	
0606		P	S	P	Se divulga accidentalmente información sensible debido al incumplimiento con las pautas de manejo de la información.	Se anima continuamente a los empleados a ser embajadores de la cultura de la empresa, la ética y la buena conducta, incluyendo las prácticas relacionadas con el manejo de la información.
0607		P	S	P	Se modifican intencionalmente datos (contabilidad, datos relacionados con la seguridad, cifras de ventas, etc.).	Se aplica el principio de cuatro ojos para el ingreso/la modificación de datos específicos con el fin de crear una revisión por parte de pares y disminuir el estímulo para la modificación intencional.
0608		P	S	P	Se divulga información sensible a través de correo electrónico o redes sociales.	Se anima continuamente a los empleados a ser embajadores de la cultura de la empresa, la ética y la buena conducta, incluyendo las prácticas que involucran la distribución de información a través de correo electrónico y redes sociales.
0609		P	S	P	Se descubre información sensible debido a la retención/archivado/eliminación ineficientes de la información.	La política de retención de datos se actualiza periódicamente y se fomenta el cumplimiento estricto de todos los empleados.
0610		P	S	P	Se pierde propiedad intelectual y/o se filtra información competitiva debido a que miembros clave del equipo abandonan la empresa.	Se incorporan cláusulas de propiedad intelectual a cada contrato, lo que permite a la empresa aprovechar plenamente los beneficios de toda la PI creada en la empresa.
0611		P	S	P	La empresa tiene un desbordamiento de datos y no puede deducir la información relevante del negocio de entre los datos (p. ej., problema de datos grandes).	La empresa ha implementado un proceso efectivo para procesar los datos que tiene a información relevante del negocio y utilizar esa información para crear valor comercial.
0701	Arquitectura (visión y diseño arquitectónicos)	P	P	P	La arquitectura empresarial es compleja e inflexible, obstaculizando una mayor evolución y expansión, lo que deriva en oportunidades de negocio perdidas.	La arquitectura moderna y flexible soporta la agilidad/innovación del negocio.
0702		P	S	P	La arquitectura empresarial no es apta para el propósito y no apoya las prioridades del negocio.	
0703		P	S	S	Hay un fracaso para adoptar y explotar la nueva infraestructura de manera oportuna.	
0704		P	S	S	Hay un fracaso para adoptar y explotar el nuevo software (funcionalidad, optimización, etc.) de manera oportuna.	

Figura 14: Ejemplo de escenario de riesgo *(cont.)*						
		Tipo de riesgo			Escenarios de ejemplo	
Ref.	Categoría del escenario de riesgo	Habilitación del beneficio/valor de TI	Entrega del proyecto y programa de TI	Entrega del servicio y operaciones de TI	Escenarios de ejemplos negativos	Escenarios de ejemplos positivos
0801	Infraestructura (hardware, sistema operativo y tecnología de control) (selección/implementación, operaciones y desmantelamiento)	P	S	P	Se instala una infraestructura nueva (innovadora) y, como resultado, los sistemas se vuelven inestables y provocan incidentes operativos, p. ej., el programa traiga su propio dispositivo (BYOD).	Se realizan pruebas apropiadas antes de establecer la infraestructura en el entorno de producción para garantizar la disponibilidad y el funcionamiento adecuado de todo el sistema.
0802		P	S	P	Los sistemas no pueden manejar los volúmenes de transacciones cuando aumentan los volúmenes de usuarios.	
0803		P	S	P	Los sistemas no pueden manejar la carga del sistema cuando se implementan nuevas aplicaciones o iniciativas.	
0804		P	S	P	Intermitentemente, hay fallas de los servicios (telecomunicaciones, electricidad, etc.).	Se prevén líneas de respaldo y permanecen en stand by las 24 horas para apoyar la ejecución continua de las transacciones críticas del negocio.
0805		P	S	P	La TI en uso es obsoleta y no puede satisfacer nuevos requerimientos del negocio (redes, seguridad, base de datos, almacenamiento, etc.).	La TI es innovadora, garantizando la interacción bidireccional entre el área de negocios y de TI.
0806				P	El hardware falla debido al sobrecalentamiento.	
0901	Software	P		S	Hay una incapacidad para usar el software con el fin de lograr los resultados deseados (p. ej., no hacer los cambios necesarios al modelo u organizacionales).	El software en uso estimula la generación de nuevas ideas.
0902		P		S	Se implementa software inmaduro (usuarios pioneros, errores, etc.).	
0903		P		S	El software incorrecto (costo, rendimiento, funciones, compatibilidad, etc.) se selecciona para su implementación.	Se realiza un análisis inicial y se prepara un caso de negocios para garantizar la selección adecuada de software.
0904		P		S	Existen fallas operativas cuando se pone en funcionamiento un nuevo software.	El entrenamiento adaptado por el usuario y las pruebas de aceptación del usuario se realizan antes de la decisión de lanzar el software en vivo con el fin de garantizar una transición impecable al nuevo software y la continua generación de valor para el negocio.
0905		P		S	Los usuarios no pueden usar y explotar el nuevo software de aplicación.	
0906		P		S	Modificación intencional del software que deriva en datos erróneos o acciones fraudulentas.	Se aplica el principio de cuatro ojos para el ingreso/la modificación de datos específicos con el fin de crear una revisión por parte de pares y disminuir el estímulo para acciones fraudulentas o simplemente de resultados inesperados.
0907		P		S	La modificación no intencional del software deriva en resultados inesperados.	
0908		P		S	Se producen una configuración accidental y errores en la gestión de cambios.	La gestión de la configuración de toda la empresa reduce el tiempo de resolución para la gestión de incidentes y problemas.
0909		P		S	Se produce regularmente un mal funcionamiento del software de aplicación crítico.	Se realizan pruebas apropiadas antes de tomar la decisión de lanzarlo en vivo para garantizar la disponibilidad y el funcionamiento adecuado del software.
0910		P		S	Se producen problemas intermitentes con el software de sistema importante.	
0911		P		S	El software de aplicación está obsoleto (p. ej., tecnología antigua, mal documentada, costosa de mantener, difícil de extender, no integrada a la arquitectura actual).	La TI es innovadora, garantizando la interacción bidireccional entre el área de negocios y de TI.
0912		P		S	Hay una incapacidad de volver a versiones anteriores en caso de problemas operativos con la nueva versión.	Los puntos de copia de seguridad y de restauración se establecen de acuerdo con la criticidad comercial del software para garantizar los procedimientos de restauración.

Figura 14: Ejemplo de escenario de riesgo *(cont.)*

Ref.	Categoría del escenario de riesgo	Tipo de riesgo			Escenarios de ejemplo	
		Habilitación del beneficio/valor de TI	Entrega del proyecto y programa de TI	Entrega del servicio y operaciones de TI	Escenarios de ejemplos negativos	Escenarios de ejemplos positivos
1001	**Propiedad empresarial de TI**	P	P	S	El negocio no asume la responsabilidad sobre las áreas de TI por las que debería, p. ej., requerimientos funcionales, prioridades de desarrollo, evaluación de oportunidades a través de nuevas tecnologías.	El negocio asume la responsabilidad apropiada sobre las TI y co-determina la estrategia de TI, especialmente la cartera de aplicaciones.
1002		P	S	S	Existe una extensa dependencia y uso de la computación del usuario final y de soluciones *ad hoc* para las necesidades de información importantes, lo que deriva en deficiencias de seguridad, datos imprecisos o el aumento de costes/uso ineficiente de los recursos.	
1003		P	S	S	El coste y la ineficacia están relacionados con compras vinculadas a TI fuera del proceso de adquisición.	Siempre se prepara un caso de negocio para garantizar el coste óptimo y la compra eficaz de software.
1004				P	Los requerimientos inadecuados derivan en acuerdos de nivel de servicio (SLA) ineficaces.	
1101	**Proveedor (selección/ rendimiento, cumplimiento contractual, terminación de servicio y transferencia)**		S	P	Existe una falta de debida diligencia para los proveedores con respecto a la viabilidad financiera, capacidad de entrega y sostenibilidad del servicio del proveedor.	El tercero actúa como socio estratégico.
1102			S	P	Se aceptan términos de negocio irrazonables por parte de proveedores de TI.	
1103			S	P	El soporte y los servicios ofrecidos por los proveedores son inadecuados y no están en línea con el SLA.	Los indicadores clave de desempeño (KPI) apropiados, vinculados a recompensas y penalizaciones, garantizan una prestación de servicios y soporte adecuados.
1104			S	P	El rendimiento de un proveedor externo es inadecuado en un acuerdo a gran escala de outsourcing a largo plazo.	
1105			S	P	Hay un incumplimiento con los acuerdos de licencia de software (uso y/o distribución de software sin licencia, etc.).	Se aceptan acuerdos contractuales sobre el uso de software de terceros y software registrado.
1106			S	P	Hay una incapacidad para transferir funciones a proveedores alternativos debido a la dependencia excesiva con el proveedor actual.	Una cláusula de eliminación gradual y de transferencia de conocimiento se agrega al contrato con el proveedor, requiriéndole hacer una transferencia con los nuevos proveedores. Se establece una combinación de empleados internos y externos para cada proceso, evitando que el conocimiento del proceso completo solo esté en los empleados externos.
1107			S	P	El negocio compra servicios en la nube sin la consulta/participación del área de TI, lo que deriva en la incapacidad de integrar el servicio con los servicios internos.	
1201	**Cumplimiento normativo**	P	S	S	Hay un incumplimiento con las regulaciones, p. ej., privacidad, contabilidad, fabricación.	Se aprovecha el cumplimiento pleno con las regulaciones para que los clientes generen un valor extra para el negocio.
1202		P	S	S	El desconocimiento de los posibles cambios regulatorios tiene un impacto en el entorno operativo de TI.	La empresa establece un departamento jurídico y de cumplimiento para dar seguimiento a los cambios normativos y garantizar la continuación de la generación de valor para el negocio.
1203		P	S	S	El regulador evita el flujo de datos transfronterizo debido a controles insuficientes.	

Figura 14: Ejemplo de escenario de riesgo *(cont.)*						
		Tipo de riesgo			Escenarios de ejemplo	
Ref.	Categoría del escenario de riesgo	Habilitación del beneficio/valor de TI	Entrega del proyecto y programa de TI	Entrega del servicio y operaciones de TI	Escenarios de ejemplos negativos	Escenarios de ejemplos positivos
1301	Geopolítica			P	No hay acceso debido a incidentes disruptivos en otras instalaciones.	El claro cumplimiento de las políticas nacionales y el apoyo a las iniciativas locales garantizan el apoyo del gobierno local y la generación de valor para el negocio.
1302				P	La interferencia gubernamental y las políticas nacionales limitan la capacidad de los servicios.	
1303				P	Acciones dirigidas contra la empresa derivan en la destrucción de infraestructura.	
1401	Robo o destrucción de infraestructura	S	S	P	Hay un robo de un dispositivo con datos sensibles.	Los componentes clave de la infraestructura son monitorizados las 24 horas del día para verificar el rendimiento, la disponibilidad, etc. Se levantan alarmas en caso de irregularidades y se actúa inmediatamente.
1402		S	S	P	Hay un robo de un número sustancial de servidores de desarrollo.	
1403		S	S	P	Se produce la destrucción del centro de datos (sabotaje, etc.).	El centro de datos está protegido debidamente, permitiendo solo el acceso a personal de TI autorizado.
1404		S	S	P	Hay una destrucción accidental de dispositivos individuales.	
1501	Malware	S		P	Hay una intrusión de malware en los servidores operativos críticos.	La infraestructura de TI estará protegida adecuadamente detrás de un cortafuegos (firewall) y a través de la monitorización continua de la red para garantizar la ejecución de las actividades diarias.
1502		S		P	Regularmente hay infección de ordenadores portátiles con malware.	
1503		S		P	Un empleado descontento implementa una bomba de tiempo que deriva en la pérdida de datos.	
1504		S		P	Los datos de la empresa son robados a través del acceso no autorizado obtenido por un ataque de phishing.	
1601	Ataques lógicos	S		P	Usuarios no autorizados intentan penetrar los sistemas.	
1602		S		P	Hay una interrupción del servicio debido a un ataque de denegación de servicio (DDoS)	
1603		S		P	El sitio web es alterado.	
1604		S		P	Se produce espionaje industrial.	
1605		S		P	Hay un ataque de virus.	
1606		S		P	Se produce hacktivismo.	
1701	Acción industrial	S	S	P	Las instalaciones y el edificio no son accesibles debido a una huelga sindical.	Un plan de continuidad del negocio prevé que se tomen medidas para siempre garantizar la ejecución de tareas críticas del negocio en caso de que el edificio no sea accesible.
1702		S	S	P	El personal clave no está disponible por una acción industrial (p. ej., huelga de transporte).	Una política de trabajo flexible, que permite a los empleados trabajar desde otra ubicación que no sea el edificio de oficinas, simula la libertad y crea un ambiente de trabajo positivo.
1703		S	S	P	Un tercero no puede prestar servicios debido a una huelga.	
1704		S	S	P	No hay acceso al capital causado por una huelga de la industria bancaria.	

Figura 14: Ejemplo de escenario de riesgo *(cont.)*

Ref.	Categoría del escenario de riesgo	Tipo de riesgo: Habilitación del beneficio/valor de TI	Tipo de riesgo: Entrega del proyecto y programa de TI	Tipo de riesgo: Entrega del servicio y operaciones de TI	Escenarios de ejemplo: Escenarios de ejemplos negativos	Escenarios de ejemplo: Escenarios de ejemplos positivos
1801	Medio ambiente	S	S	P	El equipo utilizado no es ecológico (p. ej., consumo de energía, embalaje).	Ser galardonado por procesos ecológicos crea una atención mediática positiva, atrae a nuevos clientes y empleados, y asegura la creación de valor.
1901	Actos de la naturaleza	S	S	P	Ocurre un terremoto.	
1902		S	S	P	Ocurre un tsunami.	
1903		S	S	P	Ocurren grandes tormentas y ciclones tropicales.	
1904		S	S	P	Ocurre un gran incendio forestal.	
1905		S	S	P	Ocurre una inundación.	
1906		S	S	P	El nivel freático está subiendo.	
2001	Innovación	P	S	S	No se identifican nuevas e importantes tendencias tecnológicas.	Se respaldan y alientan la innovación y la monitorización de tendencias, garantizando que las nuevas tecnologías (tendencias) se evalúen a tiempo respecto a su impacto en el negocio y se adopten si es necesario.
2002		P		S	Hay un fracaso para adoptar y explotar el nuevo software (funcionalidad, optimización, etc.) de manera oportuna.	Se respaldan y alientan la innovación y la monitorización de tendencias, garantizando que las nuevas tecnologías (tendencias) se evalúen a tiempo respecto a su impacto en el negocio y se adopten si es necesario.
2003		P		S	No se identifican nuevas e importantes tendencias de software (consumo de TI).	

Fuente: *COBIT® 5 para Riesgos*, ISACA, EE.UU., 2013, figura 38

El Capítulo 5, Uso de Habilitadores de COBIT 5 para Mitigar Escenarios de Riesgo de TI, proporciona un conjunto de ejemplos que muestran cómo los habilitadores de COBIT 5 se pueden usar para responder a los escenarios de riesgo descritos en la **figura 14**. Otros marcos de gestión de TI, como la Biblioteca de Infraestructuras de Tecnologías de Información (ITIL), la Organización Internacional para la Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) 27001/2, también se pueden usar para ese propósito, pero no se incluyen enlaces/mapeos detallados.

Capítulo 5
Uso de Habilitadores de COBIT 5 para Mitigar Escenarios de Riesgo de TI[5]

Durante el proceso de respuesta al riesgo, la mitigación del riesgo es una de las opciones que se pueden utilizar para responder al riesgo. La mitigación de riesgos relacionados con TI es equivalente a implementar una serie de controles de TI. En términos de COBIT 5, los controles de TI pueden ser cualquier habilitador, p. ej., principios, políticas y marcos; procesos; estructuras organizacionales; cultura, ética y conducta; información; servicios, infraestructura y aplicaciones; o personas, habilidades y competencias.

Este capítulo proporciona ejemplos que muestran cómo se pueden utilizar los habilitadores de COBIT 5 para responder a los escenarios de riesgo. Para cada una de las categorías de escenarios de riesgo identificadas en el Capítulo 4, se proporcionan posibles acciones de mitigación relacionadas con los siete habilitadores de COBIT 5, con una referencia, título y descripción para cada habilitador.

Al usar los ejemplos en este capítulo, el lector debe tener en cuenta que:
- Los ejemplos no reemplazan el ejercicio de análisis de riesgos. Las categorías de escenarios de riesgo presentadas aquí son genéricas y, por sí mismas, pueden cubrir muchos escenarios derivados y variados. Cada empresa necesita primero personalizar y definir su propio conjunto de escenarios de riesgo.
- Los ejemplos se deben personalizar para incluir todos los riesgos y todos los factores de riesgo que se deben considerar antes que se definan las medidas de mitigación del riesgo.
- Los controles/habilitadores de TI sugeridos no son absolutos. Se deben ponderar en términos de coste y beneficio, es decir, cuán efectivos serán para abordar el riesgo y el coste para implementarlos. Se debe estimar el efecto de la acción mitigadora sobre el impacto potencial y la frecuencia del riesgo y depende de la madurez de la implementación del control/habilitador de TI, el contexto de la empresa, etc. Cuando se estima que el efecto sobre el impacto y la frecuencia es "alto", la acción puede considerarse "esencial" para la empresa.
- La lista sugerida de controles/habilitadores de TI podría no estar completa para una situación particular, así que el usuario debe estar preparado para analizar cuidadosamente si es necesario agregar o eliminar controles según cada situación. Para algunos escenarios, se puede requerir orientación adicional y más detallada. Ejemplos de ello son los elementos y controles de riesgos de seguridad de la información, como la gestión de vulnerabilidades o el escaneo de seguridad de aplicaciones.

El valor de esta sección se relaciona con:
- **Evaluación y análisis de riesgos**. Cuando se necesita evaluar la frecuencia y el impacto, es necesario tener en cuenta los controles/habilitadores de TI para determinar el impacto y una evaluación realista de la frecuencia. La madurez del habilitador es un factor de riesgo muy importante.
- **Mitigación de riesgos**. Cuando el riesgo se puede mitigar, es necesario definir, evaluar y aplicar los controles/habilitadores de TI. Los ejemplos de este capítulo proporcionan una serie de controles/habilitadores de TI sugeridos para cada riesgo en los ejemplos.

Nota: Las tablas que unen cada categoría de escenarios de riesgo con un conjunto de habilitadores atenuantes se mantienen a un nivel muy genérico, proporcionando así un punto de partida para preparar los planes de mitigación. Cada empresa necesitará adaptar el conjunto de habilitadores requeridos para analizar y mitigar cada escenario de riesgo específico en su alcance.

[5] El contenido de este capítulo se basa en la siguiente publicación: ISACA, *COBIT® 5 para Riesgos*, EE.UU., 2013.

Categoría del escenario de riesgo 1: Establecimiento y mantenimiento de la cartera		
Categoría del escenario de riesgo	Establecimiento y mantenimiento de la cartera	
Habilitador de principios, políticas y marco de trabajo		
Referencia		**Contribución a la respuesta**
Política de gestión de programas/proyectos		Imponer el uso de la metodología general del programa/proyecto, incluyendo la política corporativa sobre el caso de negocio o la debida diligencia para mejorar la visibilidad del valor relativo de los programas (comparados entre sí). Esta política debe describir los umbrales de inversión de aprobación para el valor del programa.
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
EDM02.01	Evaluar la optimización del valor.	Evaluar continuamente la cartera de inversiones, servicios y activos habilitados por TI con el fin de determinar la probabilidad de alcanzar los objetivos de la empresa y entregar un valor a un costo razonable. Identificar y hacer un juicio sobre cualquier cambio en la dirección que debe ofrecerse a la gerencia para optimizar la creación de valor.
EDM02.02	Dirigir la optimización del valor.	Dirigir los principios y las prácticas de gestión de valor para permitir una obtención óptima de valor con las inversiones habilitadas para TI durante todo su ciclo de vida económico.
EDM02.03	Monitorizar la optimización del valor.	Monitorizar las metas y métricas clave para determinar la medida en que el negocio está generando el valor y los beneficios esperados para el negocio a través de las inversiones y los servicios habilitados por TI. Identificar problemas significativos y considerar acciones correctivas.
APO01.01	Definir la estructura organizacional.	Establecer una estructura organizacional interna y extendida que refleje las necesidades del negocio y las prioridades de TI. Establecer las estructuras de gestión requeridas (p. ej., comités) que permitan que la toma de decisiones de gestión se lleve a cabo de la manera más eficaz y eficiente.
APO01.04	Comunicar los objetivos y la dirección de la gerencia.	Concienciar y comunicar, buscando la comprensión de los objetivos y la dirección de TI a las partes interesadas apropiadas y los usuarios en toda la empresa.
APO02.03	Definir las capacidades objetivo de TI.	Definir las capacidades objetivo del negocio y de TI, así como los servicios de TI requeridos. Esto debe basarse en el entendimiento del entorno y los requerimientos de la empresa; la evaluación de los procesos comerciales actuales y el entorno y los problemas de TI; y considerando los estándares de referencia, las mejores prácticas y las tecnologías emergentes validadas o las propuestas de innovación.
APO04.03	Monitorizar y escanear el entorno tecnológico.	Monitorizar y escanear sistemáticamente el entorno externo de la empresa para identificar las tecnologías emergentes con el potencial de crear valor (p. ej., ejecutar la estrategia empresarial, optimizar costes, evitar la obsolescencia y habilitar de mejor manera los procesos empresariales y de TI). Monitorizar el mercado, el entorno competitivo, los sectores de la industria y las tendencias legales y regulatorias para poder analizar las tecnologías emergentes o las ideas de innovación en el contexto empresarial.
APO05.01	Establecer el objetivo de la mezcla de inversión.	Revisar y asegurarse que las estrategias y los servicios actuales de la empresa y de TI sean claros. Definir una mezcla de inversión apropiada con base en el coste, la alineación con la estrategia, y las medidas financieras como el coste y el retorno de la inversión (ROI) anticipado durante todo el ciclo de vida económico, el grado de riesgo y el tipo de beneficio para los programas en la cartera. Ajustar las estrategias empresariales y de TI cuando sea necesario.
APO05.03	Evaluar y seleccionar programas para financiar.	Basándose en los requerimientos generales de la mezcla de la cartera de inversión, evaluar y establecer prioridades de los casos de negocio del programa y tomar decisiones sobre las propuestas de inversión. Asignar fondos e iniciar los programas.
APO05.05	Mantener las carteras.	Mantener las carteras de los programas y proyectos de inversión, servicios de TI y activos de TI.
APO06.02	Establecer prioridades para la asignación de recursos.	Implementar un proceso de toma de decisiones para establecer prioridades sobre la asignación de recursos y reglas para las inversiones discrecionales por unidades del negocio individuales. Incluir el posible uso de proveedores de servicios externos y considerar las opciones de compra, desarrollo y alquiler.
BAI02.01	Definir y mantener los requerimientos funcionales y técnicos del negocio.	Basándose en el caso de negocio, identificar, priorizar, especificar y acordar los requerimientos de información empresarial, funcionales, técnicos y de control que cubran el alcance/la comprensión de todas las iniciativas necesarias para lograr los resultados esperados de la solución empresarial habilitada para TI propuesta.
Habilitador de estructuras organizacionales		
Referencia		**Contribución a la respuesta**
Oficina de gestión de proyectos y programas (PMO)		Responsable de la calidad de los casos de negocio.
Consejo de Dirección		Se requiere la aprobación cuando los programas superan un cierto umbral de valor y un nivel de riesgo.
Director de Finanzas (CFO)		Ayuda con la alineación de la estrategia y las prioridades y la visión general sobre los programas.

Categoría del escenario de riesgo 1: Establecimiento y mantenimiento de la cartera *(cont.)*	
Habilitador de cultura, ética y comportamiento	
Referencia	**Contribución a la respuesta**
La selección de programas incluye decisiones basadas en datos	Las decisiones deben ser objetivas, no sesgadas y basadas en información fundamentada.
Participación de las partes interesadas	La gama completa de factores de éxito se tendrá en cuenta al seleccionar programas.
Enfoque en objetivos empresariales	Asegurar la alineación con la estrategia y las prioridades corporativas.
Habilitador de información	
Referencia	**Contribución a la respuesta**
Caso de negocio del programa	Mejora la visibilidad del valor relativo de los programas (comparados entre sí).
Mezcla de inversión definida	Mejora la visibilidad del valor relativo de los programas (comparados entre sí).
Habilitador de servicios, infraestructura y aplicaciones	
Referencia	**Contribución a la respuesta**
Herramientas de gestión de cartera	Disminuye la complejidad y aumenta la visión general de los programas y proyectos.
Habilitador de personas, habilidades y competencias	
Referencia	**Contribución a la respuesta**
Habilidades de financiación de programas/ proyectos	Crear visibilidad sobre el valor del programa.
Análisis de requerimientos del negocio	Transparencia en la estrategia empresarial, requerimientos del negocio relacionados y prioridades.
Habilidades relacionadas con el márketing	Crear visibilidad sobre el valor del programa.

Categoría del escenario de riesgo 2: Gestión del ciclo de vida del programa/proyecto		
Categoría del escenario de riesgo		Gestión del ciclo de vida del programa/proyecto Alcance: Iniciación de programas/proyectos, economía, entrega, calidad y terminación
Habilitador de principios, políticas y marco de trabajo		
Referencia		**Contribución a la respuesta**
Política de gestión de programas/proyectos		La medición de la visibilidad y el estado real de los tomadores de decisiones deben basarse en un lenguaje y una metodología comunes: • Reconocimiento de los proyectos fallidos (en términos de coste, retrasos, requerimientos imprevistos, cambios en las prioridades del negocio, etc.) y crear flujos de información para inducir acciones correctivas. • Para prevenir el fracaso, los cambios de alcance en los proyectos existentes se deben gestionar estrictamente.
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
EDM02.03	Monitorizar la optimización del valor.	Monitorizar las metas y métricas clave para determinar la medida en que el negocio está generando el valor y los beneficios esperados para el negocio a través de las inversiones y los servicios habilitados por TI. Identificar problemas significativos y considerar acciones correctivas.
APO01.01	Definir la estructura organizacional.	Establecer una estructura organizacional interna y extendida que refleje las necesidades del negocio y las prioridades de TI. Establecer las estructuras de gestión requeridas (p. ej., comités) que permitan que la toma de decisiones de gestión se lleve a cabo de la manera más eficaz y eficiente.
APO06.04	Modelar y asignar los costes.	Establecer y usar un modelo de costes de TI basado en la definición del servicio, asegurando que esta asignación de costes para servicios sea identificable, medible y predecible, para fomentar el uso responsable de los recursos, incluyendo aquellos proporcionados por proveedores de servicios. Revisar y comparar periódicamente la idoneidad del modelo de costes/recargos para mantener su relevancia e idoneidad para las actividades empresariales y de TI en evolución.
APO06.05	Gestionar los costos.	Implementar un proceso de gestión de costos que compare los costes actuales con los presupuestos. Es necesario monitorizar e informar sobre los costes, y en caso de desviaciones, identificarlos de forma oportuna, así como su impacto sobre los procesos empresariales y los servicios analizados.
BAI01.01	Mantener un enfoque estándar para la gestión de programas y proyectos.	Mantener un enfoque estándar para la gestión de programas y proyectos que permita la evaluación del gobierno y la gestión, así como las actividades de gestión de toma de decisiones y de entrega, enfocadas en el logro de valor y de las metas (requerimientos, riesgos, costes, calendario, calidad) para el negocio de forma consistente.
BAI01.02	Iniciar un programa.	Iniciar un programa para confirmar los beneficios esperados y obtener la autorización para proceder. Esto incluye acordar el apoyo a los programas, confirmar el mandato del programa mediante la aprobación del caso comercial conceptual, asignando una junta directiva o un comité para el programa, produciendo el resumen del programa, revisando y actualizando el caso comercial, desarrollando un plan de objetivos de beneficios y obteniendo la aprobación de los patrocinadores para proceder.
BAI01.03	Gestionar la participación de las partes interesadas.	Gestionar la participación de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna que llegue a todas las partes interesadas relevantes. Esto incluye planificar, identificar e involucrar a las partes interesadas y gestionar sus expectativas.
BAI01.04	Desarrollar y mantener el plan del programa.	Formular un programa que establezca las bases iniciales y una posición para la ejecución exitosa al formalizar el alcance del trabajo que debe alcanzarse e identificar los entregables que satisfarán las metas y producirán valor. Mantener y actualizar el plan del programa y el caso de negocio durante todo el ciclo de vida económico del programa, asegurando la alineación con los objetivos estratégicos y reflejando el estado actual y la información actualizada que se obtiene diariamente.
BAI01.05	Lanzar y ejecutar el programa.	Lanzar y ejecutar el programa para adquirir y dirigir los recursos necesarios para lograr las metas y beneficios del programa tal como se define en el plan del programa. De acuerdo con los criterios de revisión de aprobación o publicación, prepararse para las revisiones de aprobación, iteración o publicación para informar sobre el avance del programa y poder presentar argumentos para la financiación hasta la siguiente revisión de aprobación o publicación.
BAI01.06	Monitorizar, controlar e informar sobre los resultados del programa.	Monitorizar y controlar el programa (entrega de la solución) y el rendimiento de la empresa (valor/resultado) en comparación con el plan durante todo el ciclo de vida económica de la inversión. Informar sobre este rendimiento al Comité de Dirección del programa y a los patrocinadores.
BAI01.07	Establecer e iniciar proyectos dentro de un programa.	Definir y documentar la naturaleza y el alcance del proyecto para confirmar y desarrollar con las partes interesadas un entendimiento común del alcance del proyecto y cómo se relaciona con otros proyectos dentro del programa general de inversiones habilitadas para TI. La definición debe ser aprobada formalmente por los patrocinadores del programa y el proyecto.
BAI01.08	Planificar proyectos.	Establecer y mantener un plan de proyecto formal, integrado y aprobado (que cubra los recursos del negocio y de TI) para guiar la ejecución y el control del proyecto durante la vida útil del proyecto. El alcance de los proyectos debe definirse claramente y vincularse al desarrollo o mejora de las capacidades empresariales.
BAI01.09	Gestionar programas y proyectos de calidad.	Preparar y ejecutar un plan de gestión de la calidad, procesos y prácticas, alineadas con el sistema de gestión de calidad (QMS) que describe el programa y el enfoque de calidad hacia el proyecto y cómo se implementará. Todas las partes relevantes deben evaluar y aceptar formalmente el plan y después deben incorporarse al programa integrado y a los planes del proyecto.

Categoría del escenario de riesgo 2: Gestión del ciclo de vida del programa/proyecto *(cont.)*		
Habilitador del proceso *(cont.)*		
Referencia	**Título**	**Prácticas de gobierno y gestión**
BAI01.10	Gestionar el programa y el riesgo del proyecto.	Eliminar o minimizar el riesgo específico asociado con los programas y proyectos mediante un proceso sistemático de planificación, identificación, análisis, respuesta y monitorización y controlando las áreas o eventos que tienen el potencial de ocasionar un cambio no deseado. Establecer y registrar centralmente el riesgo al que se enfrenta el programa y el proyecto.
BAI01.11	Monitorizar y controlar proyectos.	Medir el rendimiento del proyecto en comparación con los criterios clave de rendimiento del proyecto, como el calendario, la calidad, el coste y el riesgo. Identificar las desviaciones de las expectativas. Evaluar el impacto de las desviaciones en el proyecto y en el programa general y reportar los resultados a las partes interesadas clave.
BAI01.12	Gestionar los recursos del proyecto y los paquetes de trabajo.	Gestionar los paquetes de trabajo del proyecto estableciendo requerimientos formales para autorizar y aceptar paquetes de trabajo, y asignando y coordinando los recursos del negocio y de TI apropiados.
BAI01.13	Cerrar un proyecto o iteración.	Al final de cada proyecto, liberación o iteración, requerir a las partes interesadas del proyecto que determinen si el proyecto, liberación o iteración han dado los resultados y el valor previstos. Identificar y comunicar las actividades pendientes necesarias para lograr los resultados del proyecto y los beneficios del programa previstos, e identificar y documentar las lecciones aprendidas para su uso en futuros proyectos, lanzamientos, iteraciones y programas.
Habilitador de estructuras organizacionales		
Referencia		**Contribución a la respuesta**
Oficina de gestión de proyectos y programas (PMO)		Asegurar la consistencia del enfoque dentro de la monitorización del programa/proyecto.
Director de Informática (CIO)		Tomar las acciones correctivas, si es necesario.
Patrocinador del programa/proyecto		Responsable general del seguimiento presupuestario y la demostración de valor.
Gerente del programa/proyecto		Responsable general del seguimiento presupuestario y demostración de valor.
Habilitador de cultura, ética y comportamiento		
Referencia		**Contribución a la respuesta**
La monitorización del programa/proyecto incluye actividades basadas en datos		Las decisiones deben ser objetivas, no sesgadas y basadas en información fundamentada.
La admisión de las malas noticias es apoyada por la alta gerencia		Permite una toma de decisiones más temprana y minimiza el impacto.
Habilitador de información		
Referencia		**Contribución a la respuesta**
Plan de realización de los beneficios del programa		Esta información proporcionará los datos necesarios para seguir el avance y estimar el rebasamiento presupuestario potencial.
Registro del presupuesto y los beneficios del programa		Esta información proporcionará los datos necesarios para seguir el avance y estimar el rebasamiento presupuestario potencial.
Reporte del estado del programa		La medición de la visibilidad y el estado real de los tomadores de decisiones deben basarse en un lenguaje y una metodología comunes.
Habilitador de servicios, infraestructura y aplicaciones		
Referencia		**Contribución a la respuesta**
Herramientas de gestión de cartera		Aumentar la transparencia de la situación presupuestaria.
Habilitador de personas, habilidades y competencias		
Referencia		**Contribución a la respuesta**
Habilidades de control de rendimiento y presupuesto		Las habilidades analíticas correctas permitirán estimar las consecuencias de proyectos fallidos, como los posibles rebasamientos presupuestarios.

Categoría del escenario de riesgo 3: Toma de decisiones sobre inversiones en TI		
Categoría del escenario de riesgo	Toma de decisiones sobre inversiones en TI	
Habilitador de principios, políticas y marco de trabajo		
Referencia	**Contribución a la respuesta**	
Política de gestión de programas/proyectos	La política debe definir quién necesita participar en las decisiones de inversión y la cadena de aprobación.	
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
APO05.06	Gestionar el logro de beneficios.	Monitorizar los beneficios de ofrecer y mantener servicios y capacidades de TI apropiados, con base en el caso de negocio acordado y actual.
APO06.02	Establecer prioridades para la asignación de recursos.	Implementar un proceso de toma de decisiones para establecer prioridades sobre la asignación de recursos y reglas para las inversiones discrecionales por unidades del negocio individuales. Incluir el posible uso de proveedores de servicios externos y considerar las opciones de compra, desarrollo y alquiler.
APO06.03	Crear y mantener presupuestos.	Preparar un presupuesto que refleje las prioridades de inversión y que apoye los objetivos estratégicos basados en la cartera de programas habilitados por TI y los servicios de TI.
APO07.01	Mantener una dotación de personal suficiente y adecuada.	Evaluar los requerimientos de personal de forma periódica o ante cambios mayores en los entornos empresariales, operativos o de TI para garantizar que la empresa cuente con suficientes recursos humanos para apoyar las metas y los objetivos empresariales. La dotación de personal incluye tanto los recursos internos como externos.
BAI01.03	Gestionar la participación de las partes interesadas.	Gestionar la participación de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna que llegue a todas las partes interesadas relevantes. Esto incluye planificar, identificar e involucrar a las partes interesadas y gestionar sus expectativas.
BAI03.04	Obtener los componentes de la solución.	Adquirir componentes de la solución basados en el plan de adquisiciones de acuerdo con los requerimientos y los diseños detallados, los principios y estándares de la arquitectura, y los procedimientos generales de adquisiciones y contratos de la empresa, requerimientos de aseguramiento de calidad (QA) y estándares de aprobación. Asegurarse de que el proveedor identifique y aborde todos los requerimientos legales y contractuales.
Habilitador de estructuras organizacionales		
Referencia	**Contribución a la respuesta**	
Consejo de Dirección	Responsable de la adecuada toma de decisiones sobre la inversión.	
Director de Informática (CIO)	Responsable de la adecuada toma de decisiones sobre la inversión.	
Director de Finanzas (CFO)	Responsable de la adecuada toma de decisiones sobre la inversión.	
Habilitador de cultura, ética y comportamiento		
Referencia	**Contribución a la respuesta**	
El proceso de toma de decisiones se basa en datos	Las decisiones deben ser objetivas, no sesgadas y basadas en información fundamentada.	
Habilitador de información		
Referencia	**Contribución a la respuesta**	
Casos de negocio	Aclarar el propósito, costo y retorno de la inversión de las iniciativas de TI.	
Priorización y clasificación de las iniciativas de TI	Visión general de las iniciativas de TI para facilitar la selección.	
Presupuesto y plan de TI	Información general sobre el presupuesto y las pautas de TI disponibles.	
Habilitador de personas, habilidades y competencias		
Referencia	**Contribución a la respuesta**	
Asignación de costes y presupuesto	Capacidad para detallar los aspectos financieros de las iniciativas de TI.	
Análisis del caso de negocio	Aclarar el propósito, coste y retorno de la inversión de las iniciativas de TI.	

Categoría del escenario de riesgo 4: Experiencia y habilidades en TI		
Categoría del escenario de riesgo	Experiencia y habilidades en TI	
Habilitador de principios, políticas y marco de trabajo		
Referencia		**Contribución a la respuesta**
Política de RR.HH.		Describe el desarrollo de requerimientos para la selección y evaluación de perfiles de TI a lo largo de toda la carrera.
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
APO01.01	Definir la estructura organizacional.	Establecer una estructura organizacional interna y extendida que refleje las necesidades del negocio y las prioridades de TI. Establecer las estructuras de gestión requeridas (p. ej., comités) que permitan que la toma de decisiones de gestión se lleve a cabo de la manera más eficaz y eficiente.
APO01.04	Comunicar los objetivos y la dirección de la gerencia.	Concienciar y comunicar, buscando la comprensión de los objetivos y la dirección de TI a las partes interesadas apropiadas y los usuarios en toda la empresa.
APO02.01	Comprender la dirección de la empresa.	Considerar el entorno empresarial actual, así como los procesos de negocio, la estrategia empresarial y los objetivos futuros. También considerar el entorno externo de la empresa (impulsores de la industria, regulaciones relevantes y bases de la competencia).
APO03.01	Desarrollar la visión de arquitectura empresarial.	La visión de la arquitectura ofrece una descripción de alto nivel de la línea de referencia y las arquitecturas objetivo, cubriendo los dominios empresariales, de información, de datos, de aplicación y de tecnología. La visión de la arquitectura ofrece al patrocinador una herramienta clave para promover los beneficios de las capacidades propuestas a las partes interesadas de la empresa. La visión de la arquitectura describe cómo la nueva capacidad cumplirá con las metas y los objetivos empresariales estratégicos, y abordará las preocupaciones de las partes interesadas cuando se implemente.
APO07.01	Mantener una dotación de personal suficiente y adecuada.	Evaluar los requerimientos de personal de forma periódica o ante cambios mayores en los entornos empresariales, operativos o de TI para garantizar que la empresa cuente con suficientes recursos humanos para apoyar las metas y los objetivos empresariales. La dotación de personal incluye tanto los recursos internos como externos.
APO07.02	Identificar al personal clave de TI.	Identificar al personal clave de TI mientras se minimiza la dependencia en una sola persona que realice una función de trabajo crítica a través de la captura de conocimientos (documentación), compartir los conocimientos, planificar la sucesión y tener un respaldo de personal.
APO07.03	Mantener las habilidades y las competencias del personal.	Definir y administrar las habilidades y las competencias del personal necesario. Verificar periódicamente que el personal cuente con las competencias necesarias para realizar sus funciones con base en su educación, capacitación y/o experiencia, y verificar que estas competencias se mantengan usando programas de cualificación y certificación cuando sea apropiado. Dar a los empleados oportunidades de aprendizaje continuas para mantener sus conocimientos, habilidades y competencias al nivel requerido para alcanzar las metas empresariales.
APO07.04	Evaluar el rendimiento laboral de los empleados.	Realizar evaluaciones de rendimiento oportunas de manera periódica de acuerdo con los objetivos individuales derivados de las metas empresariales, los estándares establecidos, las responsabilidades específicas del trabajo, y el marco de habilidades y competencias. Los empleados deben recibir asesoramiento sobre el rendimiento y la conducta cuando sea apropiado.
APO07.05	Planificar y seguir el uso de recursos de TI y humanos.	Comprender y seguir la demanda actual y futura de recursos humanos empresariales y de TI con responsabilidades para las TI empresariales. Identificar las carencias y proporcionar comentarios sobre los planes de adquisiciones, y los procesos de selección de personal y de TI.
Habilitador de estructuras organizacionales		
Referencia		**Contribución a la respuesta**
Director de Informática (CIO)		Responsable del análisis de brechas en las habilidades y competencias de TI.
Director de RR.HH.		Responsable de establecer las expectativas del personal.
Funciones gerenciales específicas de TI		Responsable de identificar los requerimientos específicos.
Habilitador de cultura, ética y comportamiento		
Referencia		**Contribución a la respuesta**
Conocimiento de las actividades empresariales por parte del personal de TI		El personal de TI debe conocer las actividades empresariales básicas de la empresa que apoyan.
Fomentar el desarrollo de competencias con el personal de TI		Desarrollo continuo de las habilidades de TI existentes.

Categoría del escenario de riesgo 4: Experiencia y habilidades en TI *(cont.)*	
Habilitador de información	
Referencia	**Contribución a la respuesta**
Matriz de habilidades y competencias	Describir las habilidades y competencias existentes dentro de la organización de TI y permitir el análisis de brechas.
Planes de desarrollo de competencias y profesionales/habilidades	Describir la evolución requerida de perfiles de TI específicos.
Descripciones genéricas de la función del trabajo	Describir los requerimientos de habilidades/experiencia y conocimientos para perfiles genéricos dentro de las organizaciones de TI.
Repositorios de conocimientos	Minimizar el efecto de la indisponibilidad parcial de recursos al compartir conocimientos sobre procesos, tecnología, etc.
Habilitador de personas, habilidades y competencias	
Referencia	**Contribución a la respuesta**
Habilidades de gestión de recursos humanos	Contratar personal calificado y gestionar el proceso de desarrollo de habilidades.
Análisis del negocio	Emparejar las necesidades del negocio con las habilidades de TI requeridas.

Categoría del escenario de riesgo 5: Operaciones del personal		
Categoría del escenario de riesgo	Operaciones del personal Alcance: Error humano e intención maliciosa	
Habilitador de principios, políticas y marco de trabajo		
Referencia	**Contribución a la respuesta**	
Política de RR.HH.	Describe las restricciones continuadas después de dejar de la organización.	
Política de seguridad de la información	Define las limitaciones técnicas de compartir y usar información.	
Política de ética	Reglas de conducta, uso aceptable de la tecnología y precauciones necesarias.	
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
APO07.01	Mantener una dotación de personal suficiente y adecuada.	Evaluar los requerimientos de personal de forma periódica o ante cambios mayores en los entornos empresariales, operativos o de TI para garantizar que la empresa cuente con suficientes recursos humanos para apoyar las metas y los objetivos empresariales. La dotación de personal incluye tanto los recursos internos como externos.
APO07.03	Mantener las habilidades y las competencias del personal.	Definir y administrar las habilidades y las competencias del personal necesario. Verificar periódicamente que el personal cuente con las competencias necesarias para realizar sus funciones con base en su educación, capacitación y/o experiencia, y verificar que estas competencias se mantengan usando programas de cualificación y certificación cuando sea apropiado. Dar a los empleados oportunidades de aprendizaje continuas para mantener sus conocimientos, habilidades y competencias al nivel requerido para alcanzar las metas empresariales.
APO07.06	Gestionar al personal por contrato.	Asegurarse que los consultores y el personal por contrato que dan soporte a la empresa con habilidades de TI conozcan y cumplan con las políticas de la organización y con los requerimientos contractuales acordados.
BAI03.07	Prepararse para las pruebas de la solución.	Establecer un plan de pruebas y los entornos requeridos para probar los componentes de la solución individuales e integrados, incluyendo los procesos de negocio, y los servicios, las aplicaciones y la infraestructura de soporte.
DSS01.01	Realizar procedimientos operativos.	Mantener y realizar procedimientos operativos y tareas operativas de forma confiable y consistente.
DSS01.04	Gestionar el ambiente.	Mantener medidas de protección contra los factores ambientales. Instalar equipo y dispositivos especializados para monitorizar y controlar el ambiente.
DSS01.05	Gestionar las instalaciones.	Gestionar las instalaciones, incluyendo el equipo de suministro eléctrico y comunicaciones, en línea con las leyes y regulaciones, los requerimientos técnicos y del negocio, las especificaciones del proveedor y las pautas de salud y seguridad.
DSS04.03	Desarrollar e implementar una respuesta de continuidad de negocio.	Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información en preparación para su uso en un incidente con el fin de permitir que la empresa continúe con sus actividades críticas.
DSS04.04	Ejercer, probar y revisar el BCP.	Probar los protocolos de continuidad de forma periódica para ejercer los planes de recuperación ante resultados predeterminados, para permitir que se desarrollen soluciones innovadoras y para ayudar a verificar a través del tiempo que el plan funcionará tal como se anticipa.
DSS05.05	Gestionar el acceso físico a los activos de TI.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a las instalaciones, edificios y áreas debe justificarse, autorizarse, registrarse y monitorizarse. Esto debe aplicarse a todas las personas que entren en las instalaciones, incluyendo personal, personal temporal, clientes, proveedores, visitantes y cualquier otra persona.
DSS06.02	Controlar el procesamiento de información.	Operar la ejecución de las actividades de los procesos de negocio y los controles relacionados, basándose en el riesgo empresarial, para garantizar que el procesamiento de información sea válido, completo, preciso, oportuno y seguro (p. ej., refleja el uso comercial legítimo y autorizado).
DSS06.03	Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Gestionar las funciones del negocio, responsabilidades, niveles de autoridad y segregación de funciones necesarias para apoyar los objetivos de proceso de negocio. Autorizar el acceso a cualquier activo de información relacionado con los procesos de información del negocio, incluyendo aquellos bajo custodia del negocio, TI y terceros. Esto asegura que la empresa sepa dónde están los datos y quién está manejando los datos en su nombre.
Habilitador de estructuras organizacionales		
Referencia	**Contribución a la respuesta**	
Gerente de seguridad de la información	Responsable de la protección técnica de los activos e información.	
Director de RR.HH.	Responsable de establecer las expectativas sobre el personal.	
Jefe de operaciones de TI	Responsable de gestionar el entorno operativo.	
Habilitador de cultura, ética y comportamiento		
Referencia	**Contribución a la respuesta**	
Todos son responsables de la protección de la información dentro de la empresa	Predicar con el ejemplo.	
La gente respeta la importancia de las políticas y los procedimientos	Prevenir errores y accidentes.	

Categoría del escenario de riesgo 5: Operaciones del personal *(cont.)*	
Habilitador de información	
Referencia	**Contribución a la respuesta**
Contrato de dotación de personal	Obligaciones contractuales, restricciones y derechos del personal.
Registros de acceso y eventos	Detectar la actividad indebida.
Funciones y responsabilidades/niveles de autoridad asignados	Brindar claridad sobre la distribución organizacional.
Habilitador de servicios, infraestructura y aplicaciones	
Referencia	**Contribución a la respuesta**
Control de acceso	Prevenir el acceso lógico no autorizado.
Sistema de seguridad de alarma y monitorización	Prevenir el acceso físico no autorizado.
Habilitador de personas, habilidades y competencias	
Referencia	**Contribución a la respuesta**
Habilidades de seguridad	Prevenir las intenciones maliciosas.

Categoría del escenario de riesgo 6: Información		
Categoría del escenario de riesgo	Información Alcance: Daños, fugas y acceso	
Habilitador de principios, políticas y marco de trabajo		
Referencia	**Contribución a la respuesta**	
Política de seguridad física	El acceso solo se debe proporcionar al personal autorizado.	
Política de copias de respaldo	Las copias de respaldo están disponibles y se pueden usar.	
Política de continuidad del negocio y de recuperación frente a desastres	Validar la recuperabilidad de los datos.	
Política de seguridad de la información	Define las limitaciones de compartir y usar información.	
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
APO01.06	Definir la propiedad de la información (datos) y del sistema.	Definir y mantener las responsabilidades de propiedad de información (datos) y sistemas de información. Asegurarse de que los propietarios tomen decisiones acerca de clasificar la información y los sistemas y protegerlos conforme a esta clasificación.
BAI02.01	Definir y mantener los requerimientos funcionales y técnicos del negocio.	Basándose en el caso de negocio, identificar, priorizar, especificar y acordar los requerimientos de información empresarial, funcionales, técnicos y de control que cubran el alcance/la comprensión de todas las iniciativas necesarias para lograr los resultados esperados de la solución empresarial habilitada por la TI propuesta.
BAI04.05	Investigar y abordar las cuestiones de disponibilidad, rendimiento y capacidad.	Abordar las desviaciones al investigar y resolver los problemas de disponibilidad, rendimiento y capacidad identificados.
DSS01.01	Realizar procedimientos operativos.	Mantener y realizar procedimientos operativos y tareas operativas de forma confiable y consistente.
DSS01.05	Gestionar las instalaciones.	Gestionar las instalaciones, incluyendo el equipo de suministro eléctrico y comunicaciones, en línea con las leyes y regulaciones, los requerimientos técnicos y del negocio, las especificaciones del proveedor y las pautas de salud y seguridad.
DSS04.03	Desarrollar e implementar una respuesta de continuidad de negocio.	Desarrollar un plan de continuidad del negocio (BCP) basado en la estrategia que documente los procedimientos y elementos de información que permitan a la empresa continuar sus actividades críticas después de un incidente.
DSS04.04	Ejercer, probar y revisar el BCP.	Probar los protocolos de continuidad de forma periódica para ejercer los planes de recuperación ante resultados predeterminados, para permitir que se desarrollen soluciones innovadoras y para ayudar a verificar en el tiempo que el plan funcionará tal como se anticipa.
DSS05.02	Gestionar la seguridad de la red y las conexiones.	Usar medidas de seguridad y procedimientos de gestión relacionados para proteger la información a través de todos los métodos de conectividad.
DSS05.05	Gestionar el acceso físico a los activos de TI.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a las instalaciones, edificios y áreas debe justificarse, autorizarse, registrarse y monitorizarse. Esto debe aplicarse a todas las personas que entren en las instalaciones, incluyendo personal, personal temporal, clientes, proveedores, visitantes y cualquier otra persona.
DSS05.06	Gestionar documentos sensibles y dispositivos de salida.	Establecer protecciones físicas apropiadas, prácticas de contabilización y gestión de inventario para activos de TI sensibles, como formularios especiales, instrumentos negociables, impresoras para fines especiales o tokens de seguridad.
DSS06.04	Gestionar errores y excepciones.	Gestionar las excepciones y los errores del proceso de negocio y facilitar su corrección. Incluir el escalado de los errores del proceso de negocio, las excepciones y la ejecución de las acciones correctivas definidas. Esto ofrece una garantía de la precisión e integridad de los procesos de información del negocio.
DSS06.05	Asegurar la trazabilidad de los eventos de información y la responsabilidad.	Asegurarse que la información del negocio pueda rastrearse hasta el evento del negocio que la originó y a las partes responsables. Esto permite la trazabilidad de la información durante su ciclo de vida y los procesos relacionados. Esto ofrece la seguridad de que la información que impulsa al negocio es confiable y que se ha procesado de acuerdo con objetivos definidos.
Habilitador de estructuras organizacionales		
Referencia		**Contribución a la respuesta**
Gerente de seguridad de la información		Proporcionar asesoría sobre los controles y medidas apropiados para proteger los datos y el hardware.
Jefe de operaciones de TI		Responsable de implementar controles apropiados para proteger los datos y el hardware.

Categoría del escenario de riesgo 6: Información *(cont.)*	
Habilitador de cultura, ética y comportamiento	
Referencia	**Contribución a la respuesta**
La seguridad de la información se practica en las operaciones diarias	Siempre seleccionar la opción más segura respecto a las operaciones diarias.
Solo con la necesidad de acceso	Limitar el acceso del personal sin afectar al rendimiento.
Todos son responsables de la protección de la información dentro de la empresa	La gerencia ofrece capacitación para crear concientización y responsabilidad.
Habilitador de información	
Referencia	**Contribución a la respuesta**
Informes de copia de seguridad	Describe el estado sobre las copias de respaldo.
Campañas de prevención de pérdida de datos	Aumentar la concientización dentro de la empresa.
Acuerdos de no divulgación	Proteger contractualmente la propiedad intelectual (IP), al disuadir al personal divulgar propiedad intelectual a personal no autorizado.
Registros de acceso y eventos	Detectar la actividad sospechosa.
Habilitador de servicios, infraestructura y aplicaciones	
Referencia	**Contribución a la respuesta**
Control de acceso	Prevenir el acceso lógico no autorizado.
Sistemas de copia de seguridad	Garantizar la correcta recuperación en caso de pérdida, modificación o corrupción de los datos.
Infraestructura y aplicaciones de protección de datos	Cifrado, contraseñas, monitorización del correo electrónico, etc., para aplicar el principio de necesidad de saber.
Habilitador de personas, habilidades y competencias	
Referencia	**Contribución a la respuesta**
Habilidades técnicas	Implementar controles y medidas apropiados para proteger los datos y el hardware (p. ej., copia de seguridad de datos, almacenamiento).

Categoría del escenario de riesgo 7: Arquitectura		
Categoría del escenario de riesgo	Arquitectura Alcance: Visión y diseño arquitectónicos	
Habilitador de principios, políticas y marco de trabajo		
Referencia	**Contribución a la respuesta**	
Principios de arquitectura	Los principios de arquitectura definen las reglas y pautas generales subyacentes para el uso y desarrollo de todos los recursos y activos de TI en toda la empresa.	
Procedimiento de excepciones	En casos específicos, se pueden permitir excepciones a las reglas de arquitectura existentes. Se deben describir los casos específicos y el procedimiento a seguir para su aprobación.	
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
APO02.01	Comprender la dirección de la empresa.	Considerar el entorno empresarial actual, así como los procesos de negocio, la estrategia empresarial y los objetivos futuros. También considerar el entorno externo de la empresa (impulsores de la industria, regulaciones relevantes y bases de la competencia).
APO02.03	Definir las capacidades objetivo de TI.	Definir las capacidades objetivo del negocio y de TI, así como los servicios de TI requeridos. Esto debe basarse en el entendimiento del entorno y los requerimientos de la empresa; la evaluación de los procesos comerciales actuales y el entorno y los problemas de TI; y considerando los estándares de referencia, las mejores prácticas y las tecnologías emergentes validadas o las propuestas de innovación.
APO03.01	Desarrollar la visión de arquitectura empresarial.	La visión de la arquitectura ofrece una descripción de alto nivel de la línea de referencia y las arquitecturas objetivo, cubriendo los dominios empresariales, de información, de datos, de aplicación y de tecnología. La visión de la arquitectura ofrece al patrocinador una herramienta clave para promover los beneficios de las capacidades propuestas a las partes interesadas de la empresa. La visión de la arquitectura describe cómo la nueva capacidad cumplirá con las metas y los objetivos empresariales estratégicos, y abordará las preocupaciones de las partes interesadas cuando se implemente.
APO03.02	Definir la arquitectura de referencia.	La arquitectura de referencia describe las arquitecturas actuales y objetivo para los dominios de negocio, información, datos, aplicación y tecnología.
APO03.03	Seleccionar oportunidades y soluciones.	Racionalizar las brechas entre las arquitecturas de referencia y objetivo, tomando tanto las perspectivas de negocio como técnicas, y agruparlas lógicamente en paquetes de trabajo del proyecto. Integrar el proyecto con todos los programas de inversión habilitados por TI relacionados para asegurarse de que las iniciativas arquitectónicas estén alineadas con, y habilitar estas iniciativas como parte de, un cambio empresarial general. Hacer de este un esfuerzo colaborativo con las partes interesadas clave del negocio y de TI para evaluar la disposición de transformación de la empresa, e identificar oportunidades, soluciones y todas las restricciones de implementación.
APO03.04	Definir la implementación de la arquitectura.	Crear una aplicación viable y plan de migración en alineación con las carteras de programas y proyectos. Asegurarse de que el plan esté estrechamente coordinado para garantizar que se brinde valor y los recursos necesarios estén disponibles para completar el trabajo necesario.
APO03.05	Proporcionar servicios de arquitectura empresarial.	La prestación de servicios de arquitectura empresarial dentro de la empresa incluye orientación y monitorización de proyectos de implementación, formalización de formas de trabajar a través de contratos de arquitectura y medición y comunicación de la creación de valor agregado y monitorización del cumplimiento.
APO04.03	Monitorizar y escanear el entorno tecnológico.	Monitorizar y escanear sistemáticamente el entorno externo de la empresa para identificar las tecnologías emergentes con el potencial de crear valor (p. ej., ejecutar la estrategia empresarial, optimizar costes, evitar la obsolescencia y habilitar de mejor manera los procesos empresariales y de TI). Monitorizar el mercado, el entorno competitivo, los sectores de la industria y las tendencias legales y regulatorias para poder analizar las tecnologías emergentes o las ideas de innovación en el contexto empresarial.
APO04.04	Evaluar el potencial de las tecnologías emergentes y las ideas de innovación.	Analizar las tecnologías emergentes identificadas y/u otras sugerencias de innovación en TI. Trabajar con las partes interesadas para validar las suposiciones sobre el potencial de nuevas tecnologías e innovación.
APO04.06	Monitorizar la implementación y el uso de la innovación.	Monitorizar la implementación y el uso de las tecnologías emergentes y las innovaciones durante la integración, adopción y todo el ciclo de vida económica para garantizar que se obtengan los beneficios prometidos y para identificar las lecciones aprendidas.
Habilitador de estructuras organizacionales		
Referencia	**Contribución a la respuesta**	
Consejo de arquitectura	Garantizar el cumplimiento con la arquitectura objetivo y permitir excepciones solo cuando sean necesarias.	
Habilitador de cultura, ética y comportamiento		
Referencia	**Contribución a la respuesta**	
Respetar los estándares acordados	La empresa debe estimular el uso de estándares acordados.	
Habilitador de información		
Referencia	**Contribución a la respuesta**	
Modelo de arquitectura	Modelo de arquitectura objetivo.	

Categoría del escenario de riesgo 7: Arquitectura *(cont.)*	
Habilitador de servicios, infraestructura y aplicaciones	
Referencia	**Contribución a la respuesta**
Software de modelado de arquitectura	La aplicación de modelado optimizará el desarrollo de la arquitectura y minimizará el esfuerzo de analizar el impacto a la arquitectura en caso de excepciones o cambios.
Habilitador de personas, habilidades y competencias	
Referencia	**Contribución a la respuesta**
Liderazgo y comunicación	Aclarar los motivos de la arquitectura y las consecuencias potenciales.
Habilidades de arquitectura	Desarrollar una arquitectura eficiente y eficaz alineada con los requerimientos del negocio.

Categoría del escenario de riesgo 8: Infraestructura		
Categoría del escenario de riesgo		Infraestructura Alcance: Hardware, sistema operativo y tecnología de control; selección/implementación, operaciones y desmantelamiento
Habilitador de principios, políticas y marco de trabajo		
Referencia		**Contribución a la respuesta**
Principios de arquitectura		Definir las reglas y pautas generales subyacentes para el uso y desarrollo de todos los recursos y activos de TI en toda la empresa.
Política de gestión de cambios		Definir las reglas y pautas para cambiar los componentes de la infraestructura de una manera controlada y segura.
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
APO02.03	Definir las capacidades objetivo de TI.	Definir las capacidades objetivo del negocio y de TI, así como los servicios de TI requeridos. Esto debe basarse en el entendimiento del entorno y los requerimientos de la empresa; la evaluación de los procesos comerciales actuales y el entorno y los problemas de TI; y considerando los estándares de referencia, las mejores prácticas y las tecnologías emergentes validadas o las propuestas de innovación.
APO04.03	Monitorizar y escanear el entorno tecnológico.	Monitorizar y escanear sistemáticamente el entorno externo de la empresa para identificar las tecnologías emergentes con el potencial de crear valor (p. ej., ejecutar la estrategia empresarial, optimizar costos, evitar la obsolescencia y habilitar de mejor manera los procesos empresariales y de TI). Monitorizar el mercado, el entorno competitivo, los sectores de la industria y las tendencias legales y regulatorias para poder analizar las tecnologías emergentes o las ideas de innovación en el contexto empresarial.
BAI03.03	Desarrollar los componentes de la solución.	Desarrollar progresivamente los componentes de la solución de acuerdo con los diseños detallados siguiendo métodos de desarrollo y estándares de documentación, requerimientos de aseguramiento de calidad (QA) y estándares de aprobación. Asegurarse que se aborden todos los requerimientos de control en los procesos de negocio, apoyando las aplicaciones de TI y los servicios de infraestructura, los servicios y productos de tecnología, y los socios/proveedores.
BAI04.01	Evaluar la disponibilidad, el rendimiento y la capacidad actuales, y crear una línea de referencia.	Evaluar la disponibilidad, el rendimiento y la capacidad de servicios y recursos para asegurarse de que exista una capacidad y rendimiento con un costo justificable disponibles para dar apoyo a las necesidades del negocio y que cumplan con los acuerdos de nivel de servicio (SLA). Crear líneas de referencia de disponibilidad, rendimiento y capacidad para la comparación en el futuro.
BAI04.02	Evaluar el impacto en el negocio.	Identificar servicios importantes para la empresa, asignar servicios y recursos a los procesos de negocio, e identificar dependencias comerciales. Asegurarse de que el impacto de los recursos no disponibles sea totalmente comprendido y aceptado por el propietario del negocio. Asegurarse de que, para funciones del negocio críticas, se puedan satisfacer los requisitos de disponibilidad de los SLA.
BAI04.03	Planificar los requerimientos de los servicios nuevos o modificados.	Planificar y priorizar las implicaciones de disponibilidad, rendimiento y capacidad de las necesidades cambiantes del negocio y los requisitos de servicio.
BAI04.04	Monitorizar y revisar la disponibilidad y capacidad.	Monitorizar, medir, analizar, reportar y revisar la disponibilidad, rendimiento y capacidad. Identificar desviaciones de las líneas de referencia establecidas. Revisar los reportes de análisis de tendencias que identifican problemas y variaciones significativos, iniciando acciones cuando sea necesario, y asegurándose que se le dé seguimiento a todos los problemas pendientes.
BAI04.05	Investigar y abordar las cuestiones de disponibilidad, rendimiento y capacidad.	Abordar las desviaciones al investigar y resolver los problemas de disponibilidad, rendimiento y capacidad identificados.
BAI10.04	Generar informes del estado y la configuración.	Definir y generar informes de configuración sobre los cambios de estado de los elementos de configuración.
BAI10.05	Verificar y revisar la integridad del repositorio de configuración.	Revisar periódicamente el repositorio de configuración y verificar su integridad y precisión en comparación con la meta deseada.
DSS05.05	Gestionar el acceso físico a los activos de TI.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a las instalaciones, edificios y áreas debe justificarse, autorizarse, registrarse y monitorizarse. Esto debe aplicarse a todas las personas que entren en las instalaciones, incluyendo personal, personal temporal, clientes, proveedores, visitantes y cualquier otra persona.
Habilitador de estructuras organizacionales		
Referencia		**Contribución a la respuesta**
Jefe de operaciones de TI		Responsable de la gestión y mantenimiento correctos de la infraestructura de TI.
Jefe de arquitectura		Diseñar la arquitectura de una manera óptima.
Habilitador de cultura, ética y comportamiento		
Referencia		**Contribución a la respuesta**
Respetar los activos disponibles		A todo el personal se le requiere mantener los activos de una manera apropiada.

Categoría del escenario de riesgo 8: Infraestructura *(cont.)*	
Habilitador de información	
Referencia	**Contribución a la respuesta**
Modelo de arquitectura	Modelo de arquitectura objetivo.
(Actualizaciones del) inventario de activos	Rastrear todos los activos a lo largo de la empresa.
Plan de mantenimiento	Planificar el mantenimiento de la infraestructura de TI.
Informes de estado de la configuración	Rastrear los cambios a la configuración.
Habilitador de servicios, infraestructura y aplicaciones	
Referencia	**Contribución a la respuesta**
Base de datos de gestión de configuración (CMDB)	Ayudar a identificar las áreas de mejora.
Habilitador de personas, habilidades y competencias	
Referencia	**Contribución a la respuesta**
Habilidades de arquitectura	Desarrollar una arquitectura eficiente y eficaz alineada con los requerimientos del negocio.
Habilidades técnicas	Gestionar los diferentes componentes de la infraestructura.

Categoría del escenario de riesgo 9: Software		
Categoría del escenario de riesgo	Software Alcance: Selección/implementación, operaciones y desmantelamiento	
Habilitador de principios, políticas y marco de trabajo		
Referencia	**Contribución a la respuesta**	
Política de gestión de cambios	Definir las reglas y pautas para cambiar los componentes de la infraestructura de una manera controlada y segura.	
Procedimiento de respaldo	Pautas en caso de que la restauración sea necesaria.	
Principios de arquitectura	Los principios de arquitectura definen las reglas y pautas generales subyacentes para el uso y desarrollo de todos los recursos y activos de TI en toda la empresa.	
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
BAI03.01	Diseño de soluciones de alto nivel.	Desarrollar y documentar diseños de alto nivel usando técnicas acordadas de desarrollo con las etapas apropiadas o ágiles y rápidas. Asegurar la alineación con la estrategia de TI y la arquitectura empresarial. Volver a evaluar y actualizar los diseños cuando se presenten problemas significativos durante las fases de diseño detallado o construcción o conforme evolucione la solución. Asegurarse de que las partes interesadas participen activamente en el diseño y la aprobación de cada versión.
BAI03.02	Diseñar componentes detallados para la solución.	Desarrollar, documentar y elaborar diseños detallados progresivamente usando técnicas acordadas de desarrollo ágiles y rápidas, o con las fases apropiadas, abordando todos los componentes (procesos de negocio y controles automatizados y manuales relacionados, apoyando las aplicaciones de TI, los servicios de infraestructura y los productos de tecnología, así como a los socios/proveedores). Asegurarse de que el diseño detallado incluya acuerdos de nivel de servicio (SLA) internos y externos, así como acuerdos de nivel operativo (OLA).
BAI03.03	Desarrollar los componentes de la solución.	Desarrollar progresivamente los componentes de la solución de acuerdo con los diseños detallados siguiendo métodos de desarrollo y estándares de documentación, requerimientos de aseguramiento de calidad (QA) y estándares de aprobación. Asegurarse que se aborden todos los requerimientos de control en los procesos de negocio, apoyando las aplicaciones de TI y los servicios de infraestructura, los servicios y productos de tecnología, y los socios/proveedores.
BAI03.05	Desarrollar soluciones.	Instalar y configurar las soluciones e integrarlas con las actividades del proceso empresarial. Implementar medidas de control, seguridad y auditabilidad durante la configuración y durante la integración del hardware y el software de infraestructura, para proteger los recursos y asegurar la disponibilidad y la integridad de los datos. Actualizar el catálogo de servicios para reflejar las soluciones nuevas.
BAI03.06	Realizar el aseguramiento de calidad (QA).	Desarrollar, aprovisionar y ejecutar un plan de aseguramiento de calidad (QA) alineado con el sistema de gestión de calidad (QMS) para obtener la calidad especificada en la definición de los requerimientos y las políticas y procedimientos de calidad de la empresa.
BAI03.07	Prepararse para las pruebas de la solución.	Establecer un plan de pruebas y los entornos requeridos para probar los componentes de la solución individuales e integrados, incluyendo los procesos de negocio, y los servicios, las aplicaciones y la infraestructura de soporte.
BAI03.08	Ejecutar las pruebas de la solución.	Ejecutar pruebas continuamente durante el desarrollo, incluyendo pruebas de control, de acuerdo con el plan de pruebas definido y las prácticas de desarrollo en el entorno apropiado. Incluir a los propietarios de los procesos de negocio y a los usuarios finales en el equipo de pruebas. Identificar, registrar y priorizar los errores y los problemas que se identificaron durante las pruebas.
BAI03.09	Gestionar los cambios de los requerimientos.	Rastrear el estado de requerimientos individuales (incluyendo todos los requerimientos rechazados) durante el ciclo de vida del proyecto, y gestionar la aprobación de cambios de los requerimientos.
BAI03.10	Mantener soluciones.	Desarrollar y ejecutar un plan para el mantenimiento de los componentes de la solución y la infraestructura. Incluir revisiones periódicas en comparación con las necesidades del negocio y los requerimientos operativos.
BAI05.05	Habilitar las operaciones y el uso.	Planificar e implementar todos los aspectos técnicos, operativos y de uso, de forma que todas las personas involucradas en el futuro estado del entorno puedan ejercer sus responsabilidades.
BAI06.01	Evaluar, priorizar y autorizar solicitudes de cambio.	Evaluar todas las solicitudes de cambio para determinar el impacto en los procesos de negocio y servicios de TI; y evaluar si el cambio afectará negativamente al entorno operativo y presentará riesgos inaceptables. Asegurarse de que los cambios se registren, categoricen, evalúen, autoricen, prioricen, planifiquen y programen.
BAI06.02	Gestionar cambios de emergencia.	Gestionar cuidadosamente los cambios de emergencia para minimizar futuros incidentes y asegurarse de que el cambio esté controlado y se realice de forma segura. Verificar que los cambios de emergencia sean evaluados adecuadamente y autorizados después del cambio.
BAI06.03	Rastrear y reportar el estado de los cambios.	Mantener un sistema de rastreo e informes para documentar los cambios rechazados, comunicar el estado de los cambios aprobados y en proceso y los cambios finalizados. Asegurarse que los cambios aprobados se implementen según lo previsto.
BAI06.04	Cerrar y documentar los cambios.	Siempre que se implementen cambios, actualizar acordemente la documentación de la solución y del usuario, así como los procedimientos afectados por el cambio.
BAI07.01	Establecer un plan de implementación.	Establecer un plan de implementación que cubra la conversión de sistemas y datos, los criterios de pruebas de aceptación, la comunicación, la capacitación, la preparación de lanzamientos, la promoción a producción, el apoyo a la producción temprana, un plan de respaldo/abandono y una revisión postimplementación. Obtener la aprobación de las partes relevantes.
BAI07.03	Pruebas de aceptación del plan.	Establecer un plan de pruebas basado en estándares de toda la empresa que definen roles, responsabilidades y criterios de entrada y salida. Asegurarse de que el plan sea aprobado por las partes relevantes.

Categoría del escenario de riesgo 9: Software *(cont.)*		
Habilitador del proceso *(cont.)*		
Referencia	**Título**	**Prácticas de gobierno y gestión**
BAI07.05	Realizar pruebas de aceptación.	Probar los cambios de forma independiente de acuerdo con el plan de prueba definido antes de la migración al entorno operativo en producción.
BAI07.08	Realizar una revisión post-implementación.	Realizar una revisión post-implementación para confirmar los resultados, identificar las lecciones aprendidas y desarrollar un plan de acción. Evaluar y verificar el rendimiento y los resultados reales del servicio nuevo o cambiado, en comparación con el rendimiento y los resultados previstos (el servicio esperado por el usuario o el cliente).
BAI08.01	Fomentar y facilitar una cultura de intercambio de conocimientos.	Implementar procesos y herramientas que faciliten una cultura de intercambio de conocimientos.
BAI08.04	Utilizar y compartir conocimientos.	Transmitir los recursos de conocimiento disponibles a las partes interesadas relevantes y comunicar cómo estos recursos pueden utilizarse para abordar diferentes necesidades (p. ej., resolución de problemas, aprendizaje, planificación estratégica y toma de decisiones).
BAI10.04	Generar informes del estado y la configuración.	Definir y generar informes de configuración sobre los cambios de estado de los elementos de configuración.
BAI10.05	Verificar y revisar la integridad del repositorio de configuración.	Revisar periódicamente el repositorio de configuración y verificar su integridad y precisión en comparación con la meta deseada.
Habilitador de estructuras organizacionales		
Referencia		**Contribución a la respuesta**
Jefe de desarrollo de software		Responsable del diseño y desarrollo adecuados de los componentes de software.
Jefe de arquitectura		Diseñar la arquitectura de una manera óptima.
Habilitador de cultura, ética y comportamiento		
Referencia		**Contribución a la respuesta**
Las pruebas se realizan en todos los niveles apropiados		Los usuarios y desarrolladores cooperan para probar los componentes del software.
Habilitador de información		
Referencia		**Contribución a la respuesta**
Modelo de arquitectura		Modelo de arquitectura objetivo.
Especificaciones de diseño		Aclarar las necesidades de los usuarios.
Plan de aseguramiento de la calidad (QA) (plan de prueba y procedimientos)		Definir los pasos a seguir para garantizar la calidad.
Plan de mantenimiento		Planificar el mantenimiento del software.
Habilitador de servicios, infraestructura y aplicaciones		
Referencia		**Contribución a la respuesta**
Ambiente de desarrollo integrado (IDE)		Facilitar el desarrollo que consiste de un editor de código fuente, herramientas de automatización de desarrollo y un depurador.
Repositorios de conocimientos		Compartir y coordinar conocimientos sobre las actividades de desarrollo.
Habilitador de personas, habilidades y competencias		
Referencia		**Contribución a la respuesta**
Habilidades de arquitectura		Desarrollar una arquitectura eficiente y eficaz alineada con los requerimientos del negocio.
Habilidades técnicas		Diseñar y desarrollar los componentes de software adecuados.

Categoría del escenario de riesgo 10: Propiedad empresarial de TI		
Categoría del escenario de riesgo	Responsabilidad del negocio sobre TI	
Habilitador de principios, políticas y marco de trabajo		
Referencia		**Contribución a la respuesta**
Principios rectores del gobierno empresarial		Involucrar al negocio y al área de TI.
Principios de reportes y comunicación		Aclarar los medios de comunicación.
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
EDM01.01	Evaluar el sistema de gobierno.	Identificar e involucrarse continuamente con las partes interesadas de la empresa, documentar una comprensión de los requisitos y hacer un juicio sobre el diseño actual y futuro del gobierno de TI empresarial.
EDM01.02	Orientar el sistema de gobierno.	Informar a los líderes y obtener su apoyo, aprobación y compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de TI en línea con los principios de diseño de gobierno acordados, los modelos de toma de decisiones y los niveles de autoridad. Definir la información requerida para la toma de decisiones adecuadas.
EDM01.03	Monitorizar el sistema de gobierno.	Monitorizar la efectividad y el desempeño del gobierno de TI de la empresa. Evaluar si el sistema de gobierno y los mecanismos implementados (incluyendo las estructuras, los principios y los procesos) están operando de forma efectiva y ofrecen una supervisión apropiada de TI.
APO01.04	Comunicar los objetivos y la dirección de la gerencia.	Concienciar y comunicar, buscando la comprensión de los objetivos y la dirección de TI a las partes interesadas en toda la empresa.
APO02.01	Comprender la dirección de la empresa.	Considerar el entorno empresarial actual, así como los procesos de negocio, la estrategia empresarial y los objetivos futuros. También considerar el entorno externo de la empresa (impulsores de la industria, regulaciones relevantes y bases de la competencia).
APO05.06	Gestionar la consecución de objetivos.	Monitorizar los beneficios de ofrecer y mantener servicios y capacidades de TI apropiados, con base en el caso de negocio acordado y actual.
APO09.03	Definir y preparar acuerdos de servicio.	Definir y preparar acuerdos de nivel de servicio (SLAs) basados en las opciones en los catálogos de servicio. Incluir acuerdos de nivel operacional (OLAs) internos.
APO09.04	Monitorizar y reportar los niveles de servicio.	Monitorizar los niveles de servicio, identificar tendencias y proporcionar reportes que la gerencia pueda utilizar para tomar decisiones y gestionar los requisitos de rendimiento futuros.
BAI01.03	Gestionar la participación de las partes interesadas.	Gestionar la participación de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna que llegue a todas las partes interesadas relevantes. Esto incluye planificar, identificar e involucrar a las partes interesadas y gestionar sus expectativas.
BAI02.01	Definir y mantener los requerimientos funcionales y técnicos del negocio.	Basándose en el caso de negocio, identificar, priorizar, especificar y acordar los requerimientos de información empresarial, funcionales, técnicos y de control que cubran el alcance/la comprensión de todas las iniciativas necesarias para lograr los resultados esperados de la solución TI propuesta.
Habilitador de estructuras organizacionales		
Referencia		**Contribución a la respuesta**
Oficina de gestión de proyectos y programas (PMO)		Proporcionar una metodología común, utilizada por el negocio y por el área de TI, para definir los requerimientos apropiados.
Finanzas		Proporcionar una metodología común, utilizada por el negocio y por el área de TI, para evaluar las oportunidades en términos de valor para la empresa.
Comité de estrategia (ejecutivo de TI)		Estructura clave que debe asumir la responsabilidad sobre la cooperación entre el área de TI y el negocio.
Consejo de Dirección		Responsable del establecimiento y mantenimiento del marco de gobierno.
Habilitador de cultura, ética y comportamiento		
Referencia		**Contribución a la respuesta**
El negocio y el área de TI trabajan juntos como socios		El negocio toma en cuenta las dificultades a las que se enfrenta el área de TI, y ésta entiende los problemas del negocio para encontrar soluciones comunes.
Habilitador de información		
Referencia		**Contribución a la respuesta**
Estrategia de TI		Alinear los planes del área de TI con los objetivos del negocio para lograr una monitorización más eficiente del negocio sobre las TI.
Niveles de autoridad		Aclarar las responsabilidades de toma de decisiones.
Acuerdos de nivel de servicio (SLA)		Describir los objetivos de nivel de servicio para satisfacer las expectativas del negocio.

Categoría del escenario de riesgo 10: Propiedad empresarial de TI *(cont.)*	
Habilitador de personas, habilidades y competencias	
Referencia	**Contribución a la respuesta**
Habilidades de gestión de relaciones	Los empleados de TI deberían tener las habilidades adecuadas para desarrollar relaciones con las partes interesadas relevantes del negocio.
Habilidades/afinidades relacionadas con TI	Los empleados de negocios deberían ser capacitados para tener una afinidad mínima con TI.

Categoría del escenario de riesgo 11: Proveedores		
Categoría del escenario de riesgo		Proveedores Alcance: Selección,rendimiento, cumplimiento contractual, terminación de servicio y transferencia
Habilitador de principios, políticas y marco de trabajo		
Referencia		**Contribución a la respuesta**
Política de Compras		Proporcionar un enfoque formal para seleccionar proveedores, incluyendo los criterios de aceptación por parte del negocio.
Principios de arquitectura		Los principios de arquitectura definen las reglas y pautas generales subyacentes para el uso y desarrollo de todos los recursos y activos de TI en toda la empresa.
Política de seguridad de la información		Define las limitaciones técnicas de compartir y usar información.
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
APO10.02	Seleccionar proveedores.	Seleccionar proveedores de acuerdo a una práctica justa y formal para garantizar un ajuste viable basado en los requerimientos especificados. Los requerimientos deberían optimizarse con la participación de los proveedores potenciales y las partes interesadas de la empresa.
APO10.03	Gestionar los contratos y las relaciones con los proveedores.	Formalizar y gestionar la relación con el proveedor para los proveedores estratégicos. Gestionar, mantener y supervisar los contratos y la prestación de servicios. Asegurarse de que los contratos nuevos o modificados cumplan con los estándares de la empresa y con los requerimientos legales y regulatorios.
APO10.04	Gestionar el riesgo con los proveedores.	Identificar y gestionar el riesgo con los proveedores, incluyendo la capacidad de proporcionar continuamente una prestación de servicios segura, eficiente y eficaz.
APO10.05	Monitorizar el rendimiento y el cumplimiento del proveedor.	Revisar periódicamente el rendimiento general de los proveedores, el cumplimiento con los requerimientos contractuales, la entrega de valor y abordar oportunamente los problemas identificados.
Habilitador de estructuras organizacionales		
Referencia		**Contribución a la respuesta**
Grupo legal		Revisar los términos de negocio propuestos.
Propietarios del proceso de negocio		Establecer los requerimientos y los indicadores de rendimiento, y garantizar que las expectativas adecuadas se incorporen a los contratos.
Departamento de Compras		Proporcionar el apoyo y el enfoque para interactuar eficientemente con los proveedores.
Director de Informática (CIO)		Responsable de la gestión de proveedores.
Habilitador de cultura, ética y comportamiento		
Referencia		**Contribución a la respuesta**
Respetar los procedimientos de compra		Se requiere un esfuerzo adicional para garantizar la selección apropiada de los proveedores.
Enfoque en la cultura transparente y participativa		Optimizar el resultado de la relación con el proveedor.
Habilitador de información		
Referencia		**Contribución a la respuesta**
Requerimientos del negocio		Se utiliza para las negociaciones y la definición del nivel de servicio.
Estrategia de TI		Definir los límites y los objetivos empresariales a tener en cuenta al negociar los contratos.
Catálogo de proveedores		Una presentación estructurada de proveedores conocidos, incluyendo estadísticas de rendimiento previo.
Acuerdos de nivel de servicio (SLA)		Monitorizar los niveles de servicio, identificar tendencias y proporcionar reportes que la gerencia pueda utilizar para tomar decisiones y gestionar los futuros requisitos de rendimiento.
Habilitador de servicios, infraestructura y aplicaciones		
Referencia		**Contribución a la respuesta**
Sistema de gestión de proveedores		Mantener un seguimiento del ciclo de vida de la gestión de proveedores.
Habilitador de personas, habilidades y competencias		
Referencia		**Contribución a la respuesta**
Habilidades de negociación		Asegurarse que se satisfacen los requerimientos.
Habilidades de litigio		Una vez iniciada la acción penal, se requieren las habilidades adecuadas para minimizar el impacto legal sobre la empresa.
Habilidades de análisis legal		Apoyar la cooperación con el proveedor durante la redacción de contratos y SLAs.

Categoría del escenario de riesgo 12: Cumplimiento regulatorio		
Categoría del escenario de riesgo	Cumplimiento regulatorio	
Habilitador de principios, políticas y marco de trabajo		
Referencia	**Contribución a la respuesta**	
Políticas específicas de la industria/el mercado	Definir las reglas y pautas para identificar los requerimientos de cumplimiento específicos y los procedimientos para cumplir con los requerimientos aplicables.	
Política de cumplimiento	Guiar la identificación de los requerimientos de cumplimiento externos y los procedimientos para cumplir con los requerimientos aplicados.	
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
MEA03.01	Identificar los requerimientos de cumplimiento externos.	Identificar y monitorizar de forma continua los cambios en las leyes y regulaciones locales e internacionales, así como otros requerimientos externos aplicables a la empresa.
MEA03.02	Optimizar la respuesta a los requerimientos externos.	Revisar y ajustar los principios, las políticas, los estándares, los procedimientos y las metodologías para asegurarse que se aborden y comuniquen los requerimientos legales, regulatorios y contractuales. Considerar los estándares de la industria, códigos de buenas prácticas y pautas de mejores prácticas para la adopción y adaptación de planes existentes.
MEA03.03	Confirmar el cumplimiento externo.	Confirmar los planes de cumplimiento con los requerimientos legales, regulatorios y contractuales.
Habilitador de estructuras organizacionales		
Referencia	**Contribución a la respuesta**	
Oficial de privacidad	Identificar los requerimientos de privacidad y garantizar el cumplimiento.	
Departamento de cumplimiento regulatorio	Proporcionar orientación sobre cumplimiento legal, regulatorio y contractual. Dar seguimiento a las regulaciones nuevas y cambiantes.	
Grupo legal	Apoyo legal durante el análisis y litigio relacionados con el cumplimiento regulatorio.	
Habilitador de cultura, ética y comportamiento		
Referencia	**Contribución a la respuesta**	
La cultura consciente de los riesgos y de los cumplimientos está presente en toda la empresa, incluyendo la identificación proactiva y la escalada del riesgo	Todos los miembros de la empresa son animados a facilitar el cumplimiento regulatorio.	
El cumplimiento está integrado en las operaciones diarias	Todos los miembros de la empresa son animados a facilitar el cumplimiento regulatorio.	
Habilitador de información		
Referencia	**Contribución a la respuesta**	
Apetito/tolerancia por el riesgo	Equilibrio de los requerimientos de cumplimiento con el apetito/tolerancia por el riesgo empresarial.	
Informes de aseguramiento	Auditorías internas y externas.	
Marco de control interno	Optimizar la eficiencia del control interno.	
Análisis de nuevos requerimientos de cumplimiento legal y regulatorio	Ayuda a determinar la aplicabilidad.	
Habilitador de servicios, infraestructura y aplicaciones		
Referencia	**Contribución a la respuesta**	
Bases de datos regulatorias	Facilitar el seguimiento de los requerimientos de cumplimiento.	
Herramientas de gobierno, riesgo y cumplimiento (GRC)	Descripción general de controles y prácticas para garantizar el cumplimiento	
Habilitador de personas, habilidades y competencias		
Referencia	**Contribución a la respuesta**	
Habilidades de litigio	Una vez iniciada la acción penal, se requieren las habilidades adecuadas para minimizar el impacto legal.	
Habilidades de análisis legal	Comprender las expectativas de los reguladores locales.	
Control interno	Evaluar el cumplimiento con las regulaciones relevantes y reportar los resultados a la gerencia.	

Categoría del escenario de riesgo 13: Geopolítica		
Categoría del escenario de riesgo	Geopolítica	
Habilitador de principios, políticas y marco de trabajo		
Referencia	**Contribución a la respuesta**	
Políticas de puerto seguro	Proporcionar orientación sobre las disposiciones de una ley o regulación que especifique que determinada conducta se considerará que no viola una regla determinada.	
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
DSS04.02	Mantener una estrategia de continuidad.	Evaluar las opciones de gestión de continuidad del negocio, y elegir una estrategia de continuidad viable y rentable para asegurar la recuperación y la continuidad de la empresa ante un desastre u otro incidente o interrupción mayor.
MEA03.01	Identificar los requerimientos de cumplimiento externos.	Identificar y monitorizar de forma continua los cambios en las leyes y regulaciones locales e internacionales, así como otros requerimientos externos aplicables a la empresa.
MEA03.02	Optimizar la respuesta a los requerimientos externos.	Revisar y ajustar los principios, las políticas, los estándares, los procedimientos y las metodologías para asegurarse que se aborden y comuniquen los requerimientos legales, regulatorios y contractuales. Considerar los estándares de la industria, códigos de buenas prácticas y pautas de mejores prácticas para la adopción y adaptación de planes existentes.
Habilitador de estructuras organizacionales		
Referencia	**Contribución a la respuesta**	
Oficial de privacidad	Identificar los requerimientos de privacidad y garantizar el cumplimiento.	
Departamento de cumplimiento regulatorio	Proporcionar orientación sobre los requerimientos de cumplimiento legal, regulatorio y contractual.	
Grupo legal	Apoyo legal durante el análisis y litigio relacionados con el cumplimiento.	
Plan de continuidad del negocio/recuperación ante desastres	Mantener planes detallados y requerimientos de recursos para un servicio continuo.	
Habilitador de cultura, ética y comportamiento		
Referencia	**Contribución a la respuesta**	
Crecimiento y expansión controlados	Garantizar que las regulaciones y los requerimientos externos son integrados en los planes de crecimiento.	
Habilitador de información		
Referencia	**Contribución a la respuesta**	
Análisis de nuevas regulaciones	Las regulaciones impuestas por el gobierno local se deben analizar.	
Habilitador de servicios, infraestructura y aplicaciones		
Referencia	**Contribución a la respuesta**	
Servicios legales externos	Obtener asesoramiento sobre las nuevas regulaciones de los gobiernos locales y el impacto que tienen en la empresa.	
Habilitador de personas, habilidades y competencias		
Referencia	**Contribución a la respuesta**	
Habilidades de litigio	Una vez iniciada la acción penal, se requieren las habilidades adecuadas para minimizar el impacto legal sobre la empresa.	
Habilidades de análisis legal	Comprender las expectativas de los reguladores locales.	
Habilidades para la planificación de contingencias	Mantener opciones de servicio continuo en caso de una interrupción.	

Categoría del escenario de riesgo 14: Robo o destrucción de infraestructura		
Categoría del escenario de riesgo	Robo o destrucción de infraestructura	
Habilitador de principios, políticas y marco de trabajo		
Referencia	**Contribución a la respuesta**	
Política de seguridad de la información	Restringir el acceso físico a la infraestructura para evitar la destrucción.	
Política de continuidad del negocio y de recuperación ante desastres	Validar la recuperabilidad de información, servicios, aplicaciones e infraestructura.	
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
DSS01.04	Gestionar el entorno	Mantener medidas de protección contra los factores ambientales. Instalar equipo y dispositivos especializados para monitorizar y controlar el entorno
DSS01.05	Gestionar las instalaciones.	Gestionar las instalaciones, incluyendo el equipo de suministro eléctrico y comunicaciones, en línea con las leyes y regulaciones, los requerimientos técnicos y del negocio, las especificaciones del proveedor, y las pautas de salud y seguridad.
DSS05.05	Gestionar el acceso físico a los activos de TI.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a las instalaciones, edificios y áreas debe justificarse, autorizarse, registrarse y monitorizarse. Esto debe aplicarse a todas las personas que entren en las instalaciones, incluyendo personal, personal temporal, clientes, proveedores, visitantes y cualquier otro tercero.
Habilitador de estructuras organizacionales		
Referencia	**Contribución a la respuesta**	
Gerente de seguridad de la información	Implementación de medidas de seguridad para prevenir el robo o la destrucción.	
Jefe de operaciones de TI	Responsable de la protección del entorno de TI.	
Habilitador de cultura, ética y comportamiento		
Referencia	**Contribución a la respuesta**	
La seguridad de la información se practica en las operaciones diarias	Prevenir el acceso físico no autorizado.	
Las personas respetan la importancia de las políticas y los principios de seguridad de la información	Prevenir el acceso físico no autorizado.	
Las partes interesadas son conscientes de cómo identificar y responder a amenazas a la empresa	Minimizar el impacto del robo y destrucción de la infraestructura.	
Habilitador de información		
Referencia	**Contribución a la respuesta**	
Solicitudes de acceso	Proporcionar información sobre los usuarios con acceso autorizado a las instalaciones.	
Registros de acceso	Reportar la actividad de accesos.	
Informes de evaluaciones de las instalaciones	La empresa es consciente del estado y riesgo de las instalaciones.	
Habilitador de servicios, infraestructura y aplicaciones		
Referencia	**Contribución a la respuesta**	
Control de acceso	Prevenir el acceso lógico no autorizado.	
Sistema de seguridad de alarma y monitorización	Prevenir el acceso físico no autorizado.	
Habilitador de personas, habilidades y competencias		
Referencia	**Contribución a la respuesta**	
Habilidades de seguridad de la información	Implementar controles para prevenir o reducir el impacto del robo y destrucción de la infraestructura.	

Categoría del escenario de riesgo 15: Malware		
Categoría del escenario de riesgo	Malware	
Habilitador de principios, políticas y marco de trabajo		
Referencia		**Contribución a la respuesta**
Política de seguridad de la información		Describe los acuerdos de seguridad de la información dentro de la empresa para prevenir el malware.
Política de prevención de software malicioso		Detalla las medidas preventivas, de detección y correctivas existentes en toda la empresa para proteger los sistemas de información y la tecnología contra el malware.
Principios de arquitectura		Los requerimientos de seguridad de la información están integrados a la arquitectura empresarial y se traducen a una arquitectura formal de seguridad de la información.
Política de recuperación de incidentes		Validar la recuperabilidad de la información, servicios, aplicaciones e infraestructura en caso de un incidente de seguridad.
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
APO01.03	Mantener los habilitadores del sistema de gestión.	Mantener los habilitadores del sistema de gestión y el entorno de control para las TI empresariales, y asegurarse de que estén integrados y alineados con la filosofía de gobierno y gestión y el estilo operativo de la empresa. Estos habilitadores incluyen la clara comunicación de expectativas/requerimientos. El sistema de gestión debería fomentar la cooperación y el trabajo en equipo entre las divisiones, promover el cumplimiento y la mejora continua, y manejar las desviaciones del proceso (incluyendo los incumplimientos).
APO01.08	Mantener el cumplimiento con las políticas y los procedimientos.	Implementar procedimientos para mantener el cumplimiento, medir el rendimiento de las políticas y otros habilitadores del marco de control, y hacer cumplir las consecuencias del incumplimiento o desempeño inadecuado. Dar seguimiento a las tendencias y el rendimiento y considerarlos en el futuro diseño y mejora del marco de control.
DSS05.01	Proteger contra malware.	Implementar y mantener medidas de prevención, detección y corrección (especialmente parches de seguridad y anti-malware actualizados) en toda la empresa para proteger los sistemas de información y la tecnología contra virus, gusanos, spyware, spam, etc.
DSS05.07	Monitorizar la infraestructura para detectar eventos relacionados con la seguridad.	Usar herramientas de detección de intrusos, monitorizar la infraestructura para detectar accesos no autorizados y asegurarse que los eventos se integren en la monitorización general de eventos y en los procedimientos de gestión de incidentes.
Habilitador de estructuras organizacionales		
Referencia		**Contribución a la respuesta**
Gerente de seguridad de la información		Implementación de medidas de seguridad.
Jefe de operaciones de TI		Gestionar el equipo de respuesta a incidentes para restaurar el servicio de manera oportuna.
Habilitador de cultura, ética y comportamiento		
Referencia		**Contribución a la respuesta**
La seguridad de la información se practica en las operaciones diarias		Prevenir la instalación no intencional de malware.
Las personas respetan la importancia de las políticas y los principios de seguridad de la información		Prevenir la instalación no intencional de malware.
Las partes interesadas son conscientes de cómo identificar y responder a amenazas a la empresa		Minimizar el impacto de la instalación de malware.
Concientización y capacitación sobre malware, correo electrónico y uso de internet		Prevenir la instalación no intencional de malware.
Habilitador de información		
Referencia		**Contribución a la respuesta**
Información de amenazas		Inteligencia sobre los tipos de ataques.
Informes de monitorización		Identificación de intentos de ataque, amenazas, etc.
Habilitador de servicios, infraestructura y aplicaciones		
Referencia		**Contribución a la respuesta**
Cortafuegos (firewall)		Protección contra malware.
Gestión de información y eventos de seguridad (SIEM)		Proporciona análisis en tiempo real de las alertas de seguridad generadas por el hardware y las aplicaciones de red.
Herramientas de protección contra software malicioso		Protección contra malware.
Servicios de monitorización y alerta		Notificación oportuna de amenazas potenciales.

Categoría del escenario de riesgo 15: Malware *(cont.)*	
Habilitador de personas, habilidades y competencias	
Referencia	**Contribución a la respuesta**
Habilidades de seguridad de la información	Prevenir y reducir el impacto del malware implementando controles.
Habilidades técnicas en TI	Configuración adecuada de la infraestructura de TI, como cortafuegos (firewalls) para prevenir las instalaciones accidentales de malware.

Categoría del escenario de riesgo 16: Ataques lógicos		
Categoría del escenario de riesgo	Ataques lógicos	
Habilitador de principios, políticas y marcos de trabajo		
Referencia		**Contribución a la respuesta**
Política de seguridad de la información		Describe los acuerdos de seguridad de la información dentro de la empresa.
Políticas y procedimientos técnicos de seguridad		Detalla las consecuencias técnicas de la política de seguridad de la información.
Principios de arquitectura		Los requerimientos de seguridad de la información están integrados en la arquitectura empresarial y se traducen en una arquitectura formal de seguridad de la información.
Política de continuidad del negocio y de recuperación ante desastres		Validar la recuperabilidad de la información, servicios, aplicaciones e infraestructura.
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
APO13.01	Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).	Establecer y mantener un SGSI que proporciona un enfoque estándar, formal y continuo para la gestión de seguridad de la información, habilitando tecnología segura y procesos del negocio que están alineados con los requerimientos del negocio y la gestión de la seguridad empresarial.
APO13.03	Monitorizar y revisar el SGSI.	Mantener y comunicar periódicamente la necesidad, y los beneficios, de una mejora continua de seguridad de la información. Recolectar y analizar datos sobre el SGSI, y mejorar la efectividad del SGSI. Corregir los incumplimientos para evitar la recurrencia. Promover una cultura de seguridad y mejora continua.
BAI03.07	Prepararse para las pruebas de la solución.	Establecer un plan de pruebas y los entornos requeridos para probar los componentes individuales e integrados de la solución, incluyendo los procesos de negocio y los servicios de soporte, las aplicaciones y la infraestructura.
DSS01.03	Monitorizar la infraestructura de TI.	Monitorizar la infraestructura de TI y los eventos relacionados. Almacenar suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y el examen de las secuencias temporales de las operaciones y de las otras actividades que rodean o apoyan las operaciones.
DSS04.03	Desarrollar e implementar una respuesta de continuidad del negocio.	Desarrollar un plan de continuidad del negocio (BCP) basado en la estrategia que documente los procedimientos y la información en preparación para su uso en un incidente con el fin de permitir que la empresa continúe con sus actividades críticas.
DSS05.01	Proteger contra malware.	Implementar y mantener medidas de prevención, detección y corrección (especialmente parches de seguridad y anti-malware actualizados) en toda la empresa para proteger los sistemas de información y la tecnología contra virus, gusanos, spyware, spam, etc.
DSS05.02	Gestionar la seguridad de la red y las conexiones.	Usar medidas de seguridad y procedimientos de gestión relacionados para proteger la información a través de todos los métodos de conectividad.
DSS05.07	Monitorizar la infraestructura para detectar eventos relacionados con la seguridad.	Usar herramientas de detección de intrusos, monitorizar la infraestructura para detectar accesos no autorizados y asegurarse que cualquier evento se integre a la monitorización general de eventos y a la gestión de incidentes.
Habilitador de estructuras organizacionales		
Referencia		**Contribución a la respuesta**
Gerente de seguridad de la información		Responsable de la implementación de medidas de seguridad.
Jefe de operaciones de TI		Gestionar el equipo de respuesta a incidentes para restaurar el servicio de manera oportuna.
Gerente de servicio		En caso de que los ataques tengan éxito, comunicarse con el usuario final y ayudar a gestionar la respuesta.
Director de Arquitectura de Seguridad		Diseño de medidas de seguridad.
Habilitador de cultura, ética y comportamiento		
Referencia		**Contribución a la respuesta**
La seguridad de la información se practica en las operaciones diarias		Evitar ataques lógicos.
Las personas respetan la importancia de las políticas y los principios de seguridad de la información		Evitar ataques lógicos.
Las partes interesadas son conscientes de cómo identificar y responder a amenazas a la empresa		Minimizar el impacto de ataques lógicos.

Categoría del escenario de riesgo 16: Ataques lógicos *(cont.)*	
Habilitador de información	
Referencia	**Contribución a la respuesta**
Plan de respuesta a incidentes	Detallar la acción a emprender en caso de ataque.
Información de amenazas	Inteligencia sobre los tipos de ataques.
Informes de monitorización	Identificación de intentos de ataque, amenazas, etc.
Habilitador de servicios, infraestructura y aplicaciones	
Referencia	**Contribución a la respuesta**
Cortafuegos (firewall)	Evitar ataques lógicos exitosos.
Gestión de información y eventos de seguridad (SIEM)	Proporciona análisis en tiempo real de las alertas de seguridad generadas por el hardware y las aplicaciones de red.
Herramientas de gestión de red/escáneres de vulnerabilidad	Identificar y reportar las debilidades.
Servicios de monitorización y alerta	Notificación oportuna de amenazas potenciales.
Habilitador de personas, habilidades y competencias	
Referencia	**Contribución a la respuesta**
Habilidades de seguridad de la información	Prevenir y reducir el impacto de ataques lógicos al implementar controles.
Habilidades técnicas en TI	Configuración adecuada de la infraestructura de TI, como cortafuegos (firewalls), componentes críticos de la red, etc., para prevenir los ataques lógicos.

Categoría del escenario de riesgo 17: Acción industrial		
Categoría del escenario de riesgo	Acción industrial	
Habilitador de principios, políticas y marco de trabajo		
Referencia	**Contribución a la respuesta**	
Política de RR.HH.	Definir los derechos y las obligaciones de todo el personal, detallando el comportamiento aceptable e inaceptable de los empleados, y al hacerlo, gestionar el riesgo que está vinculado al comportamiento humano.	
Política de gestión de proveedores	Definir las opciones de provisión del servicio de respaldo o de emergencia.	
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
APO01.01	Definir la estructura organizativa.	Establecer una estructura organizativa interna y extendida que refleje las necesidades del negocio y las prioridades de TI. Establecer las estructuras de gestión requeridas (p. ej., comités) que permitan que la toma de decisiones de gestión se lleve a cabo de la manera más eficaz y eficiente.
APO07.01	Mantener una dotación de personal suficiente y adecuada.	Evaluar los requerimientos de personal de forma periódica o ante cambios mayores en los entornos empresariales, operativos o de TI para garantizar que la empresa cuente con suficientes recursos humanos para apoyar las metas y los objetivos empresariales. La dotación de personal incluye tanto los recursos internos como externos.
APO07.02	Identificar al personal clave de TI.	Identificar al personal clave de TI mientras se minimiza la dependencia en una sola persona que realice una función de trabajo crítica al capturar los conocimientos (documentación), compartir los conocimientos, planificar la sucesión y tener un respaldo de personal.
APO07.05	Planificar y hacer seguimiento del uso de los recursos humanos de TI y de negocios	Comprender y hacer seguimientode la demanda actual y futura de recursos humanos empresariales y de TI con responsabilidades para las TI empresariales. Identificar las carencias y proporcionar comentarios sobre los planes de adquisiciones, planes de adquisiciones de los procesos de reclutamiento empresarial y de TI, y los procesos de reclutamiento empresarial y de TI.
Habilitador de estructuras organizacionales		
Referencia	**Contribución a la respuesta**	
Director de RR.HH.	Responsable de establecer las expectativas de y sobre el personal.	
Grupo legal	Apoyar la contratación inicial y el enjuiciamiento en caso de incumplimiento del contrato.	
Consejo de Dirección	Responsable del buen funcionamiento de la empresa y la estructura organizativade alto nivel para la comunicación de las partes interesadas.	
Ejecutivos de negocio	Facilitar la comunicación bidireccional con los empleados.	
Habilitador de cultura, ética y comportamiento		
Referencia	**Contribución a la respuesta**	
La cultura transparente y participativa es un punto de enfoque importante	Prevenir la acción industrial.	
Habilitador de información		
Referencia	**Contribución a la respuesta**	
Acuerdos contractuales con el personal	Definición clara de responsabilidades, derechos y obligaciones para el personal.	
Contratos de proveedores	Definición clara de responsabilidades, derechos y obligaciones para acuerdos específicos con proveedores.	
Repositorios de conocimientos	Minimizar el efecto de la indisponibilidad parcial de recursos al compartir conocimientos sobre procesos, tecnología, etc.	
Análisis déficit de recursos	Análisis claro del nivel crítico de recursos.	
Habilitador de servicios, infraestructura y aplicaciones		
Referencia	**Contribución a la respuesta**	
Servicios de apoyo de terceros	Apoyo temporal en caso de una acción industrial.	
Habilitador de personas, habilidades y competencias		
Referencia	**Contribución a la respuesta**	
Habilidades de RR.HH.	Gestión de habilidades y competencias.	
Habilidades de negociación	Facilitar la máxima comunicación bidireccional y asegurarse que se cumplan los requerimientos operativos mínimos después de una acción industrial.	
Habilidades de litigio	Una vez que se ha iniciado el enjuiciamiento, se requieren las habilidades adecuadas para defender los intereses de la empresa.	

Categoría del escenario de riesgo 18: Medio ambiente		
Categoría del escenario de riesgo	Medio ambiente	
Habilitador de principios, políticas y marco de trabajo		
Referencia	**Contribución a la respuesta**	
Política social y medioambiental	La concientización medioambiental debe ser parte de la política general de la empresa sobre responsabilidad corporativa.	
Política de gestión de proveedores	La concientización medioambiental debe incluirse en todos los contratos y acuerdos con los proveedores.	
Reglas de conducta (uso aceptable)	Los usuarios deben ser conscientes de su impacto individual en el medio ambiente.	
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
APO02.03	Definir las capacidades objetivo de TI.	Definir las capacidades objetivo del negocio y de TI, así como los servicios de TI requeridos. Esto debe basarse en el entendimiento del entorno y los requerimientos de la empresa; la evaluación de los procesos de negocio actuales y el entorno y los problemas de TI; y considerando los estándares de referencia, las mejores prácticas y las tecnologías emergentes validadas o las propuestas de innovación.
APO04.03	Monitorizar y escanear el entorno tecnológico.	Monitorizar y escanear sistemáticamente el entorno externo de la empresa para identificar las tecnologías emergentes con el potencial de crear valor (p. ej., ejecutar la estrategia empresarial, optimizar costos, evitar la obsolescencia y habilitar de mejor manera los procesos empresariales y de TI). Monitorizar el mercado, el entorno competitivo, los sectores de la industria y las tendencias legales y regulatorias para poder analizar las tecnologías emergentes o las ideas de innovación en el contexto empresarial.
BAI03.04	Obtener los componentes de la solución.	Adquirir componentes de la solución basados en el plan de adquisiciones de acuerdo con los requerimientos y los diseños detallados, los principios y estándares de la arquitectura, y los procedimientos generales de compra y contratos de la empresa, requerimientos de QA y estándares de aprobación. Asegurarse de que el proveedor identifique y aborde todos los requerimientos legales y contractuales.
DSS01.04	Gestionar el ambiente.	Mantener medidas de protección contra los factores medioambientales. Instalar equipo y dispositivos especializados para monitorear y controlar el ambiente.
DSS01.05	Gestionar las instalaciones.	Gestionar las instalaciones, incluyendo el equipo de suministro eléctrico y comunicaciones, en línea con las leyes y regulaciones, los requerimientos técnicos y del negocio, las especificaciones del proveedor, y las pautas de salud y seguridad.
Habilitador de estructuras organizacionales		
Referencia	**Contribución a la respuesta**	
Jefe de operaciones de TI	Responsable de gestionar el entorno y las instalaciones de TI.	
Jefe de arquitectura	Diseño de medidas ecológicas.	
Habilitador de cultura, ética y comportamiento		
Referencia	**Contribución a la respuesta**	
Se desarrolla y apoya una estructura claramente definida para la responsabilidad ética y una cultura que promueve la rendición de cuentas específica	Las personas están involucradas y son conscientes de las consecuencias de las cuestiones medioambientales, y están facultadas para manejarlas de acuerdo con las pautas éticas.	
Habilitador de información		
Referencia	**Contribución a la respuesta**	
Estrategia de TI	La concientización medioambiental debe ser parte de la estrategia de TI.	
Registro de activos	Evaluar el impacto medioambiental de la tecnología utilizada.	
Habilitador de servicios, infraestructura y aplicaciones		
Referencia	**Contribución a la respuesta**	
Inventario de activos	Ayuda a identificar los activos que deben ser reemplazados para reducir el impacto medioambiental.	
Habilitador de personas, habilidades y competencias		
Referencia	**Contribución a la respuesta**	
Desarrollo de la arquitectura	El desarrollo arquitectónico puede ayudar a reducir el impacto medioambiental de la tecnología.	
Desarrollo de sistemas	Agilizar y optimizar la tecnología usada.	

Categoría del escenario de riesgo 19: Actos de la naturaleza		
Categoría del escenario de riesgo	Actos de la naturaleza	
Habilitador de principios, políticas y marco de trabajo		
Referencia		**Contribución a la respuesta**
Política de copias de respaldo		Las copias de respaldo están disponibles.
Política de continuidad del negocio y de recuperación ante desastres		Validar la recuperabilidad de los datos.
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
DSS01.04	Gestionar el ambiente.	Mantener medidas de protección contra los factores medioambientales. Instalar equipo y dispositivos especializados para monitorizar y controlar el ambiente.
DSS01.05	Gestionar las instalaciones.	Gestionar las instalaciones, incluyendo el equipo de suministro eléctrico y comunicaciones, en línea con las leyes y regulaciones, los requerimientos técnicos y del negocio, las especificaciones del proveedor, y las pautas de salud y seguridad.
DSS04.03	Desarrollar e implementar una respuesta de continuidad del negocio.	Desarrollar un plan de continuidad del negocio (BCP) basado en la estrategia que documente los procedimientos y la información en preparación para su uso en un incidente con el fin de permitir que la empresa continúe con sus actividades críticas.
DSS04.04	Ejercer, probar y revisar el BCP.	Probar los acuerdos de continuidad de forma periódica para ejercitar los planes de recuperación contra resultados predeterminados, y para permitir que se desarrollen soluciones innovadoras, y para ayudar a verificar a través del tiempo que el plan funcionará tal como se anticipa.
DSS05.05	Gestionar el acceso físico a los activos de TI.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a las instalaciones, edificios y áreas debe justificarse, autorizarse, registrarse y monitorizarse. Esto debe aplicarse a todas las personas que entren en las instalaciones, incluyendo personal, personal temporal, clientes, proveedores, visitantes y cualquier otro tercero.
Habilitador de estructuras organizacionales		
Referencia		**Contribución a la respuesta**
Gerente de continuidad del negocio		Responsable del plan de continuidad del negocio (BCP).
Jefe de operaciones de TI		Responsable de gestionar el entorno y las instalaciones de TI.
Director de Informática (CIO)		Responsable de desarrollar e implementar los planes de recuperación ante desastres.
Propietarios del proceso de negocio		Responsable de desarrollar e implementar los planes de continuidad del negocio.
Habilitador de cultura, ética y comportamiento		
Referencia		**Contribución a la respuesta**
Las partes interesadas son conscientes de cómo identificar y responder a amenazas		Las personas están involucradas y son conscientes de cómo reaccionar cuando ocurre un incidente.
La dirección del negocio se compromete en una colaboración multifuncional continua a fin de fomentar la puesta en marcha de programas de continuidad del negocio eficientes y eficaces.		El negocio está comprometido y contribuye proactivamente a la preparación de los planes de continuidad.
Habilitador de información		
Referencia		**Contribución a la respuesta**
Póliza de seguros		Seguro disponible en caso de actos de la naturaleza.
Informes de evaluaciones de las instalaciones		La empresa es consciente del estado y riesgo de las instalaciones.
Acciones y comunicaciones para respuesta a incidentes		Las personas son conscientes de cómo reaccionar cuando ocurre un incidente.
Habilitador de servicios, infraestructura y aplicaciones		
Referencia		**Contribución a la respuesta**
Servicios de monitorización y alerta		Notificación oportuna de amenazas potenciales.
Habilitador de personas, habilidades y competencias		
Referencia		**Contribución a la respuesta**
Gestión de riesgos de la información		Identificar y formular una respuesta al riesgo de información relacionado con los actos de la naturaleza.
Comprensión técnica		Experiencia técnica sobre actos de la naturaleza específicos y relevantes.

Categoría del escenario de riesgo 20: Innovación		
Categoría del escenario de riesgo	Innovación	
Habilitador de principios, políticas y marco de trabajo		
Referencia	**Contribución a la respuesta**	
Estrategia de TI	Definir las reglas y pautas generales subyacentes para el uso y despliegue de todos los recursos y activos de TI en toda la empresa.	
Habilitador del proceso		
Referencia	**Título**	**Prácticas de gobierno y gestión**
APO02.01	Comprender la dirección de la empresa.	Considerar el entorno empresarial actual, así como los procesos de negocio, la estrategia empresarial y los objetivos futuros. También considerar el entorno externo de la empresa (impulsores de la industria, regulaciones relevantes y bases de la competencia).
APO02.03	Definir las capacidades objetivo de TI.	Definir las capacidades objetivo del negocio y de TI, así como los servicios de TI requeridos. Esto debe basarse en el entendimiento del entorno y los requerimientos de la empresa; la evaluación de los procesos de negocio actuales y el entorno y los problemas de TI; y considerando los estándares de referencia, las mejores prácticas y las tecnologías emergentes validadas o las propuestas de innovación.
APO03.01	Desarrollar la visión de arquitectura empresarial.	La visión de la arquitectura ofrece una descripción de alto nivel de la línea de referencia y las arquitecturas objetivo, cubriendo los dominios empresariales, de información, de datos, de aplicación y de tecnología. La visión de la arquitectura ofrece al patrocinador una herramienta clave para promover los beneficios de las capacidades propuestas a las partes interesadas de la empresa. La visión de la arquitectura describe cómo la nueva capacidad cumplirá con las metas y los objetivos empresariales estratégicos, y abordará las preocupaciones de las partes interesadas cuando se implemente.
APO04.01	Crear un entorno favorable a la innovación.	Crear un entorno que propicie la innovación, considerando cuestiones como la cultura, las recompensas, la colaboración, los foros de tecnología y los mecanismos para promover y capturar las ideas de los empleados.
APO04.02	Mantener un entendimiento del entorno de la empresa.	Trabajar con las partes interesadas para comprender sus desafíos. Mantener una comprensión adecuada de la estrategia empresarial y del entorno competitivo o de otras restricciones, de forma que se puedan identificar las oportunidades habilitadas por las nuevas tecnologías.
APO04.03	Monitorizar y escanear el entorno tecnológico.	Monitorizar y escanear sistemáticamente el entorno externo de la empresa para identificar las tecnologías emergentes con el potencial de crear valor (p. ej., ejecutar la estrategia empresarial, optimizar costos, evitar la obsolescencia y habilitar de mejor manera los procesos empresariales y de TI). Monitorizar el mercado, el entorno competitivo, los sectores de la industria y las tendencias legales y regulatorias para poder analizar las tecnologías emergentes o las ideas de innovación en el contexto empresarial.
APO04.04	Evaluar el potencial de las tecnologías emergentes y las ideas de innovación.	Analizar las tecnologías emergentes identificadas y/u otras sugerencias de innovación en TI. Trabajar con las partes interesadas para validar las suposiciones sobre el potencial de nuevas tecnologías e innovación.
APO04.05	Recomendar iniciativas apropiadas adicionales.	Evaluar y monitorear los resultados de las iniciativas que son prueba de concepto, y si son favorables, generar recomendaciones de iniciativas adicionales y obtener el apoyo de las partes interesadas.
APO04.06	Monitorizar la implementación y el uso de la innovación.	Monitorizar la implementación y el uso de las tecnologías emergentes y las innovaciones durante la integración, adopción y todo el ciclo de vida económica para garantizar que se obtengan los beneficios prometidos y para identificar las lecciones aprendidas.
Habilitador de estructuras organizacionales		
Referencia	**Contribución a la respuesta**	
Director General Ejecutivo (CEO)	Responsable de crear el entorno propicio para la innovación.	
Comité de estrategia	Responsable de llevar adelante y monitorear iniciativas de innovación favorables.	
Director de Informática (CIO)	Responsable de identificar las innovaciones basadas en tecnología y de evaluar su potencial.	
Grupo de innovación	Responsable de identificar las oportunidades de innovación y desarrollar casos de negocio para las iniciativas de innovación.	
Habilitador de cultura, ética y comportamiento		
Referencia	**Contribución a la respuesta**	
Disposición para tomar riesgos	La innovación, por definición, se trata de nuevas tecnologías y nuevas maneras de trabajar, lo que resulta en resistencia potencial y en beneficios inseguros. Sin embargo, no tener una disposición a tomar riesgos, excluirá de antemano cualquier potencial de innovación.	
Apoyo de la alta gerencia para las iniciativas de innovación	Se requiere el apoyo de la alta gerencia para financiar las iniciativas de innovación y apoyarlas para superar la resistencia inicial.	
"El fracaso se permite"	No todos los proyectos o iniciativas de innovación serán exitosos, y se aceptará una cierta cantidad de fracasos como parte del precio a pagar por las iniciativas exitosas.	

Categoría del escenario de riesgo 20: Innovación *(cont.)*	
Habilitador de información	
Referencia	**Contribución a la respuesta**
Plan de innovación	Las innovaciones están diseñadas claramente para que puedan ser monitoreadas e incorporadas a los planes estratégicos de la empresa.
Programa de reconocimiento	La innovación se debe recompensar adecuadamente, de acuerdo con un plan acordado y formalizado.
Evaluación de las iniciativas de innovación	La evaluación formal de las iniciativas de innovación facilita la toma de decisiones ejecutivas.
Habilitador de personas, habilidades y competencias	
Referencia	**Contribución a la respuesta**
Liderazgo y comunicación	Aclarar los motivos de la arquitectura y las consecuencias potenciales.
Habilidades de arquitectura	Desarrollar una arquitectura eficiente y eficaz alineada con los requerimientos del negocio.

Página intencionalmente en blanco

Capítulo 6
Expresión y Descripción de Riesgos[6]

Preparación de un análisis de escenario de riesgo

Los escenarios de riesgo se pueden utilizar para describir el riesgo y documentar los factores de riesgo necesarios para estimar la frecuencia y el impacto. El Apéndice 1 contiene una plantilla genérica que se ha desarrollado para facilitar la documentación de información útil para el tratamiento del escenario de riesgo bajo análisis. El Capítulo 7 proporciona ejemplos prácticos y detallados de escenarios de riesgo, basados en esta plantilla. En total, hay **60 ejemplos de escenarios de riesgo detallados que se derivan de las 20 categorías de escenarios de riesgo.**

La plantilla contiene siete secciones para documentar la siguiente información:

- **Título del escenario de riesgo**
- **Categoría del escenario de riesgo**
  Descripción de alto nivel de la categoría del escenario. En total, hay 20 categorías:
  - 01 Establecimiento y mantenimiento de la cartera
  - 02 Gestión del ciclo de vida del programa/proyectos
  - 03 Toma de decisiones sobre inversiones en TI
  - 04 Experiencia y habilidades en TI
  - 05 Operaciones del personal
  - 06 Información
  - 07 Arquitectura
  - 08 Infraestructura
  - 09 Software
  - 10 Propiedad empresarial de TI
  - 11 Proveedores
  - 12 Cumplimiento regulatorio
  - 13 Geopolítica
  - 14 Robo o destrucción de infraestructura
  - 15 Malware
  - 16 Ataques lógicos
  - 17 Acción industrial
  - 18 Medio ambiente
  - 19 Actos de la naturaleza
  - 20 Innovación
- **Escenario de riesgo**
  Una descripción detallada del escenario práctico de riesgo/oportunidad, incluyendo una discusión de los posibles resultados negativos y positivos.
- **Componentes del escenario de riesgo**
  Esta sección de la plantilla aclara el tipo de amenaza/vulnerabilidad del escenario de riesgo/oportunidad práctico detallado, e incluye los siguientes componentes:
  - Tipo de amenaza
    La naturaleza del evento, p. ej., malicioso, accidental, un error, un fallo de un proceso bien definido, un evento natural o un requerimiento externo.
  - Agente
    Quién o qué genera la amenaza que explota una vulnerabilidad. Los agentes pueden ser internos o externos a la empresa, humanos o no-humanos.
  - Evento
    El evento que tendrá un impacto (positivo o negativo) en el logro de los objetivos de la empresa. El evento puede ser una divulgación (de información confidencial), interrupción o modificación (de un sistema o proyecto), robo o destrucción. Un evento también puede incluir el diseño ineficaz (de sistemas, procesos, etc.), el uso inapropiado, cambios en las reglas y regulaciones que impacta materialmente un sistema, o la ejecución ineficaz de procesos, p. ej., procedimientos de gestión de cambios, procedimientos de adquisición o procesos de priorización de proyectos.
  - Activo/recurso

[6] El contenido de este capítulo se basa en las siguientes publicaciones: ISACA, COBIT® 5 (el marco), EE.UU., 2012; ISACA, *COBIT® 5 para el Riesgo*, EE.UU., 2013; ISACA, *Guía del Practicante para Riesgos de TI*, EE.UU., 2009.

Un activo es algo de valor tangible o intangible que vale la pena proteger, incluyendo a personas, sistemas, infraestructura, finanzas y reputación. Un recurso es cualquier cosa que ayuda a alcanzar una meta. Un activo/recurso puede ser:
. Proceso
. Personas y habilidades
. Estructura organizativa
. Infraestructura física (instalaciones, equipos, etc.)
. Infraestructura de TI, incluyendo hardware informático, redes, middleware
. Información
. Aplicaciones

Los activos y recursos pueden ser idénticos. Por ejemplo, el hardware de TI es un recurso importante porque las aplicaciones de TI lo utilizan, y es un activo porque tiene un valor para la empresa.

– Problemas de tiempo
. *Momento* de la ocurrencia (*crítico, no crítico*: ¿El evento ocurre en un momento crítico?)
. *Duración* (*corta, moderada, extensa*: La duración del evento, p. ej., interrupción prolongada de un servicio o centro de datos)
. *Detección* (*lenta, moderada, instantánea*)
. *Tiempo transcurrido* (*Inmediato, retrasado*: Tiempo transcurrido entre el evento y la consecuencia. ¿Existe una consecuencia inmediata, p. ej., falla de la red, tiempo de inactividad inmediato,o una consecuencia retardada, o una arquitectura de TI incorrecta con altos costos acumulados, durante un período de varios años?)

• **Tipo de riesgo**
Una descripción del tipo de riesgo al que encajarán los escenarios derivados del escenario genérico, utilizando los tres tipos de riesgo explicados anteriormente.

Una "**P**" indica un ajuste primario (grado más alto), y una "**S**" un ajuste secundario (grado inferior). Las celdas en blanco indican que la categoría de riesgo no es relevante para el escenario de riesgo en cuestión.

– *Habilitación del beneficio/valor de TI*
Asociado con oportunidades, u oportunidades perdidas, de usar la tecnología para mejorar la eficiencia o la efectividad de los procesos de negocio, o como un habilitador para nuevas iniciativas de negocios:
. Habilitador tecnológico para nuevas iniciativas del negocio
. Habilitador tecnológico para operaciones eficientes

– *Entrega del programa y proyecto de TI*
Asociado con la contribución de TI a soluciones empresariales nuevas o mejoradas, usualmente en forma de proyectos y programas como parte de carteras de inversión:
. Calidad del proyecto
. Relevancia del proyecto
. Rebasamiento del proyecto

– *Operaciones de TI y Prestación de Servicio:*
Asociado con todos los aspectos del negocio como el desempeño usual de los sistemas y servicios de TI, que pueden causar destrucción o reducción de valor a la empresa:
. Interrupciones del servicio de TI
. Problemas de seguridad
. Cuestiones de cumplimiento

• **Respuesta al riesgo**
Descripción de cómo la empresa responderá al riesgo. El propósito de definir una respuesta al riesgo es alinear el riesgo con el apetito y la tolerancia al riesgo definidos para la empresa. La respuesta al riesgo puede ser:
– Evitación del riesgo
– Aceptación de riesgo
– Compartir/transferir el riesgo
– Mitigación del riesgo

• **Mitigación del riesgo usando los habilitadores de COBIT 5**
Descripción de cómo la empresa trabajará para evitar que el riesgo se materialice. Para las posibilidades de mitigación del riesgo, consulte los habilitadores de COBIT 5 en el Capítulo 5. Proporcione la siguiente información:
– Referencia, título y descripción de uno o más habilitadores relevantes que pueden ayudar a mitigar el riesgo.
– El efecto estimado que la implementación de este habilitador tendrá en la frecuencia y el impacto del riesgo. Los valores posibles son bajo, medio o alto.
– Basándose en los dos parámetros de frecuencia e impacto, indique si este habilitador es esencial (una práctica clave de gestión para mitigar el riesgo). Un habilitador se considera esencial si tiene un alto efecto en la reducción del impacto o la frecuencia del escenario.

• **Indicadores clave de riesgo**
Identificación de una serie de métricas para detectar y monitorar el escenario de riesgo y la respuesta al riesgo.

El Capítulo 7 proporciona 60 ejemplos detallados de análisis de escenarios de riesgo, basados en la plantilla del Apéndice 1.

Importante: Los ejemplos de escenarios detallados no reemplaza la fase creativa y reflexiva que cada ejercicio de creación de escenarios debería contener. En otras palabras, una empresa no debería usar ciegamente los ejemplos de escenarios y asumir que no existen otros escenarios de riesgo posibles, o asumir que cada escenario contenido en la lista es aplicable a la empresa. Se necesitan inteligencia y experiencia para obtener una lista relevante y personalizada de escenarios a partir de la lista genérica.

Métodos de análisis de riesgo: Cuantitativo vs. Cualitativo

Como se mencionó anteriormente, el análisis de riesgo es el proceso de estimar las dos propiedades esenciales de cada escenario de riesgo:
- **Frecuencia**: El número de veces en un período dado (generalmente en un año) que es probable que ocurra un evento
- **Impacto**: Las consecuencias comerciales del escenario

Existen varios métodos para el análisis de riesgos, que van desde alto nivel y principalmente cualitativos, hasta muy detallados y/o cuantitativos, con métodos híbridos entre ellos. Ambas formas pueden ser necesarias en diferentes etapas del proceso de gestión de riesgos. Por ejemplo, la evaluación cualitativa tiende a ser mejor en la etapa inicial de evaluación de riesgos para establecer prioridades, y la evaluación cuantitativa puede entonces proporcionar el rigor y la precisión requeridos para las áreas de alto riesgo seleccionadas.

La cultura, los recursos, las habilidades y los conocimientos de la empresa sobre la gestión de riesgos de TI, el entorno y el apetito de riesgo, así como su enfoque actual de ERM, determinarán la metodología que se debe utilizar.

Los diferentes métodos, cuantitativos y cualitativos, tienen algunas limitaciones comunes:
- Ningún método es completamente objetivo, y los resultados de las evaluaciones de riesgos siempre dependen de la persona que las realiza y de sus habilidades y puntos de vista.
- Los datos relacionados con el riesgo de TI (como datos perdidos y factores de riesgo de TI) son muy a menudo de mala calidad o muy subjetivos (p. ej., madurez del proceso, debilidades de control). Usar estructuras o modelos puede ayudar a lograr más objetividad y puede proporcionar al menos una base para la discusión en el análisis de riesgo.
- Los enfoques cuantitativos corren el riesgo de crear un exceso de confianza en modelos complejos basados en datos insuficientes. Sin embargo, los modelos cualitativos o cuantitativos demasiado simplificados también pueden derivar en resultados poco fiables.

Análisis cualitativo de riesgos
Un enfoque cualitativo de evaluación de riesgos utiliza opiniones de expertos para estimar la frecuencia y el impacto en el negocio de eventos adversos. La frecuencia y la magnitud del impacto se estiman usando etiquetas cualitativas. Estas etiquetas pueden variar dependiendo de las circunstancias y los diferentes entornos.

Cuándo usarlo, fortalezas, limitaciones y debilidades:
- En situaciones donde solo hay información limitada o de baja calidad disponible, generalmente se aplican métodos cualitativos de análisis de riesgos.
- Las principales desventajas de utilizar el enfoque cualitativo son un alto nivel de subjetividad, una gran variación en los juicios humanos y la falta de un enfoque estandarizado durante la evaluación.
- Sin embargo, la evaluación cualitativa de riesgos suele ser menos compleja que el análisis cuantitativo, y por lo tanto, también es menos costosa.

Análisis cuantitativo de riesgos
Tan pronto como se utilizan valores cuantitativos (p. ej., rangos) para definir valores cualitativos, o cuando sólo se utilizan valores cuantitativos, se trata de un análisis cuantitativo. La esencia de la evaluación cuantitativa de riesgos consiste en derivar la frecuencia y las consecuencias de los escenarios de riesgo, basándose en métodos y datos estadísticos.

Cuándo usarlo, fortalezas, limitaciones y debilidades:
- El análisis cuantitativo de riesgos es más objetivo porque se basa en datos empíricos formales.
- El uso de métodos puramente cuantitativos requiere datos suficientes, completos y fiables sobre eventos pasados y comparables. La obtención de estos datos es, en muchos casos, muy difícil, a menos que la empresa ya haya adoptado la mejora de procesos y siga un enfoque como Six Sigma para la monitorización de TI y la mejora de la productividad.
- Algunas cosas son muy difíciles o imposibles de cuantificar: valor de la vida humana, costo de ataques terroristas o eventos similares, pérdida de reputación.

Combinación cualitativa y cuantitativa, avanzando hacia la evaluación del riesgo probabilístico

Ambas técnicas tienen algunas ventajas y desventajas. Además, ninguno de los enfoques descritos anteriormente parece satisfacer todos los requerimientos de gestión de riesgos de TI para soportar ampliamente los procesos ERM generales.

El análisis basado en opiniones subjetivas o datos estimados puede ser insuficiente. Todavía existe la cuestión de la incertidumbre. ¿Qué tan certeros pueden ser los resultados de la evaluación del riesgo? Existen algunos métodos avanzados para aumentar la confiabilidad de las evaluaciones de riesgo, pero éstos requieren habilidades estadísticas profundas. Entre ellos se incluyen:
- **Evaluación probabilística de riesgos**: Utilizar un modelo matemático para construir el enfoque de evaluación cualitativa de riesgos, utilizando las técnicas y los principios cuantitativos de evaluación de riesgos. De forma sencilla, se utilizan los modelos estadísticos, y los datos que faltan para completar estos modelos son recogidos utilizando métodos cualitativos de evaluación de riesgos (entrevistas, método Delphi, etc.).
- **Simulación Monte Carlo**: Un poderoso método para combinar enfoques cualitativos y cuantitativos, que se basa en el modelo de simulación determinista normal descrito anteriormente, pero que iterativamente evalúa el modelo utilizando conjuntos de números aleatorios como valores. Mientras que los modelos deterministas proporcionarán el valor esperado, la simulación Monte Carlo dará el valor como una distribución de probabilidad basada en la calidad de la información proporcionada.

Guía práctica para análisis de riesgos

La selección para el análisis cualitativo o cuantitativo de riesgos depende de muchos factores:
- Necesidades del usuario: ¿Es necesario tener datos altamente precisos o un enfoque cualitativo es adecuado?
- Disponibilidad y calidad de los datos relacionados con los riesgos vinculados a las TI.
- Tiempo disponible para el análisis de riesgos.
- Nivel de comodidad y experiencia de los expertos que proporcionan datos.

Los datos estadísticos pueden estar disponibles en cantidades y calidad variables, variando en una escala continua desde casi inexistente a ampliamente disponible. En el extremo superior de la escala, es decir, cuando hay una amplia gama de datos estadísticos disponibles, una evaluación cuantitativa podría ser el método preferido de evaluación de riesgos; en el otro extremo de la escala, con datos muy escasos, incompletos o deficientes, una evaluación cualitativa puede ser la única solución disponible. Los métodos híbridos de evaluación de riesgos pueden aplicarse a situaciones entre los dos extremos descritos anteriormente.

Hay muchas fuentes de datos que se pueden aprovechar para apoyar el análisis de riesgos. Algunas de estas fuentes pueden existir ya en la empresa; p. ej., la mejora de procesos del negocio (BPI), la oficina de gestión de proyectos (PMO), la arquitectura empresarial (EA), el control de calidad (QA) y otras organizaciones que recopilan datos similares para respaldar sus funciones.

La siguiente sección de este capítulo describe algunas técnicas sugeridas que son en su mayoría técnicas cualitativas y que se utilizarán con mayor frecuencia. A pesar de su menor precisión intrínseca, pueden proporcionar datos muy profundos y relevantes, ya que proporcionan un modelo mediante el cual todos los riesgos se pueden medir y describir utilizando el mismo lenguaje y base de referencia, eliminando los casos más notorios de subjetividad y ambigüedad. Por ejemplo:
- Si no se especifica un marco de tiempo en un escenario, entonces una conclusión de que la probabilidad de un evento es "alta" puede ser interpretada de manera diferente por diferentes personas. Una persona puede suponer que es muy probable que ocurra este año, mientras que otra persona podría asumir que significa que es muy probable que suceda eventualmente.
- Si las escalas no están definidas para la magnitud de la pérdida, entonces la interpretación subjetiva de una persona de "pérdida grave" puede ser significativamente diferente de la interpretación de otra persona.

Expresión del impacto en términos de negocios

Las evaluaciones significativas de riesgos de TI, y las decisiones basadas en el riesgo, requieren que el riesgo de TI se exprese en términos inequívocos y claros para el negocio. La gestión eficaz de los riesgos requiere una comprensión mutua entre el área de TI y el negocio sobre qué riesgo se necesita gestionar y por qué. Todas las partes interesadas deben tener la capacidad de comprender y expresar cómo los eventos adversos pueden afectar los objetivos del negocio. Esto significa que:
- Una persona de TI debe entender cómo las fallas o eventos relacionados con TI pueden impactar los objetivos de la empresa y causar pérdidas directas o indirectas a la empresa.
- Una persona de negocios debe entender cómo las fallas o eventos relacionados con TI pueden afectar servicios y/o procesos clave.

Es necesario establecer el vínculo entre los escenarios de riesgos de TI y el impacto final en el negocio para comprender los efectos de los eventos adversos. Existen varias técnicas y opciones que pueden ayudar a la empresa a describir los riesgos de TI en términos de negocio, y no hay opción correcta o incorrecta. Uno debe elegir la opción que mejor se ajuste a la empresa, y complementar este esquema con una variedad de escalas para cuantificar el riesgo durante el análisis de riesgo.

Los riesgos relacionados con TI puede traducirse/expresarse en términos relevantes para el negocio, pero no existe una receta para cualquier método específico. Algunos métodos disponibles se discuten en las siguientes secciones.

Es necesario hacer las siguientes consideraciones, independientemente de la elección del método de descripción del impacto:
- Definir escalas de impacto que están vinculadas al método de descripción del impacto elegido para que sean claras e inequívocas para todas las personas, y representen verdaderamente los objetivos del negocio.
- Asegurarse de que el método y las escalas elegidos permitan que el apetito de riesgo se pueda definir fácilmente, p. ej., el riesgo aceptable e inaceptable, en los mismos términos, a lo largo de toda la empresa.
- Asegurarse de que los escenarios relacionados con TI estén claramente asignados a las descripciones de impacto en el negocio. Esto significa que las dependencias entre eventos (p. ej., falla de hardware) y el impacto y la consecuencia final en el negocio (p. ej., los clientes no pueden realizar pedidos, resultando en insatisfacción del cliente) deben ser definidas e incluidas en cada análisis de riesgos.

Requerimientos del negocio sobre información

Los requerimientos del negocio sobre información permiten la expresión de aspectos del negocio relacionados con el uso de TI. Éstos expresan una condición a la cual la información (en el sentido más amplio), tal como se proporciona a través de las TI, debe conformarse para que sea beneficiosa para la empresa.

Los requerimientos del negocio sobre información son:
- Eficacia: La información es eficaz si satisface las necesidades del consumidor de información que la utiliza para una tarea específica. Si el consumidor de información puede realizar la tarea con la información, entonces ésta es efectiva. Esto corresponde a las siguientes metas de calidad de la información: cantidad adecuada, relevancia, comprensibilidad, interpretabilidad y objetividad.
- Eficiencia: Mientras que la efectividad considera la información como un producto, la eficiencia se relaciona más con el proceso de obtención y uso de la información, por lo que se alinea con la visión de "información como servicio". Si la información que satisface las necesidades del consumidor de la información se obtiene y se utiliza de una manera fácil (es decir, requiere pocos recursos: esfuerzo físico, esfuerzo cognitivo, tiempo, dinero), entonces el uso de la información es eficiente. Esto corresponde a las siguientes metas de calidad de la información: credibilidad, accesibilidad, facilidad de operación y reputación.
- Confidencialidad: La confidencialidad corresponde a la meta de calidad de la información de acceso restringido.
- Integridad: Si la información tiene integridad, entonces está libre de errores y está completa. Esto corresponde a las siguientes metas de calidad de la información: exhaustividad y precisión.
- Disponibilidad: La disponibilidad es una de las metas de calidad de la información bajo el encabezado de accesibilidad y seguridad.
- Cumplimiento: El cumplimiento, en el sentido de que la información debe ajustarse a las especificaciones, está cubierto por cualquiera de las metas de calidad de la información, dependiendo de los requerimientos. El cumplimiento con las regulaciones es a menudo una meta o requerimiento del uso de la información, no tanto una calidad inherente de la información.
- Fiabilidad: La fiabilidad se ve con frecuencia como un sinónimo de precisión; sin embargo, también se puede decir que la información es fiable si se la considera verdadera y creíble. En comparación con la integridad, la fiabilidad es más subjetiva, más relacionada con la percepción, y no solo factual. Esto corresponde a las siguientes metas de calidad de la información: credibilidad, reputación y objetividad.

El impacto en el negocio de cualquier evento relacionado con TI radica en la consecuencia de no alcanzar los criterios de información. Al describir el impacto en estos términos, esto sigue siendo una especie de técnica intermedia, que no describe completamente el impacto en el negocio, p. ej., el impacto en los clientes o en términos financieros.

Metas empresariales y cuadro de mando de COBIT 5

Otra técnica se basa en el concepto de "metas empresariales" de COBIT 5 (**figura 15**). De hecho, el riesgo del negocio radica en cualquier combinación de aquellas metas empresariales que no se alcanzan. Las metas empresariales de COBIT 5 están estructuradas en línea con las cuatro perspectivas clásicas del cuadro de mando (BSC): financiera, clientes, interna y crecimiento.

COBIT 5 define 17 metas empresariales genéricas. La **figura 15** incluye la siguiente información:
- La dimensión BSC bajo la cual se ajusta la meta empresarial
- La descripción de la meta empresarial
- La relación con los tres principales objetivos de gobierno: el logro de beneficios, la optimización de riesgos y la optimización de recursos. ("P" significa relación primaria y mayor impacto en el logro; y "S" significa relación secundaria y un menor impacto en el logro).

Para fines prácticos, uno puede imaginar que para cada meta empresarial, una traducción es posible para expresar el fracaso de alcanzar la meta en términos de su impacto en el negocio en general.

Figura 15: Metas empresariales

Dimensión BSC	Meta empresarial	Relación con los objetivos de gobierno		
		Logro de beneficios	Optimización de los riesgos	Optimización de los recursos
Finanzas	1. Valor para las partes interesadas las inversiones del negocio	P		S
	2. Cartera de productos y servicios competitivos	P	P	S
	3. Riesgo del negocio gestionado (salvaguarda de activos)		P	S
	4. Cumplimiento con las leyes y regulaciones externas		P	
	5. Transparencia financiera	P	S	S
Cliente	6. Cultura de servicio orientada al cliente	P		S
	7. Continuidad y disponibilidad del servicio del negocio		P	
	8. Respuestas ágiles a un entorno empresarial cambiante	P		S
	9. Toma de decisiones estratégicas basadas en información	P	P	P
	10. Optimización de costos de provisión del servicio	P		P
Interno	11. Optimización de la funcionalidad de procesos del negocio	P		P
	12. Optimización de costos de procesos del negocio	P		P
	13. Programas de cambios del negocio gestionados	P	P	S
	14. Productividad operativa y del personal	P		P
	15. Cumplimiento con las políticas internas		P	
Aprendizaje y crecimiento	16. Personas calificadas y motivadas	S	P	P
	17. Cultura de innovación de productos y negocios	P		

Fuente: *COBIT® 5 (el marco)*, ISACA, EE.UU., 2012, figura 5

Criterios ampliados del cuadro de mando (balanced scorecard)

Una variante del enfoque descrito en los párrafos anteriores va un paso más allá, vinculando las dimensiones BSC a un conjunto limitado de criterios más tangibles. Con frecuencia se utilizan los siguientes criterios para este propósito:

- **Financiero**
  - Valor accionario
  - Ganancias
  - Ingresos
  - Costo de capital
- **Cliente**
  - Participación de mercado
  - Satisfacción del cliente
  - Servicio al cliente
- **Interno**
  - Cumplimiento regulatorio
- **Crecimiento**
  - Ventaja competitiva
  - Reputación

Este conjunto de criterios se puede utilizar selectivamente, y el usuario debe ser consciente de que aún se incluyen relaciones de causa-efecto en esta tabla (p. ej., la [in]satisfacción del cliente puede afectar la ventaja competitiva y/o la participación de mercado). Por lo general, un subconjunto de estos criterios se utiliza para expresar el riesgo en términos de negocio.

Las 4 A de Westerman: Un enfoque alternativo para expresar el impacto en el negocio[7]

Otro medio de expresar el riesgo de TI en términos comerciales se basa en el marco 4A. Esto define el riesgo de TI como el potencial de que un evento no planeado que involucra a las TI amenace cualquiera de los cuatro objetivos empresariales interrelacionados:

- **Agilidad** (Agility): Poseer la capacidad de cambiar gestionando los costes y la velocidad.
- **Precisión** (Accuracy): Proporcionar información correcta, oportuna y completa que cumpla con los requerimientos de la gerencia, personal, clientes, proveedores y reguladores.
- **Acceso** (Access): Asegurar el acceso adecuado a los datos y sistemas para que las personas adecuadas tengan el acceso que necesitan, y no lo tengan las personas equivocadas.
- **Disponibilidad** (Availability): Mantener los sistemas (y sus procesos de negocio) en operación y recuperarse de las interrupciones.

[7] Westerman, G.; Hunter R., *IT Risk—Turning Business Threats Into Competitive Advantage*, Harvard Business School Press, EE.UU., 2007

COSO ERM

El marco integrado del Comité de Organizaciones Patrocinadoras de la Comisión Treadway para la Gestión del Riesgo Empresarial (COSO ERM) enumera los siguientes criterios para expresar el impacto en el negocio:[8]

- **Estratégicos**: Metas de alto nivel, alineadas con, y apoyando la misión de la empresa. Los objetivos estratégicos reflejan la elección de la gerencia en cuanto a cómo la empresa tratará de crear valor para sus accionistas.
- **Operaciones**: Estos se refieren a la eficacia y la eficiencia de las operaciones de la empresa, incluyendo las metas de rendimiento y rentabilidad, y la protección de los recursos contra la pérdida.
- **Informes**: Estos se refieren a la fiabilidad de los informes. Incluyen informes internos y externos y pueden incluir información financiera y no financiera.
- **Cumplimiento**: Estos se refieren a la adhesión a las leyes y regulaciones relevantes.

FAIR (Análisis Factorial del Riesgo de la Información)[9]

El método FAIR está originalmente orientado a la seguridad, pero los criterios de impacto se aplican a todo el riesgo relacionado con TI. Los criterios utilizados son:

- **Productividad**: La reducción en la capacidad de una empresa para generar su propuesta de valor primaria (p. ej., ingresos, bienes, servicios)
- **Respuestas**: Gastos relacionados con la gestión de un evento de pérdida (p. ej., horas-persona internas o externas, gastos logísticos)
- **Reemplazo**: El valor intrínseco de un activo, típicamente representado como el gasto de capital asociado con el reemplazo de activos perdidos o dañados
- **Ventaja competitiva**: Pérdidas asociadas con la ventaja competitiva disminuida
- **Legal**: Medidas legales o regulatorias impuestas a una empresa
- **Reputación**: Pérdidas asociadas con una percepción externa de que la propuesta de valor de una empresa se ha reducido o el liderazgo es incompetente, criminal o poco ético

Ejemplo de metas empresariales de COBIT 5

Debido a que hay múltiples opciones para expresar el riesgo de TI en términos comerciales, y no hay una opción correcta o incorrecta, uno debe elegir la opción que mejor se ajuste a la empresa, y complementar este esquema con una variedad de escalas para cuantificar el riesgo durante el análisis de riesgo.

El siguiente ejemplo muestra cómo se pueden utilizar las metas empresariales de COBIT 5 para lograr el vínculo entre el escenario de TI "atómico" y las metas empresariales, es decir, cómo este escenario puede poner en peligro una o varias metas empresariales:

- El impacto se expresa en términos relevantes para el negocio, usando las palabras de las "metas empresariales" utilizadas en COBIT 5. Por ejemplo, la empresa, que opera un negocio de viajes en línea, tiene como principales metas empresariales: "Cultura de servicio orientada al cliente" y continuidad y disponibilidad del servicio del negocio.
- El marco COBIT 5 conecta en cascada las metas empresariales a las metas relacionadas con TI (cómo las metas del departamento de TI apoyan el logro de las metas empresariales), y este enlace también puede leerse en la otra dirección: El no alcanzar una meta relacionada con TI podría tener un impacto negativo en el logro de una meta empresarial. En el ejemplo, la meta empresarial de "continuidad y disponibilidad de los servicios del negocio" implica que el área de TI da importancia a algunas metas específicas relacionadas con las TI, p. ej., la alineación de la estrategia de TI y del negocio, el riesgo gestionado del negocio relacionado con TI, la prestación de servicios de TI en línea con los requerimientos del negocio, el uso adecuado de aplicaciones, y las soluciones de información y tecnología.
- Esta cascada se continúa hasta el nivel de proceso de TI y el nivel de práctica de gestión de TI, utilizando el mismo principio de que no alcanzar una meta de "nivel inferior" pondrá en peligro el logro de la meta de "nivel superior". Las metas de TI establecidas en el ejemplo requerirían que una serie de procesos de TI sean excelentes, incluyendo los procesos de COBIT 5 APO09 *Gestionar acuerdos de servicio*, APO11 *Gestionar la calidad,* BAI02 *Gestionar la definición de requerimientos*, BAI04 *Gestionar la disponibilidad y capacidad* y algunos otros. Esto requeriría que las actividades (como se describe en el modelo de proceso para cada proceso TI de COBIT 5) fueran bien ejecutadas.
- Al analizar los escenarios de riesgo relacionados con TI, cada escenario puede vincularse a uno o más procesos de TI, p. ej., si el proceso no funciona, la frecuencia y/o el impacto del escenario aumentará (consulte también Factores de Riesgo de Capacidad en la sección Factor de Riesgos). Aplicando esta cascada hacia atrás, es posible rastrear todos los caminos de impacto potenciales que un evento puede tener sobre las metas del negocio, y utilizar esta información en análisis de riesgos. En el ejemplo, esto significa que cualquier interrupción de los procesos de TI mencionados, p. ej., falta de gestión de proyectos (BAI01), pruebas de software inadecuadas (BAI06), gestión de relaciones con terceros o gestión de nivel de servicio deficientes (APO09 y APO10), pueden tener un impacto negativo en el logro de las metas empresariales orientadas a los servicios. Sin embargo, cuando estos procesos son realmente maduros y se están ejecutando, esto significa que la empresa está en buena forma para lograr las metas empresariales indicadas.

[8] Adaptado del Comité de Organizaciones Patrocinadoras de la Comisión Treadway; *COSO Enterprise Risk Management Framework*, EE.UU., 2004, *www.coso.org*
[9] Jones, Jack A., An Introduction to Factor Analysis of Information Risk (FAIR), Risk Management Insight LLC, 2005

Expresión de la frecuencia

Algunos métodos de gestión de riesgos usan los términos "probabilidad" o "frecuencia". En *Escenarios de Riesgo Utilizando COBIT 5 para Riesgos*, se prefiere el término "probabilidad", indicando una medida cuantitativa como un porcentaje, frecuencia de ocurrencia u otra métrica numérica.

La **figura 16** propone un esquema que puede utilizarse para expresar la probabilidad que se produzcan los escenarios de riesgo. El ejemplo utiliza una escala de 0 a 5, con un umbral de probabilidad asociado con cada valor de escala. En el ejemplo, se ha utilizado una escala logarítmica para la probabilidad aunque, en muchos casos, esto no es obligatorio; también se pueden utilizar las escalas lineales. Alternativamente, se puede usar una escala de índice. La probabilidad se traduce entonces a un número de 0 a 100, p. ej., basándose en una escala logarítmica o cualquier otro tipo de escala. La elección de uno de los dos métodos depende de cómo se presentarán los resultados del análisis de riesgos,
p. ej., en una matriz de riesgo. En la **figura 16**, un escenario de riesgo que se estima que ocurra cinco veces en un año obtiene la puntuación de 3.

Figura 16: Clasificación de probabilidad

Clasificación de frecuencia	Veces que ocurre por año
5	100
4	10
3	1
2	0.1
1	0.01
0	0.001

Fuente: *Guía del Practicante para Riesgos de TI*, ISACA, EE.UU., 2009, figura 25

Algunas empresas prefieren una escala de tres niveles en lugar de una de cinco niveles. La ventaja de tal escala es que los análisis irán más rápido y podrían parecer un poco más fáciles; sin embargo, hay una pérdida de precisión, y el uso de una escala de tres niveles tiene una tendencia a crear una gran cantidad de valores "medios" debido a que la gente intenta evitar la creación de casos extremos, lo que lleva a más imprecisiones.

Algunas empresas asignan etiquetas, p. ej., "muy frecuente", "frecuente", "poco frecuente", "raro", a las escalas mencionadas en la **figura 16**. No se recomienda el uso sólo de estas etiquetas como medio para expresar la frecuencia porque pueden significar cosas diferentes para diferentes escenarios de riesgo, y en consecuencia, pueden generar confusión. Por ejemplo, un intento de intrusión a la red a través del cortafuegos (firewall) puede ocurrir cientos de veces al día, lo que puede considerarse "promedio"; una frecuencia "promedio" de un falla de hardware (p. ej., falla del disco) puede ser una vez cada dos o tres años. Entonces, la palabra "promedio" significa diferentes frecuencias para dos escenarios diferentes; por lo tanto, no es muy adecuado como un indicador objetivo y sin ambigüedad de la frecuencia.

Escenarios de riesgo en respuesta al riesgo (reducción)

Flujo de trabajo de la respuesta al riesgo y opciones de respuesta al riesgo

El propósito de definir una respuesta al riesgo es alinear el riesgo con el apetito al riesgo definido para la empresa. En otras palabras, es necesario definir una respuesta de manera que la mayor cantidad de riesgo residual futuro (riesgo actual con la respuesta al riesgo definida e implementada) como sea posible (normalmente dependiendo de los presupuestos disponibles) caiga dentro de los límites de tolerancia al riesgo. El flujo de trabajo de respuesta al riesgo completo se representa en la **figura 17**.

Esta evaluación de la respuesta al riesgo no es un esfuerzo único, sino que es parte del ciclo del proceso de gestión de riesgos. Se requiere una respuesta cuando el análisis de riesgo de todos los escenarios de riesgo identificados, después de ponderar el riesgo frente a la rentabilidad potencial, ha demostrado que el riesgo no está alineado con los niveles definidos de apetito y tolerancia y al riesgo. Esta respuesta puede ser cualquiera de las cuatro respuestas posibles explicadas en las subsecciones siguientes.

Evitación del riesgo

Evitación significa abandonar las actividades o condiciones que dan lugar al riesgo. La evitación de riesgos se aplica cuando no hay otra respuesta al riesgo adecuada. Este es el caso cuando:

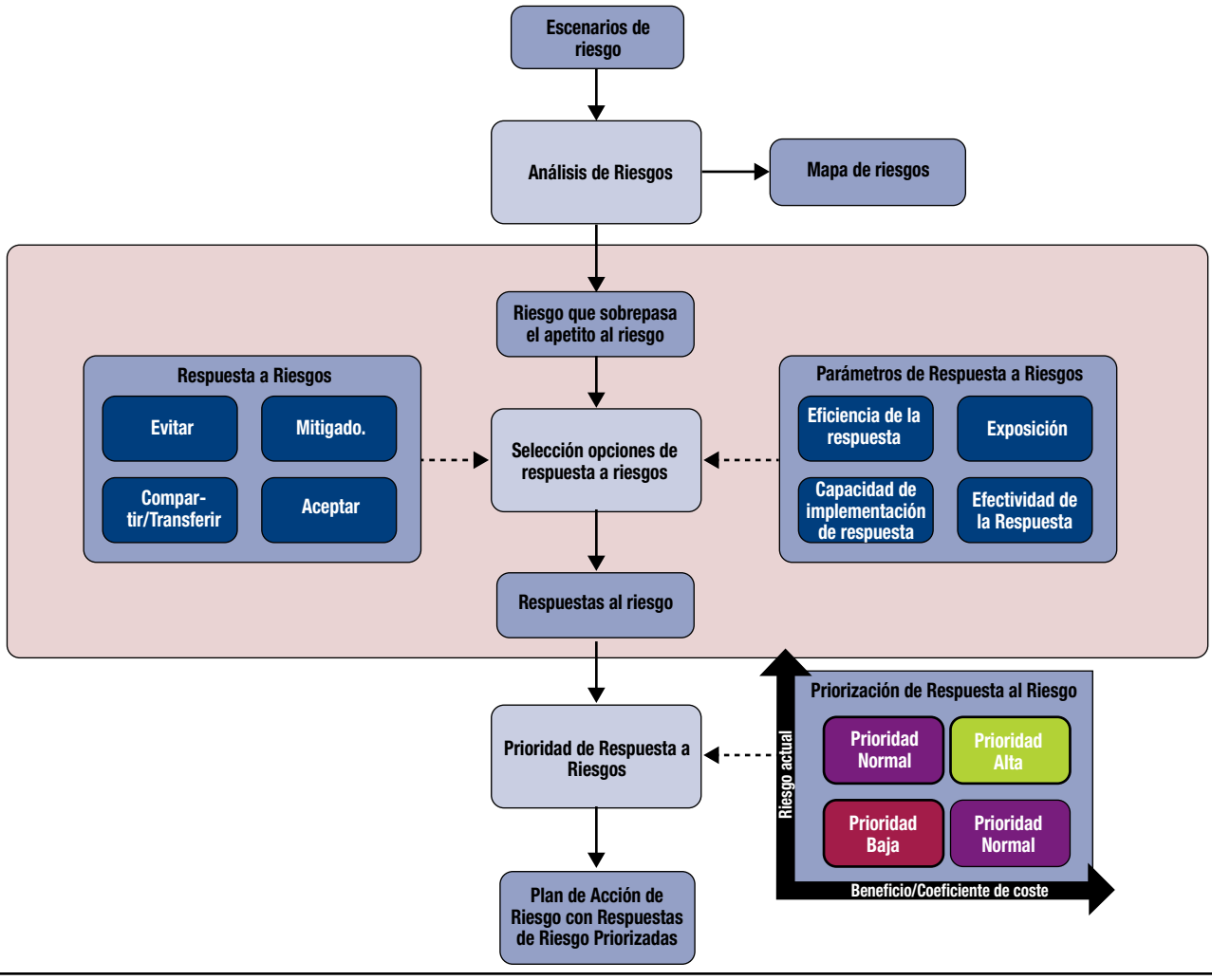
- No hay otra respuesta rentable que pueda lograr reducir la frecuencia y el impacto por debajo de los umbrales definidos para el apetito de riesgo.
- El riesgo no se puede compartir o transferir.
- La gerencia considera que el nivel de exposición es inaceptable.

Algunos ejemplos de evitación del riesgo relacionados con TI pueden incluir:

- Reubicar un centro de datos lejos de una región con peligros naturales significativos.
- Negarse a participar en un proyecto muy grande cuando el caso de negocio muestra un notable riesgo de fracaso.
- Negarse a participar en un proyecto que se basaría en sistemas obsoletos y complicados porque no hay grado aceptable de confianza que

el proyecto proporcionará algo viable.
• Negarse a utilizar una determinada tecnología o paquete de software porque impediría la expansión futura.

Figura 17: Flujo de trabajo de respuesta al riesgo



Fuente: *COBIT® 5 para Riesgos*, ISACA, EE.UU., 2013, figura 42

Aceptación de riesgo

Aceptación significa que se reconoce la exposición a pérdidas, pero no se toma ninguna medida relativa a un riesgo en particular, y la pérdida se acepta cuando/si ocurre. Esto es diferente de ser ignorante del riesgo; aceptar el riesgo asume que el riesgo es conocido, es decir, la gerencia ha tomado una decisión informada para aceptarlo como tal (p. ej., cuando el costo de la remediación supera el riesgo).

Si una empresa adopta una postura de aceptación de riesgo, debería considerarse cuidadosamente quién puede aceptar el riesgo, aún más con el riesgo de TI. El riesgo de TI debe ser aceptado sólo por la gerencia del negocio (y los propietarios del proceso de negocio), en colaboración con y respaldado por TI, y la aceptación debería ser comunicada (p.e. documentada) a la alta gerencia y al consejo (consulte las actividades detalladas 5.3 y 5.4 en la sección EDM3.02).

Algunos ejemplos de aceptación del riesgo pueden incluir:
• Puede haber un riesgo de que un determinado proyecto no ofrezca la funcionalidad comercial requerida en la fecha de entrega planificada. La gerencia puede decidir aceptar el riesgo y proceder con el proyecto.
• Si se considera que un riesgo en particular es muy poco común, pero muy importante (catastrófico) y los enfoques para reducirlo son prohibitivos, la gerencia puede decidir aceptarlo.

El seguro propio es otra forma de aceptación del riesgo, aunque esto solo gestiona la magnitud de la pérdida y no tiene impacto en la frecuencia.

Compartir/transferir el riesgo

Compartir significa reducir la frecuencia o el impacto del riesgo al transferir o compartir una parte del riesgo. Las técnicas comunes incluyen el seguro y el outsourcing. Los ejemplos incluyen la contratación de cobertura de seguros para incidentes relacionados con TI, el outsourcing de parte de las actividades de TI, o compartir el riesgo de proyectos de TI con el proveedor a través de arreglos a precio fijo o acuerdos de inversión compartida. En un sentido físico y legal, estas técnicas no eximen a una empresa de la propiedad del riesgo, pero pueden involucrar las habilidades de otra parte para la gestión del riesgo y reducir las consecuencias financieras si ocurre un evento adverso. También desde el punto de vista de la reputación, la transferencia o el intercambio de riesgos no transfiere la propiedad ni la responsabilidad sobre el riesgo.

Algunos ejemplos de compartir y transferir el riesgo relacionados con TI pueden incluir:

- Una gran organización identificó y evaluó el riesgo de incendio de su infraestructura en diversas regiones geográficas, y evaluó el costo de compartir el impacto de su riesgo a través de la cobertura de seguros. Concluyó que, debido a la ubicación de sus sitios, el costo incremental de los seguros y deducibles relacionados no era prohibitivo, y se contrató la cobertura de seguro.
- En una importante inversión relacionada con TI, el riesgo del proyecto puede ser compartido al subcontratar el desarrollo por un precio fijo basado en el riesgo/beneficio.
- Algunas empresas subcontratan parte o la totalidad de su función de TI a empresas de hosting, y contractualmente comparten una parte del riesgo.
- Cuando el hosting de aplicaciones es subcontratado, la organización siempre es responsable de proteger la privacidad del cliente, pero si el subcontratista es negligente y se produce una filtración, el riesgo (impacto financiero) se puede al menos compartir con el subcontratista.

Otras técnicas que contribuyen al riesgo compartido incluyen:

- Grandes empresas con múltiples entidades jurídicas, donde el riesgo de TI se puede transferir a otras divisiones dentro de la empresa (el reaseguro es un ejemplo común).
- El reporte de la Declaración de Estándares para Acuerdos de Atestación No. 16 (SSAE16), que permite a una organización de servicios transferir una parte de un riesgo al cliente a través de la sección de consideraciones de controles del usuario del reporte.

Mitigación del riesgo

Mitigación del riesgo significa que se toman medidas de mitigación para reducir la frecuencia y/o el impacto de un riesgo. Las maneras más comunes de mitigar el riesgo son:

- Fortalecer las prácticas generales de gestión de riesgos de TI, es decir, implementar procesos de gestión de riesgos de TI lo suficientemente maduros según lo definido por el marco COBIT 5.
- Introducción de una serie de medidas de control destinadas a reducir ya sea la frecuencia de un acontecimiento adverso y/o el impacto en el negocio de un evento, en caso de que suceda. Los controles se emplean, en el contexto de gestión de riesgos, para mitigar un riesgo, p. ej., políticas, procedimientos y prácticas, estructuras, flujos de información, etc. El conjunto de habilitadores interconectados de COBIT 5 proporciona un conjunto completo de controles que se pueden implementar. Es posible identificar, para cualquier escenario de riesgo que supere el apetito de riesgo, un conjunto de habilitadores de COBIT 5 (procesos, estructuras organizacionales, conductas, etc.) que puedan mitigar el escenario de riesgo. Consulte el Capítulo 5 para ver una lista completa de controles (expresados como habilitadores de COBIT 5) que pueden mitigar el riesgo (lista de ejemplos de escenarios de riesgo genéricos como se define en el Capítulo 4).
- La mitigación del riesgo es posible por otros medios o métodos, p. ej., hay marcos de gestión de TI bien conocidos y estándares que pueden ayudar.

Capítulo 7
Ejemplos de Análisis de Escenarios de Riesgo

Este capítulo contiene 60 ejemplos detallados de análisis de escenarios de riesgo que se han preparado utilizando las categorías de escenarios de riesgo genérico y los posibles resultados descritos en la **figura 14** del Capítulo 4. La plantilla descrita en el Capítulo 6 se ha utilizado para realizar el análisis de cada escenario de riesgo, y la lista de habilitadores de COBIT 5 descrita en el Capítulo 5 se ha utilizado para completar la sección de mitigación de riesgo.

¿Cómo leer el análisis de escenarios de riesgo?

Título del escenario de riesgo - Este es el nombre único y específico del ejemplo de análisis de escenarios de riesgo.
Categoría del escenario de riesgo - Esta es una referencia a una de las 20 categorías de escenarios de riesgo descritas en la **figura 14**, Capítulo 4.
Referencia del escenario de riesgo[12] - Esta sección es un número compuesto por el número de categoría del escenario de riesgo, y el número de referencia del escenario de riesgo. Por ejemplo, la Referencia del Escenario de Riesgo 0101 indica que este análisis particular se aplica a:

Categoría del escenario del riesgo 01	Referencia del escenario del riesgo 0101*	
"Establecimiento y mantenimiento de la cartera"	"Los programas erróneos son seleccionados para su implementación y están desalineados con la estrategia y las prioridades corporativas." (Resultado negativo)	"Los programas conducen a nuevas y exitosas iniciativas del negocio seleccionadas para su ejecución." (Resultado positivo)

* Tenga en cuenta que no hay un ejemplo para cada referencia del escenario de riesgo dentro de una categoría de escenarios de riesgo, por lo tanto, los números no son secuenciales.

Escenario del riesgo - Los ejemplos utilizados en esta sección son versiones exhaustivas de los escenarios de riesgo genéricos positivos o negativos descritos en la **figura 14**. Estos ejemplos se han preparado con mayor detalle para agregar contexto al escenario y ayudar a los profesionales de riesgo a explicar el riesgo en términos empresariales.
Componentes del escenario de riesgo - Esta sección proporciona ejemplos de la información necesaria para calcular el impacto y la frecuencia, y preparar posibles respuestas al riesgo (para obtener descripciones detalladas de las diferentes secciones del análisis de los escenarios de riesgo, consulte el Capítulo 6).
- Tipo de amenaza
- Agente
- Evento
- Activo/Recurso (causa)
- Activo/Recurso (efecto)
- Cuestiones de tiempo

Tipo de riesgo - Esto describe la relación entre el escenario de riesgo y los tres tipos de riesgo descritos en *COBIT 5 para Riesgo* y el Capítulo 2 de esta publicación (**figura 4**).
Posibles respuestas al riesgo - Estos son ejemplos de respuestas de riesgo que pueden usarse para abordar el escenario de riesgo.
Mitigación del riesgo usando los habilitadores de COBIT 5 - Esta sección ofrece una lista de habilitadores que se pueden utilizar para mitigar del impacto o la frecuencia de los riesgos.
Indicadores clave del riesgo - Esta sección ofrece una lista de indicadores clave del riesgo (KRI) que han sido definidos para las metas de TI que pueden ser impactados por el escenario de riesgo, así como los KRI definidos para el habilitador de procesos incluido en la sección de mitigación de riesgos. (La lista completa de KRI para las metas de TI se puede encontrar en el marco de COBIT 5, y la lista completa de KRI para el habilitador de procesos se puede encontrar en *COBIT 5: Procesos habilitadores*.)

[12] La referencia del escenario de riesgo se utiliza en los ejemplos proporcionados en esta publicación, pero no se incluye en la plantilla. Si es necesario, la persona que prepara el análisis del escenario de riesgo puede incluir esta sección para especificar la categoría y referencia del escenario de riesgo.

01 Establecimiento y mantenimiento de la cartera

0101 Los programas seleccionados no optimizan los beneficios del negocio

Título del escenario de riesgo	Los programas seleccionados no optimizan los beneficios del negocio	
Categoría del escenario de riesgo	01 Establecimiento y mantenimiento de la cartera	
Referencia del escenario de riesgo	0101	
Escenario de riesgo La persona responsable de la selección de los programas (director general ejecutivo [CEO]) tomó una decisión cuestionable al seleccionar los programas a financiar. La decisión fue influenciada por información poco clara y sesgada que fue proporcionada por una de las principales partes interesadas y los auditores internos y externos, quienes se centraron en fomentar controles de seguridad y formalizar los procesos, en lugar de apoyar el crecimiento empresarial.		
Componentes del escenario de riesgo		
Tipo de amenaza La naturaleza del evento es un **fallo** en el proceso de toma de decisiones al tener en cuenta todos los requerimientos de las partes interesadas y una priorización ineficaz de estos requisitos.		
Agente El agente que genera la amenaza que explota una vulnerabilidad es **interno**, el CEO.		
Evento El evento es la **ejecución ineficaz** del proceso de selección del programa.		
Activo/Recurso (causa) El recurso que conduce al impacto en el negocio es el **proceso** de selección del programa.		
Activo/Recurso (efecto) Los recursos afectados son varios **procesos de negocio.**		
Tiempo La duración del evento es **extensa** debido a la falta de apoyo al crecimiento empresarial. El momento de la ocurrencia es **no crítico**. El evento no se puede detectar inmediatamente y, por lo tanto, la detección es **lenta**. La consecuencia es **demorada** porque los programas seleccionados se implementarán a durante un extenso período de tiempo.		
Tipo de riesgo		
Habilitación del beneficio/valor de TI	**P**	La asignación de prioridades conduce a la asignación de recursos para fortalecer la seguridad de los sistemas existentes, y los recursos clave no están disponibles para desarrollar nuevos servicios que apoyen el crecimiento empresarial. En consecuencia, no se inician nuevas iniciativas del negocio.
Entrega del proyecto y programa de TI	**P**	Los proyectos en curso deben ser reprogramados debido a la falta de recursos.
Entrega del servicio y operaciones de TI	**S**	Se están abordando los problemas de seguridad de los servicios (no importantes).
Posibles respuestas al riesgo		
• **Evasión del riesgo:** N/A • **Aceptación del riesgo:** El CEO es consciente de la desalineación y acepta los impactos. • **Compartir/transferir el riesgo:** La empresa solicita a los proveedores de servicios externos que reevalúen los contratos y ajusten los plazos y los recursos sin costo adicional. • **Mitigación del riesgo:** Repriorización de los proyectos en curso para optimizar los beneficios empresariales.		

Mitigación del Riesgo Usando Habilitadores de COBIT 5					
Habilitador de principios, políticas y marco de trabajo					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Política de gestión de programas/proyectos	Hacer cumplir de la metodología general del programa/proyecto, incluyendo la política corporativa sobre el caso de negocio o la debida diligencia para mejorar la visibilidad del valor relativo de los programas (comparados entre sí). Esta política debe describir la aprobación de los umbrales de inversión para el valor del programa.		Alto	Medio	SÍ
Habilitador del proceso					
Referencia	**Título**	**Prácticas de gobierno y gestión**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
EDM01.01	Evaluar el sistema de gobierno.	Identificar e involucrarse continuamente con las partes interesadas de la empresa, documentar una comprensión de los requisitos y hacer un juicio sobre el diseño actual y futuro del gobierno de TI empresarial.	Alto	Alto	SÍ
EDM01.02	Orientar el sistema de gobierno.	Informar a los líderes y obtener su apoyo, aprobación y compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de TI en línea con los principios de diseño de gobierno acordados, los modelos de toma de decisiones y los niveles de autoridad. Definir la información requerida para la adecuada toma de decisiones.	Alto	Alto	SÍ
EDM01.03	Monitorizar el sistema de gobierno.	Monitorizar la efectividad y el desempeño del gobierno de TI de la empresa. Evaluar si el sistema de gobierno y los mecanismos implementados (incluyendo las estructuras, los principios y los procesos) están operando de forma efectiva y ofrecen una supervisión apropiada de TI.	Alto	Alto	SÍ
EDM02.01	Evaluar la optimización del valor.	Evaluar continuamente la cartera de inversiones, servicios y activos habilitados por TI con el fin de determinar la probabilidad de alcanzar el objetivo de la empresa y entregar valor a un costo razonable. Identificar y hacer un juicio sobre cualquier cambio en la dirección que debe ofrecerse a la gerencia para optimizar la creación de valor.	Alto	Alto	SÍ
EDM02.02	Dirigir la optimización del valor.	Dirigir los principios y las prácticas de gestión de valor para permitir una obtención óptima de valor con las inversiones habilitadas para TI durante todo su ciclo de vida económico.	Alto	Alto	SÍ
EDM02.03	Monitorizar la optimización del valor.	Monitorizar las metas y métricas clave para determinar la medida en que el negocio está generando el valor y los beneficios esperados para el negocio a través de las inversiones y los servicios habilitados por TI. Identificar problemas significativos y considerar acciones correctivas.	Alto	Alto	SÍ
APO05.01	Establecer el objetivo de la mezcla de inversión.	Revisar y asegurarse que las estrategias y los servicios actuales de la empresa y de TI sean claros. Definir una mezcla de inversión apropiada con base en el costo, la alineación con la estrategia, y las medidas financieras como el costo y el retorno de la inversión (ROI) anticipado durante todo el ciclo de vida económico, el grado de riesgo y el tipo o beneficio para los programas en la cartera. Ajustar las estrategias empresariales y de TI cuando sea necesario.	Medio	Medio	NO
APO05.03	Evaluar y seleccionar programas para financiar.	Basándose en los requerimientos generales de la mezcla de la cartera de inversión, evaluar y establecer prioridades de los casos de negocio del programa, y tomar decisiones sobre las propuestas de inversión. Asignar fondos e iniciar los programas.	Medio	Medio	NO
APO05.04	Monitorizar, optimizar e informar sobre el rendimiento de la cartera de inversión.	Monitorizar y optimizar de forma periódica el rendimiento de la cartera de inversión y los programas individuales durante todo el ciclo de vida de las inversiones.	Medio	Medio	NO

Habilitador del proceso *(cont.)*					
Referencia	**Título**	**Prácticas de gobierno y gestión**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
APO05.05	Mantener las carteras.	Mantener las carteras de los programas y proyectos de inversión, servicios de TI y activos de TI.	Medio	Medio	NO
APO05.06	Gestionar el logro de beneficios.	Monitorizar los beneficios de ofrecer y mantener servicios y capacidades de TI apropiados, con base en el caso de negocio acordado y actual.	Medio	Medio	NO
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director de Finanzas (CFO)	Ayuda con la alineación de la estrategia y las prioridades, y la visión general sobre los programas.		Alto	Medio	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La selección de programas incluye decisiones basadas en datos	Las decisiones deben ser objetivas, no sesgadas y basadas en información fundamentada.		Medio	Medio	NO
Participación de las partes interesadas	La gama completa de factores de éxito se tendrá en cuenta al seleccionar programas.		Alto	Medio	SÍ
Focalización en objetivos empresariales	Asegurar la alineación con la estrategia y las prioridades corporativas.		Alto	Medio	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Caso de negocio del programa	Mejora la visibilidad del valor relativo de los programas (comparados entre sí)		Alto	Medio	SÍ
Mezcla de inversión definida	Mejora la visibilidad del valor relativo de los programas (comparados entre sí).		Alto	Medio	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Herramientas de gestión de cartera	Disminuye la complejidad y aumenta la visión general de los programas y proyectos.		Medio	Bajo	NO
Habilitador de personas, habilidades y competencias					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Análisis de requerimientos del negocio	Transparencia en la estrategia empresarial, requerimientos del negocio relacionados y prioridades.		Alto	Medio	SÍ

Indicadores clave del riesgo (KRIs) relacionados con las metas de TI

- *(01) Nivel de satisfacción de las partes interesadas con el alcance de la cartera de programas y servicios planificada*
- *(05) Porcentaje de inversiones habilitadas para TI en las que se supervisa el logro de beneficios durante todo el ciclo de vida económico*
- *(05) Porcentaje de inversiones habilitadas para TI en las que los beneficios afirmados se cumplen o exceden*
- *(06) Porcentaje de casos de negocio de inversión con costos y beneficios, esperados y relacionados con TI, claramente definidos y aprobados*
- *(06) Encuesta de satisfacción de las partes clave interesadas con respecto al nivel de transparencia, comprensión y precisión de la información financiera de TI*
- *(07) Porcentaje de partes interesadas del negocio satisfechas con el cumplimiento de los niveles de servicio acordados en la prestación de servicios de TI*
- *(13) Número de programas que necesitan reelaboración significativa debido a defectos de calidad*
- *(17) Nivel de conocimiento y comprensión de los ejecutivos de negocios sobre las posibilidades de innovación en TI*

Indicadores clave del riesgo (KRIs) relacionados con las metas del proceso

- *(EDM01) Nivel de satisfacción de las partes interesadas (medida a través de encuestas)*
- *(EDM02) Nivel de satisfacción de las partes interesadas con la capacidad de la empresa para obtener valor de las iniciativas habilitadas por TI*
- *(EDM02) Porcentaje de iniciativas de TI en la cartera general donde el valor se administra durante todo el ciclo de vida*
- *(EDM02) Nivel de satisfacción de las partes interesadas con el avance hacia los objetivos identificados, con entrega de valor basada en encuestas*
- *(EDM02) Porcentaje logrado del valor esperado*
- *(APO05) Porcentaje de inversiones de TI que tienen trazabilidad en la estrategia empresarial*
- *(APO05) Grado de satisfacción con la contribución de TI a la estrategia empresarial por parte de la gerencia empresarial*
- *(APO05) Porcentaje de inversiones donde los beneficios logrados se han medido y comparado con el caso de negocio*

0103 Incompatibilidad de sistemas empresariales

Título del escenario de riesgo	Incompatibilidad de sistemas empresariales
Categoría del escenario de riesgo	01 Establecimiento y mantenimiento de la cartera
Referencia del escenario de riesgo	0103

Escenario de riesgo
En un hospital, el jefe del departamento de radiología decidió comprar un determinado sistema de rayos X a un proveedor sin consultar a otros departamentos o TI. Los jefes de departamento pueden decidir sobre los equipos/programas necesarios, y con frecuencia, toman estas decisiones sin considerar la arquitectura empresarial (EA). A medida que el nuevo sistema interactúa con otros sistemas de la empresa (p. ej., expedientes de pacientes, medicamentos), no se puede realizar un intercambio automatizado de información para mantener actualizados los expedientes de pacientes.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** en los procesos BAI03 *Gestionar la identificación y desarrollo de soluciones* y APO03 *Gestionar la arquitectura empresarial.*

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **interno**, el jefe del departamento de radiología (propietario del proceso empresarial).

Evento
El evento es un **diseño ineficaz**, y respectivamente, una **ejecución ineficaz** de los procesos BAI03 *Gestionar la identificación y desarrollo de soluciones* y APO03 *Gestionar la arquitectura empresarial.*

Activo/Recurso (causa)
Los recursos que conducen al impacto en el negocio son los **procesos** BAI03 *Gestionar la identificación y desarrollo de soluciones* y APO03 *Gestionar la arquitectura empresarial* y las **estructuras organizacionales** porque el jefe del departamento no considera la **información** como un recurso causado por la falta de un modelo de toma de decisiones.

Activo/Recurso (efecto)
El activo afectado es **información**. El sistema adquirido será potencialmente incompatible con otros sistemas hospitalarios, y por lo tanto, no puede compartir información con otros sistemas. Los expedientes de pacientes pueden no estar actualizados (precisión de la integridad de la información y falta de representación consistente).

Tiempo
La duración del evento es **extensa** debido a la inconsistencia en la presentación de los expedientes de pacientes. El momento de la ocurrencia es **no crítico**. La detección será **instantánea** porque la empresa reconocerá inmediatamente la falta de representación consistente. La consecuencia es **demorada** porque el evento necesita análisis y cambios apropiados en el sistema para hacerlo compatible con los sistemas/la arquitectura existentes.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**P**	La eficiencia de las operaciones hospitalarias se reduce y afecta a los pacientes (p. ej., no reutilización de imágenes de rayos X y retraso en los tratamientos).
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	La información no se puede intercambiar automáticamente entre los sistemas, lo que conduce a necesidades de recursos no satisfechas y a registros inconsistentes.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** El CEO y el jefe de radiología aceptan el sistema no alineado y los recursos adicionales requeridos para actualizar los sistemas incompatibles.
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Aclaración sobre los derechos de toma de decisiones para el sistema de compras, la creación de interfaces (automatizadas) y el fomento de los principios de arquitectura empresarial (p. ej., estándares mínimos para la interoperabilidad del sistema).

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de gestión de programas/proyectos	Imponer el uso de la metodología general del programa/proyecto, incluyendo la política corporativa sobre el caso de negocio o la debida diligencia para mejorar la visibilidad del valor relativo de los programas (comparados entre sí). Esta política debe describir los umbrales de inversión de aprobación para el valor del programa.	Medio	Medio	NO

Habilitador del proceso					
Referencia	**Título**	**Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
EDM01.01	Evaluar el sistema de gobierno.	Identificar e involucrarse continuamente con las partes interesadas de la empresa, documentar una comprensión de los requisitos y hacer un juicio sobre el diseño actual y futuro del gobierno de TI empresarial.	Medio	Medio	NO
EDM01.02	Orientar el sistema de gobierno.	Informar a los líderes y obtener su apoyo, aprobación y compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de TI en línea con los principios de diseño de gobierno acordados, los modelos de toma de decisiones y los niveles de autoridad. Definir la información requerida para la toma de decisiones adecuadas.	Medio	Medio	NO
EDM01.03	Monitorizar el sistema de gobierno.	Monitorizar la efectividad y el desempeño del gobierno de TI de la empresa. Evaluar si el sistema de gobierno y los mecanismos implementados (incluyendo las estructuras, los principios y los procesos) están operando de forma efectiva y ofrecen una supervisión apropiada de TI.	Medio	Medio	NO
APO05.01	Establecer el objetivo de la mezcla de inversión.	Revisar y asegurarse que las estrategias y los servicios actuales de la empresa y de TI sean claros. Definir una mezcla de inversión apropiada con base al costo, la alineación con la estrategia, y las medidas financieras como el costo y el retorno de la inversión (ROI) anticipado durante todo el ciclo de vida económico, el grado de riesgo y el tipo de beneficio para los programas en la cartera. Ajustar las estrategias empresariales y de TI cuando sea necesario.	Medio	Medio	NO
APO05.03	Evaluar y seleccionar programas para financiar.	Basándose en los requerimientos generales de la mezcla de la cartera de inversión, evaluar y establecer prioridades de los casos de negocio del programa, y tomar decisiones sobre las propuestas de inversión. Asignar fondos e iniciar los programas.	Alto	Alto	SÍ
APO05.04	Monitorizar, optimizar e informar sobre el rendimiento de la cartera de inversión.	Monitorizar y optimizar de forma periódica el rendimiento de la cartera de inversión y los programas individuales durante todo el ciclo de vida de las inversiones.	Medio	Medio	NO
APO05.05	Mantener las carteras.	Mantener las carteras de los programas y proyectos de inversión, servicios y activos de TI.	Medio	Medio	NO
APO05.06	Gestionar el logro de beneficios.	Monitorizar los beneficios de ofrecer y mantener servicios y capacidades de TI apropiados, con base en el caso de negocio acordado y actual.	Medio	Medio	NO
BAI03.04	Obtener los componentes de la solución.	Adquirir componentes de la solución basados en el plan de adquisiciones de acuerdo con los requerimientos y los diseños detallados, los principios y estándares de la arquitectura, y los procedimientos generales de adquisiciones y contratos de la empresa, requerimientos de aseguramiento de calidad (QA) y estándares de aprobación. Asegurarse de que el proveedor identifique y aborde todos los requerimientos legales y contractuales.	Alto	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Consejo de Dirección	Requerir la aprobación cuando los programas superan un cierto umbral de valor y un nivel de riesgo.		Medio	Medio	NO

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La selección de programas incluye decisiones basadas en datos	Las decisiones deben ser objetivas, no sesgadas y basadas en información fundamentada.	Alto	Medio	SÍ
Participación de las partes interesadas	La gama completa de factores de éxito se tendrá en cuenta al seleccionar programas.	Alto	Medio	SÍ
Enfoque en objetivos empresariales	Asegurar la alineación con la estrategia y las prioridades corporativas.	Alto	Medio	SÍ
Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Análisis de requerimientos del negocio	Transparencia en la estrategia empresarial, requerimientos del negocio relacionados y prioridades.	Medio	Bajo	NO
Indicadores clave del riesgo (KRIs) relacionados con las metas de TI				
• *(01) Nivel de satisfacción de las partes interesadas con el alcance de la cartera de programas y servicios planificada* • *(01) Porcentaje de impulsores de valor de TI asignados a impulsores de valor empresariales* • *(03) Porcentaje de puestos de la dirección ejecutiva con responsabilidades de decisiones de TI claramente definidas* • *(03) Número de veces que TI está en la agenda del Consejo de Dirección de manera proactiva* • *(05) Porcentaje de inversiones habilitadas para TI en las que se supervisa el logro de beneficios durante todo el ciclo de vida económico* • *(05) Porcentaje de inversiones habilitadas para TI en las que los beneficios afirmados se cumplen o exceden* • *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI* • *(13) Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto* • *(13) Número de programas que necesitan reelaboración significativa debido a defectos de calidad* • *(17) Nivel de conocimiento y comprensión de los ejecutivos de negocios sobre las posibilidades de innovación en TI*			
Indicadores clave del riesgo (KRIs) relacionados con las metas del proceso				
• *(EDM01) Nivel de satisfacción de las partes interesadas (medida a través de encuestas)* • *(APO05) Grado en que la gerencia empresarial está satisfecha con la contribución de TI a la estrategia empresarial* • *(BAI03) Número de diseños de soluciones reelaborados debido a la desalineación con los requerimientos* • *(BAI03) Tiempo necesario para aprobar que el producto de diseño ha cumplido con los requerimientos* • *(BAI03) Número de errores encontrados durante la prueba* • *(BAI03) Número de demandas de mantenimiento que no se satisfacen*			

0104 Cultura desalineada

Título del escenario de riesgo	Cultura desalineada
Categoría del escenario de riesgo	01 Establecimiento y mantenimiento de la cartera
Referencia del escenario de riesgo	0104

Escenario de riesgo
En una empresa industrial, los recursos de TI clave se utilizan para operar y mantener el sistema de información financiera; no hay un enfoque en el mantenimiento de planificación de producción y sistemas de producción, lo que resulta en una división en la cultura del personal de TI. Una parte del departamento está enfocada en el sistema de información financiera, y es considerada como la parte beneficiosa y de finanzas/negocios; la otra parte es vista como los ingenieros. Para la parte de ingeniería del personal hay diferentes caminos profesionales, una falta de motivación y desconexión, lo que conduce a una menor productividad e innovación.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** en la priorización.

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **interno**, la función que es responsable de la asignación de recursos de TI es la función de Director de Finanzas (CFO). El CFO pone el sistema de información financiera en el centro de atención. Un agente secundario **interno** es el departamento de Recursos Humanos (RR.HH.), que no apoya la motivación del personal.

Evento
El evento es la **ejecución ineficaz** del proceso APO07 *Gestionar recursos humanos*.

Activo/Recurso (causa)
El recurso que conduce al impacto en el negocio es el *proceso* APO07 **Gestionar recursos humanos** porque la gerencia de RR.HH. no puede demostrar a los ingenieros el valor que aportan y porque hay una falta de integración de cultura y procesos.

Activo/Recurso (efecto)
Los recursos afectados son **personas y habilidades** porque la empresa está perdiendo conocimientos y personal.

Tiempo
La duración del evento es **extensa** porque el personal está desmotivado. El momento de la ocurrencia es **no crítico.** Debido a que la falta de conocimiento y el aumento de la fluctuación no se pueden detectar inmediatamente, la detección es **lenta**. La consecuencia es **demorada** porque la falta de personal y conocimientos se producirá en el futuro.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**P**	El potencial para la innovación no se utiliza porque los miembros del personal no están involucrados.
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Las inversiones en RR.HH. (conocimiento) son ineficaces cuando el personal deja la empresa; pueden ocurrir interrupciones de servicio y violaciones de seguridad debido al personal restante descontento; pueden ocurrir interrupciones en los servicios de TI debido al personal que se retira.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Comunicar el valor que los ingenieros aportan a la empresa y proporcionar recompensas y motivación individuales.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de gestión de programas/proyectos	Imponer el uso de la metodología general del programa/proyecto, incluyendo la política corporativa sobre el caso de negocio o la debida diligencia para mejorar la visibilidad del valor relativo de los programas (comparados entre sí). Esta política debe describir los umbrales de inversión de aprobación para el valor del programa.	Medio	Bajo	NO

Habilitador del proceso					
Referencia	**Título**	**Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
APO04.01	Crear un entorno favorable a la innovación.	Crear un entorno que propicie la innovación, considerando cuestiones como la cultura, las recompensas, la colaboración, los foros de tecnología y los mecanismos para promover y capturar las ideas de los empleados.	Bajo	Medio	NO
APO05.06	Gestionar el logro de beneficios.	Monitorizar los beneficios de ofrecer y mantener servicios y capacidades de TI apropiados, con base en el caso de negocio acordado y actual.	Medio	Alto	SÍ
APO07.01	Mantener una dotación de personal suficiente y adecuada.	Evaluar los requerimientos de personal de forma periódica o ante cambios mayores en los entornos empresariales, operativos o de TI para garantizar que la empresa cuente con suficientes recursos humanos para apoyar las metas y los objetivos empresariales. La dotación de personal incluye tanto los recursos internos como externos.	Alto	Alto	SÍ
APO07.03	Mantener las habilidades y las competencias del personal.	Definir y administrar las habilidades y las competencias del personal necesario. Verificar periódicamente que el personal cuente con las competencias necesarias para realizar sus funciones con base en su educación, capacitación y/o experiencia, y verificar que estas competencias se mantengan usando programas de cualificación y certificación cuando sea apropiado. Dar a los empleados oportunidades de aprendizaje continuas para mantener sus conocimientos, habilidades y competencias al nivel requerido para alcanzar las metas empresariales.	Alto	Bajo	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director de Finanzas (CFO)	Ayudar con la alineación de la estrategia y las prioridades, y la visión general sobre los programas.		Medio	Medio	NO
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La selección de programas incluye decisiones basadas en datos	Las decisiones deben ser objetivas, no sesgadas y basadas en información fundamentada.		Alto	Medio	SÍ
Participación de las partes interesadas	La gama completa de factores de éxito se tendrá en cuenta al seleccionar programas.		Alto	Medio	SÍ
Enfoque en objetivos empresariales	Asegurar la alineación con la estrategia y las prioridades corporativas.		Alto	Medio	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Caso de negocio del programa	Mejora la visibilidad del valor relativo de los programas (comparados entre sí).		Alto	Bajo	SÍ
Inversión mixta definida	Mejora la visibilidad del valor relativo de los programas (comparados entre sí).		Alto	Bajo	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				

Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Análisis de requerimientos del negocio	Transparencia en la estrategia empresarial, requerimientos del negocio relacionados y prioridades.	Alto	Medio	SÍ

Indicadores clave del riesgo (KRIs) relacionados con las metas de TI

- *(05) Porcentaje de servicios de TI donde se logran los beneficios esperados*
- *(08) Porcentaje de propietarios de procesos de negocio satisfechos con los productos y servicios de soporte de TI*
- *(08) Nivel de comprensión por parte del usuario empresarial de cómo las soluciones tecnológicas apoyan sus procesos*
- *(08) Valor presente neto (VPN) que muestra el nivel de satisfacción empresarial de la calidad y utilidad de las soluciones tecnológicas*
- *(09) Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de TI a los nuevos requerimientos*
- *(09) Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas*
- *(09) Tiempo promedio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada*
- *(11) Niveles de satisfacción de ejecutivos de negocios y TI con los costos y capacidades relacionados con TI*
- *(16) Porcentaje de personal cuyas habilidades relacionadas con TI son suficientes para la competencia requerida para su función*
- *(16) Porcentaje de personal satisfecho con sus funciones relacionadas con TI*
- *(16) Número de horas de aprendizaje/capacitación por cada miembro del personal*
- *(17) Nivel de conocimiento y comprensión de los ejecutivos de negocios sobre las posibilidades de innovación en TI*
- *(17) Nivel de satisfacción de las partes interesadas con los niveles de conocimientos e ideas sobre innovación en TI*
- *(17) Número de iniciativas aprobadas como resultado de ideas innovadoras de TI*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(APO04) Aumento de la participación de mercado o competitividad debido a innovaciones*
- *(APO04) Percepciones y retroalimentación de las partes interesadas de la empresa respecto a la innovación en TI*
- *(APO04) Porcentaje de iniciativas implementadas con un claro vínculo a un objetivo empresarial*
- *(APO04) Inclusión de objetivos relacionados con la innovación o tecnología emergente en las metas de rendimiento para el personal relevante*
- *(APO04) Retroalimentación y encuestas de las partes interesadas*
- *(APO05) Porcentaje de inversiones de TI que tienen trazabilidad a la estrategia empresarial*
- *(APO05) Grado en que la gerencia empresarial está satisfecha con la contribución de TI a la estrategia empresarial*
- *(APO05) Porcentaje de unidades de negocio involucradas en el proceso de evaluación y priorización*
- *(APO07) Nivel de satisfacción ejecutiva con la toma de decisiones administrativas*
- *(APO07) Número de decisiones que no se pudieron resolver dentro de las estructuras de la gerencia y fueron escaladas a estructuras de gobierno*
- *(APO07) Porcentaje de rotación de personal*
- *(APO07) Duración promedio de las vacantes*
- *(APO07) Porcentaje de puestos de TI vacantes*

02 Gestión del ciclo de vida del programa/proyectos

0201 Terminación de proyectos fallidos

Título del escenario de riesgo	Terminación de proyectos fallidos
Categoría del escenario de riesgo	02 Gestión del ciclo de vida del programa/proyectos
Referencia del escenario de riesgo	0201

Escenario de riesgo
Una empresa decidió sustituir su sistema actual de planificación de recursos empresariales (ERP) y asignó un presupuesto de 5 millones de euros. La compañía planificó un proyecto de dos años y un enfoque de big-bang para reemplazar los sistemas y procesos existentes. El plan se basó en la estimación preparada por un proveedor que se convirtió en una parte interesada clave a lo largo del proyecto. Después de gastar 50 millones de euros y tres años de personalización, la empresa realizó una evaluación de la configuración del proyecto y decidió detener la iniciativa. Los recursos invertidos se perdieron. La falta de gestión de riesgo del proyecto y de gestión de beneficios era obvia. El proyecto se podría haber detenido en sus etapas iniciales, pero la empresa no aplicó buenas prácticas de gestión en el ciclo de vida del proyecto.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** de los procesos APO05 *Gestionar la cartera* y BAI01 *Gestionar los programas y proyectos.*

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **interno**, la función que es responsable de la monitorización y control de los proyectos, el Comité de Dirección (Programas/Proyectos).

Evento
El evento es un **diseño ineficaz** y/o **ejecución ineficaz** de los procesos APO05 *Gestionar la cartera* y BAI01 *Gestionar los programas y proyectos.*

Activo/Recurso (causa)
Los recursos que dieron lugar al impacto en el negocio son los **procesos** APO05 *Gestionar la cartera* y BAI01 *Gestionar los programas y proyectos*, lo que llevó a tomar decisiones inapropiadas. La **estructura organizacional** también puede ser el recurso que condujo al impacto en el negocio debido a la falta de un modelo de toma de decisiones que debe seguir el Comité de Dirección (Programas/Proyectos).

Activo/Recurso (efecto)
Los activos afectados son **procesos de negocio** no mejorados debido a la iniciativa detenida.

Tiempo
La duración del evento es **extensa** porque transcurre un largo período de tiempo antes de que el proyecto sea detenido. El momento de la ocurrencia es **no crítico**. El evento se detecta solo después de que el proyecto se ha ejecutado durante varios años, y por lo tanto, la detección es **lenta**. La consecuencia es **demorada** porque se debe iniciar un nuevo proyecto para mejorar los procesos de negocio.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**P**	Oportunidad perdida para lograr los beneficios empresariales planificados, como la operación mejorada de la empresa y la transparencia en la planificación.
Entrega del proyecto y programa de TI	**P**	Costos varados para la entrega del proyecto sin resultados beneficiosos.
Entrega del servicio y operaciones de TI	**N/A**	

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** Aceptación del hecho de que la empresa continúa sin mejorar la operación del negocio.
- **Compartir/transferir el riesgo:** Compartir la responsabilidad del fracaso del proyecto con el proveedor que preparó la estimación, y solicitar un reembolso de una parte del costo del proyecto.
- **Mitigación del riesgo:** Detener el proyecto (temprano) y aplicar un enfoque ágil/escalonado a los procesos y sistemas de entrega, en lugar de un reemplazo de big-bang.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de gestión de programas/proyectos	La medición de la visibilidad y el estado real de los tomadores de decisiones deben basarse en un lenguaje y una metodología comunes: • Reconocimiento de los proyectos fallidos (en términos de costo, retrasos, requerimientos imprevistos, cambios en las prioridades del negocio, etc.) y crear flujos de información para inducir acciones correctivas. • Para prevenir el fracaso, los cambios de alcance en los proyectos existentes se deben gestionar estrictamente.	Medio	Alto	SÍ

Habilitador del proceso					
Referencia	**Título**	**Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
APO05.03	Evaluar y seleccionar programas para financiar.	Basándose en los requerimientos generales de la mezcla de la cartera de inversión, evaluar y establecer prioridades de los casos de negocio del programa, y tomar decisiones sobre las propuestas de inversión. Asignar fondos e iniciar los programas.	Medio	Alto	SÍ
APO05.04	Monitorizar, optimizar e informar sobre el rendimiento de la cartera de inversión.	Monitorizar y optimizar de forma periódica el rendimiento de la cartera de inversión y los programas individuales durante todo el ciclo de vida de las inversiones.	Medio	Bajo	NO
APO05.06	Gestionar el logro de beneficios.	Monitorizar los beneficios de ofrecer y mantener servicios y capacidades de TI apropiados, con base en el caso de negocio acordado y actual.	Medio	Alto	SÍ
BAI01.11	Monitorizar y controlar proyectos.	Medir el rendimiento del proyecto en comparación con los criterios clave de rendimiento del proyecto, como el calendario, la calidad, el costo y el riesgo. Identificar las desviaciones de las expectativas. Evaluar el impacto de las desviaciones en el proyecto y en el programa general, y reportar los resultados a las partes interesadas clave.	Alto	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director de Informática (CIO)	Tomar las acciones correctivas, si es necesario.		Medio	Medio	NO
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La monitorización del programa/ proyecto incluye actividades basadas en datos	Las decisiones deben ser objetivas, no sesgadas y basadas en información fundamentada.		Bajo	Bajo	NO
La admisión de las malas noticias es apoyada por la alta gerencia	Permite la toma de decisiones más temprana y minimiza el impacto.		Alto	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Plan de realización de los beneficios del programa	Esta información proporcionará los datos necesarios para seguir el avance y estimar el rebasamiento presupuestario potencial.		Medio	Medio	NO
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Habilitador de personas, habilidades y competencias					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de control de rendimiento según el presupuesto	Las habilidades analíticas correctas permitirán estimar las consecuencias de proyectos fallidos, como los posibles rebasamientos presupuestarios.		Bajo	Medio	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI
• *(01) Nivel de satisfacción de las partes interesadas con el alcance de la cartera de programas y servicios planificada* • *(01) Porcentaje de impulsores de valor de TI asignados a impulsores de valor empresariales* • *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(05) Porcentaje de inversiones habilitadas para TI en las que se supervisa el logro de beneficios durante todo el ciclo de vida económico* • *(05) Porcentaje de servicios de TI donde se logran los beneficios esperados* • *(05) Porcentaje de inversiones habilitadas para TI en las que los beneficios afirmados se cumplen o exceden* • *(13) Número de programas/proyectos a tiempo y dentro del presupuesto* • *(13) Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto* • *(13) Número de programas que necesitan reelaboración significativa debido a defectos de calidad*
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso
• *(APO05) Grado en que la gerencia empresarial está satisfecha con la contribución de TI a la estrategia empresarial* • *(APO05) Nivel de satisfacción con los informes de monitorización de la cartera* • *(APO05) Porcentaje de inversiones donde los beneficios logrados se han medido y comparado con el caso de negocio* • *(BAI01) Nivel de satisfacción de las partes interesadas con la participación* • *(BAI01) Porcentaje de partes interesadas que aprueban la necesidad empresarial, el alcance, el resultado previsto y el nivel de riesgo del proyecto* • *(BAI01) Porcentaje de actividades alineadas con el alcance y los resultados esperados* • *(BAI01) Porcentaje de programas activos emprendidos sin mapas de valor del programa válidos y actualizados* • *(BAI01) Frecuencia de las revisiones del estado* • *(BAI01) Porcentaje de desviaciones del plan abordadas* • *(BAI01) Porcentaje de firmas de autorización de las partes interesadas para las revisiones etapa-puerta de los programas activos* • *(BAI01) Porcentaje de beneficios esperados logrados* • *(BAI01) Nivel de satisfacción de las partes interesadas expresado en la revisión de cierre del proyecto*

0204 Retrasos de rutina en proyectos de TI

Título del escenario de riesgo	Retrasos de rutina en proyectos de TI
Categoría del escenario de riesgo	02 Gestión del ciclo de vida del programa/proyectos
Referencia del escenario de riesgo	0204

Escenario de riesgo
La organización de TI de una empresa inició un proyecto de gestión de seguridad de TI (implementando un sistema de gestión de seguridad de la información [SGSI] con el objetivo de obtener un certificado) y planificó un plazo de un año. Después de seis meses, el plan tuvo que ser reprogramado debido a una serie de plazos incumplidos y una alta incertidumbre de cumplir con la línea de tiempo del proyecto. El presupuesto se ha consumido en su totalidad. La organización no tiene una visión de un resultado final y tiene incertidumbre con respecto a los fondos adicionales requeridos. El gerente de seguridad de TI está liderando el proyecto y se enfoca más en cuestiones técnicas que en la gestión del proyecto y en la entrega de resultados. El gerente de seguridad de TI no ve el retraso en la implementación del SGSI o el gasto en exceso como una preocupación.

El riesgo es la posibilidad de no obtener la certificación, lo cual tiene un impacto negativo en la imagen de la empresa y la capacidad de cumplir con los requerimientos de cumplimiento. Además, los costos iniciales y continuos del SGSI, así como el tiempo para la entrega exitosa de los resultados del proyecto, no están claros.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso BAI01 *Gestionar los programas y proyectos.*

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **interno**, la función que es responsable de la monitorización y control de los proyectos, el Comité de Dirección (Programas/Proyectos).

Evento
El evento es un **diseño ineficaz** y/o **ejecución ineficaz** del proceso BAI01 *Gestionar los programas y proyectos.*

Activo/Recurso (causa)
Los recursos que conducen a los impactos en el negocio son el **proceso** BAI01 *Gestionar los programas y proyectos* y **personas y habilidades** porque el gerente del proyecto se enfoca en el contenido del proyecto, en lugar de en la gestión del proyecto.

Activo/Recurso (efecto)
El recurso/activo afectado es el **proceso** DSS05 *Gestionar los servicios de seguridad* y la **información** porque la seguridad de la información está en peligro.

Tiempo
La duración del evento es **extensa** porque transcurre un largo período de tiempo antes de que el proyecto esté en camino al objetivo. El momento de la ocurrencia es **no crítico**. El evento se detecta solo después de que el proyecto se ha ejecutado durante algún tiempo, y por lo tanto, la detección es **lenta**. La consecuencia es **demorada** porque el proyecto se ejecuta durante la implementación y el presupuesto planificados.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**P**	Oportunidad perdida para lograr los beneficios empresariales planificados, como la operación mejorada de la empresa y la transparencia en la planificación.
Entrega del proyecto y programa de TI	**P**	Costos varados para la entrega del proyecto sin resultados beneficiosos.
Entrega del servicio y operaciones de TI	**N/A**	

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** Aceptación del hecho de que la empresa continúa sin mejorar la operación del negocio puede ser una respuesta posible. Sin embargo, la empresa debe considerar que aceptar el hecho de que continúa sin mejorar la operación del negocio significa que la empresa también acepta el riesgo de daño reputacional.
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Detener el proyecto (temprano) y aplicar un enfoque ágil/escalonado a la entrega de procesos y sistemas.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de gestión de programas/proyectos	La medición de la visibilidad y el estado real de los tomadores de decisiones deben basarse en un lenguaje y una metodología comunes: • Reconocimiento de los proyectos fallidos (en términos de costo, retrasos, requerimientos imprevistos, cambios en las prioridades del negocio, etc.) y crear flujos de información para inducir acciones correctivas. • Para prevenir el fracaso, los cambios de alcance en los proyectos existentes se deben gestionar estrictamente.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título**	**Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
APO05.03	Evaluar y seleccionar programas para financiar.	Basándose en los requerimientos generales de la mezcla de la cartera de inversión, evaluar y establecer prioridades de los casos de negocio del programa, y tomar decisiones sobre las propuestas de inversión. Asignar fondos e iniciar los programas.	Medio	Alto	SÍ
BAI01.08	Planificar proyectos.	Establecer y mantener un plan de proyecto formal, integrado y aprobado (que cubra los recursos del negocio y de TI) para guiar la ejecución y el control del proyecto durante la vida útil del proyecto. El alcance de los proyectos debe definirse claramente y vincularse al desarrollo o mejora de las capacidades empresariales.	Medio	Alto	SÍ
BAI01.11	Monitorizar y controlar proyectos.	Medir el rendimiento del proyecto en comparación con los criterios clave de rendimiento del proyecto, como el calendario, la calidad, el costo y el riesgo. Identificar las desviaciones de las expectativas. Evaluar el impacto de las desviaciones en el proyecto y en el programa general, y reportar los resultados a las partes interesadas clave.	Alto	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director de Informática (CIO)	Tomar las acciones correctivas, si es necesario.		Medio	Alto	SÍ
Patrocinador del programa/ proyecto	Responsable general del seguimiento presupuestario y la demostración de valor.		Medio	Medio	NO
Gerente del programa/proyecto	Responsable general del seguimiento presupuestario y demostración de valor.		Medio	Medio	NO
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La admisión de las malas noticias es apoyada por la alta gerencia	Permite una toma de decisiones más temprana y minimiza el impacto.		Medio	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Plan de realización de los beneficios del programa	Esta información proporcionará los datos necesarios para seguir el avance y estimar el rebasamiento presupuestario potencial.		Alto	Medio	SÍ
Registro del presupuesto y los beneficios del programa	Esta información proporcionará los datos necesarios para seguir el avance y estimar el rebasamiento presupuestario potencial.		Alto	Medio	SÍ
Registro del presupuesto y los beneficios del programa	La medición de la visibilidad y el estado real de los tomadores de decisiones deben basarse en un lenguaje y una metodología comunes.		Alto	Medio	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Herramientas de gestión de cartera	Aumentar la transparencia de la situación presupuestaria.		Alto	Bajo	SÍ
Habilitador de personas, habilidades y competencias					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de control de rendimiento según el presupuesto	Las habilidades analíticas correctas permitirán estimar las consecuencias de proyectos fallidos, como los posibles rebasamientos presupuestarios.		Medio	Medio	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI
• *(01) Porcentaje de metas y requerimientos estratégicos empresariales respaldados por metas estratégicas de TI* • *(01) Nivel de satisfacción de las partes interesadas con el alcance de la cartera de programas y servicios planificada* • *(01) Porcentaje de impulsores de valor de TI asignados a impulsores de valor empresariales* • *(05) Porcentaje de inversiones habilitadas para TI en las que se supervisa el logro de beneficios durante todo el ciclo de vida económico* • *(05) Porcentaje de servicios de TI donde se logran los beneficios esperados* • *(05) Porcentaje de inversiones habilitadas para TI en las que los beneficios afirmados se cumplen o exceden* • *(13) Número de programas/proyectos a tiempo y dentro del presupuesto* • *(13) Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto* • *(13) Número de programas que necesitan reelaboración significativa debido a defectos de calidad*
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso
• *(APO05) Porcentaje de inversiones de TI que tienen trazabilidad a la estrategia empresarial* • *(APO05) Grado en que la gerencia empresarial está satisfecha con la contribución de TI a la estrategia empresarial* • *(APO05) Proporción de los fondos asignados a los fondos utilizados* • *(APO05) Porcentaje de unidades de negocio involucradas en el proceso de evaluación y priorización* • *(APO05) Nivel de satisfacción con los informes de monitorización de la cartera* • *(APO05) Porcentaje de cambios del programa de inversiones reflejados en las carteras relevantes* • *(APO05) Porcentaje de inversiones donde los beneficios logrados se han medido y comparado con el caso de negocio* • *(BAI01) Porcentaje de partes interesadas efectivamente involucradas* • *(BAI01) Nivel de satisfacción de las partes interesadas con la participación* • *(BAI01) Porcentaje de partes interesadas que aprueban la necesidad empresarial, el alcance, el resultado previsto y el nivel de riesgo del proyecto* • *(BAI01) Porcentaje de actividades alineadas con el alcance y los resultados esperados* • *(BAI01) Frecuencia de las revisiones del estado* • *(BAI01) Porcentaje de desviaciones del plan abordadas* • *(BAI01) Porcentaje de firmas de autorización de las partes interesadas para las revisiones etapa-puerta de los programas activos* • *(BAI01) Porcentaje de beneficios esperados logrados* • *(BAI01) Porcentaje de resultados con aceptación de primera instancia* • *(BAI01) Nivel de satisfacción de las partes interesadas expresado en la revisión de cierre del proyecto*

0205 Retrasos excesivos en una iniciativa empresarial habilitada para TI

Título del escenario de riesgo	Retrasos excesivos en una iniciativa empresarial habilitada para TI
Categoría del escenario de riesgo	02 Gestión del ciclo de vida del programa/proyectos
Referencia del escenario de riesgo	0205

Escenario de riesgo
El consejo de dirección de una empresa pública de electricidad, suministro y distribución (ciclo completo) decidió redefinir el proceso del cliente (conexión de clientes, facturación, etc.) y renovar los sistemas de información subyacentes. Se planificó un programa de un año, y los primeros resultados del programa se entregaron con un retraso de dos años, mientras que todavía sufrían problemas de calidad y falta de interoperabilidad con otros sistemas empresariales (conexión de nuevos clientes, medición del consumo de energía de los clientes, etc.).

Se contrató a un proveedor externo para apoyar el cambio de los procesos del cliente y la tecnología subyacente, las cual era nueva para la empresa. El personal de la empresa no estaba convencido de la adecuación del nuevo sistema, especialmente porque el sistema antiguo proporcionaba funcionalidades específicas a los usuarios empresariales que no se consideraron en la planificación inicial del programa y debían desarrollarse en paralelo.

Los activos de TI suministrados por el programa necesitan ser corregidos/modificados ser totalmente funcionales. Se crearon especificaciones funcionales, pero los desarrolladores se desviaron de esas especificaciones sin la aprobación o retroalimentación apropiada. El trabajo adicional y las ineficiencias en el desarrollo de servicios ocasionaron retrasos en las entregas, excedieron los costos de TI y de los servicios del proveedor, y redujeron la calidad del servicio a los clientes, p. ej., por información incompleta para el servicio al cliente y el personal de soporte. El retraso del 200% y el exceso del 100% de los costos del proyecto resumen el desempeño de la ejecución del programa.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso BAI01 *Gestionar los programas y proyectos.*

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **interno**, la función que es responsable de la monitorización y control de los proyectos, el Comité de Dirección (Programas/Proyectos), o específicamente, el Director General (CEO) y el Director Informático (CIO) del cliente a cargo del proyecto.

Evento
El evento es un **diseño ineficaz** y/o **ejecución ineficaz** del proceso BAI01 *Gestionar los programas y proyectos.*

Activo/Recurso (causa)
Los recursos que dieron lugar al impacto en el negocio son los **procesos** BAI01 *Gestionar los programas y proyectos* y BAI07 *Gestionar la aceptación del cambio y transición* debido a las pruebas deficientes de los entregables. Otro recurso es **personas y habilidades** porque el gerente del proyecto se enfoca en el contenido del proyecto, en lugar de en la gestión del proyecto. Otro recurso es **infraestructura de TI** porque la adquisición de activos de TI no funcionó adecuadamente.

Activo/Recurso (efecto)
Los recursos afectados son **procesos** de negocio, como la conexión de clientes y la facturación.

Tiempo
La duración del evento es **extensa** porque transcurre un largo período de tiempo antes de que el proyecto esté en camino al objetivo. El momento de la ocurrencia es **no crítico**. El evento se detecta solo después de que el proyecto se ha ejecutado durante algún tiempo. Por lo tanto, la detección es **moderada**. La consecuencia es **demorada** porque el proyecto se ejecuta durante la implementación y el presupuesto planificados.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**P**	La mejora planificada de la eficiencia no se logró y se retrasó.
	P	Otras iniciativas tuvieron que aplazarse debido a los retrasos, y los sistemas de información correspondientes no pudieron planificarse en consecuencia.
Entrega del proyecto y programa	**P**	Retraso en la entrega de los resultados del proyecto.
	P	Rebasamiento presupuestario.
	P	Funcionalidad incompleta de las aplicaciones entregadas y errores no detectados en los sistemas debido a pruebas deficientes.
Entrega del servicio y operaciones de TI	**S**	Información incompleta/imprecisa que se proporciona a servicio al cliente, soporte y clientes.
	P	Retrasos en la prestación de servicios a los clientes finales (p. ej., conexión de nuevos clientes) debido a información incompleta/imprecisa.
	P	Problemas de seguridad de la información causados por brindar acceso a información crítica de clientes (particulares y empresas) debido a una seguridad inadecuada en el desarrollo de aplicaciones.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** Aceptar que la empresa continúa sin mejorar la operación del negocio y con rebasamientos presupuestarios.
- **Compartir/transferir el riesgo:** Compartir la responsabilidad del fracaso del proyecto con el proveedor que preparó la estimación, y solicitar un reembolso de una parte del costo del proyecto.
- **Mitigación del riesgo:** Usar una oficina de gestión de proyectos (PMO) apropiada y procesos adecuados para gestionar el programa. Mejora de las pruebas/el aseguramiento de calidad (QA) y la seguridad de las aplicaciones en las primeras fases del programa. Aplicar un riguroso requisito funcional y de seguridad, identificación y pruebas de la calidad entregada.

Mitigación del Riesgo Usando Habilitadores de COBIT 5					
Habilitador de principios, políticas y marco de trabajo					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Política de gestión de programas/proyectos	La medición de la visibilidad y el estado real de los tomadores de decisiones deben basarse en un lenguaje y una metodología comunes: • Reconocimiento de los proyectos fallidos (en términos de costo, retrasos, requerimientos imprevistos, cambios en las prioridades del negocio, etc.) y crear flujos de información para inducir acciones correctivas. • Para prevenir el fracaso, los cambios de alcance en los proyectos existentes se deben gestionar estrictamente.		Alto	Alto	SÍ
Habilitador del proceso					
Referencia	**Título**	**Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
APO05.03	Evaluar y seleccionar programas para financiar.	Basándose en los requerimientos generales de la mezcla de la cartera de inversión, evaluar y establecer prioridades de los casos de negocio del programa, y tomar decisiones sobre las propuestas de inversión. Asignar fondos e iniciar los programas.	Bajo	Alto	SÍ
BAI01.03	Gestionar la participación de las partes interesadas.	Gestionar la participación de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna que llegue a todas las partes interesadas relevantes. Esto incluye planificar, identificar e involucrar a las partes interesadas y gestionar sus expectativas.	Bajo	Alto	SÍ
BAI01.06	Monitorizar, controlar e informar sobre los resultados del programa.	Monitorizar y controlar el programa (entrega de la solución) y el rendimiento de la empresa (valor/resultado) en comparación con el plan durante todo el ciclo de vida económica de la inversión. Informar sobre este rendimiento al Comité de Dirección del programa y a los patrocinadores.	Medio	Alto	SÍ
BAI01.09	Gestionar programas y proyectos de calidad.	Preparar y ejecutar un plan de gestión de la calidad, procesos y prácticas, alineadas con el sistema de gestión de calidad (QMS) que describe el programa y el enfoque de calidad hacia el proyecto y cómo se implementará. Todas las partes relevantes deben evaluar y aceptar formalmente el plan, y después deben incorporarse al programa integrado y a los planes del proyecto.	Bajo	Alto	SÍ
BAI01.11	Monitorizar y controlar proyectos.	Medir el rendimiento del proyecto en comparación con los criterios clave de rendimiento del proyecto, como el calendario, la calidad, el costo y el riesgo. Identificar las desviaciones de las expectativas. Evaluar el impacto de las desviaciones en el proyecto y en el programa general, y reportar los resultados a las partes interesadas clave.	Alto	Alto	SÍ
BAI02.01	Definir y mantener los requerimientos funcionales y técnicos del negocio.	Basándose en el caso de negocio, identificar, priorizar, especificar y acordar los requerimientos de información empresarial, funcionales, técnicos y de control que cubran el alcance/la comprensión de todas las iniciativas necesarias para lograr los resultados esperados de la solución empresarial habilitada para TI propuesta.	Bajo	Alto	SÍ
BAI02.04	Obtener la aprobación de requerimientos y soluciones.	Coordinar la retroalimentación de las partes interesadas afectadas, y en etapas clave predeterminadas, obtener la aprobación y autorización del patrocinador del negocio o del propietario del producto para los requerimientos funcionales y técnicos, estudios de factibilidad, análisis de riesgos y soluciones recomendadas.	Bajo	Medio	NO

Habilitador del proceso *(cont.)*					
Referencia	**Título**	**Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
BAI03.02	Diseñar componentes detallados para la solución.	Desarrollar, documentar y elaborar diseños detallados progresivamente usando técnicas acordadas de desarrollo ágiles y rápidas, o con las fases apropiadas, abordando todos los componentes (procesos de negocio y controles automatizados y manuales relacionados, apoyando las aplicaciones de TI, los servicios de infraestructura y los productos de tecnología, así como a los socios/proveedores). Asegurarse de que el diseño detallado incluya acuerdos de nivel de servicio (SLA) internos y externos, así como acuerdos de nivel operativo (OLA).	Medio	Bajo	NO
BAI03.03	Desarrollar los componentes de la solución.	Desarrollar progresivamente los componentes de la solución de acuerdo con los diseños detallados siguiendo métodos de desarrollo y estándares de documentación, requerimientos de QA y estándares de aprobación. Asegurarse que se aborden todos los requerimientos de control en los procesos de negocio, apoyando las aplicaciones de TI y los servicios de infraestructura, los servicios y productos de tecnología, y los socios/ proveedores.	Medio	Alto	SÍ
BAI03.05	Desarrollar soluciones.	Instalar y configurar las soluciones e integrarlas con las actividades del proceso empresarial. Implementar medidas de control, seguridad y auditabilidad durante la configuración, y durante la integración del hardware y el software de infraestructura, para proteger los recursos y asegurar la disponibilidad y la integridad de los datos. Actualizar el catálogo de servicios para reflejar las soluciones nuevas.	Medio	Alto	SÍ
BAI03.06	Realizar el aseguramiento de calidad (QA).	Desarrollar, aprovisionar y ejecutar un plan de aseguramiento de calidad (QA) alineado con el sistema de gestión de calidad (QMS) para obtener la calidad especificada en la definición de los requerimientos y las políticas y procedimientos de calidad de la empresa.	Medio	Alto	SÍ
BAI03.07	Prepararse para las pruebas de la solución.	Establecer un plan de pruebas y los entornos requeridos para probar los componentes de la solución individuales e integrados, incluyendo los procesos de negocio, y los servicios, las aplicaciones y la infraestructura de soporte.	Medio	Medio	SÍ
BAI03.08	Ejecutar las pruebas de la solución.	Ejecutar pruebas continuamente durante el desarrollo, incluyendo pruebas de control, de acuerdo con el plan de pruebas definido y las prácticas de desarrollo en el entorno apropiado. Incluir a los propietarios de los procesos de negocio y a los usuarios finales en el equipo de pruebas. Identificar, registrar y priorizar los errores y los problemas que se identificaron durante las pruebas.	Medio	Alto	SÍ
BAI07.05	Realizar pruebas de aceptación.	Probar los cambios de forma independiente de acuerdo con el plan de prueba definido antes de la migración al entorno operativo en vivo.	Medio	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director de Informática (CIO)	Tomar las acciones correctivas, si es necesario.		Medio	Alto	SÍ
Patrocinador del programa/ proyecto	Responsable general del seguimiento presupuestario y la demostración de valor.		Medio	Medio	NO
Gerente del programa/proyecto	Responsable general del seguimiento presupuestario y demostración de valor.		Medio	Medio	NO

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La admisión de las malas noticias es apoyada por la alta gerencia	Permite una toma de decisiones más temprana y minimiza el impacto.	Medio	Alto	SÍ
Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Plan de realización de los beneficios del programa	Esta información proporcionará los datos necesarios para seguir el avance y estimar el rebasamiento presupuestario potencial.	Alto	Medio	SÍ
Registro del presupuesto y los beneficios del programa	Esta información proporcionará los datos necesarios para seguir el avance y estimar el rebasamiento presupuestario potencial.	Alto	Medio	SÍ
Registro del presupuesto y los beneficios del programa	La medición de la visibilidad y el estado real de los tomadores de decisiones deben basarse en un lenguaje y una metodología comunes.	Alto	Medio	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Herramientas de gestión de cartera	Aumentar la transparencia de la situación presupuestaria.	Alto	Bajo	SÍ
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de control de rendimiento según el presupuesto	Las habilidades analíticas correctas permitirán estimar las consecuencias de proyectos fallidos, como los posibles rebasamientos presupuestarios.	Medio	Medio	NO
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				

- *(01) Nivel de satisfacción de las partes interesadas con el alcance de la cartera de programas y servicios planificada*
- *(05) Porcentaje de inversiones habilitadas para TI en las que se supervisa el logro de beneficios durante todo el ciclo de vida económico*
- *(05) Porcentaje de servicios de TI donde se logran los beneficios esperados*
- *(05) Porcentaje de inversiones habilitadas para TI en las que los beneficios afirmados se cumplen o exceden*
- *(07) Porcentaje de partes interesadas del negocio satisfechas que la prestación de servicios de TI cumple con los niveles de servicio acordados*
- *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI*
- *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI*
- *(08) Porcentaje de propietarios de procesos de negocio satisfechos con los productos y servicios de soporte de TI*
- *(08) Nivel de comprensión por parte del usuario empresarial de cómo las soluciones tecnológicas apoyan sus procesos*
- *(08) Valor presente neto (VPN) que muestra el nivel de satisfacción empresarial de la calidad y utilidad de las soluciones tecnológicas*
- *(12) Número de incidentes del procesamiento de negocios causados por errores de integración tecnológica*
- *(12) Número de cambios en los procesos de negocio que deben ser aplazados o reelaborados debido a problemas de integración tecnológica*
- *(12) Número de programas empresariales habilitados para TI retrasados o que incurren en costes adicionales debido a problemas de integración tecnológica*
- *(12) Número de aplicaciones o infraestructuras críticas que operan en silos y no están integradas*
- *(13) Número de programas/proyectos a tiempo y dentro del presupuesto*
- *(13) Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto*
- *(13) Número de programas que necesitan reelaboración significativa debido a defectos de calidad*
- *(13) Coste del mantenimiento de la aplicación frente al coste total de TI*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso
• *(APO05) Grado en que la gerencia empresarial está satisfecha con la contribución de TI a la estrategia empresarial*
• *(APO05) Ratio entre los fondos asignados y los fondos utilizados*
• *(APO05) Nivel de satisfacción con los informes de monitorización de la cartera*
• *(APO05) Porcentaje de inversiones donde los beneficios logrados se han medido y comparado con el caso de negocio*
• *(BAI01) Porcentaje de partes interesadas efectivamente involucradas*
• *(BAI01) Nivel de satisfacción de las partes interesadas con la participación*
• *(BAI01) Porcentaje de partes interesadas que aprueban la necesidad empresarial, el alcance, el resultado previsto y el nivel de riesgo del proyecto*
• *(BAI01) Porcentaje de actividades alineadas con el alcance y los resultados esperados*
• *(BAI01) Frecuencia de las revisiones del estado*
• *(BAI01) Porcentaje de desviaciones del plan abordadas*
• *(BAI01) Porcentaje de firmas de autorización de las partes interesadas para las revisiones etapa-puerta de los programas activos*
• *(BAI01) Porcentaje de beneficios esperados logrados*
• *(BAI01) Porcentaje de resultados con aceptación de primera instancia*
• *(BAI01) Nivel de satisfacción de las partes interesadas expresado en la revisión de cierre del proyecto*
• *(BAI02) Porcentaje de requerimientos reelaborados debido a la desalineación con las necesidades y expectativas de la empresa*
• *(BAI02) Nivel de satisfacción de las partes interesadas con los requerimientos*
• *(BAI02) Porcentaje de requerimientos satisfechos por la solución propuesta*
• *(BAI02) Porcentaje de objetivos del caso de negocio satisfechos por la solución propuesta*
• *(BAI02) Porcentaje de partes interesadas que no aprueban la solución en relación con el caso de negocio*
• *(BAI03) Número de diseños de soluciones reelaborados debido a la desalineación con los requerimientos*
• *(BAI03) Tiempo necesario para aprobar que el producto de diseño ha cumplido con los requerimientos*
• *(BAI03) Número de errores encontrados durante la prueba*
• *(BAI03) Número de demandas de mantenimiento que no se satisfacen*
• *(BAI07) Porcentaje de partes interesadas satisfechas con la exhaustividad del proceso de prueba*
• *(BAI07) Número y porcentaje de versiones no listas para lanzarse según el calendario*
• *(BAI07) Número o porcentaje de versiones que no se estabilizan dentro de un período aceptable*
• *(BAI07) Porcentaje de versiones que causan tiempo de inactividad*

Página intencionalmente en blanco

03 Toma de decisiones sobre inversiones en TI

0302 Construcción de software nicho

Título del escenario de riesgo	Construcción de software nicho
Categoría del escenario de riesgo	03 Toma de decisiones sobre inversiones en TI
Referencia del escenario de riesgo	0302

Escenario de riesgo
Una empresa especializada en un nicho de mercado con muchas décadas de experiencia e investigación ofrece soluciones de última generación que son comúnmente aceptadas en el mercado.

Sin tener en cuenta este hecho, un cliente con un departamento de desarrollo interno y personal asignado, pero sin la madurez necesaria en sus procesos del ciclo de vida de desarrollo de software (SDLC) y su departamento de Aseguramiento de Calidad (QA), decide desarrollar su propia solución. El cliente no considera la ventaja de comprar este software sobre el desarrollo de la solución internamente, y no tiene una comprensión real de los requerimientos empresariales y de cumplimiento normativo.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso BAI03 *Gestionar la identificación y el desarrollo de soluciones*, pero también se podría clasificar como un **accidente/error** porque no se consideró una solución externa.

Agente
Los agentes que generan la amenaza que explota una vulnerabilidad son **internos**, el Comité de Dirección (Programas/Proyectos) y el Director Informático (CIO).

Evento
El evento se puede clasificar como **diseño ineficaz** y/o **ejecución ineficaz** de los procesos BAI03 *Gestionar la identificación y el desarrollo de soluciones.*

Activo/Recurso (causa)
El recurso / activo que ocasiona el impacto en el negocio es el **proceso** BAI03 *Gestionar la identificación y el desarrollo de soluciones.*

Activo/Recurso (efecto)
Los recursos/activos afectados son **procesos, información** y **aplicaciones** empresariales porque la solución desarrollada internamente no se ajusta a los requerimientos del negocio y de cumplimiento normativo debido a una falta de comprensión.

Tiempo
El momento de la ocurrencia es **crítico** porque los competidores ya utilizan soluciones que cumplen con los requisitos de cumplimiento. La duración del evento es **extensa** porque la solución desarrollada internamente debe ser modificada para ajustarse a los requerimientos de negocio y de cumplimiento normativo. La detección es **lenta** porque la solución desarrollada internamente está desalineada con los requerimientos de negocio y de cumplimiento, lo cual no se detecta antes de las pruebas de aceptación final o antes de que la implementación esté en producción. Los resultados son **demorados** porque la solución desarrollada internamente debe ser mejorada o se debe implementar una solución externa.

Tipo de riesgo

Provisión del beneficio/valor de TI	**P**	Oportunidad perdida de utilizar la solución de última generación para mejorar la eficiencia y la eficacia.
Entrega del proyecto y programa de TI	**S**	Falta de comprensión de los requerimientos de negocio y de cumplimiento.
Entrega de servicio y operaciones	**P**	Sistemas sometidos a pruebas indebidas debido a la madurez insuficiente en QA.

Posibles respuestas al riesgo

- **Evitación del riesgo:** N/A
- **Aceptación del riesgo:** La empresa acepta que los costes derivados del desarrollo interno serán mayores debido al tiempo necesario para comprender y desarrollar los procesos de SDLC y QA, así como el marco de gobierno. La compañía también acepta el riesgo de que sus competidores puedan obtener una ventaja competitiva por la adopción temprana de una solución en paquete mientras la compañía diseña y desarrolla su propia solución. La empresa también acepta el riesgo de sanciones impuestas por los reguladores debido a incumplimientos.
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Desarrollar y mantener un enfoque estándar para la gestión de programas y proyectos, y para la identificación y desarrollo de soluciones.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de gestión de programas/proyectos	La política debe definir quién necesita participar en las decisiones de inversión y cuál es la cadena de aprobación.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título**	**Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
APO03.01	Desarrollar la visión de arquitectura empresarial.	La visión de la arquitectura ofrece una descripción de alto nivel de la línea de referencia y las arquitecturas objetivo, cubriendo los dominios empresariales, de información, de datos, de aplicación y de tecnología. La visión de la arquitectura ofrece al patrocinador una herramienta clave para promover los beneficios de las capacidades propuestas a las partes interesadas de la empresa. La visión de la arquitectura describe cómo la nueva capacidad cumplirá con las metas y los objetivos empresariales estratégicos, y abordará las preocupaciones de las partes interesadas cuando se implemente.	Bajo	Alto	SÍ
APO05.03	Evaluar y seleccionar programas para financiar.	Basándose en los requerimientos generales de la mezcla de la cartera de inversión, evaluar y establecer prioridades de los casos de negocio del programa, y tomar decisiones sobre las propuestas de inversión. Asignar fondos e iniciar los programas.	Alto	Alto	SÍ
APO06.04	Modelar y asignar los costes.	Establecer y usar un modelo de costes de TI basado en la definición del servicio, asegurando que esta asignación de costes para servicios sea identificable, medible y predecible, para fomentar el uso responsable de los recursos, incluyendo aquellos proporcionados por proveedores de servicios. Revisar y comparar periódicamente la idoneidad del modelo de costes/ recargos para mantener su relevancia e idoneidad para las actividades empresariales y de TI en evolución.	Bajo	Bajo	NO
APO06.05	Gestionar los costes.	Implementar un proceso de gestión de costes que compare los costes reales con los presupuestados. Es necesario monitorizar e informar sobre los costes, y en caso de desviaciones, identificarlos de forma oportuna, así como su impacto sobre los procesos empresariales y los servicios analizados.	Bajo	Alto	NO
BAI01.01	Mantener un enfoque estándar para la gestión de programas y proyectos.	Mantener un enfoque estándar para la gestión de programas y proyectos que permita a los órganos de gobierno y gestión la revisión, la toma de decisiones y proporcionar actividades de gestión, focalizadas en la consecución del valor y de los objetivos (requerimientos, riesgos, costes, calendario, calidad) del negocio de forma consistente.	Alto	Alto	SÍ
BAI03.03	Desarrollar los componentes de la solución.	Desarrollar progresivamente los componentes de la solución de acuerdo con los diseños detallados siguiendo métodos de desarrollo y estándares de documentación, requerimientos de QA y estándares de aprobación. Asegurar que se aborden todos los requerimientos de control en las aplicaciones de TI y en los servicios de infraestructura, en los servicios y productos de tecnología, y en los socios/proveedores que soportan los procesos de negocio.	Alto	Alto	SÍ
MEA03.03	Confirmar el cumplimiento externo.	Confirmar el cumplimiento con los requerimientos legales, regulatorios y contractuales.	Alto	Alto	SÍ
Habilitador de estructuras organizativas					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
El proceso de toma de decisiones se basa en datos	Las decisiones deben ser objetivas, no sesgadas y basadas en información fundamentada.		Alto	Medio	SÍ

Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Casos de negocio	Aclarar el propósito, coste y retorno de la inversión (ROI) de las iniciativas de TI.	Medio	Medio	NO
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Análisis de caso de negocio	Aclarar el propósito, coste y ROI de las iniciativas de TI.	Medio	Medio	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(01) Nivel de satisfacción de las partes interesadas con el alcance de la cartera de programas y servicios planificada*
- *(02) Coste de incumplimiento de TI, incluyendo acuerdos y multas, y el impacto de la pérdida reputacional*
- *(02) Número de asuntos de incumplimiento relacionados con la TI reportados a la junta o que causan comentarios o vergüenza públicos*
- *(02) Cobertura de las evaluaciones de cumplimiento*
- *(05) Porcentaje de inversiones habilitadas para TI en las que se supervisa el logro de beneficios durante todo el ciclo de vida económico*
- *(05) Porcentaje de servicios de TI donde se logran los beneficios esperados*
- *(05) Porcentaje de inversiones habilitadas para TI en las que los beneficios afirmados se cumplen o exceden*
- *(06) Porcentaje de casos de negocio de inversión con costes y beneficios, esperados y relacionados con TI, claramente definidos y aprobados*
- *(06) Porcentaje de servicios de TI con costes operativos claramente definidos y aprobados y beneficios esperados*
- *(06) Encuesta de satisfacción de las partes interesadas clave con respecto al nivel de transparencia, comprensión y precisión de la información financiera de TI*
- *(07) Porcentaje de partes interesadas del negocio satisfechas que la prestación de servicios de TI cumple con los niveles de servicio acordados*
- *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI*
- *(09) Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de TI a los nuevos requerimientos*
- *(09) Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas*
- *(09) Tiempo promedio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada*
- *(11) Frecuencia de las evaluaciones de madurez de capacidad y optimización de costes*
- *(11) Niveles de satisfacción de ejecutivos de negocios y TI con los costes y capacidades relacionados con TI*
- *(13) Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto*
- *(13) Número de programas que necesitan reelaboración significativa debido a defectos de calidad*
- *(13) Coste del mantenimiento de la aplicación frente al coste total de TI*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(APO03) Número de excepciones a los estándares y líneas de referencia de la arquitectura solicitadas y concedidas*
- *(APO03) Nivel de retroalimentación de los clientes para la arquitectura*
- *(APO03) Beneficios logrados del proyecto que pueden rastrearse a la participación en la arquitectura (p. ej., reducción de costes mediante la reutilización)*
- *(APO03) Porcentaje de proyectos que utilizan servicios de arquitectura empresarial*
- *(APO03) Nivel de retroalimentación de los clientes para la arquitectura*
- *(APO03) Número de brechas identificadas en los modelos a lo largo de los dominios empresariales, de información, de datos, de aplicación y de arquitectura tecnológica*
- *(APO03) Nivel de retroalimentación de los clientes para la calidad de la información proporcionada*
- *(APO03) Porcentaje de proyectos que utilizan el marco y la metodología para reutilizar componentes definidos*
- *(APO03) Número de personas capacitadas en la metodología de arquitectura y conjunto de herramientas*
- *(APO05) Grado en que la gerencia empresarial está satisfecha con la contribución de TI a la estrategia empresarial*
- *(APO05) Ratio entre los fondos asignados a los fondos utilizados*
- *(APO05) Ratio entre los fondos disponibles a los fondos asignados*
- *(APO05) Porcentaje de unidades de negocio involucradas en el proceso de evaluación y priorización*
- *(APO05) Nivel de satisfacción con los informes de monitorización de la cartera*
- *(APO05) Porcentaje de inversiones donde los beneficios logrados se han medido y comparado con el caso de negocio*
- *(APO06) Número de cambios presupuestarios debido a omisiones y errores*
- *(APO06) Número de desviaciones entre las categorías presupuestarias esperadas y reales*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso *(cont.)*
• *(APO06) Porcentaje de alineación de recursos de TI con iniciativas de alta prioridad*
• *(APO06) Número de problemas escalados sobre la asignación de recursos*
• *(APO06) Porcentaje de costes generales de TI que se asignan de acuerdo con los modelos de costes acordados*
• *(APO06) Porcentaje de variación entre presupuestos, previsiones y costes reales*
• *(BAI01) Porcentaje de partes interesadas efectivamente involucradas*
• *(BAI01) Nivel de satisfacción de las partes interesadas con la participación*
• *(BAI01) Porcentaje de partes interesadas que aprueban la necesidad empresarial, el alcance, el resultado previsto y el nivel de riesgo del proyecto*
• *(BAI01) Porcentaje de proyectos acometidos sin casos de negocio aprobados*
• *(BAI01) Porcentaje de actividades alineadas con el alcance y los resultados esperados*
• *(BAI01) Porcentaje de programas activos acometidos sin mapas de valor del programa válidos y actualizados*
• *(BAI01) Porcentaje de firmas de autorización de las partes interesadas para las revisiones etapa-puerta de los programas activos*
• *(BAI01) Número de problemas de recursos (p. ej., habilidades, capacidad)*
• *(BAI01) Porcentaje de beneficios esperados logrados*
• *(BAI01) Porcentaje de resultados con aceptación de primera instancia*
• *(BAI01) Nivel de satisfacción de las partes interesadas expresado en la revisión de cierre del proyecto*
• *(BAI03) Número de diseños de soluciones reelaborados debido a la desalineación con los requerimientos*
• *(BAI03) Tiempo necesario para aprobar que el producto de diseño ha cumplido con los requerimientos*
• *(BAI03) Número de errores encontrados durante la prueba*
• *(BAI03) Número de demandas de mantenimiento que no se satisfacen*
• *(MEA03) Tiempo promedio transcurrido entre la identificación de problemas de cumplimiento externos y su resolución*
• *(MEA03) Frecuencia de las evaluaciones de cumplimiento*
• *(MEA03) Número de problemas críticos de incumplimiento identificados por año*
• *(MEA03) Porcentaje de propietarios de procesos que aprueban y confirman el cumplimiento*

0303 Actualización de la plataforma de infraestructura

Título del escenario de riesgo	Actualización de la plataforma de infraestructura
Categoría del escenario de riesgo	03 Toma de decisiones sobre inversiones en TI
Referencia del escenario de riesgo	0303

Escenario de riesgo
Una gran empresa necesita actualizar el software de misión crítica de sus sucursales para mejorar su funcionalidad con nuevas operaciones empresariales que son necesarias para obtener mayores ingresos. La compañía conoce de antemano que esta actualización de software necesita una modernización crítica de las infraestructuras de TI de las sucursales porque el nuevo software no funcionará con la versión actual.

Los componentes de las infraestructuras de TI de las sucursales son diversos y requieren de muchos proveedores para construir la arquitectura completa. Después de desarrollar la solicitud de propuesta (RFP), la compañía no considera los diferentes calendarios que cada proveedor necesita para entregar el hardware necesario. Cuando se inicia el proceso de adquisición, la compañía descubre que no se puede proporcionar un componente específico, lo que dificulta la implementación de la infraestructura completa.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** en los procesos BAI03 *Gestionar la identificación y desarrollo de soluciones*, BAI02 *Gestionar la definición de requerimientos* y APO03 *Gestionar la arquitectura empresarial*, y es un **fallo** del proceso de gobierno EDM02 *Asegurar la entrega de beneficios.*

Agente
Los agentes que generan la amenaza que explota una vulnerabilidad son **internos**, en general, el Comité de Dirección (Programas/Proyectos), el Director Informático (CIO) y el arquitecto líder.

Evento
El evento se puede clasificar como **diseño ineficaz** y/o **ejecución ineficaz** de los procesos EDM02 *Asegurar la entrega de beneficios*, BAI03 *Gestionar la identificación y el desarrollo de soluciones*, BAI02 *Gestionar la definición de requerimientos* y APO03 *Administre la arquitectura empresarial.*

Activo/Recurso (causa)
El recurso / activo que ocasiona el impacto enimpacto en el negocio es el **proceso** BAI03 *Gestionar la identificación y el desarrollo de soluciones.*

Activo/Recurso (efecto)
Los recursos/activos afectados son los **procesos, información, infraestructura** y **aplicaciones** empresariales porque la compañía no puede actualizar los sistemas de misión crítica de sus sucursales, así como el **personal** y la **empresa** porque deben trabajar con las aplicaciones desactualizadas.

Tiempo
Porque la compañía necesita nuevos sistemas para que sus sucursales obtengan mayores ingresos, el momento de la ocurrencia es **crítico**. La duración del evento es **extensa** porque la implementación de la infraestructura se ve obstaculizada. La detección es **moderada** porque el evento se detecta durante el proceso de adquisición. Las consecuencias son **demoradas** porque la compañía tiene que continuar sus negocios mientras utiliza la arquitectura de TI incorrecta, con altos costes acumulados, en un lapso de varios años.

Tipo de riesgo

Habilitar el beneficio/valor de TI	**P**	Oportunidad perdida de obtener más ingresos con los nuevos sistemas para las sucursales.
Entrega del proyecto y programa de TI	**P**	Las soluciones identificadas no coinciden con los requisitos.
Entrega del servicio y operaciones de TI	**P**	Arquitectura inflexible con altos costes acumulados.

Posibles respuestas al riesgo

- **Evitación del riesgo:** N/A
- **Aceptación del riesgo:** La empresa acepta y tolera la arquitectura inflexible, no logra mayores ingresos y pierde competitividad empresarial.
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** La empresa considera proveedores alternativos para entregar la pieza de hardware requerida. Se considerarán contratos adicionales y se aceptarán las pérdidas de tiempo y el coste de oportunidad. El programa de trabajo se vuelve a priorizar para asegurarse de que los prerrequisitos se hayan completado para permitir el éxito. Se debe seguir el marco de gobierno para el proceso de actualizaciones de infraestructura y se debe capacitar a los gerentes de departamento.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de gestión de programas/proyectos	La política debe definir quién necesita participar en las decisiones de inversión y cuál es la cadena de aprobación.	Medio	Medio	NO

Habilitador del proceso					
Referencia	**Título**	**Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
EDM02.01	Evaluar la optimización del valor.	Evaluar continuamente la cartera de inversiones, servicios y activos habilitados por TI con el fin de determinar la probabilidad de alcanzar el objetivo empresarial y proporcionar valor a un coste razonable. Identificar y hacer un juicio sobre cualquier cambio en la dirección que debe ofrecerse a la gerencia para optimizar la creación de valor.	Bajo	Alto	SÍ
EDM02.02	Dirigir la optimización del valor.	Dirigir los principios y las prácticas de gestión de valor para permitir una obtención óptima de valor con las inversiones habilitadas para TI durante todo su ciclo de vida económico.	Bajo	Alto	SÍ
BAI01.01	Mantener un enfoque estándar para la gestión de programas y proyectos.	Mantener un enfoque estándar para la gestión de programas y proyectos que permita a los órganos de gobierno y gestión la revisión, la toma de decisiones y proporcionar actividades de gestión, focalizadas en la consecución del valor y de los objetivos (requerimientos, riesgos, costes, calendario, calidad) del negocio de forma consistente.	Bajo	Alto	SÍ
BAI01.08	Planificar proyectos.	Establecer y mantener un plan de proyecto formal, integrado y aprobado (que cubra los recursos del negocio y de TI) para guiar la ejecución y el control del proyecto durante su vida útil. El alcance de los proyectos debe definirse claramente y vincularse al desarrollo o mejora de las capacidades empresariales.	Bajo	Alto	SÍ
BAI02.01	Definir y mantener los requerimientos funcionales y técnicos del negocio.	Basándose en el caso de negocio, identificar, priorizar, especificar y acordar los requerimientos de información empresarial, funcionales, técnicos y de control que cubran el alcance/la comprensión de todas las iniciativas necesarias para lograr los resultados esperados de la solución empresarial proporcionada por TI.	Bajo	Alto	SÍ
BAI03.04	Obtener los componentes de la solución.	Adquirir componentes de la solución basados en el plan de adquisiciones de acuerdo con los requerimientos y los diseños detallados, los principios y estándares de la arquitectura, y los procedimientos generales de adquisiciones y contratos de la empresa, requerimientos de aseguramiento de calidad (QA) y estándares de aprobación. Asegurar que el proveedor identifique y aborde todos los requerimientos legales y contractuales.	Alto	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director de Informática (CIO)	Responsable de la adecuada toma de decisiones sobre la inversión.		Medio	Medio	NO
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
El proceso de toma de decisiones se basa en datos	Las decisiones deben ser objetivas, no sesgadas y basadas en información fundamentada.		Bajo	Bajo	NO
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				

Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(01) Porcentaje de metas y requerimientos estratégicos empresariales respaldados por metas estratégicas de TI*
- *(01) Nivel de satisfacción de las partes interesadas con el alcance de la cartera de programas y servicios planificada*
- *(01) Porcentaje de impulsores de valor de TI asignados a impulsores de valor empresariales*
- *(05) Porcentaje de inversiones habilitadas para TI en las que se supervisa el logro de beneficios durante todo el ciclo de vida económico*
- *(05) Porcentaje de servicios de TI donde se logran los beneficios esperados*
- *(05) Porcentaje de inversiones de TI en las que los beneficios afirmados se cumplen o exceden*
- *(12) Número de cambios en los procesos de negocio que deben ser aplazados o reelaborados debido a problemas de integración tecnológica*
- *(12) Número de programas empresariales habilitados por TI retrasados o que incurren en costes adicionales debido a problemas de integración tecnológica*
- *(12) Número de aplicaciones o infraestructuras críticas que operan en silos y no están integradas*
- *(13) Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto*
- *(13) Número de programas que necesitan reelaboración significativa debido a defectos de calidad*
- *(13) Coste del mantenimiento de la aplicación frente al coste total de TI*
- *(17) Nivel de conocimiento y comprensión de los ejecutivos de negocios sobre las posibilidades de innovación en TI*
- *(17) Nivel de satisfacción de las partes interesadas con los niveles de conocimientos e ideas sobre innovación en TI*
- *(17) Número de iniciativas aprobadas como resultado de ideas innovadoras de TI*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(EDM02) Nivel de satisfacción de las partes interesadas con la capacidad de la empresa para obtener valor de las iniciativas habilitadas para TI*
- *(EDM02) Porcentaje de iniciativas de TI en la cartera general donde el valor se administra durante todo el ciclo de vida*
- *(EDM02) Nivel de satisfacción de las partes interesadas con el avance hacia los objetivos identificados, con entrega de valor basada en encuestas*
- *(EDM02) Porcentaje logrado del valor esperado*
- *(BAI01) Porcentaje de partes interesadas que aprueban la necesidad empresarial, el alcance, el resultado previsto y el nivel de riesgo del proyecto*
- *(BAI01) Porcentaje de proyectos acometidos sin casos de negocio aprobados*
- *(BAI01) Porcentaje de actividades alineadas con el alcance y los resultados esperados*
- *(BAI01) Porcentaje de programas activos acometidos sin mapas de valor del programa válidos y actualizados*
- *(BAI01) Frecuencia de las revisiones del estado*
- *(BAI01) Porcentaje de desviaciones del plan abordadas*
- *(BAI01) Porcentaje de firmas de autorización de las partes interesadas para las revisiones etapa-puerta de los programas activos*
- *(BAI01) Porcentaje de beneficios esperados logrados*
- *(BAI01) Porcentaje de resultados con aceptación de primera instancia*
- *(BAI01) Nivel de satisfacción de las partes interesadas expresado en la revisión de cierre del proyecto*
- *(BAI02) Porcentaje de requerimientos reelaborados debido a la desalineación con las necesidades y expectativas de la empresa*
- *(BAI02) Nivel de satisfacción de las partes interesadas con los requerimientos*
- *(BAI02) Porcentaje de requerimientos satisfechos por la solución propuesta*
- *(BAI02) Porcentaje de objetivos del caso de negocio satisfechos por la solución propuesta*
- *(BAI02) Porcentaje de partes interesadas que no aprueban la solución en relación con el caso de negocio*
- *(BAI03) Número de diseños de soluciones reelaborados debido a la desalineación con los requerimientos*
- *(BAI03) Tiempo necesario para aprobar que el producto de diseño ha cumplido con los requerimientos*
- *(BAI03) Número de demandas de mantenimiento que no se satisfacen*

0304 Compra de software redundante

Título del escenario de riesgo	Compra de software redundante
Categoría del escenario de riesgo	03 Toma de decisiones sobre inversiones en TI
Referencia del escenario de riesgo	0304

Escenario de riesgo
Una empresa compra software redundante para un área de negocio clave. Este software es un software de la competencia que se compró anteriormente y está en producción. El nuevo software se compró sin referencia al proceso de adquisición ya que la compra estaba dentro del proceso de aprobación presupuestaria de la persona y era para uso dentro del departamento, durante su duración.

Esta compra en particular representó una falta de conformidad con los procesos y las políticas de la organización. El sistema no se consideró en la arquitectura empresarial (EA), y, por lo tanto, carecía de interoperabilidad con otros sistemas y software, y su funcionalidad se superponía con otras funciones del negocio.

El software fue comprado por un usuario comercial clave, y debido a que el proceso de adquisición era inmaduro, el software no se incluyó en la estrategia empresarial para la continuidad del negocio y la planificación de recuperación de desastres.

La nueva compra requirió capacitación adicional para el departamento, e inversión e integración con los sistemas existentes.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** de los procesos APO04 *Gestionar la innovación*, APO05 *Gestionar la cartera*, APO06 *Gestionar el presupuesto y coste* y BAI10 *Gestionar la configuración.*

Agente
Los agentes que generan la amenaza que explota una vulnerabilidad son **internos**, en general, el Comité de Dirección (Programas/Proyectos), y también el usuario empresarial clave que compró el software.

Evento
El evento se puede clasificar como **diseño ineficaz** y/o **ejecución ineficaz** de los procesos APO04 *Gestionar la innovación*, APO05 *Gestionar la cartera,* APO06 *Gestionar el presupuesto y coste* y BAI10 *Gestionar la configuración.*

Activo/Recurso (causa)
Los activos/recursos que ocasionan el mpacto en el negocio son principalmente los **procesos** APO04 *Gestionar la innovación* y BAI10 *Gestionar la configuración.*

Activo/Recurso (efecto)
Los recursos/activos afectados son los **procesos, información, infraestructura** y **aplicaciones** empresariales porque el nuevo software carece de interoperabilidad con otros sistemas, así como el **personal** y la **empresa** porque deben buscar soluciones alternas.

Tiempo
El momento de la ocurrencia es **no crítico**. La duración es **extensa** debido al coste asociado con esta compra inadecuada y la sobrecarga que la empresa tuvo que experimentar para garantizar la interoperabilidad con los sistemas existentes. La detección es **lenta** porque la redundancia no fue detectada antes de que el sistema estuviera listo para su uso. El tiempo transcurrido es **inmediato** debido al proceso de adquisición inmaduro.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**P**	Proceso de adquisición inmaduro.
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**S**	Falta de interoperabilidad con otros sistemas.

Posibles respuestas al riesgo

- **Evitación del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Capacitar a todos los jefes de departamento en un catálogo de software centralizado para la empresa. Los marcos de gobierno para el proceso de adquisición de software deben ser mejorados su maduración y se deben seguir. Los gerentes de departamento serán capacitados. Todas las compras de software deben agregarse al plan de continuidad del negocio (BCP) y al plan de recuperación de desastres (DRP).

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de gestión de programas/proyectos	La política debe definir quién necesita participar en las decisiones de inversión y cuál es la cadena de aprobación.	Alto	Medio	SÍ

Habilitador del proceso					
Referencia	**Título**	**Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
APO02.05	Definir el plan estratégico y mapa de ruta.	Crear un plan estratégico que defina, en cooperación con las partes interesadas relevantes, cómo las metas relacionadas con TI contribuirán a las metas estratégicas de la empresa. Incluye la manera en que la TI soportará los programas de inversión, procesos empresariales, servicios de TI y activos de TI habilitados para TI. Indicar al equipo de TI que defina las iniciativas que se necesitarán para cerrar las brechas, la estrategia de adquisición y las medidas que se usarán para monitorizar el logro de los objetivos, y después priorizar las iniciativas y combinarlas en una hoja de ruta de alto nivel.	Bajo	Alto	SÍ
APO05.03	Evaluar y seleccionar programas para financiar.	Basándose en los requerimientos generales de la cartera de inversión, evaluar y establecer prioridades de los casos de negocio del programa, y tomar decisiones sobre las propuestas de inversión. Asignar fondos e iniciar los programas.	Bajo	Alto	SÍ
APO06.05	Gestionar los costes.	Implementar un proceso de gestión de costes que compare los costes actuales con los presupuestos. Es necesario monitorizar e informar sobre los costes, y en caso de desviaciones, identificarlos de forma oportuna, así como su impacto sobre los procesos empresariales y los servicios analizados.	Bajo	Alto	SÍ
APO08.04	Coordinar y comunicar.	Trabajar con las partes interesadas y coordinar la entrega extremo a extremo de los servicios y soluciones de TI que se ofrecen a la empresa.	Bajo	Alto	SÍ
BAI10.05	Verificar y revisar la integridad del repositorio de configuración.	Revisar periódicamente el repositorio de configuración y verificar su integridad y precisión en comparación con la meta deseada.	Alto	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director de Informática (CIO)	Responsable de la adecuada toma de decisiones sobre la inversión.		Alto	Medio	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Casos de negocio	Aclarar el propósito, coste y retorno de la inversión (ROI) de las iniciativas de TI.		Medio	Bajo	NO
Priorizar y clasificar las iniciativas de TI	Visión general de las iniciativas de TI para facilitar la selección.		Medio	Bajo	NO
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Habilitador de personas, habilidades y competencias					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Análisis de caso de negocio	Aclarar el propósito, coste y ROI de las iniciativas de TI.		Medio	Bajo	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI
• *(01) Porcentaje de objetivos y requerimientos estratégicos empresariales respaldados por objetivos estratégicos de TI*
• *(01) Nivel de satisfacción de las partes interesadas con el alcance de la cartera de programas y servicios planificada*
• *(05) Porcentaje de inversiones de TI en las que se supervisa el logro de beneficios durante todo el ciclo de vida económico*
• *(05) Porcentaje de servicios de TI donde se logran los beneficios esperados*
• *(05) Porcentaje de inversiones de TI en las que los beneficios afirmados se cumplen o exceden*
• *(06) Porcentaje de casos de negocio de inversión con costes y beneficios, esperados y relacionados con TI, claramente definidos y aprobados*
• *(06) Porcentaje de servicios de TI con costes operativos claramente definidos y aprobados, y beneficios esperados*
• *(07) Porcentaje de partes interesadas del negocio satisfechas que la prestación de servicios de TI cumple con los niveles de servicio acordados*
• *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI*
• *(08) Porcentaje de propietarios de procesos de negocio satisfechos con los productos y servicios de soporte de TI*
• *(08) Nivel de comprensión por parte del usuario empresarial de cómo las soluciones tecnológicas apoyan sus procesos*
• *(08) Valor presente neto (VPN) que muestra el nivel de satisfacción empresarial de la calidad y utilidad de las soluciones tecnológicas*
• *(09) Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de TI a los nuevos requerimientos*
• *(09) Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas*
• *(11) Frecuencia de las evaluaciones de madurez de capacidad y optimización de costes*
• *(11) Niveles de satisfacción de ejecutivos de negocios y de TI con los costes y capacidades relacionados con TI*
• *(12) Número de incidentes del procesamiento de negocios causados por errores de integración tecnológica*
• *(12) Número de cambios en los procesos de negocio que deben ser aplazados o reelaborados debido a problemas de integración tecnológica*
• *(12) Número de programas empresariales habilitados por TI retrasados o que incurren en costes adicionales debido a problemas de integración tecnológica*
• *(12) Número de aplicaciones o infraestructuras críticas que operan en silos y no están integradas*
• *(13) Coste del mantenimiento de la aplicación frente al coste total de TI*
• *(14) Relación y extensión de las decisiones de negocio erróneas en las que la información errónea o no disponible fue un factor clave*
• *(17) Nivel de conocimiento y comprensión de los ejecutivos de negocio sobre las posibilidades de innovación en TI*
• *(17) Nivel de satisfacción de las partes interesadas con los niveles de conocimientos e ideas sobre innovación en TI*
• *(17) Número de iniciativas aprobadas como resultado de ideas innovadoras de TI*
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso
• *(APO02) Porcentaje de objetivos empresariales abordados en la estrategia de TI*
• *(APO02) Nivel de retroalimentación de la encuesta de satisfacción de las partes interesadas de la empresa en la estrategia de TI*
• *(APO02) Porcentaje de objetivos empresariales estratégicos obtenidos como resultado de iniciativas estratégicas de TI*
• *(APO02) Porcentaje de iniciativas/proyectos de TI promovidos por propietarios de procesos de negocios*
• *(APO02) Porcentaje de iniciativas estratégicas con responsabilidad asignada*
• *(APO04) Aumento de la cuota de mercado o competitividad debido a innovaciones*
• *(APO04) Percepciones y retroalimentación de las partes interesadas de la empresa respecto a la innovación en TI*
• *(APO04) Porcentaje de iniciativas implementadas que logran los beneficios previstos*
• *(APO04) Porcentaje de iniciativas implementadas con un claro vínculo a un objetivo empresarial*
• *(APO04) Inclusión de objetivos relacionados con la innovación o tecnología emergentes en las metas de rendimiento para el personal relevante*
• *(APO05) Porcentaje de inversiones de TI que tienen trazabilidad a la estrategia empresarial*
• *(APO05) Grado en que la gerencia empresarial está satisfecha con la contribución de TI a la estrategia empresarial*
• *(APO05) Ratio entre los fondos asignados a los fondos utilizados*
• *(APO05) Porcentaje de unidades de negocio involucradas en el proceso de evaluación y priorización*
• *(APO05) Nivel de satisfacción con los informes de monitorización de la cartera*
• *(APO05) Porcentaje de cambios del programa de inversiones reflejados en las carteras relevantes*
• *(APO05) Porcentaje de inversiones donde los beneficios logrados se han medido y comparado con el caso de negocio*
• *(APO06) Número de cambios presupuestarios debido a omisiones y errores*
• *(APO06) Número de desviaciones entre las categorías presupuestarias esperadas y reales*
• *(APO06) Porcentaje de alineación de recursos de TI con iniciativas de alta prioridad*
• *(APO06) Número de problemas escalados sobre la asignación de recursos*
• *(APO06) Porcentaje de variación entre presupuestos, previsiones y costes reales*
• *(APO08) Porcentaje de alineación de los servicios de TI con los requerimientos de negocio de la empresa*
• *(APO08) Calificaciones de encuestas de satisfacción de usuarios y personal de TI*
• *(APO08) Encuesta sobre el nivel de conocimiento tecnológico de las partes interesadas del negocio*
• *(APO08) Tasa de inclusión de las oportunidades tecnológicas en las propuestas de inversión*
• *(BAI10) Número de desviaciones entre el repositorio de configuración y la configuración en vivo*
• *(BAI10) Número de discrepancias en relación con la información de configuración incompleta o ausente*

04 Pericia y habilidades en TI

0401 Políticas de contratación de recursos humanos

Título del escenario de riesgo	Políticas de contratación de recursos humanos
Categoría del escenario de riesgo	04 Pericia y habilidades en TI
Referencia del escenario de riesgo	0401

Escenario de riesgo
El departamento de Recursos Humanos (RR.HH.) tiene normas generales estrictas con respecto a la edad máxima para el reclutamiento de personal interno. Este tema particular está afectando las áreas técnicas que necesitan elevar ese límite para asegurarse de que los conocimientos y destrezas adecuados estén presentes en el nuevo personal, debido a las tecnologías (nuevas y antiguas) que continúan en uso y se depende de ellas para la arquitectura empresarial (EA).

Actualmente, la empresa espera que en los próximos cinco años se jubile el 35% de sus profesionales especializados. El conocimiento estándar mínimo que se requiere es la base para iniciar la capacitación interna del siguiente nivel. Debido a la complejidad de los sistemas de producción, el proceso de capacitación del nuevo personal para que obtenga la experiencia necesaria para poder llevar a cabo las operaciones diarias ha requerido, históricamente, tres años.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso APO07 *Gestionar recursos humanos*, especialmente las prácticas de gestión para mantener personal adecuado y mantener las habilidades y competencias del personal.

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **interno**, el área de RR.HH.

Evento
El evento es un **diseño ineficaz** del proceso APO07 *Gestionar recursos humanos.*

Activo/Recurso (causa)
El recurso que ocasiona el impacto en el negocio es el **proceso** APO07 *Gestionar recursos humanos.*

Activo/Recurso (efecto)
Los recursos afectados son los **procesos** de TI en el área técnica debido a la falta de personal competente, y la arquitectura de (**información** y **aplicaciones**) de TI porque no se puede mantener y mejorar adecuadamente debido a la falta de pericia y habilidades.

Tiempo
La duración del evento es **moderada** porque la política se puede cambiar fácilmente. El momento de la ocurrencia es **no crítico**. La falta de pericia y experiencia se detectará en un plazo **moderado**. La consecuencia puede ser fácilmente **demorada** porque es necesario reclutar el personal adecuado, y este proceso puede tomar mucho tiempo.

Tipo de riesgo

Habilitar el beneficio/valor de TI	**P**	Falta de habilidades y experiencia para usar la tecnología para nuevas iniciativas del negocio.
Entrega del proyecto y programa de TI	**P**	La falta de habilidades y experiencia puede derivar en mala calidad de los proyectos.
Entrega del servicio y operaciones de TI	**P**	El entorno técnico no se puede mantener adecuadamente.

Posibles respuestas al riesgo

- **Evitación del riesgo:** N/A
- **Aceptación del riesgo:** La empresa acepta el riesgo de que es posible que no pueda contratar las habilidades y la experiencia adecuadas, lo que limitará la capacidad de la empresa para diseñar, desarrollar y entregar soluciones de TI para ayudar a alcanzar las metas del negocio. Además, es posible que la empresa tenga que pagar una prima por trabajadores potenciales con las habilidades y experiencia requeridas.
- **Compartir/transferir el riesgo:** RR.HH. y TI deben compartir sus responsabilidades por el riesgo que la empresa está tomando al no poder contratar al personal adecuado.
- **Mitigación del riesgo:** TI puede subcontratar y usar contratistas para cubrir la escasez de habilidades críticas.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de RR.HH.	Describe el desarrollo de requerimientos para la selección y evaluación de perfiles de TI a lo largo de toda la carrera.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título**	**Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
APO01.01	Definir la estructura organizativa.	Establecer una estructura organizativa interna y extendida que refleje las necesidades del negocio y las prioridades de TI. Establecer las estructuras de gestión requeridas (p. ej., comités) que permitan que la toma de decisiones de gestión se lleve a cabo de la manera más eficaz y eficiente.	Bajo	Bajo	NO
APO01.04	Comunicar los objetivos y la dirección de la gerencia.	Comunicar y comprender los objetivos y la dirección de TI a las partes interesadas y a los usuarios en toda la empresa.	Medio	Bajo	NO
APO07.01	Mantener una dotación de personal suficiente y adecuada.	Evaluar los requerimientos de personal de forma periódica o ante cambios mayores en los entornos empresariales, operativos o de TI para garantizar que la empresa cuente con suficientes recursos humanos para apoyar las metas y los objetivos empresariales. La dotación de personal incluye tanto los recursos internos como externos.	Alto	Alto	SÍ
APO07.02	Identificar al personal clave de TI.	Identificar al personal clave de TI mientras se minimiza la dependencia en una sola persona que realice una función de trabajo crítica al capturar los conocimientos (documentación), compartir los conocimientos, planificar la sucesión y tener un respaldo de personal.	Medio	Medio	NO
APO07.03	Mantener las habilidades y las competencias del personal.	Definir y administrar las habilidades y las competencias del personal necesario. Verificar periódicamente que el personal cuente con las competencias necesarias para realizar sus funciones fundamentándose en su formación, capacitación y/o experiencia, y verificar que estas competencias se mantengan usando programas de cualificación y certificación cuando sea apropiado. Dar a los empleados oportunidades de aprendizaje continuas para mantener sus conocimientos, habilidades y competencias al nivel requerido para alcanzar las metas empresariales.	Alto	Alto	SÍ
APO07.05	Planificar y hacer seguimiento del uso de recursos humanos de TI y de negocio.	Comprender y hacer seguimiento de la demanda actual y futura de recursos humanos empresariales y de TI con responsabilidades en la TI corporativa. Identificar las carencias y proporcionar comentarios sobre los planes de aprovisionamiento, los planes de aprovisionamiento y de contratación de personal de negocio y de TI así como sus procesos asociados.	Alto	Bajo	SÍ
APO07.06	Gestionar el personal contratado.	Asegurar que los consultores y el personal contratado con habilidades de TI que da soporte a la empresa, conozca y cumpla con las políticas de la empresa y con los requerimientos contractuales acordados.	Bajo	Medio	NO

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director de Informática (CIO)	Responsable del análisis de las deficiencias en las habilidades y competencias de TI.	Alto	Alto	SÍ
Director de RR.HH.	Responsable de establecer las expectativas sobre el personal.	Alto	Alto	SÍ
Funciones gerenciales específicas de TI	Responsable de identificar los requerimientos específicos.	Alto	Alto	SÍ

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			

Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Matriz de habilidades y competencias	Describir las habilidades y competencias existentes dentro de la organización de TI y permitir el análisis de deficiencias.	Alto	Bajo	SÍ
Planes de desarrollo de competencias y de habilidades/ carrera profesional	Describir el crecimiento requerido de perfiles de TI específicos.	Alto	Medio	SÍ
Descripciones genéricas de la función del trabajo	Describir los requerimientos de habilidades/experiencia y conocimientos para perfiles genéricos dentro de las organizaciones de TI.	Alto	Alto	SÍ
Repositorios de conocimientos	Minimizar el efecto de la indisponibilidad parcial de recursos al compartir conocimientos sobre procesos, tecnología, etc.	Medio	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de RR.HH.	Gestión de habilidades y competencias.	Alto	Alto	SÍ
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(09) Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de TI a los nuevos requerimientos* • *(11) Frecuencia de las evaluaciones de madurez de capacidad y optimización de costes* • *(11) Tendencia de resultados de la evaluación* • *(11) Niveles de satisfacción de ejecutivos de negocio y de TI con los costes y capacidades relacionados con TI* • *(13) Coste del mantenimiento de la aplicación frente al coste total de TI* • *(16) Porcentaje de personal cuyas habilidades relacionadas con TI son suficientes para la competencia requerida para su función* • *(16) Porcentaje de personal satisfecho con sus funciones relacionadas con TI* • *(16) Número de horas de aprendizaje/capacitación por cada miembro del personal* • *(17) Nivel de conocimiento y comprensión de los ejecutivos de negocio sobre las posibilidades de innovación en TI* • *(17) Nivel de satisfacción de las partes interesadas con los niveles de conocimientos e ideas sobre innovación en TI*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(APO07) Porcentaje de rotación de personal* • *(APO07) Duración promedio de las vacantes* • *(APO07) Porcentaje de puestos de TI vacantes*				

0403 Destrezas de liderazgo ineficaces

Título del escenario de riesgo	Destrezas de liderazgo ineficaces		
Categoría del escenario de riesgo	04 Experiencia y habilidades en TI		
Referencia del escenario de riesgo	0403		
Escenario de riesgo El Director de Informática (CIO) de una gran empresa tiene una sólida formación en operaciones técnicas; sin embargo, no se comunica regularmente con otros gerentes de unidades de negocio. Carece de perspicacia para los negocios y, por lo tanto, no comunica la comprensión del negocio a su personal, ni mantiene la necesaria alineación requerida para el gobierno de TI.			
Componentes del escenario de riesgo			
Tipo de amenaza La naturaleza del evento es un **fallo** del proceso APO01 *Gestionar el marco de gestión de TI*, especialmente, un **fallo** de comunicación de los objetivos y dirección de la gerencia.			
Agente El agente que genera la amenaza que explota una vulnerabilidad es **interno**, el CIO.			
Evento El evento es una **ejecución ineficaz** del proceso APO01 *Gestionar el marco de gestión de TI*, pero eventualmente también puede ser un **diseño ineficaz** de la estructura organizativa.			
Activo/Recurso (causa) Los activos/recursos que ocasionan el impacto en impacto en el negocio son los **procesos** APO01 *Gestionar el marco de gestión de TI* y la **estructura organizativa.**			
Activo/Recurso (efecto) Los recursos afectados son los **procesos** de negocio porque el personal de TI no sabe o no entiende las necesidades de la empresa. El personal de TI también se ve afectado ya que no están satisfechos porque no pueden proporcionar la solución y los servicios que se esperan de ellos.			
Tiempo La duración del evento es **extensa** porque no se espera que el CIO cambie su comportamiento en el corto plazo. El momento de la ocurrencia es **no crítico**. La detección es **moderada** hasta que se detecte el comportamiento del CIO. La consecuencia es **demorada** porque el CIO no puede ser reemplazado, ni su comportamiento se puede cambiar, inmediatamente.			
Tipo de riesgo			
Habilitar el beneficio/valor de TI	**P**	Debido a que el personal de TI no entiende las necesidades del negocio, el departamento de TI pierde la oportunidad de ser un habilitador de iniciativas del negocio exitosas.	
Entrega del proyecto y programa de TI	**P**	La entrega del proyecto afectará la calidad porque los requerimientos no se cumplirán con éxito.	
Entrega del servicio y operaciones de TI	**S**	Las partes interesadas del negocio no están satisfechas con la prestación de servicios de TI.	
Posibles respuestas al riesgo			
• **Evitación del riesgo:** N/A • **Aceptación del riesgo:** N/A • **Compartir/transferir el riesgo:** N/A • **Mitigación del riesgo:** La Junta de Gobierno y la alta dirección (nivel C) deben ser conscientes de esta situación y decidir quién es la persona correcta para el trabajo.			
Mitigación del Riesgo Usando Habilitadores de COBIT 5			
Habilitador de principios, políticas y marco de trabajo			

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de Recursos Humanos (RR.HH.)	Describe el desarrollo de requerimientos para la selección y evaluación de perfiles de TI a lo largo de toda la carrera.	Medio	Medio	NO

Habilitador del proceso					
Referencia	**Título**	**Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
APO01.01	Definir la estructura organizativa.	Establecer una estructura organizativa interna y extendida que refleje las necesidades del negocio y las prioridades de TI. Establecer las estructuras de gestión requeridas (p. ej., comités) que permitan que la toma de decisiones de gestión se lleve a cabo de la manera más eficaz y eficiente.	Alto	Alto	SÍ
APO01.04	Comunicar los objetivos y la dirección de la gerencia.	Comunicar y comprender los objetivos y la dirección de TI a las partes interesadas en toda la empresa.	Alto	Alto	SÍ
APO03.01	Desarrollar la visión de arquitectura empresarial.	La visión de la arquitectura ofrece una descripción de alto nivel de la línea de referencia y las arquitecturas objetivo, cubriendo los dominios empresariales, de información, de datos, de aplicación y de tecnología. La visión de la arquitectura ofrece al patrocinador una herramienta clave para promover los beneficios de las capacidades propuestas a las partes interesadas de la empresa. La visión de la arquitectura describe cómo la nueva capacidad cumplirá con las metas y los objetivos empresariales estratégicos, y abordará las preocupaciones de las partes interesadas cuando se implemente.	Bajo	Bajo	NO
APO07.01	Mantener una dotación de personal suficiente y adecuada.	Evaluar los requerimientos de personal de forma periódica o ante cambios mayores en los entornos empresarial, operativo o de TI para garantizar que la empresa cuente con suficientes recursos humanos para apoyar las metas y los objetivos empresariales. La dotación de personal incluye tanto los recursos internos como externos.	Alto	Alto	SÍ
APO07.02	Identificar al personal clave de TI.	Identificar al personal clave de TI mientras se minimiza la dependencia en una sola persona que realice una función de trabajo crítica al capturar los conocimientos (documentación), compartir los conocimientos, planificar la sucesión y tener un respaldo de personal.	Medio	Medio	NO
APO07.03	Mantener las habilidades y las competencias del personal.	Definir y administrar las habilidades y las competencias del personal necesario. Verificar periódicamente que el personal cuente con las competencias necesarias para realizar sus funciones con base en su formación, capacitación y/o experiencia, y verificar que estas competencias se mantengan usando programas de cualificación y certificación cuando sea apropiado. Dar a los empleados oportunidades de aprendizaje continuas para mantener sus conocimientos, habilidades y competencias al nivel requerido para alcanzar las metas empresariales.	Alto	Alto	SÍ
APO07.05	Planificar y hacer seguimiento del uso de recursos humanos de TI y de negocio.	Comprender y hacer seguimiento de la demanda actual y futura de recursos humanos empresariales y de TI con responsabilidades en las TI corporativas. Identificar las carencias y proporcionar comentarios sobre los planes de aprovisionamiento, y los planes de aprovisionamiento y de contratación de personal de negocio y de TI así como sus procesos asociados	Bajo	Bajo	NO
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director de RR.HH.	Responsable de establecer las expectativas sobre el personal.		Alto	Bajo	SÍ

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Conocimiento de las actividades empresariales por parte del personal de TI	El personal de TI debe conocer las actividades empresariales básicas de la empresa que apoyan.	Medio	Medio	NO
Habilitador de información				
Matriz de habilidades y competencias	Describir las habilidades y competencias existentes dentro de la organización de TI y permitir el análisis de deficiencias.	Alto	Medio	SÍ
Planes de desarrollo de competencias y habilidades/carrera profesional.	Describir las actividades de crecimiento requerido de perfiles de TI específicos.	Medio	Medio	NO
Descripciones genéricas de la función	Describir los requerimientos de habilidades/experiencia y conocimientos para perfiles genéricos dentro de la organización de TI.	Alto	Medio	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de RR.HH.	Gestión de habilidades y competencias.	Medio	Medio	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(01) Porcentaje de objetivos y requerimientos estratégicos empresariales respaldados por objetivos estratégicos de TI*
- *(01) Nivel de satisfacción de las partes interesadas con el alcance de la cartera de programas y servicios planificada*
- *(01) Porcentaje de palancas de valor de TI asignados a palancas de valor empresariales*
- *(09) Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de TI a los nuevos requerimientos*
- *(09) Número de procesos de negocio críticos soportados por infraestructuras y aplicaciones actualizadas*
- *(09) Tiempo promedio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada*
- *(11) Niveles de satisfacción de ejecutivos de negocios y TI con los costes y capacidades relacionados con TI*
- *(13) Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto*
- *(13) Número de programas que necesitan reelaboración significativa debido a defectos de calidad*
- *(15) Porcentaje de las partes interesadas que entiende las políticas*
- *(15) Porcentaje de las políticas respaldadas por estándares y prácticas de trabajo eficaces*
- *(16) Porcentaje de personal cuyas habilidades relacionadas con TI son suficientes para la competencia requerida para su función*
- *(16) Porcentaje de personal satisfecho con sus funciones relacionadas con TI*
- *(16) Número de horas de aprendizaje/capacitación por cada miembro del personal*
- *(17) Nivel de conocimiento y comprensión de los ejecutivos de negocio sobre las posibilidades de innovación en TI*
- *(17) Nivel de satisfacción de las partes interesadas con el nivel de conocimientos e ideas sobre innovación en TI*
- *(17) Número de iniciativas aprobadas como resultado de ideas innovadoras de TI*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(APO07) Nivel de satisfacción ejecutiva con la toma de decisiones de gestión*
- *(APO07) Número de decisiones que no se pudieron resolver dentro de las estructuras de la gerencia y fueron escaladas a estructuras de gobierno*
- *(APO07) Porcentaje de rotación de personal*
- *(APO07) Duración promedio de las vacantes*
- *(APO07) Porcentaje de puestos de TI vacantes*

0404 Rotación de personal crítico

Título del escenario de riesgo	Rotación de personal crítico
Categoría del escenario de riesgo	04 Experiencia y habilidades en TI
Referencia del escenario de riesgo	0404

Escenario de riesgo
Una empresa de software bien establecida con baja rotación de personal, no tomó en cuenta el tiempo necesario para preparar a nuevo personal especializado de recursos humanos para la jubilación inminente de una gran proporción de su personal. Esta situación afecta principalmente a la moral del personal restante debido al exceso de trabajo necesario para apoyar las operaciones actuales.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso APO07 *Gestionar recursos humanos*, especialmente la gestión para mantener personal adecuado y mantener las habilidades y competencias del personal.

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **interno**, el área de recursos humanos (RR.HH.).

Evento
El evento es un **diseño ineficaz** y/o **ejecución ineficaz** del proceso APO07 *Gestionar recursos humanos*. El evento también es una interrupción del desarrollo y/o mantenimiento del software con el que trabaja la empresa.

Activo/Recurso (causa)
El recurso que conduce al impacto en el negocio es el **proceso** APO07 *Gestionar recursos humanos*.

Activo/Recurso (efecto)
Los recursos afectados son los **procesos** de desarrollo y mantenimiento del software con el que la empresa trabaja.

Tiempo
La duración del evento es **extensa** porque el nuevo personal especialista no es fácil de encontrar. El momento de la ocurrencia es **crítico** porque la empresa no puede satisfacer los deseos del cliente, pero los competidores sí pueden hacerlo. El tiempo para detectar la falta de conocimientos y experiencia será **lento**. La consecuencia puede ser fácilmente **demorada** porque es necesario contratar al personal adecuado, y este proceso puede tomar mucho tiempo.

Tipo de riesgo

Habilitar el beneficio/valor de TI	**P**	Falta de habilidades y experiencia para desarrollar y mantener los productos de software.
Entrega del proyecto y programa de TI	**P**	La falta de habilidades y experiencia puede derivar en mala calidad de los proyectos y la insatisfacción de los clientes.
Entrega del servicio y operaciones de TI	**P**	El entorno técnico no puede mantenerse adecuadamente para apoyar el desarrollo y mantenimiento de los productos de software.

Posibles respuestas al riesgo

- **Evitación del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** Contratación de personal externo
- **Mitigación del riesgo:** La empresa considera un programa para retener al personal crítico, mientras hace la transición a personal eficaz para construir un modelo.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de RR.HH.	Describe el desarrollo de requerimientos para la selección y evaluación de perfiles de TI a lo largo de toda la carrera.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título**	**Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
APO02.01	Comprender la dirección de la empresa.	Considerar el entorno empresarial actual, así como los procesos de negocio, la estrategia empresarial y los objetivos futuros. Considerar también el entorno externo de la empresa (palancas del sector, regulaciones relevantes y bases de la competencia).	Medio	Bajo	NO
APO06.02	Establecer prioridades para la asignación de recursos.	Implementar un proceso de toma de decisiones para establecer prioridades sobre la asignación de recursos y reglas para las inversiones discrecionales por unidades del negocio individuales. Incluir el posible uso de proveedores de servicios externos y considerar las opciones de compra, desarrollo y alquiler.	Medio	Bajo	NO
APO07.01	Mantener una dotación de personal suficiente y adecuada.	Evaluar los requerimientos de personal de forma periódica o ante cambios mayores en los entornos empresariales, operativos o de TI para garantizar que la empresa cuente con suficientes recursos humanos para apoyar las metas y los objetivos empresariales. La dotación de personal incluye tanto los recursos internos como externos.	Alto	Medio	SÍ
APO07.02	Identificar al personal clave de TI.	Identificar al personal clave de TI mientras se minimiza la dependencia en una sola persona que realice una función de trabajo crítica al capturar los conocimientos (documentación), compartir los conocimientos, planificar la sucesión y tener un respaldo de personal.	Alto	Medio	SÍ
APO07.03	Mantener las habilidades y las competencias del personal.	Definir y administrar las habilidades y las competencias del personal necesario. Verificar periódicamente que el personal cuente con las competencias necesarias para realizar sus funciones con base en su formación, capacitación y/o experiencia, y verificar que estas competencias se mantengan usando programas de cualificación y certificación cuando sea apropiado. Dar a los empleados oportunidades de aprendizaje continuas para mantener sus conocimientos, habilidades y competencias al nivel requerido para alcanzar las metas empresariales.	Alto	Alto	SÍ

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director de Informática (CIO)	Responsable del análisis de deficiencias en las habilidades y competencias de TI.	Alto	Alto	SÍ
Director de RR.HH.	Responsable de establecer las expectativas sobre el personal.	Alto	Alto	SÍ
Funciones gerenciales específicas de TI	Responsable de identificar los requerimientos específicos.	Alto	Alto	SÍ

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			

Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Repositorios de conocimientos	Minimizar el efecto de la indisponibilidad parcial de recursos al compartir conocimientos sobre procesos, tecnología, etc.	Medio	Alto	Sí

Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de RR.HH.	Gestión de habilidades y competencias.	Medio	Medio	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(01) Porcentaje de objetivos y requerimientos estratégicos empresariales respaldados por objetivos estratégicos de TI*
- *(01) Nivel de satisfacción de las partes interesadas con el alcance de la cartera de programas y servicios planificada*
- *(01) Porcentaje de palancas de valor de TI asignados a palancas de valor empresariales*
- *(05) Porcentaje de servicios de TI donde se logran los beneficios esperados*
- *(05) Porcentaje de inversiones de TI en las que los beneficios esperados se cumplen o exceden*
- *(07) Porcentaje de partes interesadas del negocio satisfechas que la prestación de servicios de TI cumple con los niveles de servicio acordados*
- *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI*
- *(11) Frecuencia de las evaluaciones de madurez de capacidad y optimización de costes*
- *(11) Tendencia de resultados de la evaluación*
- *(11) Niveles de satisfacción de ejecutivos de negocios y TI con los costes y capacidades relacionados con TI*
- *(13) Número de programas/proyectos a tiempo y dentro del presupuesto*
- *(13) Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto*
- *(16) Porcentaje de personal cuyas habilidades relacionadas con TI son suficientes para la competencia requerida para su función*
- *(16) Porcentaje de personal satisfecho con sus funciones relacionadas con TI*
- *(16) Número de horas de aprendizaje/capacitación por cada miembro del personal*
- *(17) Nivel de conocimiento y comprensión de los ejecutivos de negocios sobre las posibilidades de innovación en TI*
- *(17) Nivel de satisfacción de las partes interesadas con los niveles de conocimientos e ideas sobre innovación en TI*
- *(17) Número de iniciativas aprobadas como resultado de ideas innovadoras de TI*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(APO02) Porcentaje de objetivos en la estrategia de TI que apoyan la estrategia empresarial*
- *(APO02) Porcentaje de objetivos empresariales abordados en la estrategia de TI*
- *(APO02) Tendencias en ROI de las iniciativas incluidas en la estrategia de TI*
- *(APO02) Nivel de retroalimentación de la encuesta de satisfacción de las partes interesadas de la empresa en la estrategia de TI*
- *(APO02) Porcentaje de proyectos en la cartera de proyectos de TI que pueden vincularse directamente a la estrategia de TI*
- *(APO02) Porcentaje de objetivos empresariales estratégicos obtenidos como resultado de iniciativas estratégicas de TI*
- *(APO02) Número de nuevas oportunidades empresariales logradas como resultado directo de los desarrollos de TI*
- *(APO02) Logro de resultados medibles de la estrategia de TI que son parte de las metas de rendimiento del personal*
- *(APO02) Frecuencia de actualizaciones del plan de comunicación de la estrategia de TI*
- *(APO02) Porcentaje de iniciativas estratégicas con responsabilidad asignada*
- *(APO06) Porcentaje de alineación de recursos de TI con iniciativas de alta prioridad*
- *(APO06) Número de problemas escalados sobre la asignación de recursos*
- *(APO07) Nivel de satisfacción ejecutiva con la toma de decisiones de gestión*
- *(APO07) Porcentaje de rotación de personal*
- *(APO07) Duración promedio de las vacantes*
- *(APO07) Porcentaje de puestos de TI vacantes*

0408 Desastre pandémico

Título del escenario de riesgo	Desastre pandémico
Categoría del escenario de riesgo	04 Experiencia y habilidades en TI
Referencia del escenario de riesgo	0408

Escenario de riesgo
Una nueva cepa de la gripe aviar (desarrollada en un laboratorio secreto) ha surgido en las oficinas centrales de una determinada empresa. La cepa de la gripe ha infectado a un gran número de empleados de la empresa. Esto ha incluido a varias personas del consejo de dirección y la mayoría del personal clave de TI. Se debe invocar inmediatamente el programa de continuidad del negocio porque el gobierno y los servicios clave de TI se interrumpen debido a la ausencia de tomadores de decisiones y personal de apoyo, lo que afecta gravemente las operaciones del negocio.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es el acto **malicioso** de desarrollar la nueva cepa de la gripe aviar y su liberación al medio ambiente por parte del laboratorio secreto.

Agente
El agente que genera la amenaza que explota la vulnerabilidad es **externo**, el laboratorio secreto.

Evento
El evento es la **interrupción** de servicios de TI y los procesos de negocio.

Activo/Recurso (causa)
Los activos/recursos que conducen al impacto en el negocio son las **personas** del laboratorio secreto.

Activo/Recurso (efecto)
Los activos/recursos afectados son las **personas** y **la estructura organizativa**, específicamente el personal clave de las oficinas centrales de la empresa y los procesos de negocio.

Tiempo
La duración del evento es **extensa** debido a la falta de personal clave porque el personal afectado por la gripe aviar no se aliviará pronto, si logra hacerlo. El momento de la ocurrencia es **crítico** porque afecta a la mayoría del consejo de dirección y el nivel C al mismo tiempo, lo que significa que el personal clave y su respaldo o suplentes no están disponibles. La detección del evento puede clasificarse como **inmediata** porque el personal afectado por la gripe no se presenta en las oficinas. Por la misma razón, el tiempo transcurrido entre el evento y la consecuencia es **inmediato**.

Tipo de riesgo

Habilitar el beneficio/valor de TI	**S**	Ya que la innovación se detiene completamente, se pierden oportunidades de utilizar la tecnología para mejorar la eficiencia y/o eficacia.
Entrega del proyecto y programa de TI	**P**	Los programas y proyectos se detienen, y no hay una aportación de TI a soluciones empresariales nuevas o mejoradas durante algún tiempo.
Entrega del servicio y operaciones de TI	**P**	La estabilidad, disponibilidad y protección operativa que pueden derivar en la destrucción o reducción de valor a la empresa.

Posibles respuestas al riesgo

- **Evitación del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** La empresa necesita actualizar el plan de desastres pandémicos para garantizar la cadena de mando y la política de seguridad física del sitio.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de Recursos Humanos (RR.HH.)	Describe el desarrollo de requerimientos para la selección y evaluación de perfiles de TI a lo largo de toda la carrera.	Bajo	Bajo	NO

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
DSS01.04	Gestionar el entorno.	Mantener medidas de protección contra los factores ambientales. Instalar equipos y dispositivos especializados para monitorizar y controlar el entorno.	Bajo	Alto	SÍ
DSS01.05	Gestionar las instalaciones.	Gestionar las instalaciones, incluyendo el equipo de suministro eléctrico y comunicaciones, de acuerdo con las leyes y regulaciones, los requerimientos técnicos y del negocio, las especificaciones del proveedor, y las pautas de salud y seguridad.	Bajo	Alto	SÍ
DSS04.05	Revisar, mantener y mejorar el plan de continuidad.	Realizar, en intervalos regulares, una revisión gerencial de la capacidad de continuidad para asegurar que su idoneidad, propiedad y efectividad sean continuas. Gestionar los cambios al plan de acuerdo con el proceso de control de cambios para asegurar que el plan de continuidad se mantenga actualizado y que refleje continuamente los requerimientos del negocio actuales.	Bajo	Medio	NO
DSS05.05	Gestionar el acceso físico a los activos de TI.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a las instalaciones, edificios y áreas debe justificarse, autorizarse, registrarse y monitorizarse. Esto debe aplicarse a todas las personas que entren en las instalaciones, incluyendo personal, personal temporal, clientes, proveedores, visitantes y cualquier otro tercero.	Alto	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director de Informática (CIO)	Responsable del análisis de deficiencias en las habilidades y competencias de TI.		Bajo	Medio	NO
Funciones gerenciales específicas de TI	Responsable de identificar los requerimientos específicos.		Bajo	Medio	NO
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Repositorios de conocimientos	Minimizar el efecto de la indisponibilidad parcial de recursos al compartir conocimientos sobre procesos, tecnología, etc.		Bajo	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Habilitador de personas, habilidades y competencias					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Análisis del negocio	Emparejar las necesidades del negocio con las habilidades de TI requeridas.		Bajo	Medio	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo* • *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI* • *(10) Frecuencia de la evaluación de seguridad con respecto a los estándares y pautas más recientes*
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso
• *(DSS01) Número de procedimientos operativos no estándar ejecutados* • *(DSS01) Número de incidentes causados por problemas operativos* • *(DSS04) Número de sistemas empresariales críticos no cubiertos por el plan de continuidad del negocio* • *(DSS04) Porcentaje de mejoras acordadas en el plan de continuidad del negocio que se han incorporado* • *(DSS04) Porcentaje de problemas identificados que se han abordado posteriormente en el plan* • *(DSS04) Porcentaje de partes interesadas internas y externas que han recibido capacitación en continuidad del negocio* • *(DSS04) Porcentaje de problemas identificados que se han abordado posteriormente en los materiales de formación sobre continuidad del negocio* • *(DSS05) Porcentaje de pruebas periódicas de dispositivos de seguridad ambiental* • *(DSS05) Calificación promedio de las evaluaciones de seguridad física* • *(DSS05) Número de incidentes relacionados con la seguridad física*

05 Operaciones del personal

0501 Derechos de acceso inapropiados

Título de escenario de riesgo	Derechos de acceso inapropiados
Categoría de escenario de riesgo	05 Operaciones del personal
Referencia de escenario de riesgo	0501

Escenario de riesgo
Un usuario desarrolla derechos de acceso inapropiados con el paso del tiempo, por el desempeño de diferentes funciones dentro de la empresa. Esto resulta en un fallo en la segregación de funciones, lo que permite al usuario cometer acciones fraudulentas. El usuario comercial establece un nuevo proveedor, introduce una factura ficticia y paga la factura a una cuenta que le pertenece a él.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso DSS06 *Gestión de los controles de procesos de negocio*, especialmente, la práctica de gestión de funciones, responsabilidades, privilegios de acceso y niveles de autoridad.

Agente
El agente que genera la amenaza que explota la vulnerabilidad es **interno**, el usuario de negocio.

Evento
El evento es un **diseño ineficaz** y/o **ejecución ineficaz** del proceso DSS06 *Gestionar los controles de procesos de negocio,* lo que conduce a controles de acceso que invocan una segregación inadecuada e ineficaz de las funciones.

Activo/Recurso (causa)
El recurso que conduce al impacto en el negocio es el **proceso** DSS06 *Gestionar los controles de procesos de negocio.*

Activo/Recurso (efecto)
Los activos/recursos afectados son las **estructuras organizacionales** (segregación de funciones).

Tiempo
La duración del evento es **extensa** porque el usuario empresarial puede defraudar a la compañía durante un largo período de tiempo antes de que el fraude se detecte. El momento de la ocurrencia es **no crítico**. El evento no se detecta fácilmente. Por lo general, es solo por accidente que tal fraude se descubre, y por lo tanto, la detección es **lenta**. Las consecuencias son **demoradas** porque el usuario empresarial tiene que desarrollar los diferentes derechos de acceso inapropiados a través del tiempo, hasta que pueda usarlos indebidamente para defraudar a la compañía.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Problemas de seguridad y cuestiones de cumplimiento.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Revisión frecuente y eliminación inmediata de los derechos de acceso inapropiados.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de seguridad de la información	• Define las limitaciones de compartir y usar información. • Reglas de conducta, uso aceptable de la tecnología y precauciones necesarias, como la separación de funciones.	Alto	Alto	Sí

Habilitador del proceso

Referencia	Título Descripción	Efecto en la frecuencia	Efecto en el impacto	Control esencial	Control esencial
DSS06.03	Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Gestionar las funciones del negocio, responsabilidades, niveles de autoridad y segregación de funciones necesarias para apoyar los objetivos de proceso del negocio. Autorizar el acceso a cualquier activo de información relacionado con los procesos de información del negocio, incluyendo aquellos bajo custodia del negocio, TI y terceros. Esto asegura que la empresa sepa dónde están los datos y quién está manejando los datos en su nombre.	Alto	Bajo	SÍ

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director de RR.HH.	Responsable de establecer las expectativas sobre el personal.	Medio	Medio	NO
Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Predicar con el ejemplo	Todos son responsables de la protección de la información dentro de la empresa.	Medio	Medio	NO
Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Registros de acceso y eventos	Detección de actividad indebida.	Bajo	Alto	SÍ
Funciones y responsabilidades/ niveles de autoridad asignados	Brindar claridad sobre la distribución organizacional.	Alto	Medio	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de administración de la seguridad	Evitar la actividad maliciosa.	Sí	Bajo	NO
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(DSS06) Porcentaje de inventario completado de procesos críticos y controles clave* • *(DSS06) Porcentaje de cobertura de controles clave dentro de los planes de prueba* • *(DSS06) Número de incidentes y hallazgos del reporte de auditoría que indican una falla de los controles clave* • *(DSS06) Porcentaje de roles de procesos de negocio con derechos de acceso y niveles de autoridad asignados* • *(DSS06) Porcentaje de roles de proceso de negocios con clara separación de funciones* • *(DSS06) Número de incidentes y hallazgos de auditoría debido a violaciones de acceso o de separación de funciones* • *(DSS06) Porcentaje de integridad del registro de transacciones rastreables* • *(DSS06) Número de incidencias en las que no se puede recuperar el historial de transacciones*				

0503 Fallo en el proceso de copias de respaldo

Título del escenario de riesgo	Fallo en el proceso de copias de respaldo
Categoría del escenario de riesgo	05 Operaciones del personal
Referencia del escenario de riesgo	0503

Escenario de riesgo
El proceso diario de copia de seguridad no puede realizar correctamente la copia de seguridad de todos los archivos de datos, y el fallo no se detecta. Se produce un problema operativo que requiere que se restablezca la copia de seguridad. Solo entonces se descubre que no es posible hacerlo, requiriendo que se restaure la última copia de seguridad exitosa, que tiene más de una semana de antigüedad. Esto resulta en la pérdida de varios días de transacciones procesadas y la información de gestión resultante.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** de los procesos DSS01 *Gestionar las operaciones* y DSS04 *Gestionar la continuidad*. La práctica de gestión que falla es gestionar los procesos de copias de respaldo.

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **interno**, un fallo de un proceso interno de copia de seguridad que no es detectado por el personal operativo de TI.

Evento
El evento es un **diseño ineficaz** y/o **ejecución ineficaz** de los procesos DSS01 *Gestionar las operaciones* y DSS04 *Gestionar la continuidad*. Debido a que se trata de un fallo de un proceso interno de copia de seguridad, el sistema envía una alerta sobre el fallo, pero la alerta no es detectada por el personal operativo de TI.

Activo/Recurso (causa)
Los activos/recursos que conducen al impacto en el negocio son los **procesos** DSS01 *Gestionar las operaciones* y DSS04 *Gestionar la continuidad* y **personas y habilidades**, debido al fallo del personal operativo de TI para detectar la alerta de falla de la copia de seguridad de los datos.

Activo/Recurso (efecto)
Los activos/recursos afectados son los **procesos** de negocio en los que se pierden las transacciones procesadas, así como la **información** de gestión.

Tiempo
La duración del evento es **extensa** porque toma algo de tiempo reprocesar las transacciones comerciales. El momento de la ocurrencia es **no crítico** en el momento del fallo. La detección es **inmediata** porque tan pronto como el personal operativo quiere restaurar la copia de seguridad descubre que no es posible hacerlo. El tiempo transcurrido entre el evento y la consecuencia varía porque el fallo de la copia de seguridad podría no detectarse hasta que se requiera para su recuperación.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Problemas de seguridad: disponibilidad de información y problemas de cumplimiento.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Realizar pruebas periódicas de las copias de respaldo.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de seguridad de la información	Reglas de conducta, uso aceptable de la tecnología y precauciones necesarias.	Medio	Medio	NO

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
DSS01.01	Realizar procedimientos operativos.	Mantener y realizar procedimientos operativos y tareas operativas de forma confiable y consistente.	Alto	Alto	SÍ
DSS04.04	Ejercer, probar y revisar el plan de continuidad del negocio (BCP).	Probar los preparativos de continuidad de forma periódica para ejercitar los planes de recuperación ante resultados predeterminados, así como para permitir que se desarrollen soluciones innovadoras, y para ayudar a verificar con el tiempo que el plan funcionará tal como se anticipa.	Alto	Alto	SÍ
DSS04.07	Administrar los procesos de respaldo.	Mantener la disponibilidad de información crítica para el negocio.	Alto	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gerente de seguridad de la información	Responsable de la protección técnica de los activos e información.		Alto	Alto	SÍ
Jefe de operaciones de TI	Responsable de gestionar el entorno operativo.		Alto	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Predicar con el ejemplo	Todos son responsables de la protección de la información dentro de la empresa.		Medio	Medio	NO
Cultura de prevención de errores y accidentes	La gente respeta la importancia de las políticas y los procedimientos.		Alto	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Habilitador de personas, habilidades y competencias					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI					
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo* • *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI* • *(11) Frecuencia de las evaluaciones de madurez de capacidad y optimización de costos* • *(11) Tendencia de resultados de la evaluación* • *(14) Número de incidentes de procesos de negocio causados por la falta de disponibilidad de información* • *(14) Relación y extensión de las decisiones de negocio erróneas en las que la información errónea o no disponible fue un factor clave*					

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso
• *(DSS01) Número de procedimientos operativos no estándar ejecutados* • *(DSS01) Número de incidentes causados por problemas operativos* • *(DSS01) Proporción de eventos en comparación con el número de incidentes* • *(DSS01) Porcentaje eventos operativos críticos cubiertos por sistemas de detección automática* • *(DSS04) Porcentaje de restauración exitosa y oportuna de copias de respaldo o copias de medios alternativos* • *(DSS04) Porcentaje de medios de copia de seguridad transferidos y almacenados de forma segura* • *(DSS04) Número de ejercicios y pruebas que han alcanzado los objetivos de recuperación* • *(DSS04) Frecuencia de pruebas de recuperación de desastres* • *(DSS04) Porcentaje de mejoras acordadas en el plan de continuidad del negocio que se han incorporado* • *(DSS04) Porcentaje de problemas identificados que se han abordado posteriormente en el plan de continuidad del negocio* • *(DSS04) Porcentaje de partes interesadas internas y externas que han recibido capacitación en continuidad del negocio* • *(DSS04) Porcentaje de problemas identificados que se han abordado posteriormente en los materiales de capacitación sobre continuidad del negocio*

0506 Divulgación de datos de clientes a un competidor

Título del escenario de riesgo	Divulgación de datos de clientes a un competidor
Categoría del escenario de riesgo	05 Operaciones del personal
Referencia del escenario de riesgo	0506

Escenario de riesgo
Un miembro interno del personal, que tiene acceso autorizado a información de ventas, hace una copia no autorizada de datos comercialmente sensibles. Este representante de ventas descarga y copia la base de datos de clientes a una unidad USB y luego la entrega a un competidor de la empresa.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es una acción **maliciosa** de un empleado.

Agente
El agente que genera la amenaza que explota la vulnerabilidad es un miembro **interno** del personal, que tiene acceso autorizado a la información de ventas y hace una copia no autorizada de la información.

Evento
El evento es **robo** y **divulgación** De información comercial.

Activo/Recurso (causa)
El recurso que conduce al impacto en el negocio es una **persona**, el representante de ventas.

Activo/Recurso (efecto)
El activo/recurso afectado es la **información** comercial/ de negocio sensible.

Tiempo
La duración del evento probablemente será **extensa** porque la divulgación de datos comerciales puede continuar durante un largo período de tiempo antes de ser detectada. El momento de la ocurrencia es **no crítico**. Debido a que el robo de datos usualmente solo se detecta por accidente, el evento no se puede detectar inmediatamente y la detección se clasifica como **lenta**. El tiempo transcurrido entre el evento y la consecuencia es **demorado**, usualmente mayor cantidad de clientes se irán con un competidor.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Problemas de seguridad.
	S	Cuestiones de cumplimiento.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Se implementarán y/o mejorarán los procedimientos de reclutamiento, controles de acceso y controles de prevención de pérdida de datos (DLP).

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de seguridad de la información	• Define las limitaciones de compartir y usar información. • Reglas de conducta, uso aceptable de la tecnología y requerimientos de precauciones, como la separación de funciones.	Alto	Bajo	SÍ

Habilitador del proceso

Referencia	Título Descripción	Efecto en la frecuencia	Efecto en el impacto	Control esencial	Control esencial
APO07.01	Mantener una dotación de personal suficiente y adecuada.	Evaluar los requerimientos de personal de forma periódica o ante cambios mayores en los entornos empresariales, operativos o de TI para garantizar que la empresa cuente con suficientes recursos humanos para apoyar las metas y los objetivos empresariales. La dotación de personal incluye tanto los recursos internos como externos.	Bajo	Bajo	NO
APO07.02	Identificar al personal clave de TI.	Identificar al personal clave de TI mientras se minimiza la dependencia en una sola persona que realice una función de trabajo crítica mediante la recogida los conocimientos (documentación), compartir los conocimientos, planificar la sucesión y tener un respaldo de personal.	Bajo	Bajo	NO

Habilitador del proceso *(cont.)*					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO07.04	Evaluar el rendimiento laboral de los empleados.	Realizar evaluaciones de rendimiento oportunas de manera periódica de acuerdo con los objetivos individuales derivados del objetivode la empresa, los estándares establecidos, las responsabilidades específicas de trabajo, y el marco de habilidades y competencias. Los empleados deberían recibir asesoramiento sobre el rendimiento y la conducta cuando sea apropiado.	Medio	Bajo	NO
APO07.06	Gestionar al personal por contrato.	Asegurarse de que los consultores y el personal contratado que dan soporte a la empresa con habilidades de TI conozcan y cumplan con las políticas de la empresa y con los requerimientos contractuales acordados.	Medio	Bajo	NO
DSS05.03	Gestionar la seguridad de los terminales.	Asegurarse de que los terminales (p. ej., portátil, computadora de sobremesa, servidor y otros dispositivos móviles o de red o software) estén asegurados a un nivel igual o superior al de los requerimientos de seguridad definidos para la información procesada, almacenada o transmitida.	Alto	Bajo	NO
DSS05.05	Gestionar el acceso físico a los activos de TI.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a las instalaciones, edificios y áreas debe justificarse, autorizarse, registrarse y monitorizarse. Esto debe aplicarse a todas las personas que entren en las instalaciones, incluyendo personal, personal temporal, clientes, proveedores, visitantes y cualquier otro tercero.	Medio	Medio	NO
DSS05.06	Gestionar documentos sensibles y dispositivos de salida.	Establecer protecciones físicas apropiadas, prácticas de contabilización y gestión de inventario para activos de TI sensibles, como formularios especiales, instrumentos negociables, impresoras para fines especiales o tokens de seguridad.	Medio	Bajo	NO
DSS06.02	Controlar el procesamiento de información.	Operar la ejecución de las actividades de los procesos de negocio y los controles relacionados, basándose en el riesgo empresarial, para garantizar que el procesamiento de información sea válido, completo, preciso, oportuno y seguro (p. ej., refleja el uso de negocio legítimo y autorizado).	Alto	Bajo	SÍ
DSS06.03	Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Gestionar las funciones del negocio, responsabilidades, niveles de autoridad y segregación de funciones necesarias para apoyar los objetivos de proceso del negocio. Autorizar el acceso a cualquier activo de información relacionado con los procesos de información del negocio, incluyendo aquellos bajo custodia del negocio, TI y terceros. Esto asegura que la empresa sepa dónde están los datos y quién está manejando los datos en su nombre.	Bajo	Bajo	NO
DSS06.06	Asegurar los activos de información.	Asegurar los activos de información a los que tiene acceso el negocio a través de métodos aprobados, incluyendo información en formato electrónico (como métodos que crean nuevos activos en cualquier forma, dispositivos de medios portátiles, aplicaciones de usuario y dispositivos de almacenamiento), información en forma física (como documentos originales o informes de salida) e información en tránsito. Esto beneficia al negocio al ofrecer una protección de extremo a extremo de la información.	Alto	Bajo	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gerente de seguridad de la información	Responsable de la protección técnica de los activos e información.		Alto	Bajo	SÍ

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Registros de acceso y eventos	Detección de actividad indebida.	Bajo	Alto	SÍ
Funciones y responsabilidades/ niveles de autoridad asignados	Brindar claridad sobre la distribución organizacional.	Alto	Bajo	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gestión de control de acceso	Evitar el acceso físico no autorizado.	Alto	Bajo	SÍ
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de gestión de la seguridad	Evitar la actividad maliciosa.	Alto	Medio	SÍ

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(02) Costo de incumplimiento de TI, incluyendo acuerdos y sanciones, y el impacto de la pérdida reputacional*
- *(02) Número de asuntos de incumplimiento relacionados con la TI reportados a la junta o que causan comentarios o vergüenza públicos*
- *(02) Cobertura de las evaluaciones de cumplimiento*
- *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas de negocio habilitados por TI cubiertos por la evaluación de riesgos*
- *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos*
- *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI*
- *(04) Frecuencia de actualización del perfil de riesgo*
- *(10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o pérdida de reputación*
- *(10) Número de servicios de TI con requisitos de seguridad pendientes*
- *(10) Frecuencia de la evaluación de seguridad con respecto a los estándares y pautas más recientes*
- *(16) Porcentaje de personal satisfecho con sus funciones*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(DSS05) Número de vulnerabilidades descubiertas*
- *(DSS05) Porcentaje de personas que reciben concienciación relacionado con el uso de dispositivos*
- *(DSS05) Número de incidentes que implican dispositivos*
- *(DSS05) Número de dispositivos no autorizados detectados en la red o en el entorno del usuario final*
- *(DSS05) Porcentaje de pruebas periódicas de dispositivos de seguridad ambiental*
- *(DSS05) Calificación promedio de las evaluaciones de seguridad física*
- *(DSS05) Número de incidentes relacionados con la seguridad física*
- *(DSS05) Número de incidentes relacionados con el acceso no autorizado a la información*
- *(DSS06) Porcentaje de inventario completado de procesos críticos y controles clave*
- *(DSS06) Porcentaje de cobertura de los controles clave con planes de prueba*
- *(DSS06) Número de incidentes y hallazgos del reporte de auditoría que indican una falla de los controles clave*
- *(DSS06) Porcentaje de roles de procesos de negocio con derechos de acceso y niveles de autoridad asignados*
- *(DSS06) Porcentaje de roles de proceso de negocios con clara separación de funciones*
- *(DSS06) Número de incidentes y hallazgos de auditoría debido a violaciones de acceso o de separación de funciones*

06 Información

0602 Apagado no controlado

Título del escenario de riesgo	Apagado no controlado
Categoría del escenario de riesgo	06 Información
Referencia del escenario de riesgo	0602

Escenario de riesgo
Una empresa que depende en gran medida de su sistema de ventas de comercio electrónico no está protegida por un sistema de alimentación ininterrumpida (SAI), generador de respaldo, sistema de gestión de bases de datos (DBMS) o una instalación de restauración de transacciones. Después de un fallo en la energía, el servidor que ejecuta el sistema de ventas de comercio electrónico no realiza un apagado controlado, lo que resulta que las tablas de la base de datos se corrompan.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del **proceso** DSS06 *Gestionar controles de procesos de negocio.* Es la falla de la práctica de gestión de control del procesamiento de la información y la actividad respectiva, así como mantener la integridad de los datos durante interrupciones inesperadas en el procesamiento de negocios y confirmar la integridad de los datos después de fallas en el procesamiento.

Agente
No todo tipo de amenaza requiere un agente, p. ej., fallas de equipos o causas naturales. Este evento es una clara falla del equipo (SAI) o el procedimiento "apagado controlado", y no hay ningún agente para este evento.

Evento
El evento es ya sea un **diseño ineficaz** o una **ejecución ineficaz** de un proceso o procedimiento operativo (apagado del sistema). Sin embargo, el evento también se puede clasificar como **destrucción** de la base de datos.

Activo/Recurso (causa)
El activo que conduce al impacto en el negocio es la **infraestructura** (suministro de energía).

Activo/Recurso (efecto)
El activo/recurso afectado es la **información**, la base de datos corrompida.

Tiempo
La duración del evento es **extensa** porque la base de datos permanece dañada y debe ser recuperada de las copias de respaldo. El momento de la ocurrencia del evento (falla de la alimentación) es **crítico** porque, en ese momento, el equipo no estaba en un estado que permitiera un apagado controlado. La detección es **inmediata** porque la falta de integridad de la base de datos se descubre inmediatamente después de la reanudación de los sistemas. El tiempo transcurrido entre el evento y la consecuencia es **inmediato** porque la base de datos es corrompida directamente por el evento (apagado no controlado).

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Interrupción del servicio de TI.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Mantener la integridad de los datos durante interrupciones inesperadas en el proceso de negocio, y confirmar la integridad de los datos después de fallas en el procesamiento. La instalación de un SAI, generador de respaldo e instalación de restauración de transacciones.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de copias de respaldo	Las copias de respaldo están disponibles.	Bajo	Alto	SÍ
Política de continuidad del negocio y de recuperación de desastres	Validar la recuperabilidad de los datos.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
BAI04.05	Investigar y abordar las cuestiones de disponibilidad, rendimiento y capacidad.	Abordar las desviaciones al investigar y resolver los problemas de disponibilidad, rendimiento y capacidad identificados.	Bajo	Medio	NO
DSS01.05	Gestionar las instalaciones.	Gestionar las instalaciones, incluyendo el equipo de suministro eléctrico y comunicaciones, en línea con las leyes y regulaciones, los requerimientos técnicos y del negocio, las especificaciones del proveedor, y las pautas de salud y seguridad.	Alto	Alto	SÍ
DSS04.04	Ejercer, probar y revisar el plan de continuidad del negocio (BCP).	Probar los arreglos de continuidad de forma periódica para ejercer los planes de recuperación ante resultados predeterminados, para permitir que se desarrollen soluciones innovadoras, y para ayudar a verificar a través del tiempo que el plan funcionará tal como se anticipa.	Bajo	Alto	SÍ
DSS06.02	Controlar el procesamiento de información.	Operar la ejecución de las actividades de los procesos de negocio y los controles relacionados, basándose en el riesgo empresarial, para garantizar que el procesamiento de información sea válido, completo, preciso, oportuno y seguro (p. ej., refleja el uso de negocio legítimo y autorizado).	Bajo	Medio	NO
DSS06.04	Gestionar errores y excepciones.	Gestionar las excepciones y los errores del proceso de negocio, y facilitar su corrección. Incluir el escalamiento de los errores del proceso de negocio, las excepciones y la ejecución de las acciones correctivas definidas. Esto ofrece una garantía de la precisión e integridad de los procesos de información del negocio.	Bajo	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Jefe de operaciones de TI	Responsable de implementar controles y medidas apropiados para proteger los datos y el hardware.		Alto	Medio	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La seguridad de la información se practica en las operaciones diarias	Siempre seleccionar la opción más segura para llevar a cabo las operaciones diarias.		Medio	Medio	NO
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Informes de copia de seguridad	Describe el estado de las copias de respaldo.				
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Sistemas de copia de seguridad	Garantizar la correcta recuperación en caso de pérdida, modificación o corrupción de los datos.		Bajo	Alto	SÍ
Habilitador de personas, habilidades y competencias					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades técnicas	Implementar controles y medidas apropiados para proteger los datos y el hardware (p. ej., copia de seguridad de datos, almacenamiento).		Alto	Alto	SÍ

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo* • *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI* • *(14) Número de incidentes de procesos de negocio causados por la falta de disponibilidad de información* • *(14) Relación y extensión de las decisiones erróneas de negocio en las que la información errónea o no disponible fue un factor clave*
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso
• *(BAI04) Número de actualizaciones no planificadas de capacidad, rendimiento o disponibilidad* • *(BAI04) Número de incidentes de disponibilidad* • *(BAI04) Número y porcentaje de problemas sin resolver de disponibilidad, rendimiento y capacidad* • *(DSS01) Número de procedimientos operativos no estándar ejecutados* • *(DSS01) Número de incidentes causados por problemas operativos* • *(DSS01) Proporción de eventos en comparación con el número de incidentes* • *(DSS01) Porcentaje eventos operativos críticos cubiertos por sistemas de detección automática* • *(DSS04) Porcentaje de servicios de TI que satisfacen los requisitos de tiempo de actividad* • *(DSS04) Porcentaje de restauración exitosa y oportuna de copias de respaldo o copias de medios alternativos* • *(DSS04) Porcentaje de medios de copia de seguridad transferidos y almacenados de forma segura* • *(DSS04) Número de sistemas de negocio críticos que no están cubiertos por el plan de copia de seguridad* • *(DSS04) Número de ejercicios y pruebas que han alcanzado los objetivos de recuperación* • *(DSS04) Frecuencia de las pruebas de continuidad del negocio y de recuperación de desastres* • *(DSS04) Porcentaje de mejoras acordadas en el plan de continuidad del negocio que se han incorporado* • *(DSS04) Porcentaje de problemas identificados que se han abordado posteriormente en el plan de continuidad del negocio* • *(DSS04) Porcentaje de partes interesadas internas y externas que han recibido capacitación en continuidad del negocio* • *(DSS04) Porcentaje de problemas identificados que se han abordado posteriormente en los materiales de capacitación sobre continuidad del negocio* • *(DSS06) Porcentaje de inventario completado de procesos críticos y controles clave* • *(DSS06) Porcentaje de cobertura de los controles clave con planes de prueba* • *(DSS06) Número de incidentes y hallazgos del reporte de auditoría que indican una falla de los controles clave* • *(DSS06) Porcentaje de integridad del registro de transacciones rastreables* • *(DSS06) Número de incidencias en las que no se puede recuperar el historial de transacciones*

0607 Modificación de datos del cliente

Título del escenario de riesgo	Modificación de datos del cliente
Categoría del escenario de riesgo	06 Información
Referencia del escenario de riesgo	0607

Escenario de riesgo
En una empresa con procedimientos deficientes de gestión de derechos de acceso, un gerente de ventas recibe por error derechos de gestión de bases de datos (DBA). Este nivel privilegiado de acceso se utiliza entonces para la modificación no autorizada de datos de ventas, lo que resulta en la tergiversación de la actividad de ventas e infla el bono por objetivo de ventas del gerente de ventas. La modificación de datos no se detecta, se emiten los pagos adicionales por los bonos de ventas, y la conducta fraudulenta no se detecta.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un acto **malicioso** y fraudulento.

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **interno**, el gerente de ventas (usuario de negocio).

Evento
El evento es una **modificación no autorizada** de los datos de ventas que fue permitida por el **diseño ineficaz** y/o **ejecución ineficaz** del proceso DSS05 *Gestionar servicios de seguridad*, su práctica de gestión DSS05.04 *Gestionar la identidad del usuario y el acceso lógico*, el proceso DSS06 *Gestionar los controles del proceso de negocio*, y su práctica de gestión DSS06.05 *Garantizar la trazabilidad de los eventos de información y rendición de cuentas*, lo que permitió el gerente de ventas heredar los derechos de acceso de DBA.

Activo/Recurso (causa)
Los activos/recursos que conducen al impacto en el negocio son el proceso DSS05 *Gestionar servicios de seguridad*, y su práctica de gestión DSS05.04 *Gestionar la identidad del usuario y el acceso lógico*, y el proceso DSS06 *Gestionar los controles del proceso de negocio*, y su práctica de gestión DSS06.05 *Garantizar la trazabilidad de los eventos de información y rendición de cuentas*, lo que permitió el gerente de ventas heredar los derechos de acceso de DBA.

Activo/Recurso (efecto)
El activo/recurso afectado es la **información**, los datos de ventas.

Tiempo
La duración del evento es **extensa** porque la modificación de los datos de ventas y la conducta fraudulenta puede pasar desapercibida durante un largo periodo de tiempo antes que se detecte. Debido a que el bono no se calculado ni pagado en el momento de la modificación de los datos de ventas, el momento de la ocurrencia es **crítico**. Debido a que tales modificaciones de datos y acciones fraudulentas generalmente solo se detectaron por accidente, el tiempo de detección se clasifica como **lento**. Por la misma razón, el tiempo transcurrido entre el evento y la consecuencia se clasifica como **demorado**.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Problemas de seguridad.
	S	Cuestiones de cumplimiento.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** La empresa implementará una gestión eficaz de los derechos de acceso privilegiado, incluyendo la revisión periódica de los derechos de acceso heredados y la gestión de cambios en datos, que incluye la trazabilidad de los cambios realizados en los datos, por quién y cuándo.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de seguridad de la información	• Define las limitaciones de compartir y usar información. • Reglas de conducta, uso aceptable de la tecnología y precauciones necesarias, como la separación de funciones.	Alto	Bajo	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
DSS05.04	Gestionar la identidad del usuario y el acceso lógico.	Asegurarse de que todos los usuarios tengan derechos de acceso a la información de acuerdo con sus requerimientos del negocio, y que haya coordinación con las unidades del negocio que gestionan sus propios derechos de acceso en los procesos de negocio.	Alto	Bajo	SÍ
DSS06.01	Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales.	Evaluar y monitorizar continuamente la ejecución de las actividades de los procesos de negocio y los controles relacionados, basándose en el riesgo empresarial, para asegurarse de que los controles de procesamiento estén alineados con las necesidades del negocio.	Medio	Bajo	NO
DSS06.02	Controlar el procesamiento de información.	Operar la ejecución de las actividades de los procesos de negocio y los controles relacionados, basándose en el riesgo empresarial, para garantizar que el procesamiento de información sea válido, completo, preciso, oportuno y seguro (p. ej., refleja el uso de negocio legítimo y autorizado).	Medio	Bajo	NO
DSS06.03	Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Gestionar las funciones del negocio, responsabilidades, niveles de autoridad y segregación de funciones necesarias para apoyar los objetivos de proceso del negocio. Autorizar el acceso a cualquier activo de información relacionado con los procesos de información del negocio, incluyendo aquellos bajo custodia del negocio, TI y terceros. Esto asegura que la empresa sepa dónde están los datos y quién está manejando los datos en su nombre.	Alto	Medio	SÍ
DSS06.04	Gestionar errores y excepciones.	Gestionar las excepciones y los errores del proceso de negocio, y facilitar su corrección. Incluir el escalamiento de los errores del proceso de negocio, las excepciones y la ejecución de las acciones correctivas definidas. Esto ofrece una garantía de la precisión e integridad de los procesos de información del negocio.	Bajo	Bajo	NO
DSS06.05	Asegurar la trazabilidad de los eventos de información y la rendición de cuentas.	Asegurarse de que la información del negocio pueda rastrearse hasta el evento del negocio que la originó y a las partes responsables. Esto permite la trazabilidad de la información durante su ciclo de vida y los procesos relacionados. Esto ofrece la seguridad de que la información que impulsa al negocio es confiable y que se ha procesado de acuerdo con objetivos definidos.	Medio	Alto	SÍ

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gerente de seguridad de la información	Proporcionar asesoría sobre los controles y medidas apropiados para proteger los datos y el hardware.	Medio	Medio	NO

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La seguridad de la información se practica en las operaciones diarias	Siempre seleccionar la opción más segura respecto a las operaciones diarias.	Medio	Bajo	NO
Solo necesidad de acceso	Limitar el acceso del personal sin afectar al rendimiento.	Alto	Bajo	SÍ
Todos son responsables de la protección de la información dentro de la empresa	Predicar con el ejemplo.	Bajo	Bajo	NO

Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Campañas de prevención de pérdida de datos	Aumentar la conciencia dentro de la empresa.	Medio	Bajo	NO
Acuerdos de no divulgación	Proteger contractualmente la propiedad intelectual (IP), al disuadir al personal divulgar información a partes maliciosas.	Medio	Medio	NO
Registros de acceso y eventos	Detección de actividad indebida.	Bajo	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Control de acceso	Prevenir el acceso físico no autorizado.	Alto	Bajo	SÍ
Infraestructura y aplicaciones de protección de datos	Encriptación, contraseñas, monitorización del correo electrónico, etc., para hacer cumplir el principio de privilegios mínimos.	Medio	Medio	NO
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A	Medio	Medio	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(02) Coste de incumplimiento de TI, incluyendo acuerdos y sanciones, y el impacto de la pérdida reputacional*
- *(02) Número de asuntos de incumplimiento relacionados con la TI reportados a la junta o que causan comentarios o vergüenza públicos*
- *(02) Cobertura de las evaluaciones de cumplimiento*
- *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas de negocio habilitados por TI cubiertos por la evaluación de riesgos*
- *(10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o pérdida de reputación*
- *(10) Número de servicios de TI con requisitos de seguridad pendientes*
- *(10) Plazo para otorgar, cambiar o eliminar los privilegios de acceso, en comparación con los niveles de servicio acordados*
- *(10) Frecuencia de la evaluación de seguridad con respecto a los estándares y pautas más recientes*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(DSS05) Número de vulnerabilidades descubiertas*
- *(DSS05) Tiempo promedio entre el cambio y la actualización de las cuentas*
- *(DSS05) Número de cuentas (frente al número de usuarios/personal no autorizados)*
- *(DSS05) Número de incidentes relacionados con el acceso no autorizado a la información*
- *(DSS06) Porcentaje de inventario completado de procesos críticos y controles clave*
- *(DSS06) Porcentaje de cobertura de los controles clave con planes de prueba*
- *(DSS06) Número de incidentes y hallazgos del reporte de auditoría que indican una falla de los controles clave*
- *(DSS06) Porcentaje de roles de procesos de negocio con derechos de acceso y niveles de autoridad asignados*
- *(DSS06) Porcentaje de roles de proceso de negocios con clara separación de funciones*
- *(DSS06) Número de incidentes y hallazgos de auditoría debido a violaciones de acceso o de separación de funciones*
- *(DSS06) Porcentaje de integridad del registro de transacciones rastreables*
- *(DSS06) Número de incidencias en las que no se puede recuperar el historial de transacciones*

0608 Divulgación de datos del paciente

Título del escenario de riesgo	Divulgación de datos del paciente
Categoría del escenario de riesgo	06 Información
Referencia del escenario de riesgo	0608

Escenario de riesgo
Un auxiliar administrativo en una compañía de seguros crea un mensaje de correo electrónico en texto simple que contiene los datos de identificación del paciente, detallando las condiciones médicas, y lo envía a la lista de distribución de correo electrónico incorrecta por error. El auxiliar administrativo no se da cuenta de su error, o se da cuenta, pero no dice nada sobre el error. Esto resulta en la divulgación inapropiada de información de identificación del paciente.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es divulgación **accidental** inapropiada de información de identificación del paciente.

Agente
El agente que genera la amenaza que explota una vulnerabilidad es interno, un **usuario** de negocio (el auxiliar administrativo).

Evento
El evento es la **divulgación** de información de identificación del paciente.

Activo/Recurso (causa)
El recurso que conduce al impacto en el negocio es **personas y habilidades** porque el auxiliar administrativo comete el error. Una cultura de asignar culpabilidades también podría derivar en la no divulgación del error, que se aplicaría a **estructuras organizacionales**.

Activo/Recurso (efecto)
El recurso afectado es la **información** (los datos del paciente).

Tiempo
El momento es **crítico**. Cuando un usuario se da cuenta de que ha enviado información confidencial a la dirección de correo electrónico equivocada, es esencial que el usuario informe a su supervisor para permitir que la situación se gestione con eficacia. Sin embargo, en la mayoría de las empresas, existe una cultura de culpabilidad, y es poco probable que el usuario admita el error. Por lo tanto, la duración probablemente será **extensa**, la detección probablemente será **lenta**, y el tiempo transcurrido entre el acontecimiento y la consecuencia es **demorado** porque es probable que el error no se detecte durante un largo período de tiempo.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Problemas de seguridad y cuestiones de cumplimiento.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Se definen la clasificación de datos y los controles de seguridad, como la encriptación de información confidencial antes de enviar mensajes de correo electrónico.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de seguridad de la información	• Define las limitaciones de compartir y usar información. • Reglas de conducta, uso aceptable de la tecnología y precauciones necesarias, como la separación de funciones.	Medio	Medio	NO

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO01.06	Definir la propiedad de la información (datos) y del sistema.	Colocar la capacidad de TI en la estructura organización general para reflejar un modelo empresarial relevante a la importancia de las TI dentro de la empresa, específicamente, su criticidad para la estrategia empresarial y el nivel de dependencia operativa en las TI. La línea jerárquica del Director de Informática (CIO) debe ser proporcional a la importancia de las TI dentro de la empresa.	Bajo	Alto	SÍ
DSS05.06	Gestionar documentos sensibles y dispositivos de salida.	Establecer protecciones físicas apropiadas, prácticas de contabilización y gestión de inventario para activos de TI sensibles, como formularios especiales, instrumentos negociables, impresoras para fines especiales o tokens de seguridad.	Alto	Alto	SÍ
DSS06.01	Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales.	Evaluar y monitorizar continuamente la ejecución de las actividades de los procesos de negocio y los controles relacionados, basándose en el riesgo empresarial, para asegurarse de que los controles de proceso estén alineados con las necesidades del negocio.	Medio	Bajo	NO
DSS06.02	Controlar el procesamiento de información.	Operar la ejecución de las actividades de los procesos de negocio y los controles relacionados, basándose en el riesgo empresarial, para garantizar que el procesamiento de información sea válido, completo, preciso, oportuno y seguro (p. ej., refleja el uso comercial legítimo y autorizado).	Alto	Alto	SÍ
DSS06.04	Gestionar errores y excepciones.	Gestionar las excepciones y los errores del proceso de negocio, y facilitar su corrección. Incluir el escalamiento de los errores del proceso de negocio, las excepciones y la ejecución de las acciones correctivas definidas. Esto ofrece una garantía de la precisión e integridad de los procesos de información del negocio.	Bajo	Medio	NO
DSS06.05	Asegurar la trazabilidad de los eventos de información y la rendición de cuentas.	Asegurarse de que la información del negocio pueda rastrearse hasta el evento del negocio que la originó y a las partes responsables. Esto permite la trazabilidad de la información durante su ciclo de vida y los procesos relacionados. Esto ofrece la seguridad de que la información que impulsa al negocio es confiable y que se ha procesado de acuerdo con objetivos definidos.	Bajo	Bajo	NO
DSS06.06	Asegurar los activos de información.	Los activos de información seguros a los que tiene acceso el negocio a través de métodos aprobados, incluyendo información en formato electrónico (como métodos que crean nuevos activos en cualquier forma, dispositivos de medios portátiles, aplicaciones de usuario y dispositivos de almacenamiento), información en forma física (como documentos originales o informes de salida) e información en tránsito. Esto beneficia al negocio al ofrecer una protección de extremo a extremo para la información.	Bajo	Alto	SÍ

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gerente de seguridad de la información	Proporcionar asesoría sobre los controles y medidas apropiados para proteger los datos y el hardware.	Alto	Alto	SÍ

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La seguridad de la información se practica en las operaciones diarias	Siempre seleccionar la opción más segura para llevar a cabo las operaciones diarias.	Alto	Alto	SÍ
Predicar con el ejemplo	Todos son responsables de la protección de la información dentro de la empresa.	Alto	Alto	SÍ

Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Campañas de prevención de pérdida de datos	Aumentar la concientización dentro de la empresa.	Alto	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Infraestructura y aplicaciones de protección de datos	Encriptación, contraseñas, monitorización del correo electrónico, etc., para hacer cumplir el principio de privilegios mínimos.	Medio	Medio	NO
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A	Medio	Medio	NO
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(02) Número de problemas de incumplimiento en relación con acuerdos contractuales con los proveedores de servicios de TI* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo* • *(09) Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas* • *(10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o pérdida de reputación* • *(10) Número de servicios de TI con requisitos de seguridad pendientes* • *(10) Frecuencia de la evaluación de seguridad con respecto a los estándares y pautas más recientes* • *(15) Número de incidentes relacionados al incumplimiento con la política* • *(15) Porcentaje de las partes interesadas que entienden las políticas* • *(15) Porcentaje de las políticas respaldadas por estándares y prácticas de trabajo eficaces*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(APO01) Número de exposiciones de riesgo debido a las deficiencias en el diseño del ambiente de control* • *(DSS05) Número de vulnerabilidades descubiertas* • *(DSS06) Porcentaje de inventario completado de procesos críticos y controles clave* • *(DSS06) Porcentaje de cobertura de los controles clave con planes de prueba* • *(DSS06) Número de incidentes y hallazgos del reporte de auditoría que indican una falla de los controles clave*				

Página dejada intencionadamente en blanco

07 Arquitectura

0701 Incapacidad para implementar la banca móvil

Título del escenario de riesgo	Incapacidad para implementar la banca móvil
Categoría del escenario de riesgo	07 Arquitectura
Referencia del escenario de riesgo	0701

Escenario de riesgo
Un banco de Estados Unidos de tamaño medio está aplicando sistemas host para las aplicaciones de banca básicas, en particular, para la banca personal. El Director de Banca Personal, que es un miembro del consejo de dirección, solicitó que se ofreciera una solución de banca móvil (aplicación) para el mercado minorista y esperaba un retorno de la inversión (ROI) de dos años. Sin embargo, el sistema principal del banco, no es capaz de manejar las comunicaciones con un entorno de aplicación móvil. El Director de Informática (CIO) mantiene una buena relación con el proveedor host y, en una posición defensiva hacia los nuevos sistemas, analizó los requisitos. El CIO llegó a la conclusión de que la solución se puede implementar, pero solo mediante el uso de middleware y sistemas de comunicaciones nuevos. Estas adiciones sobrepasaban el presupuesto previsto, y eran tecnologías nuevas para el banco. Por lo tanto, la iniciativa no fue considerada capaz de crear un ROI aceptable y no se inició.

Sin embargo, los competidores actualmente proporcionan una solución móvil a sus clientes, y los clientes del banco se están cambiando a esos otros bancos.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso APO03 *Gestionar la arquitectura empresarial.*

Agente
Los agentes que generan la amenaza que explota una vulnerabilidad son **internos**, el Director de Banca Personal y el CIO.

Evento
El evento es un **diseño ineficaz** y/o **ejecución ineficaz** del proceso APO03 *Gestionar la arquitectura empresarial.*

Activo/Recurso (causa)
Los recursos que conducen al impacto en el negocio son la falta de un **proceso** eficaz APO03 *Gestionar la arquitectura empresarial* y la **infraestructura TI** porque el sistema host es inflexible e incapaz de satisfacer las expectativas de los clientes.

Activo/Recurso (Efecto)
El recurso afectado es el **proceso** de negocio de banca personal porque no está disponible para dispositivos móviles.

Tiempo
La duración del evento es **extensa** porque no se puede ofrecer la aplicación de software para la banca en dispositivos móviles. El momento de la ocurrencia es **crítico** porque los competidores ya ofrecen soluciones móviles a sus clientes. El evento se detecta durante el estudio y antes de iniciar el proyecto, y por lo tanto, es **moderado**. La consecuencia es **demorada** y continua porque el proyecto no se puede ejecutar.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**P**	Las expectativas de los clientes de disponer de procesos eficientes usando dispositivos móviles no se pueden satisfacer. Los clientes insatisfechos están abandonando el banco.
Entrega del proyecto y programa de TI	**P**	Nuevas soluciones no se pueden desarrollar sin cambios significativos en el entorno de software y hardware, lo que resulta en una falta de agilidad.
Entrega del servicio y operaciones de TI	**N/A**	

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** El consejo está aceptando la incapacidad de aplicar nuevas opciones tecnológicas. El consejo también acepta que la empresa perderá competitividad comercial porque los competidores están proporcionando actualmente un servicio similar a sus clientes, y por lo tanto, pueden perder participación de mercado.
- **Compartir/transferir el riesgo:** El director general ejecutivo (CEO) puede subcontratar la infraestructura de banca móvil y transferir el riesgo a través del contrato de outsourcing.
- **Mitigación del riesgo:** Aplicar la gestión de arquitectura y los escenarios para modificar las capacidades del host y/o para reemplazar el sistema host.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Principios de arquitectura	Los principios de arquitectura definen las reglas y pautas generales subyacentes para el uso y desarrollo de todos los recursos y activos de TI en toda la empresa.	Alto	Alto	SÍ
Procedimiento de excepciones	En casos específicos, se pueden permitir excepciones a las reglas de arquitectura existentes. Se deben describir los casos específicos y el procedimiento a seguir para su aprobación.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO03.01	Comprender la dirección de la empresa.	Considerar el entorno empresarial actual, así como los procesos de negocio, la estrategia empresarial y los objetivos futuros. También considerar el entorno externo de la empresa (impulsores de la industria, regulaciones relevantes y bases de la competencia).	Alto	Alto	SÍ
APO03.02	Desarrollar la visión de arquitectura empresarial.	La visión de la arquitectura ofrece una descripción preliminar de la línea de referencia y las arquitecturas objetivo, cubriendo los dominios empresariales, de información, de datos, de aplicación y de tecnología. La visión de la arquitectura ofrece al patrocinador una herramienta clave para promover los beneficios de las capacidades propuestas a las partes interesadas de la empresa. La visión de la arquitectura describe cómo la nueva capacidad cumplirá con las metas y los objetivos empresariales estratégicos, y abordará las preocupaciones de las partes interesadas cuando se implemente.	Alto	Alto	SÍ
APO03.03	Seleccionar oportunidades y soluciones.	Racionalizar las brechas entre las arquitecturas de referencia y las objetivo, tomando tanto las perspectivas de negocio como las técnicas, y agruparlas lógicamente en paquetes de trabajo del proyecto. Integrar el proyecto con todos los programas de inversión TI habilitados relacionados para asegurarse de que las iniciativas arquitectónicas estén alineadas y habilitar estas iniciativas como parte de un cambio empresarial general. Hacer de esto un esfuerzo colaborativo con las partes interesadas clave del negocio y de TI para evaluar la disposición de transformación de la empresa, e identificar oportunidades, soluciones y todas las restricciones de implementación.	Bajo	Alto	SÍ
APO03.04	Definir la implementación de la arquitectura.	Crear una aplicación viable y plan de migración en alineación con las carteras de programas y proyectos. Asegurarse de que el plan esté estrechamente coordinado para garantizar que se brinde valor y los recursos necesarios estén disponibles para completar el trabajo necesario.	Medio	Alto	SÍ

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Consejo de arquitectura	Garantizar el cumplimiento con la arquitectura objetivo y permitir excepciones cuando sean necesarias.	Alto	Alto	SÍ

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Respetar los estándares acordados	La empresa debe estimular el uso de estándares acordados.	Medio	Medio	NO

Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Modelo de arquitectura	Modelo de arquitectura objetivo.	Alto	Alto	SÍ

Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Software de modelado de arquitectura	La aplicación de modelado optimizará el desarrollo de la arquitectura y minimizará el esfuerzo de analizar el impacto a la arquitectura en caso de excepciones o cambios.	Medio	Alto	SÍ

Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Liderazgo y comunicación	Aclarar los motivos de la arquitectura y las consecuencias potenciales.	Alto	Alto	SÍ
Habilidades de arquitectura	Desarrollar una arquitectura eficiente y eficaz alineada con los requerimientos del negocio.	Alto	Alto	SÍ
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(01) Porcentaje de metas y requerimientos estratégicos empresariales respaldados por metas estratégicas de TI* • *(01) Nivel de satisfacción de las partes interesadas con el alcance de la cartera de programas y servicios planificada* • *(01) Porcentaje de impulsores de valor de TI asignados a impulsores de valor empresariales* • *(09) Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de TI a los nuevos requerimientos* • *(09) Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas* • *(09) Tiempo promedio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada* • *(11) Frecuencia de las evaluaciones de madurez de capacidad y optimización de costos* • *(11) Niveles de satisfacción de ejecutivos de negocios y TI con los costos y capacidades relacionados con TI*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(APO03) Número de excepciones a los estándares y líneas de referencia de la arquitectura solicitadas y concedidas* • *(APO03) Nivel de retroalimentación de los clientes para la arquitectura* • *(APO03) Beneficios logrados del proyecto que pueden rastrearse a la participación en la arquitectura (p. ej., reducción de costos mediante la reutilización)* • *(APO03) Porcentaje de proyectos que utilizan servicios de arquitectura empresarial* • *(APO03) Nivel de retroalimentación de los clientes para la arquitectura* • *(APO03) Fecha de la última actualización de las arquitecturas de dominio y/o federadas* • *(APO03) Número de brechas identificadas en los modelos a lo largo de los dominios empresariales, de información, de datos, de aplicación y de arquitectura tecnológica* • *(APO03) Nivel de retroalimentación de los clientes para la calidad de la información proporcionada* • *(APO03) Porcentaje de proyectos que utilizan el marco y la metodología para reutilizar componentes definidos*				

0702 No se pueden implementar productos nuevos

Título del escenario de riesgo	No se pueden implementar productos nuevos
Categoría del escenario de riesgo	07 Arquitectura
Referencia del escenario de riesgo	0702

Escenario de riesgo
El director general ejecutivo (CEO) de una gran compañía de seguros planea lanzar al mercado ocho nuevos productos por año. No consulta al departamento de TI. El área de desarrollo de productos inicia el proyecto y crea los ocho nuevos productos. A medida que involucran al departamento de TI en el proyecto, se enteran de que, basándose en la arquitectura existente y los antiguos sistemas heredados, el área de TI es capaz únicamente de introducir la administración de cuatro productos nuevos por año. Por lo tanto, se desperdicia al menos la mitad del trabajo del equipo de desarrollo de productos.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso APO03 *Gestionar la arquitectura empresarial.*

Agente
Los agentes que generan la amenaza que explota una vulnerabilidad son **internos**, el CEO y el equipo de desarrollo de productos, ya que no involucran al departamento de TI al inicio del proyecto.

Evento
El evento es un **diseño ineficaz** y/o **ejecución ineficaz** del proceso APO03 *Gestionar la arquitectura empresarial.*

Activo/Recurso (causa)
Los recursos que conducen al impacto en el negocio son la falta de un **proceso** eficaz APO03 *Gestionar la arquitectura empresarial* y la **esa infraestructura** porque el sistema host es incapaz de satisfacer las expectativas de los clientes.

Activo/Recurso (efecto)
El recurso afectado es el **proceso** de negocio de nuevos productos porque la empresa no puede comenzar a vender los nuevos productos.

Tiempo
La duración del evento es **extensa** porque solo cuatro de los nuevos productos se pueden comenzar, y los cuatro restantes se deben retener hasta el año siguiente. El momento de la ocurrencia es **crítico** porque los competidores actualmente ofrecen productos nuevos. El evento no se detecta antes de que la compañía quiera comenzar con los nuevos productos, por lo tanto, es **lento**. La consecuencia es **demorada** y continua porque el proyecto no se puede ejecutar.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**P**	Las expectativas del cliente de emisión de nuevos productos no se pueden satisfacer.
	P	Los clientes insatisfechos están abandonando la compañía de seguros.
Entrega del proyecto y programa de TI	**P**	Los productos nuevos no se pueden desarrollar sin cambios significativos en el entorno de software y hardware, lo que resulta en una falta de agilidad.
Entrega del servicio y operaciones de TI	**N/A**	

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** El consejo de administración está aceptando la incapacidad de lanzar nuevos productos tan rápido como se esperaba, perdiendo así la oportunidad de obtener una ventaja comercial.
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Aplicar la gestión de arquitectura y los escenarios para modificar las capacidades del host y/o para reemplazar el sistema host.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Principios de arquitectura	Los principios de arquitectura definen las reglas y pautas generales subyacentes para el uso y desarrollo de todos los recursos y activos de TI en toda la empresa.	Medio	Medio	NO

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO03.01	Comprender la dirección de la empresa.	Considerar el entorno empresarial actual, así como los procesos de negocio, la estrategia empresarial y los objetivos futuros. También considerar el entorno externo de la empresa (impulsores de la industria, regulaciones relevantes y bases de la competencia).	Alto	Alto	SÍ
APO03.02	Desarrollar la visión de arquitectura empresarial.	La visión de la arquitectura ofrece una descripción preliminar de la línea de referencia y las arquitecturas objetivo, cubriendo los dominios empresariales, de información, de datos, de aplicación y de tecnología. La visión de la arquitectura ofrece al patrocinador una herramienta clave para promover los beneficios de las capacidades propuestas a las partes interesadas de la empresa. La visión de la arquitectura describe cómo la nueva capacidad cumplirá con las metas y los objetivos empresariales estratégicos, y abordará las preocupaciones de las partes interesadas cuando se implemente.	Alto	Alto	SÍ
APO03.03	Seleccionar oportunidades y soluciones.	Racionalizar las brechas entre las arquitecturas de referencia y objetivo, tomando tanto las perspectivas de negocio como técnicas, y agruparlas lógicamente en paquetes de trabajo del proyecto. Integrar el proyecto con todos los programas de inversión habilitados por TI relacionados para asegurarse de que las iniciativas arquitectónicas estén alineadas con, y habilitar estas iniciativas como parte de, un cambio empresarial general. Hacer de este un esfuerzo colaborativo con las partes interesadas clave del negocio y de TI para evaluar la disposición de transformación de la empresa, e identificar oportunidades, soluciones y todas las restricciones de implementación.	Bajo	Alto	SÍ
APO03.04	Definir la implementación de la arquitectura.	Crear una aplicación viable y plan de migración en alineación con las carteras de programas y proyectos. Asegurarse de que el plan esté estrechamente coordinado para garantizar que se brinde valor y los recursos necesarios estén disponibles para completar el trabajo necesario.	Medio	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Consejo de arquitectura	Garantizar el cumplimiento con la arquitectura objetivo y permitir excepciones cuando sean necesarias.		Bajo	Bajo	NO
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Modelo de arquitectura	Modelo de arquitectura objetivo.		Alto	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Software de modelado de arquitectura	La aplicación de modelado optimizará el desarrollo de la arquitectura y minimizará el esfuerzo de analizar el impacto a la arquitectura en caso de excepciones o cambios.		Medio	Alto	SÍ

Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Liderazgo y comunicación	Aclarar los motivos de la arquitectura y las consecuencias potenciales.	Alto	Alto	SÍ
Habilidades de arquitectura	Desarrollar una arquitectura eficiente y eficaz alineada con los requerimientos del negocio.	Alto	Alto	SÍ

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(01) Porcentaje de metas y requerimientos estratégicos empresariales respaldados por metas estratégicas de TI*
- *(01) Nivel de satisfacción de las partes interesadas con el alcance de la cartera de programas y servicios planificada*
- *(01) Porcentaje de impulsores de valor de TI asignados a impulsores de valor empresariales*
- *(09) Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de TI a los nuevos requerimientos*
- *(09) Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas*
- *(09) Tiempo promedio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada*
- *(11) Frecuencia de las evaluaciones de madurez de capacidad y optimización de costos*
- *(11) Niveles de satisfacción de ejecutivos de negocios y TI con los costos y capacidades relacionados con TI*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(APO03) Número de excepciones a los estándares y líneas de referencia de la arquitectura solicitadas y concedidas*
- *(APO03) Nivel de retroalimentación de los clientes para la arquitectura*
- *(APO03) Beneficios logrados del proyecto que pueden rastrearse a la participación en la arquitectura (p. ej., reducción de costos mediante la reutilización)*
- *(APO03) Porcentaje de proyectos que utilizan servicios de arquitectura empresarial*
- *(APO03) Nivel de retroalimentación de los clientes para la arquitectura*
- *(APO03) Fecha de la última actualización de las arquitecturas de dominio y/o federadas*
- *(APO03) Número de brechas identificadas en los modelos a lo largo de los dominios empresariales, de información, de datos, de aplicación y de arquitectura tecnológica*
- *(APO03) Nivel de retroalimentación de los clientes para la calidad de la información proporcionada*
- *(APO03) Porcentaje de proyectos que utilizan el marco y la metodología para reutilizar componentes definidos*

0703 Distribución de dispositivos móviles

Título del escenario de riesgo	Distribución de dispositivos móviles
Categoría del escenario de riesgo	07 Arquitectura
Referencia del escenario de riesgo	0703

Escenario de riesgo
Para satisfacer los requerimientos de la gestión empresarial (miembros del consejo y directivos), el Director de Informática (CIO) distribuyó dispositivos móviles (p. ej., teléfonos inteligentes y tabletas) para que la dirección pueda tener acceso fácilmente a las aplicaciones y el correo electrónico empresariales desde cualquier parte. El CIO no desarrolló un programa para abordar todos los requerimientos de los dispositivos móviles al seguir las buenas prácticas de arquitectura empresarial (p. ej., The Open Group Architecture Framework [TOGAF]). No se desarrollaron políticas y procedimientos de seguridad apropiados. Los dispositivos no están equipados con funciones de seguridad (p. ej., encriptación de información y conexión segura) para conservar la información empresarial en caso de violaciones de seguridad (p. ej., dispositivos robados/perdidos, acceso no autorizado a los dispositivos y su información). Antes de distribuir los dispositivos, su gestión no se basó en buenas prácticas (p. ej., gestión del ciclo de vida y configuración de la línea de referencia).

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso APO03 *Gestionar la arquitectura empresarial.*

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **interno**, el CIO y el gerente de seguridad de la información.

Evento
El evento es un **diseño ineficaz** y/o **ejecución ineficaz** del proceso APO03 *Gestionar la arquitectura empresarial.*

Activo/Recurso (causa)
Los recursos que conducen al impacto empresarial son los **procesos** BAI09 *Gestionar activos*, BAI10 *Gestionar la configuración* y DSS05 *Gestionar servicios de seguridad* debido a la falta de asegurar la cobertura de todas las capacidades, tales como capacitación, seguridad, reemplazo y mesa de ayuda. Otro recurso es **personas y habilidades** porque el CIO está tratando de cumplir con los requisitos del consejo con poca antelación, y el oficial de seguridad de la información no está deteniendo la iniciativa. La **información** también es un recurso debido a la falta de una política para manejar la seguridad de la información sobre la nueva tecnología.

Activo/Recurso (efecto)
El recurso afectado es la **información**, específicamente, la información de seguridad en los dispositivos móviles y en el transporte.

Tiempo
La duración del evento es **extensa** porque El equipar los dispositivos con las funciones de seguridad adecuadas requiere algo de tiempo. El momento de la ocurrencia es **no crítico**. El evento se detecta cuando los dispositivos comienzan a usarse y es **moderado**. La consecuencia es **demorada** y continua porque las debilidades de la seguridad no se pueden abordar inmediatamente y necesitan el análisis apropiado.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**S**	Mayor eficiencia del personal administrativo
Entrega del proyecto y programa de TI	**S**	Retraso en la entrega de resultados de la iniciativa si se consideraron todos los requerimientos
	P	Los dispositivos móviles entregados no son capaces de satisfacer los requerimientos empresariales y legales, en particular, con respecto a las líneas de referencia de seguridad.
Entrega del servicio y operaciones de TI	**P**	La información empresarial puede ser comprometida, lo que conduce a posibles problemas de cumplimiento.

Posibles respuestas al riesgo

- **Evasión del riesgo:** No distribuir dispositivos móviles hasta que la mitigación de riesgos se haya implementado.
- **Aceptación del riesgo:** El consejo acepta la falta de seguridad.
- **Compartir/transferir el riesgo:** Los usuarios móviles son considerados responsables de cualquier daño producido con el dispositivo móvil.
- **Mitigación del riesgo:** Definir una política para personalizar los dispositivos móviles antes de su distribución. Implementar las funciones de seguridad, monitorizar los dispositivos y mantener su seguridad (eliminación remota de los dispositivos perdidos/robados, etc.).

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Principios de arquitectura	Los principios de arquitectura definen las reglas y pautas generales subyacentes para el uso y desarrollo de todos los recursos y activos de TI en toda la empresa.	Alto	Alto	SÍ
Procedimiento de excepciones	En casos específicos, se pueden permitir excepciones a las reglas de arquitectura existentes. Se deben describir los casos específicos y el procedimiento a seguir para su aprobación.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
BAI02.01	Definir y mantener los requerimientos funcionales y técnicos del negocio.	Basándose en el caso de negocio, identificar, priorizar, especificar y acordar los requerimientos de información empresarial, funcionales, técnicos y de control que cubran el alcance/la comprensión de todas las iniciativas necesarias para lograr los resultados esperados de la solución empresarial habilitada para TI propuesta.	Alto	Alto	SÍ
BAI09.03	Gestionar el ciclo de vida del activo.	Gestionar los activos, desde la adquisición hasta su eliminación, para que éstos se usen con la mayor eficacia y eficiencia como sea posible, y se puedan contabilizar y proteger físicamente.	Bajo	Medio	NO
BAI10.02	Establecer y mantener un repositorio de configuración y una línea de referencia.	Establecer y mantener un repositorio de gestión de la configuración y crear líneas de referencias controladas de la configuración.	Bajo	Alto	SÍ
BAI10.03	Mantener y controlar los elementos de configuración.	Mantener un repositorio actualizado de los elementos de configuración completándolo con cambios.	Medio	Medio	NO
BAI10.05	Verificar y revisar la integridad del repositorio de configuración.	Revisar periódicamente el repositorio de configuración y verificar su integridad y precisión en comparación con la meta deseada.	Bajo	Bajo	NO
DSS05.01	Proteger contra malware.	Implementar y mantener medidas de prevención, detección y corrección (especialmente parches de seguridad y anti-malware actualizados) en toda la empresa para proteger los sistemas de información y la tecnología contra virus, gusanos, spyware, spam, etc.	Alto	Bajo	SÍ
DSS05.02	Gestionar la seguridad de la red y las conexiones.	Usar medidas de seguridad y procedimientos de gestión relacionados para proteger la información a través de todos los métodos de conectividad.	Bajo	Alto	SÍ
DSS05.03	Gestionar la seguridad de los terminales.	Asegurarse de que los terminales (p. ej., laptop, computadora de escritorio, servidor y otros dispositivos o software móviles o de red) estén asegurados a un nivel igual o superior al de los requerimientos de seguridad definidos para la información procesada, almacenada o transmitida.	Bajo	Alto	SÍ
DSS05.07	Monitorizar la infraestructura para eventos relacionados con la seguridad.	Usar herramientas de detección de intrusos, monitorizar la infraestructura para detectar accesos no autorizados y asegurarse que los eventos se integren en la monitorización general de eventos y en los procedimientos de gestión de incidentes.	Medio	Medio	NO

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Consejo de arquitectura	Garantizar el cumplimiento con la arquitectura objetivo y permitir excepciones cuando sean necesarias.	Alto	Alto	SÍ

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Respetar políticas y estándares	La empresa debe estimular el uso de estándares acordados.	Alto	Alto	SÍ

Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Modelo de arquitectura	Modelo de arquitectura objetivo.	Medio	Medio	NO

Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Software de modelado de arquitectura	La aplicación de modelado optimizará el desarrollo de la arquitectura y minimizará el esfuerzo de analizar el impacto a la arquitectura en caso de excepciones o cambios.	Medio	Medio	NO
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Liderazgo y comunicación	Aclarar los motivos de la arquitectura y las consecuencias potenciales.	Alto	Alto	SÍ
Habilidades de arquitectura	Desarrollar una arquitectura eficiente y eficaz alineada con los requerimientos del negocio.	Alto	Alto	SÍ
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(02) Costo de incumplimiento de TI, incluyendo acuerdos y multas, y el impacto de la pérdida reputacional* • *(02) Número de asuntos de incumplimiento relacionados con la TI reportados a la junta o que causan comentarios o vergüenza públicos* • *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o pérdida de reputació* • *(10) Número de servicios de TI con requisitos de seguridad pendientes* • *(10) Frecuencia de la evaluación de seguridad con respecto a los estándares y pautas más recientes*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(BAI09) Número de activos no utilizados* • *(BAI09) Número de activos obsoletos* • *(BAI10) Número de desviaciones entre el repositorio de configuración y la configuración en vivo* • *(BAI10) Número de discrepancias en relación con la información de configuración incompleta o faltante* • *(DSS05) Número de vulnerabilidades descubiertas* • *(DSS05) Número de violaciones del firewall (cortafuegos)* • *(DSS05) Porcentaje de personas que reciben entrenamiento de concientización relacionado con el uso de dispositivos de punto final* • *(DSS05) Número de incidentes que implican dispositivos de punto final* • *(DSS05) Número de dispositivos no autorizados detectados en la red o en el entorno del usuario final* • *(DSS05) Número de incidentes relacionados con el acceso no autorizado a la información*				

08 Infraestructura

0802 Sistema no escalable para satisfacer el crecimiento del negocio

Título del escenario de riesgo	Sistema no escalable para satisfacer el crecimiento del negocio
Categoría del escenario de riesgo	08 Infraestructura
Referencia del escenario de riesgo	0802

Escenario de riesgo
Un pequeño comercio tradicional opera una tienda en línea, está aumentando su base de clientes e invierte fuertemente en iniciativas de marketing. Todo el equipo de TI es adquirido por el personal de la tienda que no tiene las habilidades técnicas apropiadas para aplicar las mejores prácticas y las recomendaciones de uso del proveedor. La infraestructura de TI estaba estable y disponible en el pasado, pero cuando la base de usuarios y el uso del sistema aumentan, la disponibilidad del sistema disminuye significativamente, comprometiendo el nivel de servicio necesario para este mercado vertical.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento está en el diseño inadecuado de la infraestructura causado por **accidente/error.**

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **interno**, el propietario de la tienda (director general ejecutivo [CEO]).

Evento
El evento es la **interrupción** causada por una caída significativa de la disponibilidad del sistema y el **diseño ineficaz** de la infraestructura.

Activo/Recurso (causa)
Los recursos que conducen al impacto en el negocio son el **proceso** BAI04 *Gestionar la disponibilidad y capacidad* y los servidores de la **infraestructura de TI** que no son capaces de satisfacer la creciente demanda.

Activo/Recurso (efecto)
Los recursos afectados son los **procesos**, como el proceso de venta (tienda en línea), que con frecuencia no está disponible, así como las **aplicaciones** porque la tienda en línea no está disponible regularmente.

Tiempo
La duración del evento es **extensa** porque se necesita un largo período de tiempo para actualizar o reemplazar la infraestructura. La tienda en línea no está disponible regularmente, por lo que se pierden negocios. Por lo tanto, el momento de la ocurrencia es **crítico**. Debido a que la tienda en línea no está disponible, la detección es **instantánea**. Debido a que momentáneamente no hay negocios, la consecuencia es **inmediata**.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**P**	Las ventas en línea no están disponibles, lo que resulta en negocios perdidos.
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Interrupciones del servicio de TI.

Posibles respuestas al riesgo

- **Evasión del riesgo:** No ofrecer una tienda en línea.
- **Aceptación del riesgo:** El propietario de la tienda acepta los negocios perdidos.
- **Compartir/transferir el riesgo:** Outsourcing del servicio de TI y disponibilidad del acuerdo de nivel de servicio (SLA) acordado, con las penalizaciones apropiadas.
- **Mitigación del riesgo:** Outsourcing del servicio de TI y la disponibilidad del SLA acordado. Actualización del sistema existente para aumentar la capacidad de TI.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Principios de arquitectura	Definir las reglas y pautas generales subyacentes para el uso y desarrollo de todos los recursos y activos de TI en toda la empresa.	Medio	Medio	NO
Política de gestión de cambios	Definir las reglas y pautas para cambiar los componentes de la infraestructura de una manera controlada y segura.	Medio	Medio	NO

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO02.01	Comprender la dirección de la empresa.	Considerar el entorno empresarial actual y los procesos de negocio, así como la estrategia empresarial y los objetivos futuros. También considerar el entorno externo de la empresa (impulsores de la industria, regulaciones relevantes y bases de la competencia).	Alto	Alto	SÍ
APO02.02	Evaluar el entorno, las capacidades y el desempeño actuales.	Evaluar el rendimiento de las capacidades internas actuales del negocio y de TI, así como los servicios de TI externos, y desarrollar una comprensión de la arquitectura empresarial en relación con TI. Identificar los problemas que se están experimentando actualmente y desarrollar recomendaciones en áreas que podrían beneficiarse con una mejora. Considerar los diferenciadores y las opciones de proveedores de servicios, y el impacto financiero y los costos y beneficios potenciales de usar servicios externos.	Alto	Alto	SÍ
BAI04.01	Evaluar la disponibilidad, el rendimiento y la capacidad actuales, y crear una línea de referencia.	Evaluar la disponibilidad, el rendimiento y la capacidad de servicios y recursos para asegurarse de que exista una capacidad y rendimiento con un costo justificable disponibles para dar apoyo a las necesidades del negocio y que cumplan con los acuerdos de nivel de servicio (SLA). Crear líneas de referencia de disponibilidad, rendimiento y capacidad para la comparación en el futuro.	Bajo	Alto	SÍ
BAI04.02	Evaluar el impacto en el negocio.	Identificar servicios importantes para la empresa, asignar servicios y recursos a los procesos de negocio, e identificar dependencias comerciales. Asegurarse de que el impacto de los recursos no disponibles sea totalmente comprendido y aceptado por los propietarios del negocio. Asegurarse de que, para funciones del negocio críticas, se puedan satisfacer los requisitos de disponibilidad de los SLA.	Bajo	Bajo	NO
BAI04.03	Planificar los requerimientos de los servicios nuevos o modificados.	Planificar y priorizar las implicaciones de disponibilidad, rendimiento y capacidad de las necesidades cambiantes del negocio y los requisitos de servicio.	Bajo	Medio	NO
BAI04.04	Monitorizar y revisar la disponibilidad y capacidad.	Monitorizar, medir, analizar, reportar y revisar la disponibilidad, rendimiento y capacidad. Identificar desviaciones de las líneas de referencia establecidas. Revisar los reportes de análisis de tendencias que identifican problemas y variaciones significativos, iniciando acciones cuando sea necesario, y asegurándose que se le dé seguimiento a todos los problemas pendientes.	Bajo	Medio	NO
BAI04.05	Investigar y abordar las cuestiones de disponibilidad, rendimiento y capacidad.	Abordar las desviaciones al investigar y resolver los problemas de disponibilidad, rendimiento y capacidad identificados.	Alto	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Jefe de operaciones de TI	Responsable de la gestión y mantenimiento correctos de la infraestructura de TI.		Bajo	Bajo	NO
Jefe de arquitectura	Diseñar la arquitectura de una manera óptima.		Medio	Medio	NO
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				

Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Modelo de arquitectura	Modelo de arquitectura objetivo.	Alto	Alto	SÍ
Informes de estado de la configuración	Rastrear los cambios a la configuración.	Medio	Medio	NO
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Base de datos de gestión de configuración (CMDB)	Ayudar a identificar las áreas de mejora.	Alto	Alto	SÍ
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de arquitectura	Desarrollar una arquitectura eficiente y eficaz alineada con los requerimientos del negocio.	Alto	Alto	SÍ
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(07) Porcentaje de partes interesadas del negocio satisfechas que la prestación de servicios de TI cumple con los niveles de servicio acordados* • *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI* • *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI* • *(11) Frecuencia de las evaluaciones de madurez de capacidad y optimización de costos* • *(11) Tendencia de resultados de la evaluación* • *(11) Niveles de satisfacción de ejecutivos de negocios y TI con los costos y capacidades relacionados con TI* • *(14) Número de incidentes de procesos de negocio causados por la falta de disponibilidad de información*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(BAI04) Número de actualizaciones no planificadas de capacidad, rendimiento o disponibilidad* • *(BAI04) Número de picos de transición en los que se supera el rendimiento objetivo* • *(BAI04) Número de incidentes de disponibilidad* • *(BAI04) Número de eventos en los que la capacidad ha excedido los límites planificados* • *(BAI04) Número y porcentaje de problemas sin resolver de disponibilidad, rendimiento y capacidad*				

0804 Servicios secundarios

Título del escenario de riesgo	Servicios secundarios
Categoría del escenario de riesgo	08 Infraestructura
Referencia del escenario de riesgo	0804

Escenario de riesgo
Los reguladores del sector requieren a una empresa en particular tener doble centro de datos para apoyar las operaciones de sus sistemas en línea de misión crítica las 24 horas del día, los 7 días de la semana. Ambas instalaciones fueron construidas con infraestructura tecnológica redundante y están conectadas usando fibras ópticas de anillo dual (redundantes). Cuando se redactó la solicitud de propuesta (RFP), no contenía el pre-requisito de que cada anillo de comunicación debía ser ofrecido por diferentes proveedores. El proveedor de comunicaciones que ofreció el servicio intentó reducir sus costos de instalación aprovechando los túneles de metro existentes para desplegar las fibras en lugar de construir su propio sistema de túneles, como lo requieren las regulaciones.

Durante un turno de mantenimiento, los empleados del sistema del metro local estaban reparando los rieles y accidentalmente cortaron la fibra óptica, lo que causó una interrupción en el servicio ofrecido por el proveedor. Esta situación fue detectada inmediatamente por el sistema de monitorización remoto de la empresa, y se enviaron alertas al proveedor de comunicaciones, el cual incumplió con sus acuerdos de nivel de servicio (SLA) y tomó más de tres días para encontrar el lugar donde se cortó la fibra.

Durante ese tiempo, el centro de datos operó en modo de alerta amarilla con servicio reducido y sin capacidad para equilibrar las transacciones o mantener la replicación de datos entre los dos dispositivos existentes de almacenamiento conectado a la red (NAS). Debido a la pérdida de comunicación, la empresa invocó los procedimientos de copia de seguridad de datos en medios de almacenamiento portátiles, y estableció cuatro puntos sincronizados por día, los cuales incurrieron en costos de servicio adicionales.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo accidental** de la infraestructura de TI. Secundariamente, también es un **fallo** del proceso de adquisición.

Agente
Los agentes que generan la amenaza que explota la vulnerabilidad son **internos** y **externos**. El actor interno es el Comité de Dirección (Programas/Proyectos). El actor externo son los empleados del sistema del metro.

Evento
El evento es principalmente una **destrucción** de la infraestructura de TI (red), lo que causó la **interrupción** de los servicios de TI. El evento también es un **diseño ineficaz** y/o **ejecución ineficaz** de los procesos BAI01 *Gestionar programas y proyectos,* específicamente, las prácticas de gestión *Mantener un enfoque estándar para la gestión de programas y proyectos* y *Gestionar los recursos y paquetes de trabajo del proyecto*; y el**diseño ineficaz** y/o **ejecución ineficaz** del proceso BAI03 *Gestionar la identificación y desarrollo de soluciones,* específicamente, la práctica de gestión de *Adquisición de componentes de la solución.*

Activo/Recurso (causa)
Los activos/recursos que conducen al impacto en el negocio son los **procesos** BAI01 *Gestionar programas y proyectos* y BAI03 *Gestionar la identificación y desarrollo de soluciones* y las **personas** del sistema del metro.

Activo/Recurso (efecto)
Los activos/recursos afectados por el evento son los **físicos** y la **estructura de TI** que fue destruida, así como la **información** y las **aplicaciones** que interrumpidas.

Tiempo
La duración del evento es **extensa** porque el proveedor incumplió con sus SLA y tomó más de tres días para encontrar el lugar donde se cortó la fibra. El momento de la ocurrencia es **crítico** porque la compañía actualmente no tiene líneas de comunicación redundantes. El evento fue detectado **inmediatamente** por el sistema de monitorización remoto de la compañía, y se enviaron alertas al proveedor de servicios de comunicaciones. El tiempo transcurrido entre el evento y las consecuencias es también **inmediato** porque en el momento en que se cortó la fibra, ya no había acceso a la red.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**P**	Debido a que la infraestructura de TI no se puede usar para la innovación, se pierden oportunidades de utilizar la tecnología para mejorar la eficiencia y/o eficacia.
Entrega del proyecto y programa de TI	**S**	Debido a que la infraestructura de TI no se puede usar para soportar programas y proyectos, no hay contribución de las TI a soluciones empresariales nuevas o mejoradas durante mucho tiempo.
Entrega del servicio y operaciones de TI	**P**	La estabilidad, disponibilidad y protección operativas se ven afectadas, lo que puede derivar en la destrucción o reducción de valor para la empresa.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Asegurarse de que los programas y proyectos estén correctamente definidos, con requerimientos específicos, incluyendo todas las preocupaciones ambientales.

Mitigación del Riesgo Usando Habilitadores de COBIT 5					
Habilitador de principios, políticas y marco de trabajo					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Principios de arquitectura	Definir las reglas y pautas generales subyacentes para el uso y desarrollo de todos los recursos y activos de TI en toda la empresa.		Alto	Alto	SÍ
Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO02.03	Definir las capacidades objetivo de TI.	Definir las capacidades objetivo del negocio y de TI, así como los servicios de TI requeridos. Esto debe basarse en el entendimiento del entorno y los requerimientos de la empresa; evaluar los procesos de negocio actuales y el entorno y los problemas de TI; y considerar los estándares de referencia, las mejores prácticas y las tecnologías emergentes validadas o las propuestas de innovación.	Bajo	Alto	SÍ
BAI01.01	Mantener un enfoque estándar para la gestión de programas y proyectos.	Mantener un enfoque estándar para la gestión de programas y proyectos que permita la evaluación del gobierno y la gestión, así como las actividades de gestión de toma de decisiones y de entrega, enfocadas en el logro de valor y de las metas (requerimientos, riesgos, costos, calendario, calidad) para el negocio de forma consistente.	Medio	Bajo	NO
BAI01.12	Gestionar los recursos del proyecto y los paquetes de trabajo.	Gestionar los paquetes de trabajo del proyecto estableciendo requerimientos formales para autorizar y aceptar paquetes de trabajo, y asignando y coordinando los recursos del negocio y de TI apropiados.	Medio	Bajo	NO
BAI03.04	Obtener los componentes de la solución.	Adquirir componentes de la solución basados en el plan de adquisiciones de acuerdo con los requerimientos y los diseños detallados, los principios y estándares de la arquitectura, y los procedimientos generales de adquisiciones y contratos de la empresa, requerimientos de aseguramiento de calidad (QA) y estándares de aprobación. Asegurarse de que el proveedor identifique y aborde todos los requerimientos legales y contractuales.	Bajo	Alto	SÍ
DSS01.05	Gestionar las instalaciones.	Gestionar las instalaciones, incluyendo el equipo de suministro eléctrico y comunicaciones, en línea con las leyes y regulaciones, los requerimientos técnicos y del negocio, las especificaciones del proveedor, y las pautas de salud y seguridad.	Alto	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Jefe de operaciones de TI	Responsable de la gestión y mantenimiento correctos de la infraestructura de TI.		Medio	Medio	NO
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Modelo de arquitectura	Modelo de arquitectura objetivo.		Medio	Medio	NO
Inventario actual de activos	Rastrear todos los activos a lo largo de la empresa.		Alto	Alto	SÍ

Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Base de datos de gestión de configuración (CMDB)	Ayudar a identificar las áreas de mejora.	Medio	Medio	SÍ
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de arquitectura	Desarrollar una arquitectura eficiente y eficaz alineada con los requerimientos del negocio.	Alto	Alto	SÍ
Habilidades técnicas	Gestionar los diferentes componentes de la infraestructura.	Medio	Medio	NO
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(05) Porcentaje de inversiones habilitadas para TI en las que se supervisa el logro de beneficios durante todo el ciclo de vida económico* • *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI* • *(13) Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto* • *(13) Número de programas que necesitan reelaboración significativa debido a defectos de calidad* • *(13) Costo del mantenimiento de la aplicación frente al costo total de TI* • *(17) Nivel de conocimiento y comprensión de los ejecutivos de negocios sobre las posibilidades de innovación en TI* • *(17) Nivel de satisfacción de las partes interesadas con los niveles de conocimientos e ideas sobre innovación en TI* • *(17) Número de iniciativas aprobadas como resultado de ideas innovadoras de TI*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(APO02) Porcentaje de iniciativas estratégicas con responsabilidad asignada* • *(BAI01) Porcentaje de partes interesadas efectivamente involucradas* • *(BAI01) Nivel de satisfacción de las partes interesadas con la participación* • *(BAI01) Porcentaje de partes interesadas que aprueban la necesidad empresarial, el alcance, el resultado previsto y el nivel de riesgo del proyecto* • *(BAI01) Porcentaje de actividades alineadas con el alcance y los resultados esperados* • *(BAI01) Porcentaje de desviaciones del plan abordadas* • *(BAI01) Porcentaje de firmas de autorización de las partes interesadas para las revisiones etapa-puerta de los programas activos* • *(BAI01) Porcentaje de beneficios esperados logrados* • *(BAI01) Porcentaje de resultados con aceptación de primera instancia* • *(BAI01) Nivel de satisfacción de las partes interesadas expresado en la revisión de cierre del proyecto* • *(BAI03) Número de diseños de soluciones reelaborados debido a la desalineación con los requerimientos* • *(BAI03) Tiempo necesario para aprobar que el producto de diseño ha cumplido con los requerimientos* • *(BAI03) Número de errores encontrados durante la prueba* • *(BAI03) Número de demandas de mantenimiento que no se satisfacen* • *(DSS01) Número de incidentes causados por problemas operativos* • *(DSS01) Proporción de eventos en comparación con el número de incidentes* • *(DSS01) Porcentaje eventos operativos críticos cubiertos por sistemas de detección automática*				

0805 Segregación inapropiada de redes

Título del escenario de riesgo	Segregación inapropiada de redes
Categoría del escenario de riesgo	08 Infraestructura
Referencia del escenario de riesgo	0805

Escenario de riesgo
La red de una empresa de telecomunicaciones consiste de dos redes clave: una red de oficinas dedicada a procesos corporativos, y una red de operaciones para la prestación de servicios de telecomunicaciones. Las redes son administradas por departamentos de TI separados con diferentes líneas de referencia y procedimientos que están dirigidos por diferentes requerimientos. Los sistemas de telecomunicaciones no pueden, por razones técnicas, ser parchados con poca antelación para mantener el nivel de servicio. La empresa no tiene un proceso común de gestión de incidentes y eventos que aborde ambas redes, lo que garantizaría el manejo y la resolución de incidentes en un período de tiempo apropiado.

Algunos usuarios, debido a su descripción del trabajo, necesitan acceso a ambas redes. Este acceso se realiza con dos tarjetas de interfaz de red en la computadora del usuario final. Sin embargo, estas computadoras no se parchan adecuadamente y son vulnerables a códigos maliciosos.

Una infección de malware de una de esas computadoras resultó en la infección de varias computadoras en la red de operaciones, y debido a la falta de seguridad, también en la red de oficinas.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento está en el diseño inadecuado de la arquitectura de red causada por **error**.

Agente
Los agentes que generan la amenaza que explota la vulnerabilidad son **internos** y **externos**. El agente interno es el Director de Informática (CIO), el oficial de seguridad de la información, el administrador de la red y el administrador de la red de operaciones. Los agentes externos son los desarrolladores del código malicioso.

Evento
El evento es la **interrupción** causada porque los sistemas no está disponibles y por el **diseño ineficaz** de la arquitectura de red.

Activo/Recurso (causa)
Los recursos que conducen al impacto en el negocio son el **proceso** DSS05 *Gestionar los servicios de seguridad*, con la gestión ineficaz de parches y procedimientos inadecuados de incidentes de seguridad, y la **infraestructura de TI**, con sistemas sin parches, la segregación inadecuada de las redes y capacidades de monitorización (p. ej., el sistema de prevención de intrusiones [IPS]).

Activo/Recurso (efecto)
Los recursos afectados son los **procesos**, que no se pueden operar porque no hay servicios de TI disponibles; la **infraestructura de TI** no disponible; la accesibilidad a la **información**; y la accesibilidad a las **aplicaciones**.

Tiempo
La duración del evento es **extensa** porque se requiere un largo período de tiempo para actualizar o reemplazar la infraestructura de red. El momento de la ocurrencia es **crítico** porque los procesos de negocio no están regularmente disponibles, lo que resulta en negocios perdidos. Debido a que los eventos de seguridad no se detectan inmediatamente, la detección es **moderada**. La consecuencia es **inmediata** porque no hay negocios momentáneamente.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Interrupciones del servicio de TI.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** Outsourcing de servicios de gestión de parches.
- **Mitigación del riesgo:** Separar las redes con mecanismos apropiados y aplicar un IPS. Definir y aplicar un proceso de gestión de parches para ambas redes. Monitorizar la seguridad de la red.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Principios de arquitectura	Definir las reglas y pautas generales subyacentes para el uso y desarrollo de todos los recursos y activos de TI en toda la empresa.	Medio	Medio	NO

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO03.01	Comprender la dirección de la empresa.	Considerar el entorno empresarial actual y los procesos de negocio, así como la estrategia empresarial y los objetivos futuros. También considerar el entorno externo de la empresa (impulsores de la industria, regulaciones relevantes y bases de la competencia).	Alto	Alto	SÍ
APO03.02	Desarrollar la visión de arquitectura empresarial.	La visión de la arquitectura ofrece una descripción preliminar de la línea de referencia y las arquitecturas objetivo, cubriendo los dominios empresariales, de información, de datos, de aplicación y de tecnología. La visión de la arquitectura ofrece al patrocinador una herramienta clave para promover los beneficios de las capacidades propuestas a las partes interesadas de la empresa. La visión de la arquitectura describe cómo la nueva capacidad cumplirá con las metas y los objetivos empresariales estratégicos, y abordará las preocupaciones de las partes interesadas cuando se implemente.	Alto	Alto	SÍ
BAI04.01	Evaluar la disponibilidad, el rendimiento y la capacidad actuales, y crear una línea de referencia.	Evaluar la disponibilidad, el rendimiento y la capacidad de servicios y recursos para asegurarse de que exista una capacidad y rendimiento con un costo justificable disponibles para dar apoyo a las necesidades del negocio y que cumplan con los acuerdos de nivel de servicio (SLA). Crear líneas de referencia de disponibilidad, rendimiento y capacidad para la comparación en el futuro.	Bajo	Alto	SÍ
BAI04.02	Evaluar el impacto en el negocio.	Identificar servicios importantes para la empresa, asignar servicios y recursos a los procesos de negocio, e identificar dependencias comerciales. Asegurarse de que el impacto de los recursos no disponibles sea totalmente comprendido y aceptado por los propietarios del negocio. Asegurarse de que, para funciones del negocio críticas, se puedan satisfacer los requisitos de disponibilidad de los SLA.	Bajo	Bajo	NO
BAI04.03	Planificar los requerimientos de los servicios nuevos o modificados.	Planificar y priorizar las implicaciones de disponibilidad, rendimiento y capacidad de las necesidades cambiantes del negocio y los requisitos de servicio.	Bajo	Medio	NO
BAI04.04	Monitorizar y revisar la disponibilidad y capacidad.	Monitorizar, medir, analizar, reportar y revisar la disponibilidad, rendimiento y capacidad. Identificar desviaciones de las líneas de referencia establecidas. Revisar los reportes de análisis de tendencias que identifican problemas y variaciones significativos, iniciando acciones cuando sea necesario, y asegurándose que se le dé seguimiento a todos los problemas pendientes.	Bajo	Medio	NO
BAI04.05	Investigar y abordar las cuestiones de disponibilidad, rendimiento y capacidad.	Abordar las desviaciones al investigar y resolver los problemas de disponibilidad, rendimiento y capacidad identificados.	Alto	Alto	SÍ
BAI09.01	Identificar y registrar los activos actuales.	Mantener un registro actualizado y preciso de todos los activos de TI requeridos para entregar servicios y garantizar la alineación con la gestión de configuración y la gestión financiera.	Alto	Alto	SÍ
BAI09.02	Gestionar activos críticos.	Identificar activos críticos para la provisión de la capacidad de servicio, y tomar acciones para maximizar su confiabilidad y disponibilidad para soportar las necesidades del negocio.	Alto	Alto	SÍ
BAI09.03	Gestionar el ciclo de vida del activo.	Gestionar los activos, desde la adquisición hasta su eliminación, para que éstos se usen con la mayor eficacia y eficiencia como sea posible, y se puedan contabilizar y proteger físicamente.	Bajo	Medio	NO
DSS05.02	Gestionar la seguridad de la red y las conexiones.	Usar medidas de seguridad y procedimientos de gestión relacionados para proteger la información a través de todos los métodos de conectividad.	Bajo	Alto	SÍ
DSS05.07	Monitorizar la infraestructura para detectar eventos relacionados con la seguridad.	Usar herramientas de detección de intrusos, monitorizar la infraestructura para detectar accesos no autorizados y asegurarse que los eventos se integren en la monitorización general de eventos y en los procedimientos de gestión de incidentes.	Medio	Medio	NO

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Jefe de operaciones de TI	Responsable de la gestión y mantenimiento correctos de la infraestructura de TI.	Alto	Alto	SÍ
Jefe de arquitectura	Diseñar la arquitectura de una manera óptima.	Alto	Alto	SÍ
Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Modelo de arquitectura	Modelo de arquitectura objetivo.	Alto	Alto	SÍ
Plan de mantenimiento	Planificar el mantenimiento de la infraestructura de TI.	Bajo	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Base de datos de gestión de configuración (CMDB)	Ayudar a identificar las áreas de mejora.	Medio	Medio	NO
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de arquitectura	Desarrollar una arquitectura eficiente y eficaz alineada con los requerimientos del negocio.	Alto	Alto	SÍ
Habilidades técnicas	Gestionar los diferentes componentes de la infraestructura.	Medio	Medio	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos*
- *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos*
- *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI*
- *(04) Frecuencia de actualización del perfil de riesgo*
- *(10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o pérdida de reputación*
- *(10) Número de servicios de TI con requisitos de seguridad pendientes*
- *(10) Frecuencia de la evaluación de seguridad con respecto a los estándares y pautas más recientes*
- *(11) Frecuencia de las evaluaciones de madurez de capacidad y optimización de costos*
- *(11) Niveles de satisfacción de ejecutivos de negocios y TI con los costos y capacidades relacionados con TI*
- *(14) Nivel de satisfacción del usuario empresarial con la calidad y puntualidad (o disponibilidad) de la información de gestión*
- *(14) Número de incidentes de procesos de negocio causados por la falta de disponibilidad de información*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(BAI04) Número de actualizaciones no planificadas de capacidad, rendimiento o disponibilidad*
- *(BAI04) Número de incidentes de disponibilidad*
- *(BAI04) Número y porcentaje de problemas sin resolver de disponibilidad, rendimiento y capacidad*
- *(BAI09) Número de activos obsoletos*
- *(DSS05) Número de vulnerabilidades descubiertas*
- *(DSS05) Número de violaciones del firewall (cortafuegos)*
- *(DSS05) Número de dispositivos no autorizados detectados en la red o en el entorno del usuario final*
- *(DSS05) Tiempo promedio entre el cambio y la actualización de las cuentas*
- *(DSS05) Número de cuentas (frente al número de usuarios/personal no autorizados)*
- *(DSS05) Número de incidentes relacionados con el acceso no autorizado a la información*

0806 Infraestructura del centro de datos no adaptada a las necesidades crecientes

Título del escenario de riesgo	Infraestructura del centro de datos no adaptada a las necesidades crecientes
Categoría del escenario de riesgo	08 Infraestructura
Referencia del escenario de riesgo	0806

Escenario de riesgo
Un centro de datos alberga equipos operativos, de desarrollo y de pruebas. A medida que aumentaba la demanda de los negocios, se instaló una infraestructura de TI adicional en el centro de datos, pero la infraestructura del centro de datos (p. ej., la capacidad de refrigeración del aire acondicionado) no fue adaptada a las crecientes necesidades.

En las horas pico, los sistemas de desarrollo y pruebas debían apagarse debido al sobrecalentamiento de la sala de servidores. Debido al sobrecalentamiento, algunos servidores tuvieron una falla de hardware, algunos se apagaron de forma independiente, y algunos sistemas de aire acondicionado se averiaron y tuvieron que ser reemplazados.

No había un plan adecuado para mantener la infraestructura física, y se tomaron medidas correctivas de manera *ad hoc*, en lugar de basarse en un plan de continuidad del negocio (BCP) sólido.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento está en el diseño inadecuado del centro de datos causado por **accidente/error.**

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **interno**, el jefe de operaciones.

Evento
El evento es la **interrupción** causada por una caída significativa de la disponibilidad del sistema y el **diseño ineficaz** del centro de datos.

Activo/Recurso (causa)
Los recursos que conducen al impacto en el negocio son el **proceso** BAI09 *Gestionar activos*, p. ej., la gestión ineficaz de la infraestructura, el **proceso** BAI04 *Gestionar la disponibilidad y capacidad* y la **infraestructura** física, debido a la inadecuada infraestructura del centro de datos.

Activo/Recurso (efecto)
Los recursos afectados son **procesos**, como el desarrollo y las pruebas, que no se pueden ejecutar; la **infraestructura de TI** porque el hardware se avería debido al sobrecalentamiento o al apagado; la **infraestructura física** debido a los equipos de aire acondicionado averiados; la **información** porque no está disponible; y las **aplicaciones** porque los entornos de pruebas y desarrollo no están disponibles.

Tiempo
La duración del evento es **extensa** porque se requiere un largo período de tiempo para actualizar o reemplazar la infraestructura. Se pierden negocios porque los sistemas no están disponibles regularmente. Por lo tanto, el momento de la ocurrencia es **crítico**. Debido a que la falla de hardware y la indisponibilidad del sistema son inmediatos, la detección es **instantánea**. Debido a que se requiere un largo período de tiempo para actualizar o reemplazar la infraestructura, las consecuencias son **demoradas**.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**P**	Retrasos en los proyectos porque los entornos de desarrollo y pruebas no estaban disponibles.
Entrega del servicio y operaciones de TI	**P**	Interrupciones del servicio de TI.

Posibles respuestas al riesgo

- **Evasión del riesgo:** Apagar algunos servidores.
- **Aceptación del riesgo:** El consejo de administración acepta el riesgo que se produzcan interrupciones en el servicio.
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Actualizar el equipo de infraestructura para satisfacer las necesidades de la tecnología. Reemplazar los servidores por tecnologías más nuevas y una huella ecológica menor.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Principios de arquitectura	Definir las reglas y pautas generales subyacentes para el uso y desarrollo de todos los recursos y activos de TI en toda la empresa.	Medio	Medio	NO
Política de gestión de cambios	Definir las reglas y pautas para cambiar los componentes de la infraestructura de una manera controlada y segura.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO03.01	Comprender la dirección de la empresa.	Considerar el entorno empresarial actual y los procesos de negocio, así como la estrategia empresarial y los objetivos futuros. También considerar el entorno externo de la empresa (impulsores de la industria, regulaciones relevantes y bases de la competencia).	Alto	Alto	SÍ
APO03.02	Desarrollar la visión de arquitectura empresarial.	La visión de la arquitectura ofrece una descripción preliminar de la línea de referencia y las arquitecturas objetivo, cubriendo los dominios empresariales, de información, de datos, de aplicación y de tecnología. La visión de la arquitectura ofrece al patrocinador una herramienta clave para promover los beneficios de las capacidades propuestas a las partes interesadas de la empresa. La visión de la arquitectura describe cómo la nueva capacidad cumplirá con las metas y los objetivos empresariales estratégicos, y abordará las preocupaciones de las partes interesadas cuando se implemente.	Alto	Alto	SÍ
BAI04.01	Evaluar la disponibilidad, el rendimiento y la capacidad actuales, y crear una línea de referencia.	Evaluar la disponibilidad, el rendimiento y la capacidad de servicios y recursos para asegurarse de que exista una capacidad y rendimiento con un costo justificable disponibles para dar apoyo a las necesidades del negocio y que cumplan con los acuerdos de nivel de servicio (SLA). Crear líneas de referencia de disponibilidad, rendimiento y capacidad para la comparación en el futuro.	Bajo	Alto	SÍ
BAI04.02	Evaluar el impacto en el negocio.	Identificar servicios importantes para la empresa, asignar servicios y recursos a los procesos de negocio, e identificar dependencias comerciales. Asegurarse de que el impacto de los recursos no disponibles sea totalmente comprendido y aceptado por los propietarios del negocio. Asegurarse de que, para funciones del negocio críticas, se puedan satisfacer los requisitos de disponibilidad de los SLA.	Bajo	Bajo	NO
BAI04.03	Planificar los requerimientos de los servicios nuevos o modificados.	Planificar y priorizar las implicaciones de disponibilidad, rendimiento y capacidad de las necesidades cambiantes del negocio y los requisitos de servicio.	Bajo	Medio	NO
BAI04.04	Monitorizar y revisar la disponibilidad y capacidad.	Monitorizar, medir, analizar, reportar y revisar la disponibilidad, rendimiento y capacidad. Identificar desviaciones de las líneas de referencia establecidas. Revisar los reportes de análisis de tendencias que identifican problemas y variaciones significativos, iniciando acciones cuando sea necesario, y asegurándose que se le dé seguimiento a todos los problemas pendientes.	Alto	Medio	SÍ
BAI04.05	Investigar y abordar las cuestiones de disponibilidad, rendimiento y capacidad.	Abordar las desviaciones al investigar y resolver los problemas de disponibilidad, rendimiento y capacidad identificados.	Alto	Alto	SÍ
BAI09.01	Identificar y registrar los activos actuales.	Mantener un registro actualizado y preciso de todos los activos de TI requeridos para entregar servicios y garantizar la alineación con la gestión de configuración y la gestión financiera.	Alto	Alto	SÍ
BAI09.02	Gestionar activos críticos.	Identificar activos críticos para la provisión de la capacidad de servicio, y tomar acciones para maximizar su confiabilidad y disponibilidad para soportar las necesidades del negocio.	Alto	Alto	SÍ
BAI09.03	Gestionar el ciclo de vida del activo.	Gestionar los activos, desde la adquisición hasta su eliminación, para que éstos se usen con la mayor eficacia y eficiencia como sea posible, y se puedan contabilizar y proteger físicamente.	Bajo	Medio	NO
DSS01.05	Gestionar las instalaciones.	Gestionar las instalaciones, incluyendo el equipo de suministro eléctrico y comunicaciones, en línea con las leyes y regulaciones, los requerimientos técnicos y del negocio, las especificaciones del proveedor, y las pautas de salud y seguridad.	Alto	Alto	SÍ

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Jefe de operaciones de TI	Responsable de la gestión y mantenimiento correctos de la infraestructura de TI.	Medio	Alto	SÍ
Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Modelo de arquitectura	Modelo de arquitectura objetivo.	Alto	Alto	SÍ
Inventario actual de activos	Rastrear todos los activos a lo largo de la empresa.	Medio	Bajo	NO
Plan de mantenimiento	Planificar el mantenimiento de la infraestructura de TI.	Medio	Alto	SÍ
Informes de estado de la configuración	Rastrear los cambios a la configuración.	Alto	Medio	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Base de datos de gestión de configuración (CMDB)	Ayudar a identificar las áreas de mejora.	Alto	Alto	SÍ
Habilitador de personas, habilidades y competencias				
Habilidades técnicas	Gestionar los diferentes componentes de la infraestructura.	Alto	Alto	SÍ

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos*
- *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos*
- *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI*
- *(04) Frecuencia de actualización del perfil de riesgo*
- *(07) Porcentaje de partes interesadas del negocio satisfechas que la prestación de servicios de TI cumple con los niveles de servicio acordados*
- *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI*
- *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI*
- *(11) Frecuencia de las evaluaciones de madurez de capacidad y optimización de costos*
- *(11) Tendencia de resultados de la evaluación*
- *(14) Número de incidentes de procesos de negocio causados por la falta de disponibilidad de información*
- *(14) Relación y extensión de las decisiones de negocio erróneas en las que la información errónea o no disponible fue un factor clave*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(BAI04) Número de actualizaciones no planificadas de capacidad, rendimiento o disponibilidad*
- *(BAI04) Número de picos de transición en los que se supera el rendimiento objetivo*
- *(BAI04) Número de incidentes de disponibilidad*
- *(BAI04) Número de eventos en los que la capacidad ha excedido los límites planificados*
- *(BAI04) Número y porcentaje de problemas sin resolver de disponibilidad, rendimiento y capacidad*
- *(DSS01) Número de procedimientos operativos no estándar ejecutados*
- *(DSS01) Número de incidentes causados por problemas operativos*
- *(DSS01) Proporción de eventos en comparación con el número de incidentes*
- *(DSS01) Porcentaje eventos operativos críticos cubiertos por sistemas de detección automática*

Página intencionalmente en blanco

09 Software

0908 Alto número de cambios de emergencia

Título del escenario de riesgo	Alto número de cambios de emergencia
Categoría del escenario de riesgo	09 Software
Referencia del escenario de riesgo	0908

Escenario de riesgo
Los usuarios empresariales frecuentemente requieren cambios en las aplicaciones en vivo con poca antelación, y el personal de TI (desarrollo y operaciones) usa el proceso de cambio de emergencia bien definido para acelerar estas solicitudes. Los cambios de emergencia no requieren la aceptación formal de los usuarios empresariales, y pueden ser transicionados al entorno en vivo inmediatamente. Debido a que el proceso de cambio de emergencia no requiere que se actualicen los requerimientos funcionales y la documentación crítica, a veces estos cambios se omiten en las versiones futuras.

Un análisis de los cambios mostró que el 40% de todos los cambios fueron cambios de emergencia desplegados sin ser probados adecuadamente. Estos cambios causaron el 80% de los incidentes registrados.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso BAI06 *Gestionar cambios.*

Agente
Los agentes que generan la amenaza que explota una vulnerabilidad son **internos**, los desarrolladores de TI, el área de operaciones de TI y los propietarios de negocios.

Evento
El evento es una **modificación** no autorizada y no probada de las aplicaciones.

Activo/Recurso (causa)
Los recursos que conducen al impacto en el negocio son el **proceso** ineficaz BAI06 *Gestionar cambios*, una falta de personas y habilidades para llevar a cabo el aseguramiento de calidad, y una falta de **personas y habilidades** en el personal de negocios que deben participar en el desarrollo y las pruebas. Otro activo que causa los impactos en el negocio son las **aplicaciones** porque una falta de calidad está causando errores y requiere arreglos rápidos y/o una falta de funcionalidad
requiere enmiendas.

Activo/Recurso (efecto)
Los recursos y activos afectados son **procesos** del negocio porque las aplicaciones erróneas causan interrupciones en el servicio de TI, lo que causa interrupciones en el proceso. La **información** también se ve afectada ya que puede cambiarse indebidamente o es inconsistente debido a aplicaciones no probadas y erróneas. La falta de registros de cambios y/o pistas de auditoría hacen que el efecto sobre la información sea aún peor. Las **aplicaciones** se ven afectadas porque se cambian sin ser debidamente probadas.

Tiempo
La duración del evento es **extensa** porque se requiere un largo período de tiempo para cambiar los procesos relacionados y porque el evento es también un asunto cultural. El momento de la ocurrencia puede ser **crítico** porque los sistemas y las aplicaciones no están disponibles para hacer negocios. La detección es **moderada** porque las fallas causadas por los cambios de emergencia usualmente se detectan poco tiempo después de la implementación. Debido a que los sistemas y las aplicaciones pueden estar interrumpidos en ese momento, un cambio de emergencia se pone en producción, y el período de tiempo entre el evento y la consecuencia es **inmediato**.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**S**	Las soluciones actualizadas están disponibles con poca antelación.
Entrega del proyecto y programa de TI	**S**	Entrega rápida de las soluciones.
	S	Los recursos de desarrollo apenas se pueden planificar, lo que provoca retrasos en los proyectos.
Entrega del servicio y operaciones de TI	**P**	Problemas de calidad e interrupciones de servicio debido a aplicaciones no probadas.
	S	Problemas de cumplimiento y seguridad debido a cambios no aprobados.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** Solo los propietarios de negocios que experimentan problemas de calidad y/o disponibilidad pueden aprobar cambios de emergencia.
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Definir y aplicar un proceso sólido de gestión y aprobación de cambios. Actualizar el control de acceso para los desarrolladores al entorno en vivo. Requerir, para los cambios de emergencia, una prueba y documentación exhaustivas después de la implementación en el entorno en vivo para hacer que los cambios de emergencia sean más complejos que los cambios regulares. Requerir una prueba y aprobación formal por parte de la empresa después del despliegue en el entorno en vivo para asegurarse de que el cambio de emergencia abordó el problema y el cambio era necesario con poca antelación.

Mitigación del Riesgo Usando Habilitadores de COBIT 5					
Habilitador de principios, políticas y marco de trabajo					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Política de gestión de cambios	Definir las reglas y pautas para cambiar los componentes de la infraestructura de una manera controlada y segura.		Alto	Alto	SÍ
Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
BAI03.09	Gestionar los cambios de los requerimientos.	Rastrear el estado de requerimientos individuales (incluyendo todos los requerimientos rechazados) durante el ciclo de vida del proyecto, y gestionar la aprobación de cambios de los requerimientos.	Bajo	Medio	NO
BAI06.01	Evaluar, priorizar y autorizar solicitudes de cambio.	Evaluar todas las solicitudes de cambio para determinar el impacto en los procesos de negocio y servicios de TI; y evaluar si el cambio afectará negativamente al entorno operativo y presentará riesgos inaceptables. Asegurarse de que los cambios se registren, categoricen, evalúen, autoricen, prioricen, planifiquen y programen.	Alto	Alto	SÍ
BAI06.02	Gestionar cambios de emergencia.	Gestionar cuidadosamente los cambios de emergencia para minimizar futuros incidentes y asegurarse de que el cambio esté controlado y se realice de forma segura. Verificar que los cambios de emergencia sean evaluados adecuadamente y autorizados después del cambio.	Alto	Alto	SÍ
BAI06.03	Rastrear y reportar el estado de los cambios.	Mantener un sistema de rastreo y reportes para documentar los cambios rechazados, comunicar el estado de los cambios aprobados y en proceso, y los cambios finalizados. Asegurarse de que los cambios aprobados se implementen según lo previsto.	Medio	Medio	SÍ
BAI06.04	Cerrar y documentar los cambios.	Siempre que se implementen cambios, actualizar acordemente la documentación de la solución y del usuario, así como los procedimientos afectados por el cambio.	Medio	Medio	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Jefe de desarrollo	Responsable del diseño y desarrollo adecuados de los componentes de software.		Medio	Medio	NO
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Las pruebas se realizan en todos los niveles apropiados	Los usuarios y desarrolladores cooperan para probar los componentes del software.		Alto	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Plan de aseguramiento de la calidad (QA) (plan de prueba y procedimientos)	Definir los pasos a seguir para garantizar la calidad.		Alto	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				

Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI* • *(07) Porcentaje de partes interesadas del negocio satisfechas que la prestación de servicios de TI cumple con los niveles de servicio acordados* • *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI* • *(10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o pérdida de reputación*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(BAI06) Cantidad de reelaboración causada por cambios fallidos* • *(BAI06) Tiempo y esfuerzo reducidos que se requieren para realizar cambios* • *(BAI06) Número y antigüedad de las solicitudes de cambio congestionadas* • *(BAI06) Porcentaje de cambios sin éxito a las evaluaciones de impacto inadecuadas* • *(BAI06) Porcentaje de cambios totales que son arreglos de emergencia* • *(BAI06) Número de cambios de emergencia no autorizados después del cambio* • *(BAI06) Calificaciones de retroalimentación de las partes interesadas sobre la satisfacción con las comunicaciones*				

0910 Cambios no autorizados a las aplicaciones

Título del escenario de riesgo	Cambios no autorizados a las aplicaciones
Categoría del escenario de riesgo	09 Software
Referencia del escenario de riesgo	0910

Escenario de riesgo
Debido a una falla no detectada en los controles del proceso de despliegue de producción, los desarrolladores de TI tienen la oportunidad de modificar las aplicaciones y desplegar cambios en el entorno en vivo sin la aprobación del propietario de la empresa o del personal de operaciones de TI (falta del principio de cuatro ojos). Para mantenerse al día con el mercado, con un producto en particular, hubo presión comercial significativa para implementar una nueva funcionalidad antes de que fuera probada adecuadamente por el área de aseguramiento de la calidad (QA).

Los desarrolladores, que confían en su trabajo, acordaron aplicar cambios al sistema sin las pruebas adecuadas del usuario final, y con frecuencia, sin informar a los usuarios finales de una nueva funcionalidad. Esta práctica resulta en capacidades adicionales que no se utilizan y la detección tardía de errores en los cambios, y conduce a información incorrecta, interrupción del servicio e incidentes que resultan en pérdidas de negocios.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso BAI06 *Gestionar cambios.*

Agente
Los agentes que generan la amenaza que explota una vulnerabilidad son **internos**, los desarrolladores de TI.

Evento
El evento es una **modificación** no autorizada de las aplicaciones.

Activo/Recurso (causa)
Los recursos que conducen al impacto en el negocio son los **procesos** ineficaces BAI 06 *Gestionar los cambios*, BAI07 *Gestionar la aceptación del cambio y la transición*, y DSS06 *Gestionar los controles de procesos de negocio*, y **personas y habilidades,** como los desarrolladores que están aplicando cambios sin autorización, la falta de personal suficiente para realizar el QA de desarrollo, y la falta de usuarios empresariales que estén involucrados en el desarrollo y las pruebas.

Activo/Recurso (efecto)
Los recursos afectados son los **procesos** causados por alteraciones funcionales nuevas y no planificadas/sin probar, las **aplicaciones** causadas por los cambios funcionales sin las pruebas y la aceptación adecuadas, y la **información** que se cambia indebidamente debido a las fallas de las aplicaciones.

Tiempo
La duración del evento es **extensa** porque se necesita un largo período de tiempo para cambiar los procesos relacionados. El momento de la ocurrencia es **no crítico**. La detección es **lenta** porque las fallas no siempre se pueden detectar inmediatamente. Debido a que se necesita un largo período de tiempo para cambiar el proceso relacionado y actualizar la infraestructura, las consecuencias son **demoradas**.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**P**	La funcionalidad añadida no es utilizada por las funciones del negocio.
Entrega del proyecto y programa de TI	**S**	El uso de recursos de desarrollo no está alineado con las prioridades del negocio, y los recursos apenas se pueden planificar.
Entrega del servicio y operaciones de TI	**P**	Interrupciones en los servicios de TI debido a aplicaciones con fallas.
	S	Problema de cumplimiento debido a cambios no probados y no aprobados.
	S	Problema de cumplimiento y problemas de seguridad porque los desarrolladores tienen acceso al entorno de producción.

Posibles respuestas al riesgo

- **Evasión del riesgo:** Retirar los derechos de acceso de los desarrolladores al entorno de producción.
- **Aceptación del riesgo:** Aprobación del riesgo por parte del consejo de administración. El Director de Informática (CIO) o los desarrolladores no deben tener la capacidad de aceptar la exposición significativa causada por el acceso de los desarrolladores al entorno de producción y la falta de un proceso de cambios.
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Definir y aplicar un proceso sólido de gestión y aprobación de cambios. Actualizar el control de acceso para los desarrolladores al entorno de producción.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de gestión de cambios	Definir las reglas y pautas para cambiar los componentes de la infraestructura de una manera controlada y segura.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
BAI06.01	Evaluar, priorizar y autorizar solicitudes de cambio.	Evaluar todas las solicitudes de cambio para determinar el impacto en los procesos de negocio y servicios de TI; y evaluar si el cambio afectará negativamente al entorno operativo y presentará riesgos inaceptables. Asegurarse de que los cambios se registren, categoricen, evalúen, autoricen, prioricen, planifiquen y programen.	Alto	Bajo	SÍ
BAI06.03	Rastrear y reportar el estado de los cambios.	Mantener un sistema de rastreo y reporte para documentar los cambios rechazados, comunicar el estado de los cambios aprobados y en proceso, y los cambios finalizados. Asegurarse de que los cambios aprobados se implementen según lo previsto.	Bajo	Medio	NO
BAI06.04	Cerrar y documentar los cambios.	Siempre que se implementen cambios, actualizar acordemente la documentación de la solución y del usuario, así como los procedimientos afectados por el cambio.	Bajo	Bajo	NO
BAI07.01	Establecer un plan de implementación.	Establecer un plan de implementación que cubra la conversión de sistemas y datos, los criterios de pruebas de aceptación, la comunicación, la capacitación, la preparación de lanzamientos, la promoción a producción, el apoyo a la producción temprana, un plan de respaldo/abandono, y una revisión postimplementación. Obtener la aprobación de las partes relevantes.	Alto	Alto	SÍ
BAI07.03	Pruebas de aceptación del plan.	Establecer un plan de pruebas basado en estándares de toda la empresa que definen roles, responsabilidades y criterios de entrada y salida. Asegurarse de que el plan sea aprobado por las partes relevantes.	Alto	Alto	SÍ
BAI07.04	Establecer un entorno de pruebas.	Definir y establecer un entorno de pruebas seguro y representativo del entorno planificado para el proceso de negocio y las operaciones de TI, el rendimiento y la capacidad, la seguridad, los controles internos, las prácticas operativas, los requerimientos de calidad y privacidad de datos, y las cargas de trabajo.	Alto	Alto	SÍ
BAI07.05	Realizar pruebas de aceptación.	Probar los cambios de forma independiente de acuerdo con el plan de prueba definido antes de la migración al entorno operativo en vivo.	Alto	Alto	SÍ
BAI07.06	Pasar a producción y gestionar los lanzamientos.	Promover la solución aceptada al negocio y las operaciones. Cuando sea apropiado, ejecutar la solución como una implementación piloto o en paralelo con la solución antigua durante un período definido y comparar el comportamiento y los resultados. Si se producen problemas significativos, volver al entorno original basándose en el plan de respaldo/retiro. Gestionar los lanzamientos de los componentes de la solución.	Medio	Alto	SÍ
DSS06.03	Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Gestionar las funciones del negocio, responsabilidades, niveles de autoridad y segregación de funciones necesarias para apoyar los objetivos de proceso del negocio. Autorizar el acceso a cualquier activo de información relacionado con los procesos de información del negocio, incluyendo aquellos bajo custodia del negocio, TI y terceros. Esto asegura que la empresa sepa dónde están los datos y quién está manejando los datos en su nombre.	Alto	Alto	SÍ

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Jefe de desarrollo	Responsable del diseño y desarrollo adecuados de los componentes de software.	Medio	Medio	NO
Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Las pruebas se realizan en todos los niveles apropiados	Los usuarios y desarrolladores cooperan para probar los componentes del software.	Alto	Alto	SÍ
Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Plan de aseguramiento de la calidad (QA) (plan de prueba y procedimientos)	Definir los pasos a seguir para garantizar la calidad.	Alto	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades técnicas	Diseñar y desarrollar los componentes de software adecuados.	Bajo	Bajo	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos*
- *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos*
- *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI*
- *(04) Frecuencia de actualización del perfil de riesgo*
- *(07) Porcentaje de partes interesadas del negocio satisfechas que la prestación de servicios de TI cumple con los niveles de servicio acordados*
- *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI*
- *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI*
- *(08) Porcentaje de propietarios de procesos de negocio satisfechos con los productos y servicios de soporte de TI*
- *(08) Nivel de comprensión por parte del usuario empresarial de cómo las soluciones tecnológicas apoyan sus procesos*
- *(08) Valor presente neto (VPN) que muestra el nivel de satisfacción empresarial de la calidad y utilidad de las soluciones tecnológicas*
- *(10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o pérdida de reputación*
- *(10) Número de servicios de TI con requisitos de seguridad pendientes*
- *(10) Plazo para otorgar, cambiar o eliminar los privilegios de acceso, en comparación con los niveles de servicio acordados*
- *(10) Frecuencia de la evaluación de seguridad con respecto a los estándares y pautas más recientes*
- *(12) Número de incidentes del procesamiento de negocios causados por errores de integración tecnológica*
- *(12) Número de cambios en los procesos de negocio que deben ser aplazados o reelaborados debido a problemas de integración tecnológica*
- *(12) Número de programas empresariales habilitados para TI retrasados o que incurren en costos adicionales debido a problemas de integración tecnológica*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso
• *(BAI06) Cantidad de reelaboración causada por cambios fallidos*
• *(BAI06) Tiempo y esfuerzo reducidos que se requieren para realizar cambios*
• *(BAI06) Número y antigüedad de las solicitudes de cambio congestionadas*
• *(BAI06) Porcentaje de cambios sin éxito a las evaluaciones de impacto inadecuadas*
• *(BAI06) Porcentaje de cambios totales que son arreglos de emergencia*
• *(BAI06) Número de cambios de emergencia no autorizados después del cambio*
• *(BAI06) Calificaciones de retroalimentación de las partes interesadas sobre la satisfacción con las comunicaciones*
• *(BAI07) Porcentaje de partes interesadas satisfechas con la exhaustividad del proceso de prueba*
• *(BAI07) Número y porcentaje de versiones no listas para lanzarse según el calendario*
• *(BAI07) Número o porcentaje de versiones que no se estabilizan dentro de un período aceptable*
• *(BAI07) Porcentaje de versiones que causan tiempo de inactividad*
• *(BAI07) Número y porcentaje de análisis de causa raíz completados*
• *(DSS06) Porcentaje de inventario completado de procesos críticos y controles clave*
• *(DSS06) Número de incidentes y hallazgos del reporte de auditoría que indican un fallo de los controles clave*
• *(DSS06) Porcentaje de roles de procesos de negocio con derechos de acceso y niveles de autoridad asignados*
• *(DSS06) Porcentaje de roles de proceso de negocios con clara separación de funciones*
• *(DSS06) Número de incidentes y hallazgos de auditoría debido a violaciones de acceso o de separación de funciones*
• *(DSS06) Porcentaje de integridad del registro de transacciones rastreables*
• *(DSS06) Número de incidencias en las que no se puede recuperar el historial de transacciones*

0911 Metodologías de desarrollo y pruebas no gestionadas

Título del escenario de riesgo	Metodologías de desarrollo y pruebas no gestionadas
Categoría del escenario de riesgo	09 Software
Referencia del escenario de riesgo	0911

Escenario de riesgo
El departamento de desarrollo de software de una organización de TI no mantiene un estándar común para el desarrollo de software (p. ej., marco de desarrollo, estándares de implementación) y metodologías de prueba (p. ej., tipos de prueba y requerimientos mínimos). Esta práctica conduce a enfoques diferentes para diversas iniciativas de desarrollo porque la aplicación de metodologías se deja a la discreción de las personas. Las metodologías de prueba (p. ej., pruebas de caja blanca, pruebas de volumen y pruebas de socialización) se aplican basándose en la disponibilidad de tecnología (entorno de pruebas), pero no son impulsadas por el tipo de implementación. La falta de estándares conduce a deficiencias en la calidad del software desarrollado, lo que causa numerosos incidentes. El esfuerzo para adoptar enfoques de pruebas existentes es alto porque hay una baja reutilización de las metodologías de prueba. Los equipos frecuentemente comienzan desde el principio al definir un plan de prueba, lo que lleva a la falta de recursos para las pruebas reales porque el esfuerzo está ligado a la planificación, en lugar de a la ejecución de pruebas.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** de los procesos APO11 *Gestionar la calidad* y BAI07 *Gestionar la aceptación del cambio y la transición.*

Agente
Los agentes que generan la amenaza que explota una vulnerabilidad son **internos**, los desarrolladores de TI y el área de aseguramiento de la calidad (QA) (pruebas).

Evento
El evento es una **modificación** no autorizada de las aplicaciones.

Activo/Recurso (causa)
Los recursos que dieron lugar al impacto en el negocio son los **procesos** ineficaces APO11 *Gestionar la calidad* y BAI07 *Gestionar la aceptación del cambio* porque los enfoques de pruebas consistentes están ausentes. El recurso de **infraestructura de TI** también conduce al impacto en el negocios porque hay una falta de entornos de prueba, p. ej., para pruebas paralelas.

Activo/Recurso (efecto)
Los recursos afectados son los **procesos** de negocio debido a que los procesos ineficiente de QA y de prueba conducen a **aplicaciones** inestables y a datos e **información** inconsistentes. Otros recursos afectados son **personas y habilidades** debido al uso ineficaz del personal de pruebas.

Tiempo
La duración del evento es **extensa** porque se requiere un largo período de tiempo para cambiar los procesos relacionados y la infraestructura de TI. El momento de la ocurrencia es **no crítico.** La detección es **lenta** porque los fallos no siempre se pueden detectar inmediatamente. Debido a que se requiere un largo período de tiempo para cambiar los procesos relacionados y actualizar la infraestructura de TI, las consecuencias son **demoradas**.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**P**	Falta de QA/pruebas adecuadas en los proyectos (la QA no se aplica debido a un enfoque demasiado complejo y extenuante).
	S	Uso ineficiente de recursos humanos y de TI debido a procesos de prueba inmaduros *(ad hoc).*
Entrega del servicio y operaciones de TI	**P**	Problemas de calidad e interrupciones de servicio debido a aplicaciones no probadas.
	S	Problemas de cumplimiento y seguridad debido a cambios no probados.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** Aceptar la falta de QA por parte del Director de Informática (CIO) y los dueños de negocios.
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Aplicar enfoques de pruebas profesionales y actuales (internas o subcontratadas).

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de gestión de cambios	Definir las reglas y pautas para cambiar los componentes de la infraestructura de una manera controlada y segura.	Alto	Alto	SÍ
Procedimiento de respaldo	Pautas en caso de que la restauración sea necesaria.	Bajo	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO11.05	Integrar la gestión de la calidad en soluciones para el desarrollo y la prestación de servicios.	Incorporar prácticas relevantes de gestión de la calidad en la definición, monitorización y gestión continua del desarrollo de soluciones y la oferta de servicios.	Alto	Alto	SÍ
BAI01.09	Gestionar programas y proyectos de calidad.	Preparar y ejecutar un plan de gestión de la calidad, procesos y prácticas, alineadas con el sistema de gestión de calidad (QMS) que describe el programa y el enfoque de calidad hacia el proyecto y cómo se implementará. Todas las partes relevantes deben evaluar y aceptar formalmente el plan, y después deben incorporarse al programa integrado y a los planes del proyecto.	Bajo	Medio	NO
BAI03.01	Diseño de soluciones de alto nivel.	Desarrollar y documentar diseños de alto nivel usando técnicas acordadas de desarrollo con las etapas apropiadas o ágiles y rápidas. Asegurar la alineación con la estrategia de TI y la arquitectura empresarial. Volver a evaluar y actualizar los diseños cuando se presenten problemas significativos durante las fases de diseño detallado o construcción, o conforme evoluciona la solución. Asegurarse de que las partes interesadas participen activamente en el diseño y la aprobación de cada versión.	Alto	Alto	SÍ
BAI03.02	Diseñar componentes detallados para la solución.	Desarrollar, documentar y elaborar diseños detallados progresivamente usando técnicas acordadas de desarrollo ágiles y rápidas, o con las fases apropiadas, abordando todos los componentes (procesos de negocio y controles automatizados y manuales relacionados, apoyando las aplicaciones de TI, los servicios de infraestructura y los productos de tecnología, así como a los socios/proveedores). Asegurarse de que el diseño detallado incluya acuerdos de nivel de servicio (SLA) internos y externos, así como acuerdos de nivel operativo (OLA).	Alto	Alto	SÍ
BAI03.03	Desarrollar los componentes de la solución.	Desarrollar progresivamente los componentes de la solución de acuerdo con los diseños detallados siguiendo métodos de desarrollo y estándares de documentación, requerimientos de QA y estándares de aprobación. Asegurarse que se aborden todos los requerimientos de control en los procesos de negocio, apoyando las aplicaciones de TI y los servicios de infraestructura, los servicios y productos de tecnología, y los socios/proveedores.	Alto	Alto	SÍ
BAI03.04	Adquirir los componentes de la solución.	Adquirir los componentes de la solución basados en el plan de adquisiciones de acuerdo con los requerimientos y los diseños detallados, los principios y estándares de la arquitectura, y los procedimientos generales de adquisiciones y contratos de la empresa, requerimientos de aseguramiento de calidad (QA) y estándares de aprobación. Asegurarse de que el proveedor identifique y aborde todos los requerimientos legales y contractuales.	Alto	Alto	SÍ
BAI03.05	Desarrollar soluciones.	Instalar y configurar las soluciones e integrarlas con las actividades del proceso empresarial. Implementar medidas de control, seguridad y auditabilidad durante la configuración, y durante la integración del hardware y el software de infraestructura, para proteger los recursos y asegurar la disponibilidad y la integridad de los datos. Actualizar el catálogo de servicios para reflejar las soluciones nuevas.	Alto	Alto	SÍ
BAI03.06	Realizar el aseguramiento de calidad (QA).	Desarrollar, aprovisionar y ejecutar un plan de aseguramiento de calidad (QA) alineado con el sistema de gestión de calidad (QMS) para obtener la calidad especificada en la definición de los requerimientos y las políticas y procedimientos de calidad de la empresa.	Alto	Alto	SÍ

Habilitador del proceso *(cont.)*					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
BAI03.07	Prepararse para las pruebas de la solución.	Establecer un plan de pruebas y los entornos requeridos para probar los componentes de la solución individuales e integrados, incluyendo los procesos de negocio, y los servicios, las aplicaciones y la infraestructura de soporte.	Alto	Alto	SÍ
BAI03.08	Ejecutar las pruebas de la solución.	Ejecutar pruebas continuamente durante el desarrollo, incluyendo pruebas de control, de acuerdo con el plan de pruebas definido y las prácticas de desarrollo en el entorno apropiado. Incluir a los propietarios de los procesos de negocio y a los usuarios finales en el equipo de pruebas. Identificar, registrar y priorizar los errores y los problemas que se identificaron durante las pruebas.	Alto	Alto	SÍ
BAI03.09	Gestionar los cambios de los requerimientos.	Rastrear el estado de requerimientos individuales (incluyendo todos los requerimientos rechazados) durante el ciclo de vida del proyecto, y gestionar la aprobación de cambios de los requerimientos.	Alto	Alto	SÍ
BAI03.10	Mantener soluciones.	Desarrollar y ejecutar un plan para el mantenimiento de los componentes de la solución y la infraestructura. Incluir revisiones periódicas en comparación con las necesidades del negocio y los requerimientos operativos.	Alto	Alto	SÍ
BAI03.11	Definir servicios de TI y mantener la cartera de servicios.	Definir y acordar las opciones nuevas o modificadas de servicios de TI o de nivel de servicio. Documentar las definiciones de servicio y las opciones de nivel de servicio nuevas o modificadas en la cartera de servicios.	Alto	Alto	SÍ
BAI07.03	Pruebas de aceptación del plan.	Establecer un plan de pruebas basado en estándares de toda la empresa que definen roles, responsabilidades y criterios de entrada y salida. Asegurarse de que el plan sea aprobado por las partes relevantes.	Bajo	Medio	NO
BAI07.04	Establecer un entorno de pruebas.	Definir y establecer un entorno de pruebas seguro y representativo del entorno planificado para el proceso de negocio y las operaciones de TI, el rendimiento y la capacidad, la seguridad, los controles internos, las prácticas operativas, los requerimientos de calidad y privacidad de datos, y las cargas de trabajo.	Medio	Medio	NO
BAI07.05	Realizar pruebas de aceptación.	Probar los cambios de forma independiente de acuerdo con el plan de prueba definido antes de la migración al entorno operativo en vivo.	Bajo	Medio	NO
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Jefe de desarrollo	Responsable del diseño y desarrollo adecuados de los componentes de software.		Alto	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Las pruebas se realizan en todos los niveles apropiados	Los usuarios y desarrolladores cooperan para probar los componentes del software.		Alto	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Plan de aseguramiento de la calidad (QA) (plan de prueba y procedimientos)	Definir los pasos a seguir para garantizar la calidad.		Alto	Alto	SÍ

Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Ambiente de desarrollo integrado (IDE)	Facilitar el desarrollo; consiste en un editor de código fuente, herramientas de automatización de desarrollo y un depurador.	Medio	Medio	SÍ
Repositorios de conocimientos	Compartir y coordinar conocimientos sobre las actividades de desarrollo.	Alto	Alto	SÍ
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades técnicas	Diseñar y desarrollar los componentes de software adecuados.	Medio	Medio	SÍ

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos*
- *(05) Porcentaje de inversiones habilitadas para TI en las que se supervisa el logro de beneficios durante todo el ciclo de vida económico*
- *(05) Porcentaje de servicios de TI donde se logran los beneficios esperados*
- *(05) Porcentaje de inversiones habilitadas para TI en las que los beneficios afirmados se cumplen o exceden*
- *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI*
- *(07) Porcentaje de partes interesadas del negocio satisfechas que la prestación de servicios de TI cumple con los niveles de servicio acordados*
- *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI*
- *(08) Porcentaje de propietarios de procesos de negocio satisfechos con los productos y servicios de soporte de TI*
- *(08) Valor presente neto (VPN) que muestra el nivel de satisfacción empresarial de la calidad y utilidad de las soluciones tecnológicas*
- *(12) Número de incidentes del procesamiento de negocios causados por errores de integración tecnológica*
- *(12) Número de cambios en los procesos de negocio que deben ser aplazados o reelaborados debido a problemas de integración tecnológica*
- *(12) Número de programas empresariales habilitados para TI retrasados o que incurren en costos adicionales debido a problemas de integración tecnológica*
- *(13) Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto*
- *(13) Número de programas que necesitan reelaboración significativa debido a defectos de calidad*
- *(13) Costo del mantenimiento de la aplicación frente al costo total de TI*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(APO11) Calificación promedio de satisfacción de las partes interesadas para las soluciones y los servicios*
- *(APO11) Porcentaje de partes interesadas satisfechas con la calidad de TI*
- *(APO11) Número de servicios con un plan formal de gestión de la calidad*
- *(APO11) Porcentaje de proyectos revisados que cumplen con las metas y los objetivos de calidad deseados*
- *(APO11) Porcentaje de soluciones y servicios entregados con certificación formal*
- *(APO11) Número de defectos descubiertos antes de la producción*
- *(APO11) Número de procesos con un requerimiento de calidad definido*
- *(APO11) Número de procesos con un reporte formal de evaluación de la calidad*
- *(APO11) Número de SLAs que incluyen criterios de aceptación de la calidad*
- *(BAI01) Nivel de satisfacción de las partes interesadas con la participación*
- *(BAI01) Porcentaje de partes interesadas que aprueban la necesidad empresarial, el alcance, el resultado previsto y el nivel de riesgo del proyecto*
- *(BAI01) Porcentaje de actividades alineadas con el alcance y los resultados esperados*
- *(BAI01) Porcentaje de desviaciones del plan abordadas*
- *(BAI01) Porcentaje de firmas de autorización de las partes interesadas para las revisiones etapa-puerta de los programas activos*
- *(BAI01) Número de problemas de recursos (p. ej., habilidades, capacidad)*
- *(BAI01) Porcentaje de beneficios esperados logrados*
- *(BAI01) Porcentaje de resultados con aceptación de primera instancia*
- *(BAI01) Nivel de satisfacción de las partes interesadas expresado en la revisión de cierre del proyecto*
- *(BAI03) Número de errores encontrados durante la prueba*
- *(BAI03) Número de demandas de mantenimiento que no se satisfacen*
- *(BAI07) Porcentaje de partes interesadas satisfechas con la exhaustividad del proceso de prueba*
- *(BAI07) Número y porcentaje de versiones no listas para lanzarse según el calendario*
- *(BAI07) Número o porcentaje de versiones que no se estabilizan dentro de un período aceptable*
- *(BAI07) Porcentaje de versiones que causan tiempo de inactividad*
- *(BAI07) Número y porcentaje de análisis de causa raíz completados*

10 Propiedad empresarial de TI

1001 Ausencia de asignación de responsabilidades

Título del escenario de riesgo	Ausencia de asignación de responsabilidades
Categoría del escenario de riesgo	10 Propiedad empresarial de TI
Referencia del escenario de riesgo	1001

Escenario de riesgo
Una gran empresa financiera global tiene una estrategia de crecimiento comercial con la expansión a nuevos dominios de negocio. El negocio está cambiando constantemente sus prioridades con poca o ninguna comunicación con la organización de TI. Esta práctica conduce a un cambio constante en los requerimientos de la tecnología en desarrollo y escalamientos frecuentes de la gerencia empresarial al jefe de desarrollo. Existe una situación donde el negocio y el área de TI se culpan constantemente entre sí, donde el negocio no acepta ninguna culpabilidad en el proceso y culpa al área TI. El director general ejecutivo (CEO) informó al Director de Informática (CIO) que uno de los líderes empresariales había presentado al consejo de administración un plan para subcontratar de inmediato toda el área de TI. El CEO solicitó que el CIO y el negocio trabajen juntos para resolver los retos comerciales y cumplir con los negocios.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso BAI01 *Gestionar los programas y los proyectos.*

Agente
Los agentes que generan la amenaza que explota una vulnerabilidad son **internos**, el Comité de Dirección (Programas/Proyectos), los ejecutivos del negocio y propietarios de procesos del negocio, el CIO y el jefe de desarrollo.

Evento
El evento es un **diseño ineficaz** y/o una **ejecución ineficaz** del proceso BAI01 *Gestionar los programas y proyectos.*

Activo/Recurso (causa)
El recurso que conduce al impacto en el negocio es el **proceso** BAI01 *Gestionar los programas y proyectos.* La **estructura organizacional** también conduce a un cierto impacto en el negocio debido a una cultura de asignar culpabilidades causada por el **personal** del negocio y de TI.

Activo/Recurso (efecto)
Los recursos afectados son los **procesos** del negocio porque las nuevas aplicaciones no cumplen con los requerimientos, y por lo tanto, el negocio no está satisfecho con los resultados. Toda la **empresa** se ve afectada porque existe discordia por parte del **personal** del negocio y por el lado del personal de TI.

Tiempo
La duración del evento es **extensa** porque no es fácil cambiar la cultura y no se puede hacer rápidamente. El momento de la ocurrencia es **crítico** porque la empresa está actualmente en una fase de crecimiento del negocio con expansión en nuevos dominios de negocio. A medida que surge un creciente número de disputas entre el negocio y el área de TI, la detección puede clasificarse como **moderada**. Las consecuencias durarán un largo período de tiempo porque la situación (cultura) no se puede mejorar fácil y rápidamente, y por lo tanto, las consecuencias son **demoradas**.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**S**	La cultura de asignar culpabilidades impide a la empresa mejorar la eficiencia y/o eficacia de los procesos de negocio. El área de TI no actúa como un verdadero habilitador para nuevas iniciativas del negocio.
Entrega del proyecto y programa de TI	**P**	La expansión del alcance conduce al rebasamiento presupuestario y de tiempo del proyecto, y afecta la calidad de los resultados del proyecto.
Entrega del servicio y operaciones de TI	**N/A**	

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** Implementar un proceso de gobierno para administrar y priorizar la demanda del negocio. Transferir el riesgo del negocio y del área de TI a un órgano de gobierno, como el Comité de Dirección (Programas/Proyectos).
- **Mitigación del riesgo:** Desarrollar un proceso para trabajar con las áreas de negocio a través del ciclo de vida del desarrollo del sistema (SDLC), incorporando la alineación de requerimientos y organizacional a los requerimientos del negocio. Comunicarse con el negocio sobre los aspectos financieros de la tecnología existente, incluyendo el retorno de la inversión (ROI), el costo total de propiedad (TCO) y los impactos potenciales de las tecnologías futuras.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Principios rectores del gobierno empresarial	Involucrar al negocio y al área de TI.	Alto	Alto	SÍ
Principios de reporte y comunicación	Aclarar los medios de comunicación.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO01.04	Comunicar los objetivos y la dirección de la gerencia.	Concienciar y comunicar, buscando la comprensión de los objetivos y la dirección de TI a las partes interesadas en toda la empresa.	Medio	Medio	NO
APO02.01	Comprender la dirección de la empresa.	Considerar el entorno empresarial actual, así como los procesos de negocio, la estrategia empresarial y los objetivos futuros. También considerar el entorno externo de la empresa (impulsores de la industria, regulaciones relevantes y bases de la competencia).	Medio	Medio	NO
APO05.06	Gestionar el logro de beneficios.	Monitorizar los beneficios de ofrecer y mantener servicios y capacidades de TI apropiados, con base en el caso de negocio acordado y actual.	Alto	Alto	SÍ
BAI01.03	Gestionar la participación de las partes interesadas.	Gestionar la participación de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna que llegue a todas las partes interesadas relevantes. Esto incluye planificar, identificar e involucrar a las partes interesadas y gestionar sus expectativas.	Alto	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Finanzas	Proporcionar una metodología común utilizada por el negocio y por el área de TI para evaluar las oportunidades en términos de valor para la empresa.		Alto	Alto	SÍ
Comité de estrategia (ejecutivo de TI)	Estructura clave que debe asumir la responsabilidad sobre la cooperación entre el área de TI y el negocio.		Alto	Alto	SÍ
Consejo de Dirección	Responsable del establecimiento y mantenimiento del marco de gobierno.		Medio	Medio	NO
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
El negocio y el área de TI trabajan juntos como socios	El negocio toma en cuenta las dificultades que enfrenta el área de TI, y ésta aprende los problemas del negocio.		Alto	Alto	SÍ
Habilitador de información					
Estrategia de TI	Alinear los planes del área de TI con los objetivos del negocio, y esto conducirá a una rendición de cuentas más eficiente del negocio sobre las TI.		Alto	Alto	SÍ
Niveles de autoridad	Aclarar las responsabilidades de toma de decisiones.		Alto	Alto	SÍ
Acuerdos de nivel de servicio (SLA)	Describir el nivel de servicio/los objetivos establecidos para satisfacer las expectativas del negocio.		Alto	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Habilitador de personas, habilidades y competencias					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de gestión de relaciones	El área de TI debe tener las habilidades adecuadas para desarrollar relaciones con las partes interesadas relevantes del negocio.		Medio	Medio	NO
Habilidades/afinidades relacionadas con TI	Los representantes del negocio deben ser capacitados/seleccionados basándose en una afinidad mínima requerida con TI.		Medio	Medio	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(01) Porcentaje de metas y requerimientos estratégicos empresariales respaldados por metas estratégicas de TI*
- *(01) Nivel de satisfacción de las partes interesadas con el alcance de la cartera de programas y servicios planificada*
- *(01) Porcentaje de impulsores de valor de TI asignados a impulsores de valor empresariales*
- *(05) Porcentaje de inversiones habilitadas para TI en las que se supervisa el logro de beneficios durante todo el ciclo de vida económico*
- *(05) Porcentaje de servicios de TI donde se logran los beneficios esperados*
- *(05) Porcentaje de inversiones habilitadas para TI en las que los beneficios afirmados se cumplen o exceden*
- *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI*
- *(07) Porcentaje de partes interesadas del negocio satisfechas que la prestación de servicios de TI cumple con los niveles de servicio acordados*
- *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI*
- *(09) Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de TI a los nuevos requerimientos*
- *(09) Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas*
- *(09) Tiempo promedio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada*
- *(11) Frecuencia de las evaluaciones de madurez de capacidad y optimización de costos*
- *(11) Tendencia de resultados de la evaluación*
- *(11) Niveles de satisfacción de ejecutivos de negocios y TI con los costos y capacidades relacionados con TI*
- *(13) Número de programas/proyectos a tiempo y dentro del presupuesto*
- *(13) Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto*
- *(13) Número de programas que necesitan reelaboración significativa debido a defectos de calidad*
- *(13) Costo del mantenimiento de la aplicación frente al costo total de TI*
- *(14) Nivel de satisfacción del usuario empresarial con la calidad y puntualidad (o disponibilidad) de la información de gestión*
- *(14) Número de incidentes de procesos de negocio causados por la falta de disponibilidad de información*
- *(14) Relación y extensión de las decisiones de negocio erróneas en las que la información errónea o no disponible fue un factor clave*
- *(16) Porcentaje de personal satisfecho con sus funciones relacionadas con TI*
- *(16) Número de horas de aprendizaje/capacitación por cada miembro del personal*
- *(17) Nivel de conocimiento y comprensión de los ejecutivos de negocios sobre las posibilidades de innovación en TI*
- *(17) Nivel de satisfacción de las partes interesadas con los niveles de conocimientos e ideas sobre innovación en TI*
- *(17) Número de iniciativas aprobadas como resultado de ideas innovadoras de TI*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(APO01) Número de exposiciones de riesgo debido a las deficiencias en el diseño del ambiente de control*
- *(APO01) Número de empleados que asistieron a sesiones de capacitación o concientización*
- *(APO02) Porcentaje de objetivos en la estrategia de TI que apoyan la estrategia empresarial*
- *(APO02) Porcentaje de objetivos empresariales abordados en la estrategia de TI*
- *(APO02) Porcentaje de iniciativas en la estrategia de TI que se autofinancian (beneficios financieros que exceden los costos)*
- *(APO02) Tendencias en ROI de las iniciativas incluidas en la estrategia de TI*
- *(APO02) Nivel de retroalimentación de la encuesta de satisfacción de las partes interesadas de la empresa en la estrategia de TI*
- *(APO02) Porcentaje de proyectos en la cartera de proyectos de TI que pueden rastrearse directamente a la estrategia de TI*
- *(APO02) Porcentaje de objetivos empresariales estratégicos obtenidos como resultado de iniciativas estratégicas de TI*
- *(APO02) Número de nuevas oportunidades empresariales logradas como resultado directo de los desarrollos de TI*
- *(APO02) Porcentaje de iniciativas/proyectos de TI promovidos por propietarios de negocios*
- *(APO02) Logro de resultados medibles de la estrategia de TI que son parte de las metas de rendimiento del personal*
- *(APO02) Frecuencia de actualizaciones del plan de comunicación de la estrategia de TI*
- *(APO02) Porcentaje de iniciativas estratégicas con responsabilidad asignada*
- *(APO05) Porcentaje de inversiones de TI que tienen trazabilidad a la estrategia empresarial*
- *(APO05) Grado en que la gerencia empresarial está satisfecha con la contribución de TI a la estrategia empresarial*
- *(APO05) Porcentaje de unidades de negocio involucradas en el proceso de evaluación y priorización*
- *(APO05) Nivel de satisfacción con los informes de monitorización de la cartera*
- *(APO05) Porcentaje de cambios del programa de inversiones reflejados en las carteras relevantes*
- *(APO05) Porcentaje de inversiones donde los beneficios logrados se han medido y comparado con el caso de negocio*
- *(APO09) Número de procesos de negocio con acuerdos de servicio indefinidos*
- *(APO09) Porcentaje de servicios de TI en vivo cubiertos por acuerdos de servicio*
- *(APO09) Porcentaje de clientes satisfechos de que la prestación de servicios cumple con los niveles acordados*
- *(APO09) Porcentaje de servicios que son monitorizados a niveles de servicio*
- *(APO09) Porcentaje de objetivos de servicio alcanzados*
- *(BAI01) Porcentaje de partes interesadas efectivamente involucradas*
- *(BAI01) Nivel de satisfacción de las partes interesadas con la participación*
- *(BAI01) Porcentaje de partes interesadas que aprueban la necesidad empresarial, el alcance, el resultado previsto y el nivel de riesgo del proyecto*
- *(BAI01) Porcentaje de proyectos emprendidos sin casos de negocio aprobados*
- *(BAI01) Porcentaje de actividades alineadas con el alcance y los resultados esperados*
- *(BAI01) Porcentaje de programas activos emprendidos sin mapas de valor del programa válidos y actualizados*
- *(BAI01) Frecuencia de las revisiones del estado de programas/proyectos*
- *(BAI01) Porcentaje de desviaciones del plan abordadas*
- *(BAI01) Porcentaje de firmas de autorización de las partes interesadas para las revisiones etapa-puerta de los programas activos*
- *(BAI01) Porcentaje de beneficios esperados logrados*
- *(BAI01) Porcentaje de resultados con aceptación de primera instancia*
- *(BAI01) Nivel de satisfacción de las partes interesadas expresado en la revisión de cierre del proyecto*

1003 Proveedor de servicios en la nube

Título del escenario de riesgo	Proveedor de servicios en la nube
Categoría del escenario de riesgo	10 Propiedad empresarial de TI
Referencia del escenario de riesgo	1003

Escenario de riesgo
Una empresa decide trasladar sus servicios en la nube a un país extranjero donde los costos son más bajos que los proveedores locales, sin hacer la debida diligencia apropiada con respecto a los terceros que pueden proporcionar el servicio. El negocio decide subcontratar a la nube sin el asesoramiento de TI en sus áreas de competencia. A pesar de que la empresa tiene un marco de gobierno de TI establecido, fue ignorado y no se consultó. Por lo tanto, no se consideraron la seguridad implícita, la privacidad de datos y el cumplimiento.

Los problemas transfronterizos potenciales de datos, seguridad, privacidad y cumplimiento son:
- Información personal identificable (PII) y varias leyes de privacidad de datos globales
- Información personal sensible (SPI)
- Políticas y procedimientos del proveedor de la nube
- Fuga de datos

No existe un proceso para evaluar los requisitos de cumplimiento de terceros, y la decisión se impuso sobre el área TI.

Cuando el servicio se ha establecido, la empresa detecta fugas de datos de información crítica y áreas desconocidas de datos.

Debido a este problema grave, la reputación del negocio es dañada severamente, y potencialmente, quebrará a la compañía por perder futuros contratos de servicio.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** (ignorancia) del proceso de gobierno EDM01 *Garantizar el establecimiento y mantenimiento del marco de gobierno*. La consecuencia fue el incumplimiento con las **reglas y regulaciones.**

Agente
Los agentes que generan la amenaza que explota una vulnerabilidad son **internos**, los ejecutivos de negocios que decidieron subcontratar los servicios sin involucrar al área de TI.

Evento
El evento es una **ejecución ineficaz** del proceso de gobierno EDM01 *Garantizar el establecimiento y mantenimiento del marco de gobierno* y un **diseño ineficaz** del proceso de gestión MEA03 *Monitorizar y evaluar el cumplimiento con los requerimientos externos*, lo cual conduce a un incumplimiento con las **reglas y regulaciones.** El evento también se puede clasificar como una divulgación porque se detectó la fuga de datos en información crítica.

Activo/Recurso (causa)
Los recursos/activos que conducen al impacto en el negocio son los procesos EDM01 *Garantizar el establecimiento y mantenimiento del marco de gobierno* y MEA03 *Monitorizar y evaluar el cumplimiento con los requerimientos externos* y las **personas y habilidades**, donde los ejecutivos del negocio ignoran el proceso de gobierno.

Activo/Recurso (efecto)
El recurso/activo afectado principalmente es la **información** crítica debido a la fuga de datos. Pero también toda la empresa (**estructuras organizacionales** y las **personas**) son afectadas porque su reputación se daña gravemente, lo que puede llevar la quiebra de la empresa.

Tiempo
La duración de los eventos es **extensa** porque se requiere un largo período de tiempo para corregir la situación, si es que algún día se corrige. Debido a que la empresa puede irse a
la quiebra, el momento de la ocurrencia es **crítico**. El evento se detectó tan pronto como se involucró al área de TI y se reconoció el incumplimiento, por lo tanto, la detección puede clasificarse como **moderada**. El tiempo transcurrido entre el evento y la consecuencia es **demorado** porque puede, potencialmente, llevar a la empresa a la quiebra.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**S**	La TI no se ve como un habilitador tecnológico para nuevas iniciativas del negocio.
Entrega del proyecto y programa de TI	**P**	No hay aportes de TI a soluciones empresariales nuevas o mejoradas
Entrega del servicio y operaciones de TI	**S**	Interrupción del servicio.

Posibles respuestas al riesgo
- **Evasión del riesgo:** No involucrarse con terceros.
- **Aceptación del riesgo**: Si el contrato se ha ejecutado (sin la revisión del área de TI), la empresa tiene que aceptar que no podrá recuperar activos.
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** El proceso de selección de terceros será evaluado para incluir todos los requerimientos técnicos y no técnicos.

Mitigación del Riesgo Usando Habilitadores de COBIT 5					
Habilitador de principios, políticas y marco de trabajo					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Principios rectores del gobierno empresarial	Involucrar al negocio y al área de TI.		Alto	Alto	SÍ
Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
EDM01.03	Monitorizar el sistema de gobierno.	Monitorizar la efectividad y el desempeño del gobierno de TI de la empresa. Evaluar si el sistema de gobierno y los mecanismos implementados (incluyendo las estructuras, los principios y los procesos) están operando de forma efectiva y ofrecen una supervisión apropiada de TI.	Alto	Alto	SÍ
APO02.01	Comprender la dirección de la empresa.	Considerar el entorno empresarial actual y los procesos de negocio, así como la estrategia empresarial y los objetivos futuros. También considerar el entorno externo de la empresa (impulsores de la industria, regulaciones relevantes y bases de la competencia).	Alto	Alto	SÍ
APO09.03	Definir y preparar acuerdos de servicio.	Definir y preparar acuerdos de nivel de servicio (SLAs) basados en las opciones en los catálogos de servicio. Incluir acuerdos de nivel operativos (OLAs) internos.	Alto	Alto	SÍ
APO09.04	Monitorizar y reportar los niveles de servicio.	Monitorizar los niveles de servicio, identificar tendencias y proporcionar reportes que la gerencia pueda utilizar para tomar decisiones y gestionar los requisitos de rendimiento futuros.	Alto	Alto	SÍ
APO10.01	Identificar y evaluar los contratos y relaciones con los proveedores.	Identificar proveedores y contratos asociados, y clasificarlos en tipo, importancia y criticidad. Establecer criterios de evaluación para el proveedor y el contrato, y evaluar la cartera general de proveedores y contratos actuales y alternativos.	Alto	Alto	SÍ
APO10.02	Seleccionar proveedores.	Seleccionar proveedores de acuerdo a una práctica justa y formal para garantizar un ajuste viable basado en los requerimientos especificados. Los requerimientos deben optimizarse con la participación de los proveedores potenciales y las partes interesadas de la empresa.	Alto	Alto	SÍ
BAI02.01	Definir y mantener los requerimientos funcionales y técnicos del negocio.	Basándose en el caso de negocio, identificar, priorizar, especificar y acordar los requerimientos de información empresarial, funcionales, técnicos y de control que cubran el alcance/la comprensión de todas las iniciativas necesarias para lograr los resultados esperados de la solución empresarial habilitada para TI propuesta.	Alto	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Finanzas	Proporcionar una metodología común utilizada por el negocio y por el área de TI para evaluar las oportunidades en términos de valor para la empresa.		Alto	Alto	SÍ
Comité de estrategia (ejecutivo de TI)	Estructura clave que debe asumir la responsabilidad sobre la cooperación entre el área de TI y el negocio.		Alto	Alto	SÍ
Consejo de Dirección	Responsable del establecimiento y mantenimiento del marco de gobierno.		Alto	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
El negocio y el área de TI trabajan juntos como socios	El negocio toma en cuenta las dificultades que enfrenta el área de TI, y ésta aprende los problemas del negocio.		Alto	Alto	SÍ

Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Estrategia de TI	Alinear los planes del área de TI con los objetivos del negocio, y esto conducirá a una rendición de cuentas más eficiente del negocio sobre las TI.	Alto	Alto	SÍ
Niveles de autoridad	Aclarar las responsabilidades de toma de decisiones.	Alto	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de gestión de relaciones	El área de TI debe tener las habilidades adecuadas para desarrollar relaciones con las partes interesadas relevantes del negocio.	Medio	Medio	NO
Habilidades/afinidades relacionadas con TI	Los representantes del negocio deben ser capacitados/seleccionados basándose en una afinidad mínima requerida con TI.	Medio	Medio	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(01) Porcentaje de metas y requerimientos estratégicos empresariales respaldados por metas estratégicas de TI*
- *(01) Porcentaje de impulsores de valor de TI asignados a impulsores de valor empresariales*
- *(03) Porcentaje de puestos de la dirección ejecutiva con responsabilidades de decisiones de TI claramente definidas*
- *(03) Número de veces que TI está en la agenda del Consejo de Dirección de manera proactiva*
- *(03) Frecuencia de las reuniones del comité (ejecutivo) de estrategia de TI*
- *(03) Tasa de ejecución de las decisiones ejecutivas relacionadas con las TI*
- *(07) Porcentaje de partes interesadas del negocio satisfechas que la prestación de servicios de TI cumple con los niveles de servicio acordados*
- *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI*
- *(12) Número de incidentes del procesamiento de negocios causados por errores de integración tecnológica*
- *(12) Número de cambios en los procesos de negocio que deben ser aplazados o reelaborados debido a problemas de integración tecnológica*
- *(12) Número de programas empresariales habilitados por TI retrasados o que incurren en costos adicionales debido a problemas de integración tecnológica*
- *(12) Número de aplicaciones o infraestructuras críticas que operan en silos y no están integradas*
- *(14) Nivel de satisfacción del usuario empresarial con la calidad y puntualidad (o disponibilidad) de la información de gestión*
- *(14) Número de incidentes de procesos de negocio causados por la falta de disponibilidad de información*
- *(14) Relación y extensión de las decisiones de negocio erróneas en las que la información errónea o no disponible fue un factor clave*
- *(17) Nivel de conocimiento y comprensión de los ejecutivos de negocios sobre las posibilidades de innovación en TI*
- *(17) Nivel de satisfacción de las partes interesadas con los niveles de conocimientos e ideas sobre innovación en TI*
- *(17) Número de iniciativas aprobadas como resultado de ideas innovadoras de TI*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(EDM01) Nivel de satisfacción de las partes interesadas (medida a través de encuestas)*
- *(APO02) Porcentaje de objetivos en la estrategia de TI que apoyan la estrategia empresarial*
- *(APO02) Porcentaje de objetivos empresariales abordados en la estrategia de TI*
- *(APO02) Porcentaje de iniciativas en la estrategia de TI que se autofinancian (beneficios financieros que exceden los costos)*
- *(APO02) Tendencias en ROI de las iniciativas incluidas en la estrategia de TI*
- *(APO02) Nivel de retroalimentación de la encuesta de satisfacción de las partes interesadas de la empresa en la estrategia de TI*
- *(APO02) Porcentaje de proyectos en la cartera de proyectos de TI que pueden rastrearse directamente a la estrategia de TI*
- *(APO02) Porcentaje de objetivos empresariales estratégicos obtenidos como resultado de iniciativas estratégicas de TI*
- *(APO02) Número de nuevas oportunidades empresariales logradas como resultado directo de los desarrollos de TI*
- *(APO02) Porcentaje de iniciativas/proyectos de TI promovidos por propietarios de negocios*
- *(APO02) Logro de resultados medibles de la estrategia de TI que son parte de las metas de rendimiento del personal*
- *(APO02) Frecuencia de actualizaciones del plan de comunicación de la estrategia de TI*
- *(APO02) Porcentaje de iniciativas estratégicas con responsabilidad asignada*
- *(APO09) Número de procesos de negocio con acuerdos de servicio indefinidos*
- *(APO09) Porcentaje de servicios de TI en vivo cubiertos por acuerdos de servicio*
- *(APO09) Porcentaje de clientes satisfechos de que la prestación de servicios cumple con los niveles acordados*
- *(APO09) Número y gravedad de las infracciones de servicio*
- *(APO09) Porcentaje de servicios que son monitorizados a niveles de servicio*
- *(APO09) Porcentaje de objetivos de servicio alcanzados*
- *(BAI02) Porcentaje de requerimientos reelaborados debido a la desalineación con las necesidades y expectativas de la empresa*
- *(BAI02) Nivel de satisfacción de las partes interesadas con los requerimientos*
- *(BAI02) Porcentaje de requerimientos satisfechos por la solución propuesta*
- *(BAI02) Porcentaje de objetivos del caso de negocio satisfechos por la solución propuesta*
- *(BAI02) Porcentaje de partes interesadas que no aprueban la solución en relación con el caso de negocio*

1004 Acuerdos de nivel de servicio ineficaces

Título del escenario de riesgo	Acuerdos de nivel de servicio ineficaces
Categoría del escenario de riesgo	10 Propiedad empresarial de TI
Referencia del escenario de riesgo	1004

Escenario de riesgo
Un negocio no cumple con la mayoría de los acuerdos de nivel de servicio (SLAs) para sus clientes, lo que resulta en costos por reembolsos en el flujo de ingresos de la empresa. Una evaluación de los SLA de la empresa encontró que se redactaron con una ventaja para el cliente, y no para proteger o intentar proteger a la empresa. La empresa debe solicitar a su departamento jurídico que revise y reescriba todos los contratos SLA de la compañía, en cooperación con el departamento de TI. Después de revisar los SLA, el departamento jurídico debe examinar el lenguaje de los SLA en detalle para determinar la frecuencia y el momento de los cambios con cada cliente.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso APO09 *Gestionar acuerdos de servicio.*

Agente
Los agentes que generan la amenaza que explota una vulnerabilidad son **internos**, la parte del negocio responsable de las cuentas de servicio gestionadas.

Evento
El evento es un **diseño ineficaz** y/o **ejecución ineficaz** del proceso APO09 *Gestionar acuerdos de servicio.*

Activo/Recurso (causa)
Los activos/recursos que conducen al impacto en el negocio son todos los activos y recursos, p. ej., **personas y habilidades, infraestructura (instalaciones), infraestructura de TI, información** y **aplicaciones** que permiten la prestación de servicios a los clientes.

Activo/Recurso (efecto)
Los activos/recursos afectados son los servicios (**procesos**) que se proporcionan a los clientes.

Tiempo
La duración del evento es **extensa** porque se requiere un largo período de tiempo para revisar y reescribir todos los SLA de los contratos de la empresa. Debido a que la empresa encuentra costos de reembolso en el flujo de ingresos de la empresa, el momento de la ocurrencia es **crítico**. El evento se detectó tan pronto como los clientes se quejaron, y por lo tanto, se clasifica como **instantáneo**. El tiempo transcurrido entre el evento y la consecuencia es **inmediato** porque las penalizaciones (costos de reembolso) se deben pagar inmediatamente después del incumplimiento de los acuerdos de nivel de servicio.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**P**	El flujo de ingresos de la empresa se ve afectado por los costos de reembolso.
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Interrupciones en el servicio de TI, problemas de seguridad para clientes y problemas de cumplimiento.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Reducir el escalamiento de clientes y procesar mejoras y gobiernos, la empresa necesita rendición de cuentas por los SLA incumplidos, mejora y panel de control de métricas, y prevención y alertas automatizadas. Renegociar contratos.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Principios rectores del gobierno empresarial	Involucrar al negocio y al área de TI.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO01.04	Comunicar los objetivos y la dirección de la gerencia.	Concienciar y comunicar, buscando la comprensión de los objetivos y la dirección de TI a las partes interesadas en toda la empresa.	Bajo	Alto	SÍ
APO02.01	Comprender la dirección de la empresa.	Considerar el entorno empresarial actual y los procesos de negocio, así como la estrategia empresarial y los objetivos futuros. También considerar el entorno externo de la empresa (impulsores de la industria, regulaciones relevantes y bases de la competencia).	Bajo	Alto	SÍ
APO05.06	Gestionar el logro de beneficios.	Monitorizar los beneficios de ofrecer y mantener servicios y capacidades de TI apropiados, basándose en el caso de negocio acordado y actual.	Alto	Alto	SÍ
APO09.03	Definir y preparar acuerdos de servicio.	Definir y preparar acuerdos de nivel de servicio (SLAs) basados en las opciones en los catálogos de servicio. Incluir acuerdos de nivel operativos (OLAs) internos.	Alto	Alto	SÍ
APO09.04	Monitorizar y reportar los niveles de servicio.	Monitorizar los niveles de servicio, identificar tendencias y proporcionar reportes que la gerencia pueda utilizar para tomar decisiones y gestionar los requisitos de rendimiento futuros.	Alto	Alto	SÍ
BAI01.03	Gestionar la participación de las partes interesadas.	Gestionar la participación de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna que llegue a todas las partes interesadas relevantes. Esto incluye planificar, identificar e involucrar a las partes interesadas y gestionar sus expectativas.	Bajo	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Finanzas	Proporcionar una metodología común utilizada por el negocio y por el área de TI para evaluar las oportunidades en términos de valor para la empresa.		Alto	Alto	SÍ
Comité de estrategia (ejecutivo de TI)	Estructura clave que debe asumir la responsabilidad sobre la cooperación entre el área de TI y el negocio.		Alto	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
El negocio y el área de TI trabajan juntos como socios	El negocio toma en cuenta las dificultades que enfrenta el área de TI, y ésta aprende los problemas del negocio.		Alto	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Estrategia de TI	Alinear los planes del área de TI con los objetivos del negocio, y esto conducirá a una rendición de cuentas más eficiente del negocio sobre las TI.		Alto	Alto	SÍ
Niveles de autoridad	Aclarar las responsabilidades de toma de decisiones.		Alto	Alto	SÍ
Acuerdos de nivel de servicio (SLA)	Describir el nivel de servicio/los objetivos establecidos para satisfacer las expectativas del negocio.		Alto	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				

Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de gestión de relaciones	El área de TI debe tener las habilidades adecuadas para desarrollar relaciones con las partes interesadas relevantes del negocio.	Medio	Medio	NO
Habilidades/afinidades relacionadas con TI	Los representantes del negocio deben ser capacitados/seleccionados basándose en una afinidad mínima requerida con TI.	Medio	Medio	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(01) Porcentaje de metas y requerimientos estratégicos empresariales respaldados por metas estratégicas de TI*
- *(01) Porcentaje de impulsores de valor de TI asignados a impulsores de valor empresariales*
- *(02) Costo de incumplimiento de TI, incluyendo acuerdos y multas, y el impacto de la pérdida reputacional*
- *(02) Número de asuntos de incumplimiento relacionados con la TI reportados a la junta o que causan comentarios o vergüenza públicos*
- *(02) Número de problemas de incumplimiento en relación con acuerdos contractuales con los proveedores de servicios de TI*
- *(02) Cobertura de las evaluaciones de cumplimiento*
- *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos*
- *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI*
- *(04) Frecuencia de actualización del perfil de riesgo*
- *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI*
- *(07) Porcentaje de partes interesadas del negocio satisfechas que la prestación de servicios de TI cumple con los niveles de servicio acordados*
- *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI*
- *(11) Frecuencia de las evaluaciones de madurez de capacidad y optimización de costos*
- *(11) Tendencia de resultados de la evaluación de capacidad*
- *(11) Niveles de satisfacción de ejecutivos de negocios y TI con los costos y capacidades relacionados con TI*
- *(13) Costo del mantenimiento de la aplicación frente al costo total de TI*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(APO02) Porcentaje de objetivos en la estrategia de TI que apoyan la estrategia empresarial*
- *(APO02) Porcentaje de objetivos empresariales abordados en la estrategia de TI*
- *(APO02) Porcentaje de iniciativas en la estrategia de TI que se autofinancian (beneficios financieros que exceden los costos)*
- *(APO02) Tendencias en ROI de las iniciativas incluidas en la estrategia de TI*
- *(APO02) Nivel de retroalimentación de la encuesta de satisfacción de las partes interesadas de la empresa en la estrategia de TI*
- *(APO02) Porcentaje de objetivos empresariales estratégicos obtenidos como resultado de iniciativas estratégicas de TI*
- *(APO02) Logro de resultados medibles de la estrategia de TI que son parte de las metas de rendimiento del personal*
- *(APO02) Porcentaje de iniciativas estratégicas con responsabilidad asignada*
- *(APO05) Porcentaje de inversiones de TI que tienen trazabilidad a la estrategia empresarial*
- *(APO05) Grado en que la gerencia empresarial está satisfecha con la contribución de TI a la estrategia empresarial*
- *(APO05) Porcentaje de inversiones donde los beneficios logrados se han medido y comparado con el caso de negocio*
- *(APO09) Número de procesos de negocio con acuerdos de servicio indefinidos*
- *(APO09) Porcentaje de servicios de TI en vivo cubiertos por acuerdos de servicio*
- *(APO09) Porcentaje de clientes satisfechos de que la prestación de servicios cumple con los niveles acordados*
- *(APO09) Número y gravedad de las infracciones de servicio*
- *(APO09) Porcentaje de servicios que son monitorizados a niveles de servicio*
- *(APO09) Porcentaje de objetivos de servicio alcanzados*
- *(BAI01) Porcentaje de partes interesadas efectivamente involucradas*
- *(BAI01) Nivel de satisfacción de las partes interesadas con la participación*
- *(BAI01) Número de problemas de recursos (p. ej., habilidades, capacidad)*
- *(BAI01) Porcentaje de beneficios esperados logrados*

11 Proveedores

1101 Outsourcing de servicios de implementación

Título del escenario de riesgo	Outsourcing de servicios de implementación
Categoría del escenario de riesgo	11 Proveedores
Referencia del escenario de riesgo	1101

Escenario de riesgo
Un banco necesita iniciar un proceso de implementación para un nuevo paquete de software que forma parte de su plataforma de sucursales. El proveedor de software tiene socios comerciales en la región, pero no localmente, ya que esta es la primera implementación de este tipo. El proveedor actual ofrece software de última generación y la mejor en su clase, y es la solución correcta necesaria.

Los requerimientos para este socio comercial son tener una representación local y conocer las regulaciones locales que se aplican a la industria específica. La falta de debida diligencia del proveedor con respecto a la capacidad de entrega y la sostenibilidad del servicio del proveedor son los principales problemas con la decisión que se tomó.

Después de que el banco detecta la incapacidad del socio comercial para cumplir con los acuerdos de nivel de servicio (SLA), el proceso de implementación se interrumpe con una pérdida sustancial de tiempo y recursos, debido a la dependencia excesiva en el proveedor y la falta de capacitación de su propio personal.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso de adquisición debido a que se puso demasiada ponderación en la sostenibilidad del proveedor, en lugar de emplear la misma ponderación para la sostenibilidad y la capacidad de cumplir con los SLA.

Agente
Los agentes que generan la amenaza que explota una vulnerabilidad son **internos** (función responsable del proceso de adquisición), y **externos** (proveedor de los servicios de implementación).

Evento
El evento es la **interrupción** del proceso de implementación.

Activo/Recurso (causa)
El activo/recurso que conduce al impacto en el negocio es el **proceso** APO10 *Gestionar los proveedores.*

Activo/Recurso (efecto)
Los recursos afectados por la interrupción de la implementación son principalmente la **infraestructura de TI** y las aplicaciones. Los **procesos** de negocio soportados por la **infraestructura de TI** y aplicaciones afectadas son recursos secundarios.

Tiempo
La duración del evento es **extensa** porque hay una pérdida sustancial de tiempo. El momento de la ocurrencia es **crítico** porque el banco necesita este nuevo paquete de software para sus sucursales. La detección es **lenta** porque no se reconoció hasta que la implementación ya se había iniciado. El tiempo transcurrido entre el evento y la consecuencia es **demorado** porque, en el peor caso, se debe evaluar un nuevo proveedor.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**S**	Oportunidad perdida de utilizar la tecnología para mejorar la eficiencia y la eficacia.
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Interrupción del servicio.

Posibles respuestas al riesgo

- **Evasión del riesgo:** El banco se abstendrá del outsourcing. El banco debe capacitar al personal propio en la implementación de la aplicación de servicios para contrarrestar la dependencia en el socio comercial.
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** El banco revisará su proceso de gobierno y mejorará los requerimientos al elaborar la solicitud de información (RFI) y la solicitud de propuesta (RFP) para socios comerciales calificados. El banco realizará la evaluación y selección adecuada de terceros.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de adquisiciones	Proporcionar un enfoque establecido para seleccionar proveedores, incluyendo los criterios de aceptación de los términos de negocio.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO10.02	Seleccionar proveedores.	Seleccionar proveedores de acuerdo a una práctica justa y formal para garantizar un ajuste viable basado en los requerimientos especificados. Los requerimientos deben optimizarse con la participación de los proveedores potenciales y las partes interesadas de la empresa.	Bajo	Alto	SÍ
APO10.03	Gestionar los contratos y las relaciones con los proveedores.	Formalizar y gestionar las relaciones para cada proveedor estratégico. Gestionar, mantener y supervisar los contratos y la prestación de servicios. Asegurarse de que los contratos nuevos o modificados cumplan con los estándares de la empresa y con los requerimientos legales y regulatorios.	Alto	Alto	SÍ
APO10.04	Gestionar el riesgo con los proveedores.	Identificar y gestionar el riesgo con los proveedores, incluyendo la capacidad de proporcionar continuamente una prestación de servicios segura, eficiente y eficaz.	Alto	Alto	SÍ
APO10.05	Monitorizar el rendimiento y el cumplimiento del proveedor.	Revisar periódicamente el rendimiento general de los proveedores, el cumplimiento con los requerimientos contractuales, el valor y abordar oportunamente los problemas identificados.	Bajo	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Propietario del proceso de negocio	Establecer los requerimientos y los indicadores de rendimiento, y garantizar que las expectativas adecuadas se incorporen a los contratos.		Alto	Alto	SÍ
Departamento de adquisiciones	Proporcionar el apoyo y el enfoque para interactuar eficientemente con los proveedores.		Alto	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Respetar los procedimientos de adquisición	Se requiere un esfuerzo adicional para garantizar una protección mínima con respecto a los proveedores.		Alto	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Requisitos de servicio	Conocer las metas del negocio permite tener una posición razonable para la negociación.		Alto	Alto	SÍ
Estrategia de TI	Definir los límites y los objetivos empresariales a tener en cuenta al negociar los contratos.		Alto	Alto	SÍ
Catálogo de proveedores	Una presentación estructurada de proveedores conocidos, incluyendo rendimiento previo.		Alto	Alto	SÍ
Acuerdos de nivel de servicio (SLA)	Describir el nivel de servicio/los objetivos establecidos para satisfacer las expectativas del negocio.		Medio	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Sistema de gestión de proveedores	Establece un sistema para dar seguimiento a la evolución de la exposición al riesgo durante todo el proceso, desde la selección hasta la terminación del servicio.		Alto	Alto	SÍ
Habilitador de personas, habilidades y competencias					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de negociación	Asegurarse que se satisfacen los requerimientos mínimos.		Medio	Medio	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo* • *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI* • *(07) Porcentaje de partes interesadas del negocio satisfechas que la prestación de servicios de TI cumple con los niveles de servicio acordados* • *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI* • *(09) Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de TI a los nuevos requerimientos* • *(09) Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas* • *(09) Tiempo promedio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada*
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso
• *(APO10) Porcentaje de proveedores que cumplen con los requisitos acordados* • *(APO10) Número de incumplimientos de servicio en los servicios relacionados con TI causados por proveedores* • *(APO10) Número de eventos relacionados con el riesgo que conducen a incidentes de servicio* • *(APO10) Frecuencia de las sesiones de gestión de riesgos con el proveedor* • *(APO10) Porcentaje de incidentes relacionados con el riesgo resueltos de manera aceptable (tiempo y costo)* • *(APO10) Número de reuniones de revisión de proveedores* • *(APO10) Número de disputas formales con proveedores* • *(APO10) Porcentaje de disputas resueltas amistosamente en un plazo razonable*

1103 Servicios de expansión de infraestructura

Título del escenario de riesgo	Servicios de expansión de infraestructura
Categoría del escenario de riesgo	11 Proveedores
Referencia del escenario de riesgo	1103

Escenario de riesgo
Después de una revisión de costos con respecto a la expansión del volumen de operaciones de una empresa, el departamento de TI decide trasladarse a servicios en la nube para el soporte de infraestructura (infraestructura como servicio [IaaS]). La empresa toma esta decisión sin hacer la debida diligencia adecuada con respecto a terceros. No existe un proceso para evaluar los requisitos de cumplimiento de terceros.

Después de que el servicio se ha establecido, la empresa detecta que el proveedor de servicios no puede cumplir con los acuerdos de nivel de servicio (SLA) contratados para el futuro aumento en el volumen de operaciones de la empresa, el cual está previsto para los próximos dos años. Debido a este problema grave, el crecimiento futuro y la sostenibilidad del negocio está en peligro, y amenaza la expansión del negocio planificada.

Los principales problemas que se han hecho evidentes están relacionadas con la seguridad, el cumplimiento, la planificación de continuidad del negocio y la capacidad del proveedor de la nube, de la siguiente manera:
- Rendimiento/capacidad de la red insuficientes
- Tiempo de respuesta lento para las transacciones
- No hay revisión de las políticas y procedimientos del proveedor de la nube
- Necesidad de actualizar los proceso del plan de continuidad del negocio (BCP) y del plan de recuperación de desastres (DRP) para incluir al proveedor BCP/DRP

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** en la toma de decisiones porque la decisión carecía de información adecuada de la debida diligencia inadecuada.

Agente
Los agentes que generan la amenaza que explota una vulnerabilidad son **internos** y **externos**. El agente interno es la función que es responsable de la debida diligencia dentro del proceso APO10 *Gestionar los proveedores*. El agente externo es el proveedor de servicios.

Evento
El evento es la **interrupción** de servicios y el **diseño ineficaz** de la infraestructura de TI.

Activo/Recurso (causa)
El activo/recurso que conduce al impacto en el negocio es el **proceso** APO10 *Gestionar los proveedores.*

Activo/Recurso (efecto)
Los recursos afectados son principalmente la **infraestructura de TI** y las **aplicaciones**. Los recursos secundarios afectados son los **procesos** de negocio soportados por la **infraestructura de TI** y aplicaciones afectadas.

Tiempo
La duración del evento es **extensa** porque el proveedor debe actualizar su infraestructura y sistemas, o la empresa tiene que cambiar a otro proveedor. El momento de la ocurrencia es **crítico** debido al problema grave de que el crecimiento futuro y la sostenibilidad del negocio están en peligro, lo que amenaza la expansión del negocio planificada. La detección es **lenta** porque no se reconoció hasta que el servicio se había establecido. El tiempo transcurrido entre el evento y la consecuencia es **demorado** porque, en el peor caso, se debe evaluar al nuevo proveedor.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**S**	Oportunidad perdida de utilizar la tecnología para mejorar la eficiencia y la eficacia. El crecimiento y la sostenibilidad futuros del negocio están en peligro, y la expansión del negocio planificada se ve amenazada.
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Rendimiento/capacidad de la red insuficientes, tiempo de respuesta lento de la transacción, problemas de seguridad y problemas de cumplimiento.

Posibles respuestas al riesgo
- **Evasión del riesgo:** Abstenerse del outsourcing.
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** El proceso de selección de terceros será evaluado, y la empresa ajustará todos los requerimientos técnicos y no técnicos.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de adquisiciones	Proporcionar un enfoque establecido para seleccionar proveedores, incluyendo los criterios de aceptación de los términos de negocio.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO10.02	Seleccionar proveedores.	Seleccionar proveedores de acuerdo a una práctica justa y formal para garantizar un ajuste viable basado en los requerimientos especificados. Los requerimientos deberían ser optimizados con la participación de los proveedores potenciales y las partes interesadas de la empresa.	Bajo	Alto	SÍ
APO10.03	Gestionar los contratos y las relaciones con los proveedores.	Formalizar y gestionar las relaciones para cada proveedor estratégico. Gestionar, mantener y supervisar los contratos y la prestación de servicios. Asegurarse de que los contratos nuevos o modificados cumplan con los estándares de la empresa y con los requerimientos legales y regulatorios.	Alto	Alto	SÍ
APO10.04	Gestionar el riesgo de los proveedores.	Identificar y gestionar el riesgo de los proveedores, incluyendo la capacidad de proporcionar continuamente una prestación de servicios segura, eficiente y eficaz.	Alto	Alto	SÍ
APO10.05	Monitorizar el rendimiento y el cumplimiento del proveedor.	Revisar periódicamente el rendimiento general de los proveedores, el cumplimiento de los requerimientos contractuales, y evaluar y abordar oportunamente los problemas identificados.	Bajo	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Departamento de adquisiciones	Proporcionar el apoyo y el enfoque para interactuar eficientemente con los proveedores.		Medio	Medio	NO
Director de Informática (CIO)	Responsable de la gestión de proveedores.		Medio	Medio	NO
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Respetar los procedimientos de adquisición	Se requiere un esfuerzo adicional para garantizar una protección mínima con respecto a los proveedores.		Alto	Alto	SÍ
Una cultura transparente y participativa es un punto de enfoque importante	Optimizar el resultado de la relación con el proveedor.		Alto	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Requisitos de servicio	Conocer los objetivos del negocio permite tener una posición razonable para la negociación.		Alto	Alto	SÍ
Estrategia de TI	Definir los límites y los objetivos empresariales a tener en cuenta al negociar los contratos.		Medio	Medio	NO
Catálogo de proveedores	Una presentación estructurada de proveedores conocidos, incluyendo el desempeño previo.		Alto	Alto	SÍ
Acuerdos de nivel de servicio (SLA)	Describir el nivel de servicio/los objetivos establecidos para satisfacer las expectativas del negocio.		Medio	Medio	NO
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Sistema de gestión de proveedores	Establece un sistema para dar seguimiento a la evolución de la exposición al riesgo durante todo el proceso, desde la selección hasta la terminación del servicio.		Alto	Alto	SÍ

Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de negociación	Asegurarse que los requerimientos mínimos son compatibles.	Alto	Alto	SÍ
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo* • *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI* • *(07) Porcentaje de partes interesadas del negocio satisfechas de que la prestación de servicios de TI cumple con los niveles de servicio acordados* • *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI* • *(09) Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de TI a los nuevos requerimientos* • *(09) Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas* • *(09) Tiempo promedio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(APO10) Porcentaje de proveedores que cumplen con los requisitos acordados* • *(APO10) Número de interrupciones de servicio en los servicios relacionados con TI causados por proveedores* • *(APO10) Número de eventos relacionados con el riesgo que conducen a incidentes de servicio* • *(APO10) Frecuencia de las sesiones de gestión de riesgos con el proveedor* • *(APO10) Porcentaje de incidentes relacionados con el riesgo resueltos de manera aceptable (tiempo y coste)* • *(APO10) Número de reuniones de revisión de proveedores* • *(APO10) Número de conflictos formales con proveedores* • *(APO10) Porcentaje de conflictos resueltos amistosamente en un plazo razonable*				

1107 Proveedores de servicios en la nube seleccionados directamente por el negocio

Título del escenario de riesgo	Proveedores de servicios en la nube seleccionados directamente por el negocio
Categoría del escenario de riesgo	11 Proveedores
Referencia del escenario de riesgo	1107

Escenario de riesgo
El departamento de TI, que tiene la responsabilidad de desarrollador y de la arquitectura empresarial (EA) para la empresa, identificó que la empresa se comprometía directamente con, y adquiría capacidad directamente de varios proveedores de servicios en la nube para la capacidad que se está desarrollando internamente. El departamento de TI descubrió la relación después de una solicitud de acceso del proveedor de la nube para integrarse con los sistemas internos de registro.

Después de las conversaciones con el negocio, se acuerda terminar el desarrollo de la solución externa y traspasar al área de TI la relación con el proveedor de la nube.

El área de TI está saturada ahora con un acuerdo de nivel de servicio que tiene informes de métricas de rendimiento mínimo (la mayoría de los informes de acuerdo de nivel de servicio [SLA] no tienen sentido). Sin la integración con los sistemas internos (especialmente cuadros de mando para eventos con tickets), será difícil obtener valor para la empresa.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** en la toma de decisiones porque la decisión fue tomada por el negocio sin consultar con el área de TI.

Agente
El agente que genera la amenaza que se aprovecha de una vulnerabilidad es **interno**, el ejecutivo del negocio que tomó la decisión sin consultar al área de TI.

Evento
El evento es el **uso inapropiado** de recursos y el **diseño ineficaz** de los SLA.

Activo/Recurso (causa)
El activo/recurso que conduce al impacto en el negocio es el **proceso** APO10 *Gestionar los proveedores.*

Activo/Recurso (efecto)
Los principales recursos afectados son las **aplicaciones**. Los recursos secundarios afectados son los **procesos** de negocio soportados por las aplicaciones afectadas.

Tiempo
La duración del evento es **extensa** porque el departamento de TI ahora tiene la responsabilidad de la relación y debe integrar los servicios proporcionados con los sistemas internos. El momento de la ocurrencia es **no crítico**. La detección es **moderada** porque la relación se detectó accidentalmente, después de una solicitud del proveedor de la nube. El tiempo transcurrido entre el evento y la consecuencia es **inmediato** porque la responsabilidad de la relación se transfiere inmediatamente al área TI.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**S**	Oportunidad perdida de utilizar la tecnología para mejorar la eficiencia y la eficacia. El crecimiento y la sostenibilidad futuros del negocio están en peligro, y la expansión del negocio planificada se ve amenazada.
Entrega del proyecto y programa de TI	**P**	Ejecutar proyectos redundantes.
Entrega del servicio y operaciones de TI	**N/A**	

Posibles respuestas al riesgo

- **Evitación del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartición/transferencia del riesgo:** N/A
- **Mitigación del riesgo:** El departamento de TI establece una relación con el negocio para entender las expectativas del negocio e intenta renegociar la monitorización eficaz y la prestación de servicios con el proveedor de la nube.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial

Política de adquisiciones	Proporcionar un enfoque establecido para seleccionar proveedores, incluyendo los criterios de aceptación de los términos de negocio.		Alto	Alto	SÍ
Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO09.02	Catalogar los servicios habilitados por TI.	Definir y mantener uno o más catálogos de servicios para grupos objetivo relevantes. Publicar y mantener servicios en vivo habilitados por TI en los catálogos de servicios.	Medio	Alto	SÍ
APO09.03	Definir y preparar acuerdos de servicio.	Definir y preparar acuerdos de nivel de servicio (SLAs) basados en las opciones en los catálogos de servicio. Incluir acuerdos internos de nivel operacional (OLAs).	Medio	Alto	SÍ
APO09.04	Monitorizar y reportar los niveles de servicio.	Monitorizar los niveles de servicio, identificar tendencias y proporcionar informes que la gerencia pueda utilizar para tomar decisiones y gestionar los requisitos de rendimiento futuros.	Medio	Alto	SÍ
APO09.05	Revisar los acuerdos y los contratos de servicio.	Realizar revisiones periódicas de los acuerdos de servicio y revisarlos cuando sea necesario.	Medio	Alto	SÍ
APO10.02	Seleccionar proveedores.	Seleccionar proveedores de acuerdo a una práctica justa y formal para garantizar un ajuste viable basado en los requerimientos especificados. Los requerimientos deben optimizarse con la participación de los proveedores potenciales y las partes interesadas de la empresa.	Bajo	Alto	SÍ
APO10.03	Gestionar los contratos y las relaciones con los proveedores.	Formalizar y gestionar las relaciones para cada proveedor estratégico. Gestionar, mantener y supervisar los contratos y la prestación de servicios. Asegurarse de que los contratos nuevos o modificados cumplan con los estándares de la empresa y con los requerimientos legales y regulatorios.	Alto	Alto	SÍ
APO10.04	Gestionar el riesgo con los proveedores.	Identificar y gestionar el riesgo con los proveedores, incluyendo la capacidad de proporcionar continuamente una prestación de servicios segura, eficiente y eficaz.	Bajo	Alto	SÍ
APO10.05	Monitorizar el rendimiento y el cumplimiento del proveedor.	Revisar periódicamente el rendimiento general de los proveedores, el cumplimiento con los requerimientos contractuales, y evaluar y abordar oportunamente los problemas identificados.	Medio	Medio	NO
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Departamento de adquisiciones	Proporcionar el apoyo y el enfoque para interactuar eficientemente con los proveedores.		Alto	Alto	SÍ
Director de Informática (CIO)	Responsable de la gestión de proveedores.		Bajo	Bajo	NO
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Respetar los procedimientos de adquisición	Se requiere un esfuerzo adicional para garantizar una protección mínima con respecto a los proveedores.		Alto	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Requisitos de servicio	Conocer los objetivos del negocio permite tener una posición razonable para la negociación.		Medio	Alto	SÍ
Estrategia de TI	Definir los límites y los objetivos empresariales a tener en cuenta al negociar los contratos.		Bajo	Bajo	NO

Acuerdos de nivel de servicio (SLA)	Describir el nivel de servicio/los objetivos establecidos para satisfacer las expectativas del negocio.	Medio	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A				
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo* • *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI* • *(07) Porcentaje de partes interesadas del negocio satisfechas de que la prestación de servicios de TI cumple con los niveles de servicio acordados* • *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI* • *(09) Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de TI a los nuevos requerimientos* • *(09) Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas* • *(09) Tiempo promedio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				

- *(APO10) Porcentaje de proveedores que cumplen con los requisitos acordados*
- *(APO10) Número de interrupciones de servicio en los servicios relacionados con TI causados por proveedores*
- *(APO10) Número de eventos relacionados con el riesgo que conducen a incidentes de servicio*
- *(APO10) Frecuencia de las sesiones de gestión de riesgos con el proveedor*
- *(APO10) Porcentaje de incidentes relacionados con el riesgo resueltos de manera aceptable (tiempo y coste)*
- *(APO10) Número de reuniones de revisión de proveedores*
- *(APO10) Número de conflictos formales con proveedores*
- *(APO10) Porcentaje de conflictos resueltos amistosamente en un plazo razonable*

Página intencionalmente en blanco

12 Cumplimiento regulatorio

1201 Cumplimiento PCI DSS

Título del escenario de riesgo	Cumplimiento PCI DSS
Categoría del escenario de riesgo	12 Cumplimiento regulatorio
Referencia del escenario de riesgo	1201

Escenario de riesgo
PCI DSS es el estándar de seguridad de datos (DSS) de la industria de tarjetas de pago (PCI). Es un estándar de seguridad de la información patentado para empresas que manejan la información del titular de las principales tarjetas de débito, crédito, prepago, monedero electrónico, cajero automático (ATM) y punto de servicio (POS). El estándar fue creado para aumentar los controles en torno a los datos del titular de la tarjeta para reducir el fraude de tarjetas de crédito a través de su exposición. La validación del cumplimiento se realiza anualmente por un asesor de seguridad externo cualificado (QSA), quien crea un informe de cumplimiento (ROC) para empresas que manejan grandes volúmenes de transacciones, o por un cuestionario de autoevaluación (SAQ) para empresas que manejan volúmenes más pequeños.

Una empresa realiza un cambio importante en su estrategia comercial e introduce un sitio web de comercio electrónico para vender sus productos. La empresa está aceptando pagos con tarjeta de crédito a través de este sitio web, el cual genera una gran proporción de las ventas totales de la empresa. La alta dirección no sabía o decidió salir al mercado antes de que la empresa cumpliera plenamente con las regulaciones PCI DSS. El incumplimiento con la regulación PCI DSS es detectado por el banco patrocinador de la empresa, el cual actúa. Esta acción da lugar a una multa a la empresa y tiene un impacto negativo en su reputación.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso MEA03 *Monitorizar y evaluar el cumplimiento con los requerimientos externos*, y a un nivel más detallado, un **fallo** de la práctica de gestión de identificar los requerimientos de cumplimiento externos. El tipo de amenaza también puede clasificarse como un incumplimiento con los **requerimientos externos.**

Agente
Los agentes que generan la amenaza que se aprovecha de la vulnerabilidad son **internos** y **externos**. El agente interno es la alta dirección que no sabía o decidió salir al mercado antes de que la empresa cumpliera plenamente con las regulaciones PCI DSS. Los agentes externos son el banco de la empresa y los reguladores que multan a la empresa.

Evento
El evento es el **diseño ineficaz** y/o **ejecución ineficaz** de la práctica de gestión Identificar los requerimientos de cumplimiento externos dentro del proceso MEA03 *Monitorizar y evaluar el cumplimiento con los requerimientos externos*. El evento también se puede clasificar como un incumplimiento de las **reglas y regulaciones.**

Activo/Recurso (causa)
El activo/recurso que conduce al impacto en el negocio es el **proceso** MEA03 *Monitorizar y evaluar el cumplimiento con los requerimientos externos.*

Activo/Recurso (efecto)
Los activos/recursos afectados son los **procesos** de negocio de las actividades de comercio electrónico de la empresa.

Tiempo
La duración es **prolongada** porque la empresa debe implementar medidas de seguridad adicionales para cumplir, y luego estas medidas de seguridad se deben evaluar. El momento es **no crítico** porque el incumplimiento no tendrá un impacto inmediato en el negocio. La detección es a través del banco de la empresa y es **lenta** porque tomó algún tiempo antes que se descubriera el incumplimiento. El tiempo transcurrido entre el evento y la consecuencia es **demorado** porque el regulador primero necesitará evaluar el alcance del incumplimiento de las reglas y regulaciones y luego abordará la multa.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Cuestiones de cumplimiento.

Posibles respuestas al riesgo

- **Evitación del riesgo:** La empresa decide no tener presencia de ventas en línea.
- **Aceptación del riesgo:** La alta dirección acepta el riesgo y está preparada para pagar multas y perjudicar la reputación de la empresa.
- **Compartir/transferir el riesgo:** La empresa subcontrata el procesamiento del sitio web de comercio electrónico.
- **Mitigación del riesgo:** Implementar las prácticas de seguridad de datos requeridas para cumplir con las regulaciones PCI DSS.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de cumplimiento	Guiar la identificación de los requerimientos de cumplimiento externos.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
MEA03.01	Identificar los requerimientos de cumplimiento externos.	Identificar y monitorizar de forma continua los cambios en las leyes y regulaciones locales e internacionales, así como otros requerimientos externos aplicables a la empresa.	Alto	Bajo	SÍ
MEA03.02	Optimizar la respuesta a los requerimientos externos.	Revisar y ajustar los principios, las políticas, los estándares, los procedimientos y las metodologías para asegurarse que se aborden y comuniquen los requerimientos legales, regulatorios y contractuales. Considerar los estándares de la industria, códigos de buenas prácticas y pautas de mejores prácticas para la adopción y adaptación de planes existentes.	Alto	Alto	SÍ
MEA03.03	Confirmar el cumplimiento externo.	Confirmar el cumplimiento con los requerimientos legales, regulatorios y contractuales.	Alto	Bajo	SÍ
MEA03.04	Obtener aseguramiento del cumplimiento externo.	Obtener y reportar el aseguramiento del cumplimiento y fidelidad a las políticas, principios, estándares, procedimientos y metodologías. Confirmar que las acciones correctivas para abordar las deficiencias de cumplimiento se cierren de manera oportuna.	Alto	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Departamento de cumplimiento	Proporcionar orientación sobre cumplimiento legal, regulatorio y contractual. Dar seguimiento a las regulaciones nuevas y cambiantes.		Alto	Alto	SÍ
Grupo legal	Apoyo legal durante el análisis y litigio.		Alto	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
El cumplimiento está integrado en las operaciones diarias	Todos los miembros de la empresa están facultados para facilitar el cumplimiento regulatorio.		Medio	Medio	NO
Habilitador de información					
Análisis de nuevos requerimientos de cumplimiento legal y regulatorio	Las regulaciones impuestas por el gobierno se deben analizar.		Alto	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Bases de datos regulatorias	Facilitar el seguimiento de los requerimientos de cumplimiento.		Alto	Alto	SÍ
Habilitador de personas, habilidades y competencias					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de litigio	Una vez iniciada la acción penal, se requieren las habilidades adecuadas para minimizar el impacto legal.		Bajo	Medio	SÍ
Habilidades de análisis legal	Comprender las expectativas del regulador local.		Alto	Alto	SÍ

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI
• *(02) Coste de incumplimiento de TI, incluyendo acuerdos y multas, y el impacto de la pérdida de reputación.* • *(02) Número de problemas de incumplimiento relacionados con la TI reportados a la junta o que causan comentarios o vergüenza públicos* • *(02) Número de problemas de incumplimiento en relación con acuerdos contractuales con los proveedores de servicios de TI* • *(02) Cobertura de las evaluaciones de cumplimiento* • *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo*
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso
• *(MEA03) Tiempo promedio transcurrido entre la identificación de problemas de cumplimiento externos y su resolución* • *(MEA03) Frecuencia de las evaluaciones de cumplimiento* • *(MEA03) Número de problemas críticos de incumplimiento identificados por año* • *(MEA03) Porcentaje de propietarios de procesos que aprueban y confirman el cumplimiento*

1202 Regulaciones para la industria financiera

Título del escenario de riesgo	Regulaciones para la industria financiera
Categoría del escenario de riesgo	12 Cumplimiento regulatorio
Referencia del escenario de riesgo	1202

Escenario de riesgo
Una empresa de servicios financieros desconoce y/o no se mantiene al día con las regulaciones locales e internacionales para llevar a cabo negocios en este mercado. Esto da lugar a una multa, y la empresa se ve amenazada por los reguladores externos con la cancelación de su licencia comercial en caso de recurrencia.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso MEA03 *Monitorizar y evaluar el cumplimiento con los requerimientos externos*, o a un nivel más detallado, un **fallo** de las prácticas de gestión *Identificar los requerimientos de cumplimiento externos* y *Confirmar con cumplimiento externo*. El tipo de amenaza también puede clasificarse como un incumplimiento de los **requerimientos externos.**

Agente
Los agentes que generan la amenaza que se aprovecha de la vulnerabilidad son **internos** y **externos**. El agente interno es la alta dirección que desconoce y/o no se mantiene al día con las regulaciones locales e internacionales. Los agentes externos son los reguladores que multan a la empresa.

Evento
El evento es el **diseño ineficaz** y/o **ejecución ineficaz** de las prácticas de gestión *Identificar los requerimientos de cumplimiento externo* y *Confirmar los requerimientos externos*, dentro del proceso MEA03 *Monitorizar y evaluar el cumplimiento con los requerimientos externos.*El evento también se puede clasificar como un incumplimiento de las **reglas y regulaciones.**

Activo/Recurso (causa)
El activo/recurso que conduce al impacto en el negocio es el **proceso** MEA03 *Monitorizar y evaluar el cumplimiento con los requerimientos externos.*

Activo/Recurso (efecto)
Los activos/recursos afectados son los **procesos** de negocio.

Tiempo
La duración es **prolongada** porque la empresa debe implementar controles adicionales para cumplir. El momento es **no crítico** porque el incumplimiento no tendrá un impacto inmediato en el negocio. La detección es **lenta** porque usualmente toma algún tiempo antes que se descubra el incumplimiento. El tiempo transcurrido entre el evento y la consecuencia es **demorado** porque el regulador primero tendrá que evaluar el alcance del incumplimiento de las reglas y regulaciones y luego abordará la multa.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Cuestiones de cumplimiento.

Posibles respuestas al riesgo

- **Evitación del riesgo:** N/A
- **Aceptación del riesgo:** La alta dirección acepta el riesgo y está preparada para pagar multas y perjudicar la reputación de la empresa.
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Implementar las prácticas de control requeridas para cumplir con las reglas y regulaciones locales e internacionales de la industria financiera.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de cumplimiento	Guiar la identificación de los requerimientos de cumplimiento externos.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
MEA03.01	Identificar los requerimientos de cumplimiento externos.	Identificar y monitorizar de forma continua los cambios en las leyes y regulaciones locales e internacionales, así como otros requerimientos externos aplicables a la empresa.	Alto	Bajo	SÍ
MEA03.02	Optimizar la respuesta a los requerimientos externos.	Revisar y ajustar los principios, las políticas, los estándares, los procedimientos y las metodologías para asegurarse que se aborden y comuniquen los requerimientos legales, regulatorios y contractuales. Considerar los estándares de la industria, códigos de buenas prácticas y pautas de mejores prácticas para la adopción y adaptación de planes existentes.	Alto	Bajo	SÍ
MEA03.03	Confirmar el cumplimiento externo.	Confirmar el cumplimiento con los requerimientos legales, regulatorios y contractuales.	Alto	Bajo	SÍ
MEA03.04	Obtener aseguramiento del cumplimiento externo.	Obtener y reportar el aseguramiento del cumplimiento y fidelidad a las políticas, principios, estándares, procedimientos y metodologías. Confirmar que las acciones correctivas para abordar las deficiencias de cumplimiento se cierren de manera oportuna.	Alto	Bajo	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Departamento de cumplimiento	Proporcionar orientación sobre cumplimiento legal, regulatorio y contractual. Dar seguimiento a las regulaciones nuevas y cambiantes.		Alto	Alto	SÍ
Grupo legal	Apoyo legal durante el análisis y litigio.		Alto	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La cultura consciente de los riesgos y de los cumplimientos está presente en toda la empresa, incluyendo la identificación proactiva y la escalada del riesgo	Todos los miembros de la empresa están facultados para facilitar el cumplimiento regulatorio.		Medio	Medio	NO
El cumplimiento está integrado en las operaciones diarias	Todos los miembros de la empresa están facultados para facilitar el cumplimiento regulatorio.		Medio	Medio	NO
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Análisis de nuevos requerimientos de cumplimiento legal y regulatorio	Las regulaciones impuestas por el gobierno se deben analizar.		Alto	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Bases de datos regulatorias	Facilitar el seguimiento de los requerimientos de cumplimiento.		Alto	Alto	SÍ

Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de litigio	Una vez iniciada la acción penal, se requieren las habilidades adecuadas para minimizar el impacto legal sobre la empresa.	Bajo	Alto	SÍ
Habilidades de análisis legal	Comprender las expectativas del regulador local.	Alto	Alto	SÍ
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(02) Coste de incumplimiento de TI, incluyendo acuerdos y multas, y el impacto de la pérdida de reputación* • *(02) Número de problemas de incumplimiento relacionados con la TI reportados a la junta o que causan comentarios o vergüenza públicos* • *(02) Número de problemas de incumplimiento en relación con acuerdos contractuales con los proveedores de servicios de TI* • *(02) Cobertura de las evaluaciones de cumplimiento* • *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(MEA03) Tiempo promedio transcurrido entre la identificación de problemas de cumplimiento externos y su resolución* • *(MEA03) Frecuencia de las evaluaciones de cumplimiento* • *(MEA03) Número de problemas críticos de incumplimiento identificados por año* • *(MEA03) Porcentaje de propietarios de procesos que aprueban y confirman el cumplimiento*				

1203 Transferencia de datos a través de países

Título del escenario de riesgo	Transferencia de datos a través de países
Categoría del escenario de riesgo	12 Cumplimiento regulatorio
Referencia del escenario de riesgo	1203

Escenario de riesgo
El proveedor de servicios de TI de una empresa aloja servidores que ejecutan el sistema de recursos humanos (RR.HH.) de la empresa en otro país. Este proveedor de servicios de TI está transfiriendo información personal a un país que no está cubierto por las regulaciones apropiadas de privacidad de datos, contrariamente a las regulaciones de privacidad de datos locales, lo que da lugar a una multa del regulador de la empresa y publicidad con el potencial de causar daños a la reputación.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** del proceso MEA03 *Monitorizar y evaluar el cumplimiento con los requerimientos externos*, o a un nivel más detallado, un **fallo** de las prácticas de gestión *Identificar los requerimientos de cumplimiento externos* y *Confirmar con cumplimiento externo*. El tipo de amenaza también puede clasificarse como un incumplimiento con los **requerimientos externos**.

Agente
Los agentes que generan la amenaza que se aprovecha de la vulnerabilidad son **internos** y **externos**. El agente interno es la oficina de cumplimiento que no se aseguró que el proveedor de servicios de TI de la compañía cumpliera con las reglas y regulaciones requeridas. Los agentes externos son los reguladores que multaron a la empresa.

Evento
El evento es el **diseño ineficaz** y/o **ejecución ineficaz** de las prácticas de gestión *Identificar los requerimientos de cumplimiento externo* y *Confirmar con cumplimiento externo*, dentro del proceso MEA03 *Monitorizar y evaluar el cumplimiento con los requerimientos externos*. El evento también se puede clasificar como un incumplimiento de las **reglas y regulaciones.**

Activo/Recurso (causa)
El activo/recurso que conduce al impacto en el negocio es el **proceso** MEA03 *Monitorizar y evaluar el cumplimiento con los requerimientos externos.*

Activo/Recurso (efecto)
Los activos/recursos afectados son los **procesos** de negocio y las **personas**, que podrían verse afectadas por la divulgación de información personal.

Tiempo
La duración es **prolongada** porque la empresa debe implementar controles adicionales para cumplir. El momento es **no crítico** porque el incumplimiento no tendrá un impacto inmediato en el negocio. La detección es **lenta** porque usualmente toma algún tiempo antes que se descubra el incumplimiento. El tiempo transcurrido entre el evento y la consecuencia es **demorado** porque el regulador primero tendrá que evaluar el alcance del incumplimiento de las reglas y regulaciones y luego abordará la multa.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Cuestiones de cumplimiento.

Posibles respuestas al riesgo

- **Evitación del riesgo:** Abstenerse del outsourcing.
- **Aceptación del riesgo:** La alta dirección acepta el riesgo y está preparada para pagar multas y perjudicar la reputación de la empresa.
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Implementar las prácticas de control requeridas para cumplir con las reglas y regulaciones de privacidad de datos. Asegurarse de que los servidores no estén ubicados en diferentes países.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Políticas específicas de la industria/el mercado	Definir las reglas y pautas para identificar los requerimientos de cumplimiento específicos y los procedimientos para cumplir con los requerimientos aplicables.	Alto	Alto	SÍ
Política de cumplimiento	Guiar la identificación de los requerimientos de cumplimiento externos y los procedimientos para cumplir con los requerimientos aplicables.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
MEA03.01	Identificar los requerimientos de cumplimiento externos.	Identificar y monitorizar de forma continua los cambios en las leyes y regulaciones locales e internacionales, así como otros requerimientos externos aplicables a la empresa.	Alto	Bajo	SÍ
MEA03.02	Optimizar la respuesta a los requerimientos externos.	Revisar y ajustar los principios, las políticas, los estándares, los procedimientos y las metodologías para asegurarse que se aborden y comuniquen los requerimientos legales, regulatorios y contractuales. Considerar los estándares de la industria, códigos de buenas prácticas y pautas de mejores prácticas para la adopción y adaptación de planes existentes.	Alto	Bajo	SÍ
MEA03.03	Confirmar el cumplimiento externo.	Confirmar el cumplimiento con los requerimientos legales, regulatorios y contractuales.	Alto	Bajo	SÍ
MEA03.04	Obtener aseguramiento del cumplimiento externo.	Obtener y reportar el aseguramiento del cumplimiento y fidelidad a las políticas, principios, estándares, procedimientos y metodologías. Confirmar que las acciones correctivas para abordar las deficiencias de cumplimiento se cierren de manera oportuna.	Alto	Bajo	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Oficial de privacidad	Monitorizar el impacto de las leyes y asegurarse que se cumplan las directivas de privacidad.		Alto	Alto	SÍ
Departamento de cumplimiento	Proporcionar orientación sobre cumplimiento legal, regulatorio y contractual. Dar seguimiento a las regulaciones nuevas y cambiantes.		Alto	Alto	SÍ
Grupo legal	Apoyo legal durante el análisis y litigio.		Alto	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La cultura consciente de los riesgos y de los cumplimientos está presente en toda la empresa, incluyendo la identificación proactiva y la escalada del riesgo	Todos los miembros de la empresa están facultados para facilitar el cumplimiento regulatorio.		Medio	Medio	NO
El cumplimiento está integrado en las operaciones diarias	Todos los miembros de la empresa están facultados para facilitar el cumplimiento regulatorio.		Alto	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Análisis de nuevos requerimientos de cumplimiento legal y regulatorio	Las regulaciones impuestas por el gobierno se deben analizar.		Alto	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Bases de datos regulatorias	Facilitar el seguimiento de los requerimientos de cumplimiento.		Alto	Alto	SÍ

Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de litigio	Una vez iniciada la acción penal, se requieren las habilidades adecuadas para minimizar el impacto legal sobre la empresa.	Bajo	Alto	SÍ
Habilidades de análisis legal	Comprender las expectativas del regulador local.	Alto	Alto	SÍ
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(02) Coste de incumplimiento de TI, incluyendo acuerdos y multas, y el impacto de la pérdida de reputación* • *(02) Número de problemas de incumplimiento relacionados con la TI reportados a la junta o que causan comentarios o vergüenza públicos* • *(02) Número de problemas de incumplimiento en relación con acuerdos contractuales con los proveedores de servicios de TI* • *(02) Cobertura de las evaluaciones de cumplimiento* • *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(MEA03) Tiempo promedio transcurrido entre la identificación de problemas de cumplimiento externos y su resolución* • *(MEA03) Frecuencia de las evaluaciones de cumplimiento* • *(MEA03) Número de problemas críticos de incumplimiento identificados por año* • *(MEA03) Porcentaje de propietarios de procesos que aprueban y confirman el cumplimiento*				

Página intencionalmente en blanco

13 Geopolítica

1301 Incendio causado por activistas políticos

Título del escenario de riesgo	Incendio causado por activistas políticos
Categoría del escenario de riesgo	13 Geopolítica
Referencia del escenario de riesgo	1301

Escenario de riesgo
El consejo de dirección de una empresa evalúa la probabilidad de acciones políticas en la región, donde la empresa tiene sus instalaciones de negocios y de TI clasificadas como bajas y, por lo tanto, no tiene un proceso de prevención para responder a actividades políticas como revueltas, agitaciones y disturbios civiles. Tras el estallido de un incendio grave, causado por un activista político en una refinería de petróleo vecina, las autoridades exigen a una empresa que evacúe sus oficinas debido al peligro de propagación del incendio. Al personal de la empresa no se le permite regresar a sus oficinas durante varios días. Aunque no hay daños en las instalaciones de negocios y de TI de la empresa, el acceso es denegado por las autoridades hasta que el área circundante esté segura. Por lo tanto, la empresa no tiene acceso a las instalaciones de negocios y de TI durante un largo período de tiempo, lo que tiene un impacto negativo importante en las operaciones comerciales en curso de la empresa.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es el acto **malicioso** del incendio en la refinería de petróleo vecina, y también el **requerimiento externo** por parte de las autoridades de evacuar el edificio.

Agente
Los agentes fueron los activistas políticos **externos** que iniciaron el incendio y las autoridades **externas** que exigieron la evacuación del edificio y negaron el acceso hasta que el área circundante fuera segura nuevamente.

Evento
El evento es una interrupción de los procesos de negocio causada por el hecho de que las instalaciones de negocios y de TI no están disponibles o no se puede acceder a ellas.

Activo/Recurso (causa)
El activo/recurso que conduce al impacto en el negocio son **las personas**, los activistas políticos.

Activo/Recurso (efecto)
Los activos/recursos afectados son todos los **procesos** de negocio y de TI que no se pueden realizar porque se impide el acceso a la **infraestructura física** y de **TI, instalaciones, equipo, infraestructura, información** y **aplicaciones**.

Tiempo
El momento es **crítico** porque tiene un impacto inmediato en las operaciones del negocio. La detección es **instantánea**. El tiempo transcurrido entre el evento y la consecuencia es **inmediato**. La duración del evento es **extensa** porque transcurre un largo período de tiempo antes de que las autoridades permitan nuevamente el acceso a las oficinas.

Tipo de riesgo		
Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Interrupciones en el servicio de TI (y en el negocio).
	S	Problemas de seguridad física.

Posibles respuestas al riesgo

- **Evitación del riesgo:** No colocar las instalaciones de negocios o de TI en el área crítica.
- **Aceptación del riesgo:** El consejo evalúa la probabilidad de las acciones políticas en la región como bajas y acepta el riesgo.
- **Compartir/transferir el riesgo:** Contratar un seguro contra la interrupción de los negocios.
- **Mitigación del riesgo:** Implementar un centro de datos de respaldo secundario y acceso a instalaciones del negocio alternativas, y tener un plan de continuidad del negocio (BCP) eficaz.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
N/A	N/A			

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
EDM03.01	Evaluar la gestión de riesgos.	Examinar y analizar continuamente el efecto del riesgo sobre el uso actual y futuro de TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado, y que el riesgo para el valor de la empresa relacionado con el uso de las TI sea identificado y gestionado.	Bajo	Alto	SÍ
EDM03.02	Gestión directa de riesgos.	Dirigir el establecimiento de prácticas de gestión de riesgos para ofrecer una seguridad razonable de que las prácticas de gestión de riesgos de TI son apropiadas para asegurarse de que el riesgo de TI actual no sobrepase el apetito al riesgo del consejo de dirección.	Bajo	Medio	NO
APO12.01	Recopilar datos.	Identificar y recopilar datos relevantes para habilitar una efectiva identificación, análisis y reporte de los riesgos relacionados con TI.	Medio	Alto	SÍ
APO12.02	Analizar el riesgo.	Desarrollar información útil para soportar decisiones sobre riesgos que consideren la importancia de los factores de riesgo en el negocio.	Bajo	Alto	SÍ
APO12.03	Mantener el perfil del riesgo.	Mantener un inventario de los riesgos conocidos y los atributos de riesgo (incluyendo la frecuencia esperada, el impacto potencial y las respuestas), y de recursos relacionados, capacidades y actividades de control actuales.	Bajo	Alto	SÍ
APO12.04	Expresar el riesgo.	Proporcionar información de manera oportuna sobre el estado actual de las exposiciones y oportunidades relacionadas con TI a todas las partes interesadas requeridas para obtener una respuesta apropiada.	Bajo	Alto	SÍ
APO12.05	Definir un catálogo de acción de gestión de riesgos.	Gestionar las oportunidades para reducir el riesgo a un nivel aceptable en el catálogo.	Medio	Medio	NO
APO12.06	Responder al riesgo.	Responder de manera oportuna con medidas eficaces para limitar la magnitud de la pérdida de los eventos relacionados con TI.	Bajo	Alto	SÍ
DSS04.01	Definir la política de continuidad del negocio, los objetivos y el alcance.	Definir la política de continuidad del negocio y el alcance alineado con los objetivos de la empresa y de las partes interesadas.	Bajo	Medio	NO
DSS04.02	Mantener una estrategia de continuidad.	Evaluar las opciones de gestión de continuidad del negocio y elegir una estrategia de continuidad viable y rentable para asegurar la recuperación y la continuidad de la empresa ante un desastre u otro incidente o interrupción mayor.	Bajo	Alto	SÍ
DSS04.03	Desarrollar e implementar una respuesta de continuidad del negocio.	Desarrollar un plan de continuidad del negocio (BCP) basado en la estrategia que documenta los procedimientos y elementos de información que permitan a la empresa continuar sus actividades críticas después de un incidente.	Bajo	Alto	SÍ
DSS04.05	Revisar, mantener y mejorar el plan de continuidad.	Realizar, en intervalos regulares, una revisión gerencial de la capacidad de continuidad para asegurar que su idoneidad, adecuación y eficacia sean continuas. Gestionar los cambios al plan de acuerdo con el proceso de control de cambios para asegurar que el plan de continuidad se mantenga actualizado y que refleje continuamente los requerimientos del negocio actuales.	Bajo	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Continuidad del negocio y recuperación de desastres	Mantener las opciones de servicio continuo.		Bajo	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
N/A	N/A				

Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades para la planificación de contingencias	Mantener las opciones de servicio continuo.	Bajo	Alto	SÍ

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos*
- *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI*
- *(04) Frecuencia de actualización del perfil de riesgo*
- *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI*
- *(10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o pérdida de reputación*
- *(10) Frecuencia de la evaluación de seguridad con respecto a los estándares y pautas más recientes*
- *(14) Número de incidentes de procesos de negocio causados por la falta de disponibilidad de información*
- *(14) Relación y extensión de las decisiones de negocio erróneas en las que la información errónea o no disponible fue un factor clave*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(EDM03) Nivel de alineación entre riesgo de TI y riesgo empresarial*
- *(EDM03) Número de riesgos potenciales de TI identificados y gestionados*
- *(EDM03) Índice de actualización de la evaluación del factor de riesgo*
- *(EDM03) Porcentaje de planes de acción de riesgo de TI ejecutados a tiempo*
- *(EDM03) Porcentaje de riesgo crítico que ha sido mitigado efectivamente*
- *(EDM03) Nivel de impacto empresarial inesperado*
- *(EDM03) Porcentaje de riesgo de TI que excede la tolerancia al riesgo de la empresa*
- *(APO12) Grado de visibilidad y reconocimiento en el entorno actual*
- *(APO12) Número de eventos de pérdida con características clave capturadas en repositorios*
- *(APO12) Porcentaje de auditorías, eventos y tendencias capturados en repositorios*
- *(APO12) Porcentaje de procesos de negocio clave incluidos en el perfil de riesgo*
- *(APO12) Completitud de atributos y valores en el perfil de riesgo*
- *(APO12) Porcentaje de propuestas de gestión de riesgos rechazadas por falta de consideración de otros riesgos relacionados*
- *(APO12) Número de incidentes significativos no identificados e incluidos en el catálogo de gestión de riesgos*
- *(DSS04) Número de sistemas empresariales críticos no cubiertos por el plan de continuidad del negocio*
- *(DSS04) Número de ejercicios y pruebas que han alcanzado los objetivos de recuperación*
- *(DSS04) Porcentaje de mejoras acordadas en el plan de continuidad del negocio que se han incorporado*
- *(DSS04) Porcentaje de problemas identificados que se han abordado posteriormente en el plan de continuidad del negocio*

1302 Acceso a mercados comerciales clave

Título del escenario de riesgo	Acceso a mercados comerciales clave
Categoría del escenario de riesgo	13 Geopolítica
Referencia del escenario de riesgo	1302

Escenario de riesgo
Una empresa realizó una importante inversión en una solución de comercio electrónico de empresa a empresa para vender sus productos a nivel mundial. Los mercados emergentes son los mercados clave para que la empresa alcance su retorno de la inversión (ROI) planificado para esta solución de comercio electrónico. Uno de los gobiernos de estos mercados emergentes interrumpe su conexión a internet; por lo tanto, a la empresa se le impide el acceso a uno de sus mercados comerciales clave, lo que da lugar a una caída sustancial en las ventas.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es el **requisito externo** causado por la inestabilidad política o la acción directa del gobierno extranjero en el país donde la empresa genera una gran proporción de sus ventas de productos e ingresos.

Agente
El agente que genera la amenaza que se aprovecha de la vulnerabilidad es la acción deliberada por parte de un gobierno extranjero **externo**.

Evento
El evento es la **interrupción** de las comunicaciones, lo que impacta en las ventas del negocio y da lugar a una pérdida de ingresos.

Activo/Recurso (causa)
El activo/recurso que conduce al impacto en el negocio son las personas **externas** del gobierno extranjero.

Activo/Recurso (efecto)
Los activos/recursos afectados son la pérdida de la **infraestructura física** y de **TI**, lo que da lugar a la pérdida de comunicaciones con una ruta de negocios clave en un mercado extranjero, e impacta la capacidad de procesar transacciones de ventas.

Tiempo
El momento del evento es **crítico**. La duración es **prolongada** porque no se sabe cuándo el gobierno permitirá el acceso a internet de nuevo, y el acceso a este importante mercado podría estar denegado por un largo período de tiempo. La detección es inmediata por la denegación de conexión. El tiempo transcurrido entre el evento y la consecuencia es **inmediata** porque el procesamiento de transacciones de venta no es posible desde el momento en que se interrumpe la conexión a internet.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Interrupciones del servicio de TI.

Posibles respuestas al riesgo

- **Evitación del riesgo:** No invertir en la capacidad de hacer negocios en países políticamente inestables.
- **Aceptación del riesgo:** El consejo acepta el riesgo de hacer negocios en países políticamente inestables.
- **Compartir/transferir el riesgo:** Contratar un seguro contra la interrupción de los negocios.
- **Mitigación del riesgo:** La empresa contrata a una compañía profesional como grupo de presión y mantiene una buena relación de negocios con el gobierno extranjero.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Políticas de puerto seguro	Proporcionar orientación sobre las disposiciones de una ley o regulación que especifique que cierta conducta será considerada para no violar una regla determinada.	Medio	Bajo	NO

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
EDM03.01	Evaluar la gestión de riesgos.	Examinar y analizar continuamente el efecto del riesgo sobre el uso actual y futuro de TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado, y que el riesgo para el valor de la empresa relacionado con el uso de las TI sea identificado y administrado.	Bajo	Medio	NO
APO12.01	Recopilar datos.	Identificar y recopilar datos relevantes para habilitar una efectiva identificación, análisis y reporte de los riesgos relacionados con TI.	Bajo	Alto	SÍ
APO12.02	Analizar el riesgo.	Desarrollar información útil para soportar decisiones sobre riesgos que consideren la importancia de los factores de riesgo en el negocio.	Bajo	Alto	SÍ
APO12.03	Mantener un perfil del riesgo.	Mantener un inventario de los riesgos conocidos y los atributos de riesgo (incluyendo la frecuencia esperada, el impacto potencial y las respuestas), y de recursos relacionados, capacidades y actividades de control actuales.	Bajo	Alto	SÍ
APO12.04	Expresar el riesgo.	Proporcionar información de manera oportuna sobre el estado actual de las exposiciones y oportunidades relacionadas con TI a todas las partes interesadas requeridas para obtener una respuesta apropiada.	Bajo	Alto	SÍ
APO12.05	Definir un catálogo de acción de gestión de riesgos.	Gestionar las oportunidades para reducir el riesgo a un nivel aceptable en el catálogo.	Bajo	Alto	SÍ
APO12.06	Responder al riesgo.	Responder de manera oportuna con medidas eficaces para limitar la magnitud de la pérdida de los eventos relacionados con TI.	Bajo	Alto	SÍ
DSS04.02	Mantener una estrategia de continuidad.	Evaluar las opciones de gestión de continuidad del negocio y elegir una estrategia de continuidad viable y rentable para asegurar la recuperación y la continuidad de la empresa ante un desastre u otro incidente o interrupción mayor.	Bajo	Medio	NO
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Continuidad del negocio y recuperación de desastres	Mantener las opciones de servicio continuo.		Bajo	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				

Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades para la planificación de contingencias	Mantener las opciones de servicio continuo.	Bajo	Alto	SÍ
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo* • *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(EDM03) Nivel de alineación entre riesgo de TI y riesgo empresarial* • *(EDM03) Número de riesgos potenciales de TI identificados y gestionados* • *(EDM03) Índice de actualización de la evaluación del factor de riesgo* • *(EDM03) Porcentaje de riesgo crítico que ha sido mitigado efectivamente* • *(EDM03) Nivel de impacto empresarial inesperado* • *(EDM03) Porcentaje de riesgo de TI que excede la tolerancia al riesgo de la empresa* • *(APO12) Número de eventos de pérdida con características clave capturadas en repositorios* • *(APO12) Porcentaje de auditorías, eventos y tendencias capturados en repositorios* • *(APO12) Porcentaje de procesos de negocio clave incluidos en el perfil de riesgo* • *(APO12) Completitud de atributos y valores en el perfil de riesgo* • *(APO12) Porcentaje de propuestas de gestión de riesgos rechazadas por falta de consideración de otros riesgos relacionados* • *(APO12) Número de incidentes significativos no identificados e incluidos en el catálogo de gestión de riesgos* • *(DSS04) Porcentaje de servicios de TI que satisfacen los requisitos de tiempo de actividad* • *(DSS04) Número de sistemas empresariales críticos no cubiertos por el plan de continuidad del negocio* • *(DSS04) Porcentaje de problemas identificados que se han abordado posteriormente en el plan de continuidad del negocio*				

1303 Bomba que destruye un centro de datos

Título del escenario de riesgo	Bomba que destruye un centro de datos
Categoría del escenario de riesgo	13 Geopolítica
Referencia del escenario de riesgo	1303

Escenario de riesgo
Las tensiones políticas continúan desarrollándose en todo el mundo, y con frecuencia dan lugar a ataques terroristas. En los últimos años, los grandes bancos también han sido blanco porque son culpados de gran parte de los problemas económicos del mundo. Un banco multinacional que se encuentra en Londres, Inglaterra, tiene un centro de datos que controla su red de cajeros automáticos (ATM). El banco también tiene un centro de datos de respaldo en otra ciudad del Reino Unido. Una acción deliberada de un grupo terrorista da lugar a un ataque con bomba que destruye el principal centro de datos de Londres. En un ataque coordinado, el centro de datos de respaldo también es destruido por una bomba. Este evento interrumpe toda la red de cajeros automáticos del banco.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es la acción deliberada y **maliciosa** por parte del grupo terrorista.

Agente
El agente que genera la amenaza que se aprovecha de la vulnerabilidad es **externo**, el grupo terrorista.

Evento
El evento es la **destrucción** de los dos centros de datos y la **interrupción** del servicio de la red de cajeros automáticos del banco.

Activo/Recurso (causa)
Los activos/recursos que conducen al impacto en el negocio son las **personas** del grupo terrorista.

Activo/Recurso (efecto)
Los activos/recursos afectados son el **proceso** de negocio que proporciona efectivo a los clientes a través de los cajeros automáticos, la **infraestructura física**, **instalaciones, equipos**, etc., y la **infraestructura de TI**, incluyendo el **hardware de computación, la infraestructura de red** y el **middleware**.

Tiempo
La duración del evento es **extensa** tomará muchos días restaurar los servicios de cajeros automáticos. El momento de la ocurrencia es **crítico** para la prestación de un servicio a los clientes del banco. La detección del evento es **inmediata** porque es la pérdida instantánea del servicio de cajeros automáticos. Por la misma razón, el tiempo transcurrido entre el evento y la consecuencia es **inmediato**.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Interrupciones del servicio de TI.
	S	Problemas de seguridad.

Posibles respuestas al riesgo

- **Evitación del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** Sub-contratar el alojamiento de servidores. Contratar un seguro de interrupción del negocio.
- **Mitigación del riesgo:** Implementar y/o mejorar el plan de continuidad del negocio y el plan de recuperación de desastres. Asegurarse de que los sitios de TI estén construidos y diseñados para minimizar el impacto del riesgo del entorno (p. ej., robo, aire, incendio, humo, agua, vibración, terrorismo, vandalismo, productos químicos y explosivos). Obtener un contrato con un proveedor de servicios de plan de recuperación de desastres.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
N/A	N/A			

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
EDM03.01	Evaluar la gestión de riesgos.	Examinar y analizar continuamente el efecto del riesgo sobre el uso actual y futuro de TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado, y que el riesgo para el valor de la empresa relacionado con el uso de las TI sea identificado y administrado.	Bajo	Alto	SÍ
DSS01.04	Gestionar el ambiente.	Mantener medidas de protección contra los factores ambientales. Instalar equipo y dispositivos especializados para monitorizar y controlar el ambiente.	Alto	Alto	SÍ
DSS01.05	Gestionar las instalaciones.	Gestionar las instalaciones, incluyendo el equipo de suministro eléctrico y comunicaciones, en línea con las leyes y regulaciones, los requerimientos técnicos y del negocio, las especificaciones del proveedor, y las pautas de salud y seguridad.	Bajo	Medio	NO
DSS04.01	Definir la política de continuidad del negocio, los objetivos y el alcance.	Definir la política de continuidad del negocio y el alcance alineado con los objetivos de la empresa y de las partes interesadas.	Bajo	Alto	SÍ
DSS04.02	Mantener una estrategia de continuidad.	Evaluar las opciones de gestión de continuidad del negocio y elegir una estrategia de continuidad viable y rentable para asegurar la recuperación y la continuidad de la empresa ante un desastre u otro incidente o interrupción mayor.	Bajo	Alto	SÍ
DSS04.03	Desarrollar e implementar una respuesta de continuidad del negocio.	Desarrollar un plan de continuidad del negocio (BCP) basado en la estrategia que documenta los procedimientos y elementos de información que permiten a la empresa continuar sus actividades críticas después de un incidente.	Bajo	Alto	SÍ
DSS05.05	Gestionar el acceso físico a los activos de TI.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a las instalaciones, edificios y áreas debe justificarse, autorizarse, registrarse y monitorizarse. Esto debe aplicarse a todas las personas que entren en las instalaciones, incluyendo personal, personal temporal, clientes, proveedores, visitantes y cualquier otro tercero.	Alto	Medio	SÍ

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Continuidad del negocio y recuperación de desastres	Mantener las opciones de servicio continuo.	Bajo	Alto	SÍ

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			

Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			

Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			

Personas, habilidades y competencias habilitadoras				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades para la planificación de contingencias	Mantener las opciones de servicio continuo.	Bajo	Alto	SÍ

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI*
- *(10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o pérdida de reputación*
- *(10) Número de servicios de TI con requisitos de seguridad pendientes*
- *(10) Frecuencia de la evaluación de seguridad con respecto a los estándares y pautas más recientes*
- *(14) Número de incidentes de procesos de negocio causados por la falta de disponibilidad de información*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(EDM03) Nivel de alineación entre riesgo de TI y riesgo empresarial*
- *(EDM03) Número de riesgos de TI potenciales identificados y gestionados*
- *(EDM03) Tasa de refresco de la evaluación del factor de riesgo*
- *(EDM03) Porcentaje de riesgo crítico que ha sido mitigado efectivamente*
- *(EDM03) Nivel de impacto empresarial inesperado*
- *(EDM03) Porcentaje de riesgo de TI que excede la tolerancia al riesgo de la empresa*
- *(APO12) Grado de visibilidad y reconocimiento en el entorno actual*
- *(APO12) Número de eventos de pérdida con características clave capturadas en repositorios*
- *(APO12) Porcentaje de auditorías, eventos y tendencias capturados en repositorios*
- *(APO12) Porcentaje de procesos de negocio clave incluidos en el perfil de riesgo*
- *(APO12) Integridad de atributos y valores en el perfil de riesgo*
- *(APO12) Porcentaje de propuestas de gestión de riesgos rechazadas por falta de consideración de otros riesgos relacionados*
- *(APO12) Número de incidentes significativos no identificados e incluidos en la cartera de gestión de riesgos*
- *(DSS04) Número de sistemas empresariales críticos no cubiertos por el plan de continuidad del negocio*
- *(DSS04) Porcentaje de mejoras acordadas en el plan de continuidad del negocio que se han incorporado*
- *(DSS04) Porcentaje de problemas identificados que se han abordado posteriormente en el plan de continuidad del negocio*
- *(DSS05) Número de vulnerabilidades descubiertas*
- *(DSS05) Porcentaje de pruebas periódicas de dispositivos de seguridad ambiental*
- *(DSS05) Calificación promedio de las evaluaciones de seguridad física*
- *(DSS05) Número de incidentes relacionados con la seguridad física*

Página intencionalmente en blanco

14 Robo o destrucción de infraestructura

1401 Seguimiento de cerca

Título del escenario de riesgo	Seguimiento de cerca
Categoría del escenario de riesgo	14 Robo o destrucción de la infraestructura
Referencia del escenario de riesgo	1401

Escenario de riesgo
Una pequeña empresa, con políticas y sistemas para controlar la entrada de personal autorizado a las áreas de servicio restringidas, no actualiza la relación de personal autorizado para incluir un nuevo grupo de personas que ejecutan un proyecto especial.

Se anima frecuentemente a los nuevos empleados a entrar en las instalaciones junto con otros empleados a quienes se ha concedido acceso a las mismas. No existe diferenciación clara entre las identificaciones asignadas a visitantes y empleados. Habitualmente el personal de seguridad no escolta a los visitantes.

La empresa no ha actualizado la monitorización de seguridad a un formato digital.

En una auditoría física reciente, en la que se usaron las grabaciones de videovigilancia, se observó que una persona desconocida accedió al edificio con el resultado consiguiente de espionaje industrial debido al robo de un dispositivo con información sobre el último producto de la empresa cuyo lanzamiento al mercado estaba programado para el siguiente trimestre.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es **maliciosa**.

Agente
El agente que genera la amenaza que explota una vulnerabilidad es una persona **externa**, el ladrón.

Evento
El evento es el **robo** y la **divulgación** de información sensible sobre el producto más reciente de la empresa.

Activo/Recurso (causa)
Los activos/recursos que conducen al impacto en el negocio es el **diseño ineficaz** y/o la **ejecución ineficaz** del proceso DSS05 *Gestionar los servicios de seguridad* y sus prácticas de gestión *Gestionar el acceso físico a los recursos de TI* y *Gestionar los documentos sensibles y dispositivos de salida.*

Activo/Recurso (efecto)
El activo/recurso afectado es la **información** sensible sobre el producto más reciente de la empresa.

Tiempo
La duración del evento es **extensa** porque la ventaja respecto a la competencia se ha perdido. El momento de la ocurrencia es **crítico** porque el producto de la empresa estaba a punto de llegar al mercado en el próximo trimestre. La detección es **moderada** porque se detectó a través de la revisión de las cintas de video. El tiempo transcurrido entre el evento y la consecuencia se **demora** porque la empresa aumentará los ingresos con el producto nuevo.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y del programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Problemas de seguridad física.

Posibles respuestas al riesgo

- **Evitación del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Se aplicarán las políticas de seguridad del sitio físico. El color de las identificaciones de los visitantes irá cambiando, y se instalarán barreras físicas y registros de visitantes.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de seguridad de información física y ambiental	Restringir el acceso físico a la infraestructura para evitar la destrucción.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
DSS05.05	Gestionar el acceso físico a los activos de TI.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a las instalaciones, edificios y áreas debe justificarse, autorizarse, registrarse y monitorizarse. Esto debe aplicarse a todas las personas que entren en las instalaciones, incluyendo personal, personal temporal, clientes, proveedores, visitantes y cualquier otro tercero.	Alto	Alto	SÍ
DSS05.06	Gestionar documentos sensibles y dispositivos de salida.	Establecer protecciones físicas apropiadas, prácticas de contabilización y gestión de inventario para activos de TI sensibles, como formularios especiales, instrumentos negociables, impresoras para fines especiales o tokens de seguridad.	Alto	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gerente de seguridad de la información	Implementación de medidas de seguridad.		Alto	Alto	SÍ
Jefe de operaciones de TI	Responder al robo y la destrucción de infraestructura.		Bajo	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La seguridad de la información se practica en las operaciones diarias	Prevenir el acceso físico no autorizado.		Alto	Medio	SÍ
Las personas respetan la importancia de las políticas y los principios de seguridad de la información	Prevenir el acceso físico no autorizado.		Alto	Medio	SÍ
Las partes interesadas son conscientes de cómo identificar y responder a amenazas a la empresa	Minimizar el impacto del robo y destrucción de la infraestructura.		Alto	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Solicitudes de acceso	Auditar las solicitudes de acceso y las aprobaciones.		Alto	Medio	SÍ
Registros de acceso	Monitorizar el acceso a las instalaciones.		Medio	Alto	SÍ
Informes de evaluación de instalaciones	La empresa es consciente del estado y riesgo de las instalaciones.		Alto	Bajo	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Control de acceso	Prevenir el acceso lógico no autorizado.		Alto	Medio	SÍ
Sistema de seguridad de alarma y monitorización	Prevenir el acceso físico no autorizado.		Alto	Alto	SÍ

Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de seguridad de la información	Implementar controles para prevenir o reducir el impacto del robo y destrucción de la infraestructura.	Alto	Alto	SÍ
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo* • *(10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o pérdida de reputación* • *(10) Número de servicios de TI con requisitos de seguridad pendientes* • *(10) Plazo para otorgar, cambiar o eliminar los privilegios de acceso, en comparación con los niveles de servicio acordados* • *(10) Frecuencia de la evaluación de seguridad con respecto a los estándares y pautas más recientes*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(DSS05) Número de vulnerabilidades descubiertas* • *(DSS05) Porcentaje de personas que reciben entrenamiento de concienciación relacionado con el uso de dispositivos de punto final* • *(DSS05) Número de incidentes que implican dispositivos de punto final* • *(DSS05) Tiempo promedio entre el cambio y la actualización de las cuentas* • *(DSS05) Número de cuentas (frente al número de usuarios/personal no autorizados)* • *(DSS05) Calificación promedio de las evaluaciones de seguridad física* • *(DSS05) Número de incidentes relacionados con la seguridad física* • *(DSS05) Número de incidentes relacionados con el acceso no autorizado a la información*				

1402 Robo de servidores de desarrollo

Título del escenario de riesgo	Robo de servidores de desarrollo
Categoría del escenario de riesgo	14 Robo o destrucción de infraestructura
Referencia del escenario de riesgo	1402

Escenario de riesgo
Una empresa tiene políticas y sistemas comprensibles para controlar la entrada de personal autorizado a sus principales oficinas y edificios. Debido a que la compañía creció bastante rápido y necesitaba más espacio para oficinas, decidió transferir el equipo de desarrollo a un edificio alquilado para este propósito. El edificio alquilado tenía controles de entrada y del entorno descuidados e ineficientes.

Hubo una irrupción en el edificio que albergaba al equipo de desarrollo, y la mayoría de los servidores de desarrollo fueron robados. Debido a que los servidores no pudieron ser reemplazados rápidamente, el robo provocó grandes retrasos en la mayoría de los proyectos de desarrollo.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es **maliciosa**.

Agente
El agente que genera la amenaza que explota una vulnerabilidad es una persona **externa**, el ladrón.

Evento
El evento es el **robo** de un número sustancial de servidores de desarrollo.

Activo/Recurso (causa)
El activo/recurso que conduce al impacto en el negocio es el **diseño ineficaz** y/o **ejecución ineficaz** de los controles del entorno para la **infraestructura física, las instalaciones** y el **equipo**.

Activo/Recurso (efecto)
El activo/recurso afectado es la **infraestructura de TI**, específicamente, los servidores de desarrollo.

Tiempo
La duración del evento es **extensa** porque el cambio no se puede organizar inmediatamente. El momento de la ocurrencia es **crítico** porque la empresa está trabajando en algunos proyectos de desarrollo estratégicamente importantes. La detección es **inmediata** porque se detectó la mañana después de que los servidores fueron robados. El tiempo transcurrido entre el evento y la consecuencia se **demora** porque la empresa debe adquirir, configurar e implementar los nuevos servidores, lo que puede tomar un largo período de tiempo.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**S**	Los proyectos retrasados derivaron en oportunidades perdidas como un habilitador para nuevas iniciativas del negocio.
Entrega del proyecto y del programa de TI	**S**	Retraso en la entrega del proyecto.
Entrega del servicio y operaciones de TI	**P**	Destrucción de valor para la empresa.

Posibles respuestas al riesgo

- **Evitación del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** Seguro para el equipo.
- **Mitigación del riesgo:** Se aplicarán las políticas de seguridad del sitio físico en todas las ubicaciones. Se implementarán controles del entorno para en todas las ubicaciones. Contrato para un servicio de recuperación de desastres.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de seguridad de información física y ambiental	Restringir el acceso físico a la infraestructura para evitar la destrucción.	Alto	Bajo	SÍ
Política de continuidad del negocio y de recuperación de desastres	Validar la recuperación de información, servicios, aplicaciones e infraestructura.	Bajo	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
DSS01.04	Gestionar el ambiente.	Mantener medidas de protección contra los factores ambientales. Instalar equipo y dispositivos especializados para monitorizar y controlar el ambiente.	Alto	Medio	SÍ
DSS04.03	Desarrollar e implementar una respuesta de continuidad del negocio.	Desarrollar un plan de continuidad del negocio (BCP) basado en la estrategia que documenta los procedimientos y elementos de información que permiten a la empresa continuar sus actividades críticas después de un incidente.	Bajo	Alto	SÍ
DSS05.05	Gestionar el acceso físico a los activos de TI.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a las instalaciones, edificios y áreas debe justificarse, autorizarse, registrarse y monitorizarse. Esto debe aplicarse a todas las personas que entren en las instalaciones, incluyendo personal, personal temporal, clientes, proveedores, visitantes y cualquier otro tercero.	Alto	Bajo	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gerente de seguridad de la información	Responsable de implementar las medidas de seguridad.		Alto	Bajo	SÍ
Jefe de operaciones de TI	Responder al robo y la destrucción de infraestructura.		Bajo	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La seguridad de la información se practica en las operaciones diarias	Prevenir el acceso físico no autorizado.		Alto	Bajo	SÍ
Las personas respetan la importancia de las políticas y los principios de seguridad de la información	Prevenir el acceso físico no autorizado.		Alto	Bajo	SÍ
Las partes interesadas son conscientes de cómo identificar y responder a amenazas a la empresa	Minimizar el impacto del robo y destrucción de la infraestructura.		Medio	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Solicitudes de acceso	Auditar las solicitudes de acceso y las aprobaciones.		Alto	Bajo	SÍ
Registros de acceso	Monitorizar el acceso a las instalaciones.		Medio	Bajo	NO
Informes de evaluación de instalaciones	La empresa es consciente del estado y riesgo de las instalaciones.		Alto	Bajo	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Control de acceso	Prevenir el acceso lógico no autorizado.		Alto	Bajo	SÍ
Sistema de seguridad de alarma y monitorización	Prevenir el acceso físico no autorizado.		Alto	Medio	SÍ

Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de seguridad de la información	Implementar controles para prevenir o reducir el impacto del robo y destrucción de la infraestructura.	Alto	Alto	SÍ
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo* • *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(DSS05) Número de vulnerabilidades descubiertas* • *(DSS05) Porcentaje de pruebas periódicas de dispositivos de seguridad ambiental* • *(DSS05) Calificación promedio de las evaluaciones de seguridad física* • *(DSS05) Número de incidentes relacionados con la seguridad física*				

1404 Destrucción accidental de servidores individuales

Título del escenario de riesgo	Destrucción accidental de servidores individuales		
Categoría del escenario de riesgo	14 Robo o destrucción de infraestructura		
Referencia del escenario de riesgo	1404		
Escenario de riesgo Un gerente de cuentas clave usa una tableta para todas las actividades (gestión de clientes, pedidos, etc.) de gestión de relaciones con sus clientes (CRM). Durante una visita y una presentación en las oficinas de un cliente, una tetera es derribada y el té caliente se derrama sobre la tableta, destruyéndola. Los datos de la tableta no se pueden recuperar porque la memoria interna está muy dañada. Debido a que la tableta no se incluyó en los procedimientos de copia de seguridad de la empresa, y a que el gerente de cuentas clave nunca ha respaldado sus datos, todos los datos se pierden.			
Componentes del escenario de riesgo			
Tipo de amenaza La naturaleza del evento es **accidental**, la destrucción del dispositivo al verter agua sobre éste.			
Agente El agente que genera la amenaza que explota una vulnerabilidad es **interno**, el gerente de cuentas clave que derriba la tetera.			
Evento El evento es la **destrucción** de un dispositivo y los datos de éste.			
Activo/Recurso (causa) El activo/recurso que conduce al impacto en el negocio es el **diseño ineficaz** y/o **ejecución ineficaz** de los procedimientos de respaldo para dispositivos móviles.			
Activo/Recurso (efecto) El activo/recurso afectado es la **información** en dispositivo.			
Tiempo La duración del evento es **extensa** porque los datos se pierden definitivamente y se deben reelaborar a partir de la memoria y de los documentos del gerente de cuentas clave. El momento de la ocurrencia es **crítico** porque el gerente de cuentas clave necesita la información diariamente y la empresa perderá ingresos. La detección es **inmediata** porque se detecto inmediatamente, cuando los datos se perdieron. El tiempo transcurrido entre el evento y la consecuencia se **demora** porque el gerente de cuentas clave debe recuperar la información a partir de su memoria y documentación.			
Tipo de riesgo			
Habilitación del beneficio/valor de TI	**N/A**		
Entrega del proyecto y del programa de TI	**N/A**		
Entrega del servicio y operaciones de TI	**P**	Destrucción de valor para la empresa, la pérdida del dispositivo y problemas de seguridad.	
Posibles respuestas al riesgo			
• **Evitación del riesgo:** N/A • **Aceptación del riesgo:** N/A • **Compartir/transferir el riesgo:** Seguro para el equipo. • **Mitigación del riesgo:** Incluir los dispositivos móviles en la política y los procedimientos de copia de seguridad, e implementar copias de respaldo automatizadas en línea.			
Mitigación del Riesgo Usando Habilitadores de COBIT 5			
Habilitador de principios, políticas y marco de trabajo			

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de continuidad del negocio y de recuperación de desastres	Validar la recuperación de información, servicios, aplicaciones e infraestructura.	Bajo	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
DSS04.07	Administrar los arreglos de respaldo.	Mantener la disponibilidad de la información crítica para el negocio.	Bajo	Alto	SÍ
DSS05.03	Gestionar la seguridad de los terminales.	Asegurarse de que los terminales (p. ej., laptop, computadora de escritorio, servidor y otros dispositivos o software móviles o de red) estén asegurados a un nivel igual o superior al de los requerimientos de seguridad definidos para la información procesada, almacenada o transmitida.	Alto	Alto	SÍ
DSS06.06	Asegurar los activos de información.	Los activos de información seguros a los que tiene acceso el negocio a través de métodos aprobados, incluyendo información en formato electrónico (como métodos que crean nuevos activos en cualquier forma, dispositivos de medios portátiles, aplicaciones de usuario y dispositivos de almacenamiento), información en forma física (como documentos originales o informes de salida) e información en tránsito. Esto beneficia al negocio al ofrecer una protección de extremo a extremo para la información.	Alto	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Jefe de operaciones de TI	Responder al robo y la destrucción de infraestructura.		Bajo	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Las partes interesadas son conscientes de cómo identificar y responder a amenazas a la empresa	Minimizar el impacto del robo y destrucción de la infraestructura.		Bajo	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Habilitador de personas, habilidades y competencias					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de seguridad de la información	Implementar controles para prevenir o reducir el impacto del robo y destrucción de la infraestructura.		Alto	Alto	SÍ

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI
• *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo* • *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI* • *(10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o pérdida de reputación* • *(10) Número de servicios de TI con requisitos de seguridad pendientes* • *(10) Frecuencia de la evaluación de seguridad con respecto a los estándares y pautas más recientes* • *(14) Relación y extensión de las decisiones de negocio erróneas en las que la información errónea o no disponible fue un factor clave*
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso
• *(DSS05) Porcentaje de personas que reciben entrenamiento de concienciación relacionado con el uso de dispositivos de punto final* • *(DSS05) Número de incidentes que implican dispositivos de punto final* • *(DSS05) Número de dispositivos no autorizados detectados en la red o en el entorno del usuario final*

Página intencionalmente en blanco

15 Malware

1502 Infección de virus

Título del escenario de riesgo	Infección de virus
Categoría del escenario de riesgo	15 Malware
Referencia del escenario de riesgo	1502

Escenario de riesgo
Hackers externos, para causar la interrupción del negocio usan virus para atacar los sistemas de TI de una empresa. Un virus penetra la infraestructura de TI de la empresa, infectando servidores, computadoras de escritorio y laptops, y destruyendo información. La empresa está infectada con un virus que tiene una carga malintencionada que causa la eliminación de ciertos tipos de archivos. En algunos casos, el virus fue diseñado para eliminar todo el contenido de la unidad de almacenamiento. Debido al ataque a la infraestructura de TI de la empresa, la información es destruida, lo que impide tomar a tiempo las decisiones empresariales.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un acto **malicioso**, la infección con un virus.

Agente
Los agentes que generan la amenaza que explota la vulnerabilidad son **externos**, los hackers que desean causar una interrupción en los negocios.

Evento
El evento resulta en la **destrucción** de información y la **interrupción** de los procesos de negocio.

Activo/Recurso (causa)
El activo/recurso que conduce al impacto en el negocio son las **personas**, específicamente, los hackers que atacan los sistemas con el virus.

Activo/Recurso (efecto)
Los activos/recursos afectados por el evento son los diferentes **procesos** de negocio que son interrumpidos y la **información** destruida.

Tiempo
La duración del evento es **extensa** porque el ataque a la infraestructura de TI de la empresa destruye la información. El momento de la ocurrencia es **crítico** porque evita que puedan tomarse las decisiones empresariales a tiempo. La detección del evento es **inmediata** porque la información se pierde en el momento de la infección por el virus. Por la misma razón, el tiempo transcurrido entre el evento y la consecuencia es **inmediato**.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y del programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Interrupción del servicio de TI.
	P	Problemas de seguridad.
	S	Cuestiones de cumplimiento.

Posibles respuestas al riesgo

- **Evitación del riesgo:** N/A
- **Aceptación del riesgo:** El consejo toma la decisión de que nadie estaría interesado en atacar a la empresa, "no nos sucederá a nosotros".
- **Compartir/transferir el riesgo:** Comprar un seguro de interrupción del negocio.
- **Mitigación del riesgo:** Instalar una solución antivirus en todos los activos de infraestructura de TI relativos, y mantener las soluciones actualizadas. Implementar un programa de concienciación.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de seguridad de la información	Describir los arreglos de seguridad de la información dentro de la empresa.	Alto	Alto	SÍ
Política de prevención de software malicioso	Detallar las medidas preventivas, de detección y correctivas existentes en toda la empresa para proteger los sistemas de información y la tecnología contra el malware.	Alto	Medio	SÍ
Principios de arquitectura	Los requerimientos de seguridad de la información están integrados a la arquitectura empresarial y se traducen a una arquitectura formal de seguridad de la información.	Medio	Medio	NO
Política de continuidad del negocio y de recuperación de desastres	Validar la recuperación de información, servicios, aplicaciones e infraestructura.	Bajo	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO01.08	Mantener el cumplimiento con las políticas y los procedimientos.	Implementar procedimientos para mantener el cumplimiento, medir el rendimiento de las políticas y otros habilitadores del marco de control, y hacer cumplir las consecuencias del incumplimiento o desempeño inadecuado. Dar seguimiento a las tendencias y el rendimiento y considerarlos en el futuro diseño y mejora del marco de control.	Medio	Bajo	NO
APO13.02	Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información.	Mantener un plan de seguridad de la información que describe cómo se deben manejar los riesgos de seguridad de la información y cómo se debe alinear con la estrategia y la arquitectura empresariales. Asegurarse de que las recomendaciones para implementar mejoras a la seguridad se basen en casos de negocio aprobados e implementados como una parte integral del desarrollo de servicios y soluciones, y que después se operen como una parte integral de la operación del negocio.	Alto	Medio	SÍ
DSS05.01	Proteger contra malware.	Implementar y mantener medidas de prevención, detección y corrección (especialmente parches de seguridad y anti-malware actualizados) en toda la empresa para proteger los sistemas de información y la tecnología contra virus, gusanos, spyware, spam, etc.	Alto	Medio	SÍ
DSS05.07	Monitorizar la infraestructura para detectar eventos relacionados con la seguridad.	Usar herramientas de detección de intrusos, monitorizar la infraestructura para detectar accesos no autorizados y asegurarse que los eventos se integren en la monitorización general de eventos y en los procedimientos de gestión de incidentes.	Alto	Bajo	SÍ
DSS06.06	Asegurar los activos de información.	Los activos de información seguros a los que tiene acceso el negocio a través de métodos aprobados, incluyendo información en formato electrónico (como métodos que crean nuevos activos en cualquier forma, dispositivos de medios portátiles, aplicaciones de usuario y dispositivos de almacenamiento), información en forma física (como documentos originales o informes de salida) e información en tránsito. Esto beneficia al negocio al ofrecer una protección de extremo a extremo para la información.	Alto	Alto	SÍ

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gerente de seguridad de la información	Implementar las medidas de seguridad.	Alto	Alto	SÍ
Jefe de operaciones de TI	Liderar al equipo de respuesta a incidentes para restaurar el servicio de manera oportuna.	Bajo	Alto	

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La seguridad de la información se practica en las operaciones diarias	Prevenir la instalación no intencional de malware.	Medio	Bajo	NO
Las personas respetan la importancia de las políticas y los principios de seguridad de la información	Prevenir la instalación no intencional de malware.	Alto	Bajo	SÍ
Las partes interesadas son conscientes de cómo identificar y responder a amenazas a la empresa	Minimizar el impacto de la instalación de malware.	Medio	Alto	SÍ
Concienciación y capacitación sobre malware, correo electrónico y uso de internet	Prevenir la instalación no intencional de malware.	Alto	Bajo	SÍ

Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Informes de información sobre amenazas	Inteligencia sobre los tipos de ataques.	Alto	Bajo	NO
Informes de monitorización	Identificación de intentos de ataque, amenazas, etc.	Bajo	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gestión de información y eventos de seguridad (SIEM)	Proporciona análisis en tiempo real de las alertas de seguridad generadas por el hardware y las aplicaciones de red.	Alto	Alto	SÍ
Herramientas anti-malware	Protección contra virus.	Alto	Bajo	SÍ
Servicios de monitorización y alerta	Notificación oportuna de amenazas potenciales.	Medio	Alto	SÍ
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de seguridad de la información	Prevenir y reducir el impacto del malware.	Alto	Alto	SÍ
Habilidades técnicas en TI	Configuración adecuada de la infraestructura de TI, como sistemas de detección de intrusos (IDS) para detectar infecciones y prevenir la propagación.	Alto	Medio	SÍ

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(02) Costo de incumplimiento de TI, incluyendo acuerdos y multas, y el impacto de la pérdida reputacional*
- *(02) Número de problemas de incumplimiento en relación con acuerdos contractuales con los proveedores de servicios de TI*
- *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos*
- *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos*
- *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI*
- *(04) Frecuencia de actualización del perfil de riesgo*
- *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI*
- *(10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o pérdida de reputación*
- *(10) Número de servicios de TI con requisitos de seguridad pendientes*
- *(10) Frecuencia de la evaluación de seguridad con respecto a los estándares y pautas más recientes*
- *(14) Número de incidentes de procesos de negocio causados por la falta de disponibilidad de información*
- *(15) Número de incidentes relacionados con el incumplimiento de la política*
- *(15) Porcentaje de las partes interesadas que entienden las políticas*
- *(15) Porcentaje de las políticas respaldadas por estándares y prácticas de trabajo eficaces*
- *(16) Porcentaje de personal cuyas habilidades relacionadas con TI son suficientes para la competencia requerida para su función*
- *(16) Número de horas de aprendizaje/capacitación por cada miembro del personal*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(APO01) Porcentaje de políticas activas, estándares y otros habilitadores documentados y actualizados*
- *(APO01) Número de exposiciones de riesgo debido a las deficiencias en el diseño del ambiente de control*
- *(APO01) Número de empleados que asistieron a sesiones de capacitación o concienciación*
- *(APO13) Número de incidentes relacionados con la seguridad*
- *(APO13) Nivel de satisfacción de las partes interesadas con el plan de seguridad en toda la empresa*
- *(APO13) Número de soluciones de seguridad que se desvían del plan*
- *(APO13) Número de incidentes de seguridad causados por el incumplimiento con el plan de seguridad*
- *(APO13) Número de servicios con apego confirmado al plan de seguridad*
- *(APO13) Número de incidentes de seguridad causados por el incumplimiento con el plan de seguridad*
- *(DSS05) Número de vulnerabilidades descubiertas*
- *(DSS05) Número de violaciones del firewall (cortafuegos)*
- *(DSS05) Porcentaje de personas que reciben entrenamiento de concienciación relacionado con el uso de dispositivos de punto final*
- *(DSS05) Número de incidentes que implican dispositivos de punto final*
- *(DSS05) Número de dispositivos no autorizados detectados en la red o en el entorno del usuario final*
- *(DSS05) Número de incidentes relacionados con el acceso no autorizado a la información*
- *(DSS06) Porcentaje de inventario completado de procesos críticos y controles clave*
- *(DSS06) Porcentaje de cobertura de los controles clave con planes de prueba*
- *(DSS06) Número de incidentes y hallazgos del reporte de auditoría que indican una falla de los controles clave*

1503 Finalización del contrato del empleado y robo

Título del escenario de riesgo	Finalización del contrato del empleado y robo
Categoría del escenario de riesgo	15 Malware
Referencia del escenario de riesgo	1503

Escenario de riesgo
Se notifica al empleado, debido a las restricciones presupuestarias de la empresa, será despedido en los próximos 30 días. Esta persona se considera a sí mismo un activo crítico para la empresa, y después de ser notificado, como venganza, comienza a copiar los datos básicos de la empresa y a enviarlos por correo electrónico a los competidores.

Después de guardar estos datos en su propio dispositivo de almacenamiento, diseña una bomba de tiempo y la pone en sistemas de producción para cambiar la lógica de sistemas que soporta las funciones críticas del negocio (90 días después de dejar la empresa), lo cual resultará en grandes pérdidas para la empresa.

Debido a que este empleado es muy cercano al Director de Seguridad de la Información (CISO) de la compañía, quien se jubilará, el CISO acuerda ayudar a este empleado a alterar los controles de seguridad de la empresa.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es **maliciosa**.

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **interno**, el empleado que fue despedido.

Evento
El evento es la divulgación de datos de la empresa y la **modificación** no autorizada de la lógica de sistemas por la bomba de tiempo.

Activo/Recurso (causa)
El activo/recurso que conduce al impacto en el negocio es una **persona**, el empleado despedido. El **diseño ineficaz** y la **ejecución ineficaz** de los **procesos** DSS05 *Gestionar los servicios de seguridad* y APO07 *Gestionar los recursos humanos* también son recursos.

Activo/Recurso (efecto)
Los recursos secundarios afectados son los **procesos** de negocio soportados por la lógica del sistema que fue cambiada por la bomba de tiempo, además de la **información**, como los datos empresariales básicos que se copiaron y enviaron a los competidores.

Tiempo
La duración del evento es **extensa** porque toma mucho tiempo corregir la lógica del sistema afectado, así como el daño a la reputación y el negocio debido a la divulgación de datos básicos de la empresa. El momento de la ocurrencia es **crítico** porque el CISO se jubilará. La detección es **lenta** porque la bomba de tiempo no se detecta antes de que destruya la lógica del sistema. Por la misma razón, el tiempo transcurrido entre el evento y la consecuencia se **demora**.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y del programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Problemas de seguridad.

Posibles respuestas al riesgo

- **Evitación del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** La empresa necesita actualizar la política de recursos humanos (RR.HH.) para la finalización del contrato del empleado, especialmente para empleados críticos, así como definir los procesos, incluyendo la notificación al departamento de TI. Después de la notificación, el departamento de TI debe:
  - Verificar y monitorizar activamente el registro de actividad del empleado después de que éste ha sido notificado.
  - Desarrollar informes especiales para la gerencia en este registro de actividades.
  - Limitar el acceso de datos a los recursos críticos.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de seguridad de la información	Describir los arreglos de seguridad de la información dentro de la empresa.	Alto	Alto	SÍ
Política de prevención de software malicioso	Detallar las medidas preventivas, de detección y correctivas existentes en toda la empresa para proteger los sistemas de información y la tecnología contra el malware.	Alto	Alto	SÍ
Principios de arquitectura	Los requerimientos de seguridad de la información están integrados a la arquitectura empresarial y se traducen a una arquitectura formal de seguridad de la información.	Alto	Bajo	SÍ
Política de continuidad del negocio y de recuperación de desastres	Validar la recuperación de información, servicios, aplicaciones e infraestructura.	Bajo	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
DSS05.01	Proteger contra malware.	Implementar y mantener medidas de prevención, detección y corrección (especialmente parches de seguridad y anti-malware actualizados) en toda la empresa para proteger los sistemas de información y la tecnología contra virus, gusanos, spyware, spam, etc.	Medio	Bajo	NO
DSS05.04	Gestionar la identidad del usuario y el acceso lógico.	Asegurarse de que todos los usuarios tengan derechos de acceso a la información de acuerdo con sus requerimientos del negocio, y que haya coordinación con las unidades del negocio que gestionan sus propios derechos de acceso en los procesos de negocio.	Alto	Medio	SÍ
DSS05.05	Gestionar el acceso físico a los activos de TI.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a las instalaciones, edificios y áreas debe justificarse, autorizarse, registrarse y monitorizarse. Esto debe aplicarse a todas las personas que entren en las instalaciones, incluyendo personal, personal temporal, clientes, proveedores, visitantes y cualquier otro tercero.	Alto	Bajo	SÍ
DSS05.07	Monitorizar la infraestructura para detectar eventos relacionados con la seguridad.	Usar herramientas de detección de intrusos, monitorizar la infraestructura para detectar accesos no autorizados y asegurarse que los eventos se integren en la monitorización general de eventos y en los procedimientos de gestión de incidentes.	Alto	Bajo	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gerente de seguridad de la información	Implementar las medidas de seguridad.		Alto	Alto	SÍ
Jefe de operaciones de TI	Liderar al equipo de respuesta a incidentes para restaurar el servicio de manera oportuna.		Bajo	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La seguridad de la información se practica en las operaciones diarias	Prevenir la instalación accidental de malware.		Alto	Bajo	SÍ
Las personas respetan la importancia de las políticas y los principios de seguridad de la información	Prevenir la instalación accidental de malware.		Medio	Medio	NO
Las partes interesadas son conscientes de cómo identificar y responder a amenazas a la empresa	Minimizar el impacto de la instalación de malware.		Bajo	Alto	SÍ
Concienciación y capacitación sobre malware, correo electrónico y uso de internet	Prevenir la instalación accidental de malware.		Alto	Bajo	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Informes de información sobre amenazas	Inteligencia sobre los tipos de ataques.		Medio	Medio	NO
Informes de monitorización	Identificar los intentos de ataque, amenazas, etc.		Bajo	Alto	SÍ

Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gestión de información y eventos de seguridad (SIEM)	Proporciona análisis en tiempo real de las alertas de seguridad generadas por el hardware y las aplicaciones de red.	Alto	Alto	SÍ
Herramientas de protección contra software malicioso	Protección contra malware.	Alto	Bajo	SÍ
Servicios de monitorización y alerta	Notificación oportuna de amenazas potenciales.	Bajo	Alto	SÍ
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de seguridad de la información	Prevenir y reducir el impacto del malware.	Alto	Alto	SÍ
Habilidades técnicas en TI	Configuración adecuada de la infraestructura de TI, como sistemas de detección de intrusos (IDS) para detectar infecciones y prevenir la propagación.	Medio	Medio	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos*
- *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos*
- *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI*
- *(04) Frecuencia de actualización del perfil de riesgo*
- *(10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o pérdida de reputación*
- *(10) Número de servicios de TI con requisitos de seguridad pendientes*
- *(10) Plazo para otorgar, cambiar o eliminar los privilegios de acceso, en comparación con los niveles de servicio acordados*
- *(10) Frecuencia de la evaluación de seguridad con respecto a los estándares y pautas más recientes*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(DSS05) Número de vulnerabilidades descubiertas*
- *(DSS05) Número de violaciones del firewall (cortafuegos)*
- *(DSS05) Porcentaje de personas que reciben entrenamiento de concienciación relacionado con el uso de dispositivos de punto final*
- *(DSS05) Número de incidentes que implican dispositivos de punto final*
- *(DSS05) Número de dispositivos no autorizados detectados en la red o en el entorno del usuario final*
- *(DSS05) Tiempo promedio entre el cambio y la actualización de las cuentas*
- *(DSS05) Número de cuentas (frente al número de usuarios/personal no autorizados)*
- *(DSS05) Porcentaje de pruebas periódicas de dispositivos de seguridad ambiental*
- *(DSS05) Calificación promedio de las evaluaciones de seguridad física*
- *(DSS05) Número de incidentes relacionados con la seguridad física*
- *(DSS05) Número de incidentes relacionados con el acceso no autorizado a la información*

1504 Phishing

Título del escenario de riesgo	Phishing
Categoría del escenario de riesgo	15 Malware
Referencia del escenario de riesgo	1504

Escenario de riesgo
Un grupo de hackers envía spam a un gran número de usuarios de una empresa, pretendiendo ser de la misma empresa, e informándoles que se ha producido un problema de seguridad con su cuenta de usuario solicitando que verifiquen sus credenciales de inicio de sesión. Estas credenciales serán capturadas por el malware y utilizadas en una fecha posterior para obtener acceso no autorizado a los sistemas empresariales. Esta información se vende posteriormente a un competidor.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es la acción **maliciosa** por parte de los hackers y el spam que reciben y abren empleados **accidentalmente**, lo cual causa que los usuarios sean engañados para proporcionar sus credenciales de inicio de sesión, y los hackers entonces usan estas credenciales para obtener acceso a los sistemas y la información de la empresa.

Agente
Los agentes que generan la amenaza que explota la vulnerabilidad son **externos**, los hackers que distribuyen el malware en el correo electrónico. Los empleados **internos** también son agentes al abrir el correo electrónico y confirmar la solicitud, proporcionando sus credenciales de inicio de sesión.

Evento
El evento es el **robo** y la **divulgación** de datos porque las credenciales se utilizan para obtener acceso a los sistemas y la información empresariales, y la información comercial sensible se vende a un competidor.

Activo/Recurso (causa)
El activo/recurso que conduce al impacto en el negocio es las **personas**, los hackers y también los empleados que fueron engañados.

Activo/Recurso (efecto)
El activo/recurso afectado es la **información** comercial robada y sensible, que se vende posteriormente a un competidor.

Tiempo
Cuando las credenciales son utilizadas por los hackers para obtener acceso no autorizado a los sistemas empresariales, es **crítico** que el evento sea detectado rápidamente porque la empresa está planeando una campaña de marketing y los competidores podrían entrar en el mercado antes que ellos. Sin embargo, la duración puede ser **extensa** porque la información robada puede ser usada por los competidores durante un período más largo para atraer clientes de la compañía atacada. La detección es probablemente **moderada** y el tiempo transcurrido entre el acontecimiento y la consecuencia se **demora** porque puede haber un retraso desde el momento en que los hackers obtienen las credenciales de inicio de sesión, hasta el momento en que las utilizan para obtener acceso no autorizado.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y del programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Problemas de seguridad.
	S	Interrupciones del servicio de TI.
	S	Cuestiones de cumplimiento.

Posibles respuestas al riesgo

- **Evitación del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** Usar un servicio de correo electrónico alojado, que incluye un servicio de filtrado de spam.
- **Mitigación del riesgo:** Implementar filtros de spam para identificar y poner en cuarentena los correos electrónicos de spam y educar a los usuarios finales. Implementar sistemas de detección de intrusos (IDS) para identificar los intentos de inicio de sesión procedentes del exterior de la empresa.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de seguridad de la información	Describir los arreglos de seguridad de la información dentro de la empresa.	Alto	Alto	SÍ
Política de prevención de software malicioso	Detallar las medidas preventivas, de detección y correctivas existentes en toda la empresa para proteger los sistemas de información y la tecnología contra el malware.	Alto	Alto	SÍ
Principios de arquitectura	Los requerimientos de seguridad de la información están integrados a la arquitectura empresarial y se traducen a una arquitectura formal de seguridad de la información.	Medio	Bajo	NO

Política de continuidad del negocio y de recuperación de desastres	Validar la recuperación de información, servicios, aplicaciones e infraestructura.		Bajo	Alto	SÍ
Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO01.03	Mantener los habilitadores del sistema de gestión.	Mantener los habilitadores del sistema de gestión y el entorno de control para las TI empresariales, y asegurarse de que estén integrados y alineados con la filosofía de gobierno y gestión y el estilo operativo de la empresa. Estos habilitadores incluyen la clara comunicación de expectativas/requerimientos. El sistema de gestión debe fomentar la cooperación y el trabajo en equipo entre las divisiones, promover el cumplimiento y la mejora continua, y manejar las desviaciones del proceso (incluyendo los fracasos).	Medio	Bajo	NO
APO01.04	Comunicar los objetivos y la dirección de la gerencia.	Concienciar y comunicar, buscando la comprensión de los objetivos y la dirección de TI a las partes interesadas en toda la empresa.	Medio	Bajo	NO
APO01.08	Mantener el cumplimiento con las políticas y los procedimientos.	Implementar procedimientos para mantener el cumplimiento, medir el rendimiento de las políticas y otros habilitadores del marco de control, y hacer cumplir las consecuencias del incumplimiento o desempeño inadecuado. Dar seguimiento a las tendencias y el rendimiento y considerarlos en el futuro diseño y mejora del marco de control.	Medio	Bajo	NO
APO07.03	Mantener las habilidades y las competencias del personal.	Definir y administrar las habilidades y las competencias del personal necesario. Verificar periódicamente que el personal cuente con las competencias necesarias para realizar sus funciones en base a su educación, capacitación y/o experiencia, y verificar que estas competencias se mantengan usando programas de cualificación y certificación cuando sea apropiado. Dar a los empleados oportunidades de aprendizaje continuas para mantener sus conocimientos, habilidades y competencias al nivel requerido para alcanzar las metas empresariales.	Medio	Bajo	NO
APO13.02	Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información.	Mantener un plan de seguridad de la información que describe cómo se deben manejar los riesgos de seguridad de la información y cómo se debe alinear con la estrategia y la arquitectura empresariales. Asegurarse de que las recomendaciones para implementar mejoras a la seguridad se basen en casos de negocio aprobados e implementados como una parte integral del desarrollo de servicios y soluciones, y que después se operen como una parte integral de la operación del negocio.	Alto	Medio	SÍ
DSS05.01	Proteger contra malware.	Implementar y mantener medidas de prevención, detección y corrección (especialmente parches de seguridad y anti-malware actualizados) en toda la empresa para proteger los sistemas de información y la tecnología contra virus, gusanos, spyware, spam, etc.	Alto	Medio	SÍ
DSS05.07	Monitorizar la infraestructura para detectar eventos relacionados con la seguridad.	Usar herramientas de detección de intrusos, monitorizar la infraestructura para detectar accesos no autorizados y asegurarse que los eventos se integren en la monitorización general de eventos y en los procedimientos de gestión de incidentes.	Alto	Bajo	SÍ
DSS06.06	Asegurar los activos de información.	Los activos de información seguros a los que tiene acceso el negocio a través de métodos aprobados, incluyendo información en formato electrónico (como métodos que crean nuevos activos en cualquier forma, dispositivos de medios portátiles, aplicaciones de usuario y dispositivos de almacenamiento), información en forma física (como documentos originales o informes de salida) e información en tránsito. Esto beneficia al negocio al ofrecer una protección de extremo a extremo para la información.	Alto	Alto	SÍ

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gerente de seguridad de la información	Implementar las medidas de seguridad.	Alto	Alto	SÍ
Jefe de operaciones de TI	Liderar al equipo de respuesta a incidentes para restaurar el servicio de manera oportuna.	Bajo	Alto	SÍ
Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La seguridad de la información se practica en las operaciones diarias	Prevenir la instalación accidental de malware.	Alto	Medio	SÍ
Las personas respetan la importancia de las políticas y los principios de seguridad de la información	Prevenir la instalación accidental de malware.	Alto	Alto	SÍ
Las partes interesadas son conscientes de cómo identificar y responder a amenazas a la empresa	Minimizar el impacto de la instalación de malware.	Medio	Alto	SÍ
Concienciación y capacitación sobre malware, correo electrónico y uso de internet	Prevenir la instalación accidental de malware.	Alto	Medio	SÍ
Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Informes de información sobre amenazas	Inteligencia sobre los tipos de ataques.	Alto	Medio	SÍ
Informes de monitorización	Identificar los intentos de ataque, amenazas, etc.	Bajo	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gestión de información y eventos de seguridad (SIEM)	Proporciona análisis en tiempo real de las alertas de seguridad generadas por el hardware y las aplicaciones de red.	Alto	Alto	SÍ
Herramientas de protección contra software malicioso	Protección contra malware.	Alto	Bajo	SÍ
Servicios de monitorización y alerta	Notificación oportuna de amenazas potenciales.	Medio	Alto	SÍ
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de seguridad de la información	Prevenir y reducir el impacto del malware.	Alto	Alto	SÍ
Habilidades técnicas en TI	Configuración adecuada de la infraestructura de TI, como sistemas de detección de intrusos (IDS) para detectar infecciones y prevenir la propagación.	Alto	Medio	SÍ

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI
• *(02) Costo de incumplimiento de TI, incluyendo acuerdos y multas, y el impacto de la pérdida reputacional*
• *(02) Número de asuntos de incumplimiento relacionados con la TI reportados a la junta o que causan comentarios o vergüenza públicos*
• *(02) Número de problemas de incumplimiento en relación con acuerdos contractuales con los proveedores de servicios de TI*
• *(02) Cobertura de las evaluaciones de cumplimiento*
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos*
• *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos*
• *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI*
• *(04) Frecuencia de actualización del perfil de riesgo*
• *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI*
• *(10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o pérdida de reputación*
• *(10) Número de servicios de TI con requisitos de seguridad pendientes*
• *(10) Frecuencia de la evaluación de seguridad con respecto a los estándares y pautas más recientes*
• *(14) Número de incidentes de procesos de negocio causados por la falta de disponibilidad de información*
• *(15) Número de incidentes relacionados al incumplimiento con la política*
• *(15) Porcentaje de las partes interesadas que entienden las políticas*
• *(15) Porcentaje de las políticas respaldadas por estándares y prácticas de trabajo eficaces*
• *(16) Porcentaje de personal cuyas habilidades relacionadas con TI son suficientes para la competencia requerida para su función*
• *(16) Número de horas de aprendizaje/capacitación por cada miembro del personal*
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso
• *(APO01) Porcentaje de políticas activas, estándares y otros habilitadores documentados y actualizados*
• *(APO01) Número de exposiciones de riesgo debido a las deficiencias en el diseño del ambiente de control*
• *(APO01) Número de empleados que asistieron a sesiones de capacitación o concienciación*
• *(APO13) Número de incidentes relacionados con la seguridad*
• *(APO13) Nivel de satisfacción de las partes interesadas con el plan de seguridad en toda la empresa*
• *(APO13) Número de soluciones de seguridad que se desvían del plan*
• *(APO13) Número de incidentes de seguridad causados por el incumplimiento con el plan de seguridad*
• *(APO13) Número de servicios con apego confirmado al plan de seguridad*
• *(APO13) Número de incidentes de seguridad causados por el incumplimiento con el plan de seguridad*
• *(DSS05) Número de vulnerabilidades descubiertas*
• *(DSS05) Número de violaciones del firewall (cortafuegos)*
• *(DSS05) Porcentaje de personas que reciben entrenamiento de concienciación relacionado con el uso de dispositivos de punto final*
• *(DSS05) Número de incidentes que implican dispositivos de punto final*
• *(DSS05) Número de dispositivos no autorizados detectados en la red o en el entorno del usuario final*
• *(DSS05) Número de incidentes relacionados con el acceso no autorizado a la información*
• *(DSS06) Porcentaje de inventario completado de procesos críticos y controles clave*
• *(DSS06) Porcentaje de cobertura de los controles clave con planes de prueba*
• *(DSS06) Número de incidentes y hallazgos del reporte de auditoría que indican una falla de los controles clave*

16 Ataques lógicos

1602 Penetración de red

Título del escenario de riesgo	Penetración de red
Categoría del escenario de riesgo	16 Ataques lógicos
Referencia del escenario de riesgo	1602

Escenario de riesgo
Una empresa tiene un sitio web público, a través del cual un grupo de hackers derriba los sistemas de negocio de la empresa. Esto se hace rompiendo el perímetro de red de la empresa y penetrando en la red, e introduciendo malware que derriba los servidores y deriva en un ataque de denegación de servicio (DoS) que niega a los usuarios el acceso a las aplicaciones. Las operaciones normales del negocio se interrumpen. Las ventas no se pueden procesar a través del sitio web de la empresa, causando pérdidas de ingresos y daños a la reputación.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un ataque DoS **malicioso** por parte de hackers, el cual derriba los servidores y niega a los usuarios el acceso a las aplicaciones y la información.

Agente
Los agentes que generan la amenaza que explota la vulnerabilidad son los hackers **externos**.

Evento
El evento es la **interrupción** de los servicios de TI para que los usuarios no puedan acceder a las aplicaciones e información, y por lo tanto, los procesos/las operaciones de negocio normales se interrumpen y las ventas no se pueden procesar a través del sitio web de la empresa, causando pérdidas de ingresos y daños a la reputación.

Activo/Recurso (causa)
El activo/recurso que provoca el impacto en el negocio son las **personas**, los hackers.

Activo/Recurso (efecto)
Los activos/recursos afectados son principalmente las operaciones de negocio **interrumpidas**. Sin embargo, dado que se niega el acceso a la **infraestructura de TI, la información** y las **aplicaciones** también son afectadas.

Tiempo
La respuesta al ataque DoS es **crítica** para restaurar rápidamente el acceso a los sistemas de negocio y que las ventas se puedan reanudar. La duración es **extensa** porque restaurar el sitio web oficial puede tomar bastante tiempo. La detección del evento es **inmediata**, y el tiempo transcurrido entre el evento y la consecuencia es también **inmediato**.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y del programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Interrupción de los servicios de TI (y de negocios).
	P	Problemas de seguridad.
	S	Cuestiones de cumplimiento.

Posibles respuestas al riesgo

- **Evitación del riesgo:** N/A
- **Aceptación del riesgo:** El consejo toma la decisión de que nadie está interesado en atacar a la empresa, "no nos sucederá a nosotros".
- **Compartir/transferir el riesgo:** Comprar un seguro de interrupción del negocio.
- **Mitigación del riesgo:** Instalar y configurar un cortafuegos (firewall), reforzar/bastionar el servidor y aplicar los parches de seguridad actualizados. Desplegar y monitorizar activamente un IDS. Tener procedimientos de recuperación de desastres establecidos para restaurar el sitio web, si es necesario.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de seguridad de la información	Describir los arreglos de seguridad de la información dentro de la empresa.	Alto	Alto	SÍ
Políticas y procedimientos técnicos de seguridad	Detallar las consecuencias técnicas de la política de seguridad de la información.	Alto	Alto	SÍ
Principios de arquitectura	Los requerimientos de seguridad de la información están integrados a la arquitectura empresarial y se traducen a una arquitectura formal de seguridad de la información.	Alto	Alto	SÍ
Política de continuidad del negocio y de recuperación de desastres	Validar la recuperación de información, servicios, aplicaciones e infraestructura.	Bajo	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
DSS04.03	Desarrollar e implementar una respuesta de continuidad del negocio.	Desarrollar un plan de continuidad del negocio (BCP) basado en la estrategia que documenta los procedimientos y elementos de información que permiten a la empresa continuar sus actividades críticas después de un incidente.	Bajo	Alto	SÍ
DSS05.01	Proteger contra malware.	Implementar y mantener medidas de prevención, detección y corrección (especialmente parches de seguridad y anti-malware actualizados) en toda la empresa para proteger los sistemas de información y la tecnología contra virus, gusanos, spyware, spam, etc.	Alto	Medio	SÍ
DSS05.02	Gestionar la seguridad de la red y las conexiones.	Usar medidas de seguridad y procedimientos de gestión relacionados para proteger la información a través de todos los métodos de conectividad.	Medio	Bajo	NO
DSS05.03	Gestionar la seguridad de los terminales.	Asegurarse que los terminales (p. ej., portátiles, computadora de escritorio, servidor, móviles , y otros dispositivos o software de red) estén asegurados a un nivel igual o superior al de los requerimientos de seguridad definidos para la información que procesen, almacenen o transmitan.	Alto	Bajo	SÍ
DSS05.07	Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Usar herramientas de detección de intrusión, supervisar la infraestructura para detectar accesos no autorizados y asegurarse que los eventos se integren en la supervisión general de eventos y en los procedimientos de gestión de incidentes.	Bajo	Medio	NO

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en el frecuencia**	**Efecto en el impacto**	**Control esencial**
Gerente de seguridad de la información	Implementar las medidas de seguridad.	Alto	Alto	SÍ
Jefe de operaciones de TI	Liderar al equipo de respuesta para restaurar el servicio de manera oportuna.	Bajo	Alto	SÍ
Gestor del servicio	En caso que los ataques tengan éxito, comunicarse con el usuario final y ayudar a gestionar la respuesta.	Bajo	Alto	SÍ
Director de Arquitectura de Seguridad	Diseñar medidas de seguridad.	Alto	Alto	SÍ

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La seguridad de la información se practica diariamente durante las operaciones	Evitar ataques lógicos.	Alto	Medio	SÍ
Las personas respetan la importancia de las políticas y los principios de seguridad de la información	Evitar ataques lógicos.	Medio	Bajo	NO
Las partes interesadas son conscientes de cómo identificar y responder a amenazas a la empresa	Minimizar el impacto de ataques lógicos.	Bajo	Alto	SÍ

Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Acuerdos de nivel de servicio (SLA)	Detallar la acción a emprender en caso de ataque.	Bajo	Medio	NO
Informes de información sobre amenazas	Inteligencia sobre los tipos de ataques.	Alto	Medio	SÍ
Informes de supervisión	Identificar los intentos de ataque, los eventos de amenaza, etc.	Bajo	Alto	SÍ

Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Cortafuegos (firewall)	Evitar ataques lógicos exitosos.	Alto	Bajo	SÍ
Gestión de eventos e información de seguridad (SIEM)	Proporciona análisis en tiempo real de las alertas de seguridad generadas por el hardware de red y las aplicaciones.	Alto	Alto	SÍ
Herramientas de gestión de red/escáneres de vulnerabilidad	Identificar las debilidades.	Alto	Medio	SÍ
Servicios de monitorización y alerta	Notificación oportuna de amenazas potenciales.	Bajo	Alto	SÍ
Habilitador de personas, habilidades y competencias				
Habilidades de seguridad de la información	Prevenir y reducir el impacto de los ataques lógicos.	Alto	Alto	SÍ
Habilidades técnicas en TI	Configurar la infraestructura de TI, como cortafuegos (firewalls), componentes críticos de la red, etc.	Alto	Alto	SÍ
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas TIC empresariales activados y cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo* • *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI* • *(10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o desconcierto público* • *(10) Número de servicios de TI con requisitos pendientes de seguridad* • *(10) Frecuencia de evaluaciones de seguridad con respecto a los estándares y las guías más recientes* • *(14) Número de incidentes de procesos de negocio causados por la falta de disponibilidad de información*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(DSS04) Porcentaje de servicios de TI que satisfacen los requisitos en tiempo de actividad* • *(DSS04) Número de sistemas empresariales críticos no cubiertos por el plan de continuidad del negocio* • *(DSS04) Número de ejercicios y pruebas que han alcanzado los objetivos de recuperación* • *(DSS04) Frecuencia de las pruebas de recuperación* • *(DSS05) Número de vulnerabilidades descubiertas* • *(DSS05) Número de infracciones en el cortafuegos (firewall)* • *(DSS05) Porcentaje de personas que reciben entrenamiento de concienciación relacionado en el uso de terminales* • *(DSS05) Número de incidentes que impliquen terminales* • *(DSS05) Número de dispositivos no autorizados detectados en la red o en el entorno del usuario final* • *(DSS05) Número de incidentes relacionados con el acceso no autorizado a la información*				

1604 Espionaje industrial

Título del escenario de riesgo	Espionaje industrial
Categoría del escenario de riesgo	16 Ataques lógicos
Referencia del escenario de riesgo	1604

Escenario de riesgo
Una famosa empresa farmacéutica mundial está sujeta al espionaje industrial por medio de las técnicas avanzadas de amenazas persistentes (APTs) por intrusos externos. Un gobierno extranjero financió a los intrusos para obtener secretos de las investigaciones y desarrollos con el fin de promover la industria farmacéutica en su país. Se consiguió penetrar la infraestructura TI usando técnicas de APT, y se robó y filtró información sensible sobre las investigaciones y desarrollos de productos, permitiendo que productos competidores más baratos se lanzaran al mercado.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es la penetración **maliciosa** de la infraestructura de TI mediante el uso de técnicas APT.

Agente
Los agentes que generan la amenaza que explota la vulnerabilidad son **externos**, los intrusos financiados por un gobierno **externo** extranjero.

Evento
El evento es el **robo** y la **divulgación** al penetrar dentro de **la** infraestructura TI usando técnicas de APT, y se robó información sensible sobre las investigaciones y desarrollos de productos, permitiendo que productos competidores más baratos se lanzaran al mercado.

Activo/Recurso (causa)
El activo/recurso que provoca el impacto en el negocio son las **personas**, los hackers.

Activo/Recurso (efecto)
Los activos/recursos afectados son la **infraestructura de TI** penetrada y la **información** sensible robada sobre las investigaciones y desarrollos.

Tiempo
La respuesta al ataque de denegación de servicio (DoS) es **crítica** para restaurar rápidamente el acceso a los sistemas de negocio y que las ventas se puedan reanudar. La duración es **extensa** porque puede durar bastante tiempo restaurar el sitio web oficial. La detección del evento es **inmediata**, y el tiempo transcurrido entre el evento y la consecuencia es también **inmediato**.

La duración del evento es **extensa** porque las APT generalmente permanecen sin ser detectadas durante bastante tiempo. El momento de la ocurrencia es **crítico** porque la empresa tiene un período corto de tiempo antes de lanzar un nuevo producto farmacéutico basado en los resultados de la investigación con información sensible Debido a que puede transcurrir un largo período de tiempo antes que se detecte esta fuga de información, la clasificación para la detección es **lenta**, y por la misma razón, el tiempo transcurrido entre el evento y la consecuencia se **demora.**

Tipo de riesgo

Activación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Problemas de seguridad.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** El consejo toma la decisión de que nadie estaría interesado en atacar a la empresa, "no nos sucederá a nosotros".
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Instalar y configurar apropiadamente los cortafuegos (firewalls), bastionado del servidor y asegurarse que los parches de seguridad se instalen oportunamente. Desplegar y supervisar activamente con un sistema de detección de intrusos (IDS).

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de seguridad de la información	Describir las adaptaciones de seguridad de la información dentro de la empresa.	Alto	Alto	SÍ
Políticas y procedimientos técnicos de seguridad	Detallar las consecuencias técnicas de la política de seguridad de la información.	Alto	Alto	SÍ
Principios de arquitectura	Los requerimientos de seguridad de la información están integrados a la arquitectura empresarial y se traducen a una arquitectura formal de seguridad de la información.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
DSS05.01	Proteger contra el código malicioso.	Implementar y mantener medidas de prevención, detección y corrección (especialmente parches de seguridad y anti-malware actualizados) en toda la empresa para proteger los sistemas de información y la tecnología contra virus, gusanos, software espia, spam, etc.	Alto	Medio	SÍ
DSS05.02	Gestionar la seguridad en la red y las conexiones.	Usar medidas de seguridad y procedimientos de gestión relacionados para proteger la información a través de todos los métodos de conectividad.	Medio	Bajo	NO
DSS05.03	Gestionar la seguridad de los terminales.	Asegurarse que los terminales (p. ej., portátiles, computadora de escritorio, servidor y otros dispositivos móviles o software de red) estén asegurados a un nivel igual o superior al de los requerimientos de seguridad definidos para la información procesada, almacenada o transmitida.	Alto	Bajo	SÍ
DSS05.07	Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Usar herramientas de detección de intrusos, supervisar la infraestructura para detectar accesos no autorizados y asegurarse que los eventos se integren en la supervisión general de eventos y en los procedimientos de gestión de incidentes.	Bajo	Medio	NO
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gestor de seguridad de la información	Implementar las medidas de seguridad.		Alto	Alto	SÍ
Gestor de servicio	En caso que los ataques tengan éxito, comunicarse con el usuario final y ayudar a gestionar la respuesta.		Bajo	Medio	NO
Director de Arquitectura de Seguridad	Diseñar medidas de seguridad.		Alto	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La seguridad de la información se practica en las operaciones diarias	Evitar ataques lógicos.		Alto	Bajo	SÍ
Las personas respetan la importancia de las políticas y los principios de seguridad de la información	Prevenir ataques lógicos.		Alto	Bajo	SÍ
Las partes interesadas son conscientes de cómo identificar y responder ante las amenazas a la empresa	Minimizar el impacto de ataques lógicos.		Bajo	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Acuerdos de nivel de servicio (SLA)	Detallar la acción a emprender en caso de ataque.		Bajo	Alto	SÍ
Informes sobre amenazas hacia la información	Inteligencia en cuanto a tipos de ataques.		Alto	Medio	SÍ
Informes de supervisión	Identificar los intentos de ataque, los eventos de amenaza, etc.		Bajo	Alto	SÍ

Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Cortafuegos (firewall)	Prevenir los logros de los ataques lógicos.	Alto	Bajo	SÍ
Gestión de los eventos de seguridad de la información (SIEM)	Proporciona análisis en tiempo real de las alertas de seguridad generadas por el hardware y las aplicaciones de red.	Alto	Alto	SÍ
Herramientas de gestión de red/escáneres de vulnerabilidad	Identificar las debilidades.	Alto	Bajo	SÍ
Servicios de supervisión y alerta	Notificación oportuna de amenazas potenciales.	Bajo	Alto	SÍ
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de seguridad de la información	Prevenir y reducir el impacto de los ataques lógicos.	Alto	Alto	SÍ
Habilidades técnicas en TI	Configurar la infraestructura de TI, como cortafuegos (firewalls), componentes críticos de la red, etc.	Alto	Medio	SÍ
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo* • *(10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o pérdida de reputación* • *(10) Número de servicios de TI con requisitos de seguridad pendientes* • *(10) Frecuencia de la evaluación de seguridad con respecto a los estándares y pautas más recientes*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(DSS05) Número de vulnerabilidades descubiertas* • *(DSS05) Número de infracciones del cortafuegos (firewall)* • *(DSS05) Porcentaje de personas que reciben entrenamiento de concienciación relacionado con el uso de terminales* • *(DSS05) Número de incidentes que implican terminales* • *(DSS05) Número de dispositivos no autorizados detectados en la red o en el entorno del usuario final* • *(DSS05) Número de incidentes relacionados con el acceso no autorizado a la información*				

1606 "Hacktivismo"

Título del escenario de riesgo	"Hacktivismo"
Categoría del escenario de riesgo	16 Ataques lógicos
Referencia del escenario de riesgo	1606

Escenario de riesgo
El hacktivismo (la combinación de intrusión con fines activistas) consiste en insertar o modificar el código para promover una ideología política, promoviendo formas de expresión política, libertad de expresión, derechos humanos, etc. Un grupo de activistas se introduce en el sitio web de un gobierno y cambia la información en una página web para dar publicidad a los mensajes políticos del grupo y causar desconcierto público al gobierno.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un acto malicioso de un grupo activista que explota vulnerabilidades en la infraestructura de TI del gobierno, y publica información en el sitio web oficial del gobierno que ofrece una opinión que es contraria a la política gubernamental o para promover la ideología del grupo.

Agente
El agente que genera la amenaza que explota una vulnerabilidad es una persona **externa**, los activistas.

Evento
El evento es una **interrupción** pues la infraestructura del gobierno es atacada y la información del sitio web es **modificada**.

Activo/Recurso (causa)
El activo/recurso que conduce al impacto en el negocio son las **personas**, los activistas políticos.

Activo/Recurso (efecto)
Los activos/recursos afectados son la **infraestructura de TI** del gobierno que es atacada, y la **información** cambiada en el sitio web.

Tiempo
La duración del evento es probable que sea **moderada** pues los cambios en los sitios web se identifican poco después de producirse el evento y se pueden corregir cargando la copia de seguridad del sitio web. El momento de la ocurrencia es **crítico** porque los visitantes al sitio web del gobierno generalmente necesitan de inmediato la información proporcionada. El tiempo tomado para detectar el cambio es también **moderado** porque tales cambios en los sitios web suelen ser reportados rápidamente por los visitantes del sitio web. El tiempo transcurrido entre el evento y la consecuencia es **inmediato** porque el sitio web se cambia al mismo tiempo que ocurre la intrusión.

Tipo de riesgo

Activación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Interrupciones del servicio de TI.
	P	Problemas de seguridad.
	S	Cuestiones de cumplimiento.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** El consejo toma la decisión de que nadie estaría interesado en atacar a la empresa, "no nos sucederá a nosotros".
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Instalar y configurar apropiadamente los cortafuegos (firewalls), bastionar el servidor y asegurarse que los parches de seguridad se instalen oportunamente. Desplegar y supervisar activamente un sistema de detección de intrusión (IDS).

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de seguridad de la información	Describir las adaptaciones de seguridad de la información dentro de la empresa.	Alto	Alto	SÍ
Políticas y procedimientos técnicos de seguridad	Detallar las consecuencias técnicas de la política de seguridad de la información.	Alto	Alto	SÍ
Principios de arquitectura	Los requerimientos de seguridad de la información están integrados a la arquitectura empresarial y se traducen a una arquitectura formal de seguridad de la información.	Alto	Alto	SÍ
Política de continuidad del negocio y de recuperación ante desastres	Validar la recuperación de información, servicios, aplicaciones e infraestructura.	Bajo	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
DSS01.03	Supervisar la infraestructura de TI.	Supervisar la infraestructura de TI y los eventos relacionados. Almacenar suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias temporales de las operaciones y de las otras actividades que engloban o apoyan a las operaciones.	Bajo	Alto	SÍ
DSS04.03	Desarrollar e implementar una respuesta de continuidad del negocio.	Desarrollar un plan de continuidad del negocio (BCP) basado en la estrategia que documenta los procedimientos y elementos de información que permiten a la empresa continuar sus actividades críticas después de un incidente.	Bajo	Alto	SÍ
DSS05.02	Gestionar la seguridad de la red y las conexiones.	Usar medidas de seguridad y procedimientos de gestión relacionados para proteger la información a través de todos los métodos de conectividad.	Medio	Bajo	NO
DSS05.07	Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Usar herramientas de detección de intrusos, supervisar la infraestructura para detectar accesos no autorizados y asegurarse que los eventos se integren en el supervisión general de eventos y en los procedimientos de gestión de incidentes.	Bajo	Bajo	NO
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gestor de seguridad de la información	Implementar las medidas de seguridad.		Alto	Alto	SÍ
Jefe de operaciones de TI	Liderar al equipo de respuesta para restaurar el servicio de manera oportuna.		Bajo	Alto	SÍ
Gestor de servicio	En caso de que los ataques tengan éxito, comunicarse con el usuario final y ayudar a gestionar la respuesta.		Bajo	Alto	SÍ
Director de Arquitectura de Seguridad	Diseñar medidas de seguridad.		Alto	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La seguridad de la información se practica en las operaciones diarias	Evitar ataques lógicos.		Alto	Bajo	SÍ
Las personas respetan la importancia de las políticas y los principios de seguridad de la información	Prevenir ataques lógicos.		Alto	Bajo	SÍ
Las partes interesadas son conscientes de cómo identificar y responder ante las amenazas a la empresa	Minimizar el impacto de ataques lógicos.		Medio	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Acuerdos de nivel de servicio (SLA)	Detallar la acción a emprender en caso de ataque.		Bajo	Alto	SÍ
Informes sobre amenazas a la información	Inteligencia en cuanto a los tipos de ataques.		Alto	Medio	SÍ
Informes de supervisión	Identificar los intentos de ataque, amenazas, etc.		Bajo	Alto	SÍ

Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Cortafuegos (firewall)	Prevenir los logros de los ataques lógicos.	Alto	Bajo	SÍ
Gestión de eventos de seguridad de la información (SIEM)	Proporciona análisis en tiempo real de las alertas de seguridad generadas por el hardware de red y las aplicaciones.	Alto	Alto	SÍ
Herramientas de gestión de red/escáneres de vulnerabilidad	Identificar las debilidades.	Alto	Bajo	SÍ
Servicios de supervisión y alerta	Notificación oportuna de amenazas potenciales.	Bajo	Alto	SÍ
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de seguridad de la información	Prevenir y reducir el impacto de los ataques lógicos.	Alto	Alto	SÍ
Habilidades técnicas en TI	Configurar la infraestructura de TI, como cortafuegos (firewalls), componentes críticos de la red, etc.	Alto	Medio	SÍ
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• (04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales activados por TI cubiertos por la evaluación de riesgos *• (04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* *• (04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* *• (04) Frecuencia de actualización del perfil de riesgo* *• (10) Número de incidentes de seguridad que causan pérdidas financieras, interrupción del negocio o pérdida de reputación* *• (10) Número de servicios de TI con requisitos de seguridad pendientes* *• (10) Frecuencia de la evaluación de seguridad con respecto a los estándares y pautas más recientes*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• (DSS01) Porcentaje eventos operativos críticos cubiertos por sistemas de detección automática *• (DSS04) Porcentaje de servicios de TI que satisfacen los requisitos en tiempo de actividad* *• (DSS04) Porcentaje de restauración satisfactoria y oportuna de copias de respaldo o copias de medios alternativas* *• (DSS04) Número de sistemas empresariales críticos no cubiertos por el plan de continuidad del negocio* *• (DSS04) Número de ejercicios y pruebas que han alcanzado los objetivos de recuperación* *• (DSS04) Frecuencia de las pruebas de recuperación* *• (DSS05) Número de vulnerabilidades descubiertas* *• (DSS05) Número de infracciones del cortafuegos (firewall)* *• (DSS05) Porcentaje de pruebas periódicas de dispositivos de de seguridad medioambiental* *• (DSS05) Número de incidentes relacionados con el acceso no autorizado a la información*				

Página intencionalmente en blanco

17 Acción industrial

1701 Personal en huelga

Título del escenario de riesgo	Personal en huelga
Categoría del escenario de riesgo	17 Acción industrial
Referencia del escenario de riesgo	1701

Escenario de riesgo
Todos los miembros del departamento de TI de un hospital de una gran ciudad están en una huelga sindical, y los proyectos y las iniciativas de desarrollo no están avanzando.

Los usuarios empresariales también están en huelga, así que el impacto en la prestación de servicios es significativo; todos los sistemas se han detenido.

Componentes del escenario de riesgo

Tipo de amenaza
Debido a que la huelga de los miembros del departamento de TI fue provocada por el sindicato, la naturaleza del evento se basa en un **requisito externo.**

Agente
Los agentes que generan la amenaza que explota una vulnerabilidad son **internos** (personal de TI que está en huelga) y **externos** (sindicato que provocó la huelga).

Evento
El evento es una **interrupción** de los servicios de TI generales.

Activo/Recurso (causa)
El activo/recurso que conduce al impacto en el negocio son las personas **externas** del departamento de TI que están en huelga.

Activo/Recurso (efecto)
Los recursos afectados son **procesos** de negocio que no se están realizando. Los **procesos** de TI, como el desarrollo, también se ven afectados por el paro del departamento de TI. Debido a que los desarrolladores de TI no están trabajando, las **aplicaciones** no se están actualizando ni operando.

Tiempo
Debido a que parece que la huelga no terminará pronto, y a que hay un retraso en el desarrollo de nuevas aplicaciones, la duración del evento se considera como **extensa**. Ya que los programas y los proyectos para las nuevas urgencias de aplicaciones necesarias están detenidos y seran retrasados, el momento de la ocurrencia es **crítico**. La detección es claramente **inmediata** porque el trabajo se detuvo al mismo tiempo que se inició la huelga. Por la misma razón, el intervalo de tiempo entre el evento y la consecuencia es **inmediato**.

Tipo de riesgo

Activación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**P**	No hay avance en los proyectos.
Entrega del servicio y operaciones de TI	**P**	No se proporcionan servicios a los usuarios internos.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** Aceptación del riesgo por parte del consejo.
- **Compartir/transferir el riesgo:** Subcontratación de la prestación de servicios.
- **Mitigación del riesgo:** Negociar con los miembros del personal y/o con el sindicato para mantener los servicios esenciales (p. ej., en un hospital o en una EPU).

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de Recursos Humanos (RR.HH.)	Definir los derechos y las obligaciones de todo el personal, detallando el comportamiento aceptable e inaceptable de los empleados, y al hacerlo, gestionar el riesgo que está vinculado al comportamiento humano.	Alto	Medio	SÍ
Política de gestión de proveedores	Definir las opciones de servicio de respaldo o de emergencia.	Bajo	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO01.01	Definir la estructura orgánica.	Establecer una estructura organizacional interna y extendida que refleje las necesidades del negocio y las prioridades de TI. Establecer las estructuras de gestión requeridas (p. ej., comités) que permitan que la toma de decisiones de gestión se lleve a cabo de la manera más eficaz y eficiente.	Bajo	Alto	SÍ
APO07.02	Identificar al personal clave de TI.	Identificar al personal clave de TI mientras se minimiza la dependencia en una sola persona que realice una función de trabajo crítica al capturar los conocimientos (documentación), compartir los conocimientos, planificar la sucesión y tener un respaldo de personal.	Bajo	Alto	SÍ
BAI01.10	Gestionar el programa y el riesgo del proyecto.	Eliminar o minimizar el riesgo específico asociado con los programas y proyectos mediante un proceso sistemático de planificación, identificación, análisis, respuesta y supervisión, y controlando las áreas o eventos que tienen el potencial de ocasionar un cambio no deseado. Establecer y registrar centralmente el riesgo al que se enfrenta el programa y el proyecto.	Bajo	Medio	NO
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director de RR.HH.	Responsable de establecer las expectativas de y para el personal.		Alto	Medio	SÍ
Grupo legal	Apoyar la contratación inicial y litigar en caso de incumplimiento del contrato.		Medio	Medio	NO
Consejo de Dirección	Responsable del buen funcionamiento de la empresa y la estructura organizacional de alto nivel para la comunicación de las partes interesadas.		Alto	Alto	SÍ
Ejecutivo de negocios	Facilita la comunicación bidireccional.		Medio	Medio	NO
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La cultura basada en la transparencia y la participación es un punto de enfoque importante	Prevenir la acción industrial.		Alto	Bajo	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Acuerdos contractuales con el personal	Definición clara de responsabilidades, derechos y obligaciones para todo el personal.		Alto	Medio	SÍ
Contratos con proveedores	Definición clara de responsabilidades, derechos y obligaciones para acuerdos específicos con proveedores.		Medio	Medio	NO
Repositorios de conocimientos	Minimizar el efecto de la indisponibilidad parcial de recursos al compartir conocimientos sobre procesos, tecnología, etc.		Bajo	Alto	SÍ
Análisis del déficit en recursos	Análisis claro del nivel crítico de recursos.		Medio	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Servicios de copia de seguridad de terceros	Apoyo temporal en caso de una acción industrial.		Bajo	Alto	SÍ

Habilitador de personal, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de RR.HH.	Gestión de habilidades y competencias.	Medio	Medio	NO
Habilidades de negociación	Facilitar la máxima comunicación bidireccional y asegurarse que se cumplan los requerimientos operativos mínimos.	Medio	Medio	NO
Habilidades de litigio	Una vez iniciada el litigio se requieren las habilidades adecuadas para defender los intereses de la empresa.	Bajo	Alto	SÍ
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(13) Número de programas/proyectos a tiempo y dentro del presupuesto* • *(16) Porcentaje de personal cuyas habilidades relacionadas con TI son suficientes para la competencia requerida para su función* • *(16) Porcentaje de personal satisfecho con sus funciones relacionadas con TI* • *(16) Número de horas de aprendizaje/capacitación por cada miembro del personal*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(APO07) Porcentaje de rotación de personal* • *(APO07) Duración promedio de las vacantes* • *(APO07) Porcentaje de puestos de TI vacantes* • *(BAI01) Número de problemas de recursos (p. ej., habilidades, capacidad)*				

1703 Incapacidad de terceros de proporcionar servicios

Título del escenario de riesgo	Incapacidad de terceros de proporcionar servicios
Categoría del escenario de riesgo	17 Acción industrial
Referencia del escenario de riesgo	1703

Escenario de riesgo
Una empresa de fabricación de productos químicos ha subcontratado servicios de TI a un proveedor de servicios externo. Debido a que el personal del proveedor externo está en huelga, éste no puede proporcionar sus servicios al fabricante y se niega a permitir el acceso a los datos. Estos datos son necesarios urgentemente para terminar un proyecto de investigación de un nuevo producto farmacéutico. Debido a que ya se sabe en el mercado que el competidor directo está avanzando con un proyecto similar, es fundamental terminar el proyecto antes que el competidor. Debido a que no hay una resolución entre el proveedor externo y su personal, la huelga puede prolongarse durante un largo período de tiempo.

Componentes del escenario de riesgo

Tipo de amenaza
Debido a que la huelga es causada por el personal de terceros, la naturaleza del evento es un **requerimiento externo.**

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **externo**, el personal del proveedor externo.

Evento
El evento es una **interrupción** de los servicios de TI del proveedor externo.

Activo/Recurso (causa)
El activo/recurso que conduce al impacto en el negocio es la **estructura organizacional** porque las **personas** del proveedor externo están en huelga.

Activo/Recurso (efecto)
Los recursos afectados son **procesos** de negocio que no se están realizando, **procesos** de TI que están detenidos, **información** que no es accesible y **aplicaciones** que no están disponibles.

Tiempo
Debido a que parece que la huelga no terminará pronto, la duración del evento es **extensa**. Debido a que los datos son necesarios urgentemente para la investigación, el momento de la ocurrencia es **crítico**. La detección es claramente **inmediata** porque los servicios proporcionados se detuvieron al mismo tiempo que la huelga comenzó. Por la misma razón, el intervalo de tiempo entre el evento y la consecuencia es inmediato.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**P**	Los servicios empresariales son interrumpidos.
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	No se proporcionan servicios de TI a los usuarios.
	P	Los datos no están disponibles.

Posibles respuestas al riesgo

- **Evasión del riesgo:** No subcontratar los servicios.
- **Aceptación del riesgo:** Aceptación del riesgo por parte del consejo.
- **Compartir/transferir el riesgo:** Acuerdos de fideicomiso.
- **Mitigación del riesgo:** Las copias de respaldo de datos y sistemas se mantienen por terceros de forma independiente.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de Recursos Humanos (RR.HH.)	Definir los derechos y las obligaciones de todo el personal, detallando el comportamiento aceptable e inaceptable de los empleados, y al hacerlo, gestionar el riesgo que está vinculado al comportamiento humano.	Alto	Medio	SÍ
Política de gestión de proveedores	Definir las opciones de servicio de respaldo o de emergencia.	Bajo	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO02.02	Evaluar el entorno, las capacidades y el desempeño actuales.	Evaluar el rendimiento de las capacidades internas actuales del negocio y de TI, así como los servicios de TI externos, y desarrollar una comprensión de la arquitectura empresarial en relación con TI. Identificar los problemas que se están experimentando actualmente y desarrollar recomendaciones en áreas que podrían beneficiarse con una mejora. Considerar diferentes opciones de proveedores de servicios, el impacto financiero y los costos y beneficios potenciales de usar servicios externos.	Medio	Medio	NO
APO10.01	Identificar y evaluar los contratos y relaciones con los proveedores.	Identificar proveedores y contratos asociados, y clasificarlos en tipo, importancia y criticidad. Establecer criterios de evaluación para el proveedor y el contrato, y evaluar la cartera general de proveedores y contratos actuales y alternativos.	Bajo	Alto	SÍ
APO10.02	Seleccionar proveedores.	Seleccionar proveedores de acuerdo a una práctica justa y formal para garantizar un ajuste viable basado en los requerimientos especificados. Los requerimientos deben optimizarse con la participación de los proveedores potenciales y las partes interesadas de la empresa.	Medio	Alto	SÍ
APO10.03	Gestionar los contratos y las relaciones con los proveedores.	Formalizar y gestionar las relaciones para cada proveedor estratégico. Gestionar, mantener y supervisar los contratos y la prestación de servicios. Asegurarse de que los contratos nuevos o modificados cumplan con los estándares de la empresa y con los requerimientos legales y regulatorios.	Bajo	Alto	SÍ
APO10.04	Gestionar el riesgo con los proveedores.	Identificar y gestionar el riesgo con los proveedores, incluyendo la capacidad de proporcionar continuamente una prestación de servicios segura, eficiente y eficaz.	Bajo	Alto	SÍ

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Grupo legal	Apoyar la contratación inicial y litigar en caso de incumplimiento del contrato	Alto	Alto	SÍ
Consejo de Dirección	Responsable del buen funcionamiento de la empresa y la estructura organizacional de alto nivel para la comunicación de las partes interesadas.	Medio	Medio	NO
Ejecutivo de negocios	Facilita la comunicación bidireccional.	Medio	Medio	NO

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			

Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Contratos con proveedores	Definición clara de responsabilidades, derechos y obligaciones para acuerdos específicos con proveedores.	Alto	Alto	SÍ
Repositorios de conocimientos	Minimizar el efecto de la indisponibilidad parcial de recursos al compartir conocimientos sobre procesos, tecnología, etc.	Bajo	Medio	NO
Análisis del déficit en recursos	Análisis claro del nivel crítico de recursos.	Bajo	Alto	SÍ

Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Servicios de copia de seguridad de terceros	Apoyo exporádioco en caso de una acción industrial.	Bajo	Alto	SÍ
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de negociación	Facilitar la máxima comunicación bilateral y asegurarse que se cumplan los requerimientos operativos mínimos.	Alto	Alto	SÍ
Habilidades de litigio	Una vez que se ha iniciado el litigio, se requieren las habilidades adecuadas para defender los intereses de la empresa.	Bajo	Alto	SÍ
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI* • *(07) Porcentaje de partes interesadas del negocio satisfechas que la prestación de servicios de TI cumple con los niveles de servicio acordados* • *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(APO10) Porcentaje de proveedores que cumplen con los requisitos acordados* • *(APO10) Número de incumplimientos de servicio en los servicios relacionados con TI causados por proveedores* • *(APO10) Número de eventos relacionados con el riesgo que conducen a incidentes de servicio* • *(APO10) Frecuencia de las sesiones de gestión de riesgos con el proveedor* • *(APO10) Porcentaje de incidentes relacionados con el riesgo resueltos de manera aceptable (tiempo y costo)* • *(APO10) Número de reuniones de revisión de proveedores* • *(APO10) Número de disputas formales con proveedores* • *(APO10) Porcentaje de disputas resueltas amistosamente en un plazo razonable*				

1704 Banco afectado por una huelga

Título del escenario de riesgo	Banco afectado por una huelga
Categoría del escenario de riesgo	17 Acción industrial
Referencia del escenario de riesgo	1704

Escenario de riesgo
El banco de una empresa ha estado en huelga durante más de una semana, y algunas de las operaciones críticas de la empresa están siendo afectadas.

Los clientes y los proveedores de la empresa no pueden cobrar cheques utilizando los cajeros automáticos (ATM) ni realizar otras operaciones. A pesar de que el banco tiene canales electrónicos, la huelga también está afectando los servicios relacionados que requieren procedimientos manuales en el fondo. Como resultado de la huelga, las finanzas de la empresa están siendo afectadas y no está fluyendo dinero en efectivo.

No parece que la huelga se resolverá pronto. La empresa necesita alinear los procedimientos estándar y automatizados (p. ej., asignación de crédito, período de pago, límites de los clientes), y por lo tanto, se necesitan varios cambios en los sistemas e información con poca antelación. Aunque hay un acuerdo de nivel de servicio (SLA) con un equipo de respuesta en emergencias que no está involucrado en la huelga, el banco no tiene la capacidad de aplicar esos cambios en el período de tiempo necesario.

Componentes del escenario de riesgo

Tipo de amenaza
Debido a que el banco se ve afectado por la huelga, en lugar de la empresa, la naturaleza del evento se puede clasificar como un **requerimiento externo.**

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **externo**, el banco, o específicamente, su personal.

Evento
El evento es una **interrupción** de los servicios bancarios externos.

Activo/Recurso (causa)
El recurso/activo que conduce al impacto en el negocio es la **estructura organizacional** porque es el banco externo quien no puede proporcionar los servicios.

Activo/Recurso (efecto)
Los recursos/activos afectados son los **procesos** de clientes y financieros que se necesitan modificar. Además, la **información** de **aplicaciones**, como la asignación de crédito y los plazos de pago, se ven afectados y se necesitan cambiar.

Tiempo
Porque parece que la huelga no terminará pronto, la duración del evento se puede clasificar como **extensa**. Debido a que se deben hacer pagos, y se necesita información urgentemente, como asignaciones de crédito, el momento de la ocurrencia es **crítico**. La detección es claramente **inmediata** porque los servicios proporcionados por el banco se detuvieron en el mismo momento en que se inició la huelga. Por la misma razón, el intervalo de tiempo entre el evento y la consecuencia es **inmediato**.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Interrupciones en los servicios de TI debido a los cambios de emergencia.
	S	Operaciones de servicios de TI debido a que los proveedores de servicios se niegan a prestar el servicio.
	S	Cambios en la información a medida que se relajan los controles (p. ej., al personal que se le permite cambiar la asignación de crédito también puede cambiar otra información).

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** Aceptación del riesgo por parte del consejo.
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Definir los procedimientos de emergencia y alternativos con poca antelación.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de Recursos Humanos (RR.HH.)	Definir los derechos y las obligaciones de todo el personal, detallando el comportamiento aceptable e inaceptable de los empleados, y al hacerlo, gestionar el riesgo que está vinculado al comportamiento humano.	Alto	Medio	SÍ
Política de gestión de proveedores	Definir las opciones de servicio de respaldo o de emergencia.	Bajo	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO10.04	Gestionar el riesgo con los proveedores.	Identificar y gestionar el riesgo con los proveedores, incluyendo la capacidad de proporcionar continuamente una prestación de servicios segura, eficiente y eficaz.	Bajo	Alto	SÍ
DSS04.03	Desarrollar e implementar una respuesta de continuidad del negocio.	Desarrollar un plan de continuidad del negocio (BCP) basado en la estrategia que documenta los procedimientos y elementos de información que permiten a la empresa continuar sus actividades críticas después de un incidente.	Bajo	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director de RR.HH.	Responsable de establecer las expectativas de y hacia el personal.		Alto	Medio	SÍ
Grupo legal	Apoyar la contratación inicial y litigar en caso de incumplimiento del contrato.		Medio	Medio	NO
Consejo de Dirección	Responsable del buen funcionamiento de la empresa y la estructura orgánica de alto nivel para la comunicación de las partes interesadas.		Alto	Alto	SÍ
Ejecutivo de negocios	Facilita la comunicación bilateral.		Medio	Medio	NO
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
La cultura transparente y participativa es un punto de enfoque importante	Evitar que se produzcan acciones industriales.		Alto	Medio	SÍ
Habilitador de información					
Acuerdos contractuales con el personal	Definición clara de responsabilidades, derechos y obligaciones para todo el personal.		Alto	Medio	SÍ
Contratos con proveedores	Definición clara de responsabilidades, derechos y obligaciones para arreglos específicos con proveedores.		Medio	Medio	NO
Repositorios de conocimientos	Minimizar el efecto de la indisponibilidad parcial de recursos al compartir conocimientos sobre procesos, tecnología, etc.		Bajo	Alto	SÍ
Análisis déficit de recursos	Apoyo temporal en caso de una acción industrial.		Bajo	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Servicios de copia de seguridad de terceros	Apoyo temporal en caso de una acción industrial.		Bajo	Alto	SÍ
Habilitador de personas, habilidades y competencias					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Habilidades de RR.HH.	Gestión de habilidades y competencias.		Alto	Medio	SÍ
Habilidades de negociación	Facilitar la máxima comunicación bilateral y asegurarse que se cumplan los requerimientos operativos mínimos.		Medio	Medio	SÍ
Habilidades de litigio	Una vez que se ha iniciado el litigio, se requieren las habilidades adecuadas para defender los intereses de la empresa.		Bajo	Alto	SÍ

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos*
• *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos*
• *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI*
• *(04) Frecuencia de actualización del perfil de riesgo*
• *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI*
• *(09) Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de TI a los nuevos requerimientos*
• *(09) Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas*
• *(09) Tiempo promedio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada*
• *(14) Número de incidentes de procesos de negocio causados por la falta de disponibilidad de información*
• *(14) Relación y extensión de las decisiones erróneas de negocio en las que la información errónea o no disponible fue un factor clave*
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso
• *(APO10) Porcentaje de proveedores que cumplen con los requisitos acordados*
• *(APO10) Número de incumplimientos de servicio en los servicios relacionados con TI causados por los proveedores*
• *(APO10) Número de eventos relacionados con el riesgo que conducen a incidentes de servicio*
• *(APO10) Frecuencia de las sesiones de gestión de riesgos con el proveedor*
• *(APO10) Porcentaje de incidentes relacionados con el riesgo resueltos de manera aceptable (en tiempo y costo)*
• *(APO10) Número de reuniones de revisión con los proveedores*
• *(APO10) Número de disputas formales con proveedores*
• *(APO10) Porcentaje de disputas resueltas amistosamente en un plazo razonable*
• *(DSS04) Porcentaje de servicios de TI que satisfacen los requisitos de tiempo de actividad*
• *(DSS04) Número de sistemas empresariales críticos no cubiertos por el plan de continuidad del negocio*
• *(DSS04) Frecuencia de las pruebas de continuidad*
• *(DSS04) Porcentaje de mejoras acordadas en el plan de continuidad del negocio que se han incorporado*
• *(DSS04) Porcentaje de problemas identificados que se han abordado posteriormente en el plan de continuidad del negocio*
• *(DSS04) Porcentaje de partes interesadas internas y externas que han recibido capacitación en continuidad*
• *(DSS04) Porcentaje de problemas identificados que se han abordado posteriormente en los materiales de capacitación sobre continuidad*

Página intencionalmente en blanco

18 Medio ambiente

1801 Contención de combustible del generador de emergencia

Título del escenario de riesgo	Contención de combustible del generador de emergencia
Categoría del escenario de riesgo	18 Medio ambiente
Referencia del escenario de riesgo	1801

Escenario de riesgo
El centro de datos principal de una gran empresa tiene un generador de emergencia que incluye un tanque de suministro de combustible con capacidad para tres días de uso, si es necesario. El tanque de combustible está muy oxidado, no tiene un depósito de contención de fugas y no está sellado físicamente. El suministro de energía local falla a la 1:45 p.m. un viernes por la tarde, durante la temporada de clima cálido. El generador se inició y solo funcionó durante 15 minutos. El oficial de seguridad física del local encontró que tenían una emergencia medio ambiental que había sido declarada en un evento. El oficial de seguridad notificó a la policía y a los funcionarios de seguridad locales. Se descubrió que el 95% del combustible del generador se había derramado al río de la localidad, lo que nadie había notado. Luego de evaluar el último ejercicio en vivo del plan de continuidad del negocio/plan de recuperación de desastres (BCP/DRP), programado para cinco minutos y con un resultado exitoso, no se había detectado nada. Esto se llevó a cabo durante el trimestre anterior; no hubo ninguna revisión previa del área física a las proximidades del generador de emergencia en los últimos seis meses. Además, no se hace ninguna mención del área del generador de emergencia en el plan BCP/DRP. Las investigaciones adicionales revelaron que las cámaras de seguridad habían sido desactivadas en un momento desconocido, y el departamento de seguridad estaba usando un sistema de cámara analógico, que también había sido saboteado con un bucle haciendo que se muestre el generador de emergencia en la época de invierno. Debido al sabotaje del tanque de combustible y de los sistemas de cámaras, el oficial de seguridad debió alertar a las agencias de investigación federales, estatales y locales.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento fue **maliciosa** y de mala fé pero también un **fallo** del proceso de gestión DSS01 *Gestionar las operaciones*, específicamente, la gestión práctica de la *Gestión del medio ambiente.*

Agente
Los agentes que generan la amenaza que explota una vulnerabilidad son **internos** (Director de Seguridad, quien es responsable de dar cuentas de la gestión del entorno) y también **externos** (saboteador).

Evento
El evento es la **destrucción** (por contaminación del medio ambiente, el río).

Activo/Recurso (causa)
El principal activo/recurso que conduce al impacto es la **infraestructura física**, específicamente, el tanque de combustible oxidado y con fugas, y no tener una instalación de contención de combustible para atrapar cualquier posible vertido.

Activo/Recurso (efecto)
Los activos/recursos afectados es la **infraestructura física** que fue saboteada y el medio ambiente.

Tiempo
La duración del evento es **extensa** porque la contaminación no se puede corregir oportunamente. El momento de la ocurrencia es **crítico** porque la falla de energía ocurrió cuando el tanque de combustible había sido saboteado. La detección es **inmediata** porque el generador deja de funcionar tan pronto como el tanque de combustible está vacío. El tiempo transcurrido entre el evento y la consecuencia es **inmediato** Porque el combustible se agota y el río fue contaminado inmediatamente.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y las operaciones de TI	**P**	Problemas de seguridad física.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** La empresa actualiza los planes BCP/DRP. El departamento de seguridad cambia los sistemas de cámaras de seguridad a un formato digital. Necesitan verificar que las cámaras de respaldo funcionan correctamente, asegurándose que en la política se incluya el estado de la revisión diaria del área del generador, y asegurarse de la disposición y funcionamiento de las alarmas de actividad/movimiento en el área para recibir alertas de seguridad. La empresa protege el área del generador de emergencia con una cerca física y realizará las obras de construcción de un contenedor para las posibles fugas de combustible con capacidad suficiente. La empresa tendrá que pagar penalizaciones y multas por los vertidos de combustible, por no disponer de políticas y procedimientos apropiados en los planes BCP/DRP, y por no cumplir con las regulaciones de salud y seguridad federales, estatales y locales. Para la seguridad ambiental y de salud, los departamentos de salud federales y estatales y los OSHA (Administración de Seguridad y Salud Ocupacional de los Estados Unidos) requieren que todos los tanques de combustible sean mantenidos, sellados, supervisados y que tengan una capacidad de contención mayor que la capacidad del tanque.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de responsabilidad social y medio ambiental	La concienciación ambiental debe ser parte de la política general de la empresa en responsabilidad corporativa.	Medio	Medio	NO
Reglas de conducta (uso aceptable)	Los usuarios deben ser conscientes de su impacto individual en el medio ambiente.	Medio	Medio	NO

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
DSS01.04	Gestión del medio ambiente.	Mantener medidas de protección contra los factores medio ambientales. Instalar equipo y dispositivos especializados para supervisar y controlar el medio ambiente.	Bajo	Alto	SÍ
DSS01.05	Gestionar las instalaciones.	Gestionar las instalaciones, incluyendo el equipo de suministro eléctrico y comunicaciones, en línea con las leyes y regulaciones, los requerimientos técnicos y del negocio, las especificaciones del proveedor, y las pautas de salud y seguridad.	Alto	Bajo	SÍ
DSS04.04	Ejercer, probar y revisar el BCP.	Comprobar las adaptaciones a la continuidad de forma periódica para ejecutar los planes de recuperación frente resultados predeterminados, con el fin de permitir que se desarrollen soluciones innovadoras, y para ayudar a verificar en el transcurso del tiempo que el plan funcionará tal como se prevee.	Medio	Alto	SÍ
DSS05.05	Gestionar el acceso físico a los activos de TI.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a las instalaciones, edificios y áreas debe estar justificadas, autorizadas, registradas y supervisadas. Esto debe aplicarse a todas las personas que entren en a las instalaciones, incluyendo personal, personal temporal, clientes, proveedores, visitantes y cualquier otro tercero.	Alto	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Jefe de operaciones de TI	Responsable de gestionar el entorno y las instalaciones de TI.		Alto	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Se desarrolla y apoya una estructura claramente definida para la responsabilidad ética y una cultura específica que promueva la rendición de cuentas	Las personas están involucradas y son conscientes de las consecuencias de las cuestiones medioambientales, y están facultadas para manejarlas de acuerdo con las pautas éticas.		Alto	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Estrategia de TI	La conciencia medioambiental debe ser parte de la estrategia de TI.		Medio	Medio	NO
Registro del activo	Evaluar el impacto medioambiental de la tecnología utilizada.		Alto	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A				
Habilitador de personas, habilidades y competencias					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Desarrollo de sistemas	Agilizar y optimizar la tecnología.		Bajo	Bajo	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos*
• *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos*
• *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI*
• *(04) Frecuencia de actualización del perfil de riesgo*
• *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI*
• *(11) Frecuencia de las evaluaciones de madurez de capacidad y optimización de costos*
• *(11) Tendencia de resultados de la evaluación de capacidad*
• *(11) Niveles de satisfacción de la dirección de negocio y de TI con los costes y capacidades relacionadas con TI*
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso
• *(DSS01) Número de incidentes causados por problemas operativos*
• *(DSS01) Proporción de eventos en comparación con el número de incidentes*
• *(DSS01) Porcentaje de tipos de eventos operativos críticos cubiertos por sistemas de detección automática*
• *(DSS05) Número de vulnerabilidades descubiertas*
• *(DSS05) Porcentaje de pruebas periódicas de dispositivos de seguridad ambiental*
• *(DSS05) Calificación promedio de las evaluaciones de seguridad física*
• *(DSS05) Número de incidentes relacionados con la seguridad física*

Página intencionalmente en blanco

19 Actos de la naturaleza

1903 Diseño del centro de datos

Título del escenario de riesgo	Diseño del centro de datos
Categoría del escenario de riesgo	19 Actos de la naturaleza
Referencia del escenario de riesgo	1903

Escenario de riesgo
Una empresa tiene su centro de datos principal ubicado en la planta superior de un edificio de 16 pisos, sin un recinto para su infraestructura crítica. Esta situación se detectó en los últimos dos reportes de auditoría anuales por parte de los auditores externos. Debido a las restricciones presupuestarias existentes y a los considerables costes de construir recintos especiales o una mejora del diseño del techo, el consejo de dirección, basándose en la probabilidad, descartó estas recomendaciones, creyendo que los auditores habían puesto un nivel de riesgo innecesario en esta observación.

Debido al cambio climático, durante una lluvia severa y una tormenta de granizo, la integridad del techo existente se vio comprometida, lo que resultó en escapes de agua sobre los servidores críticos. Debido a que las bolas de granizo fueron tan grandes, las principales líneas de comunicación con el centro de datos de respaldo también fueron destruidas.

Esta situación interrumpió el servicio y resultó en el incumplimiento de acuerdos de nivel de servicio (SLA) con clientes críticos y antiguos, quienes rescindieron sus contratos inmediatamente. Esta situación fue una pérdida significativa de ingresos para la empresa que ofrecía el servicio.

Componentes del escenario de riesgo

Tipo de amenaza
El principal tipo de amenaza es un evento **natural**.

Agente
No todo tipo de amenaza requiere un agente, p. ej., fallos o causas naturales. Este evento tiene una causa natural y no hay un agente.

Evento
El evento es una **interrupción** de los servicios causados por la **destrucción** del techo que resultó en un escape de agua y la **destrucción** de las líneas de comunicación principales al centro de datos de respaldo.

Activo/Recurso (causa)
El activo/recurso que conduce al impacto del negocio son las **instalaciones** (el techo del centro de datos y el recinto faltante de la **infraestructura crítica**).

Activo/Recurso (efecto)
Los activos/recursos afectados son diferentes **procesos de negocio** (especialmente los de los clientes) y la **infraestructura** e **instalaciones** que fueron destruidas por la lluvia fuerte y la tormenta de granizo.

Tiempo
En el momento de la lluvia fuerte y la tormenta de granizo, no había un recinto para la infraestructura crítica ni una línea de comunicación de respaldo, y por lo tanto, el momento de la ocurrencia es **crítico**. La duración del evento es **extensa** porque los clientes rescindieron sus contratos y no volverán, y se necesita bastante tiempo para recuperar la reputación perdida para atraer a nuevos clientes. Debido a que el agua vertida en el centro de datos y la interrupción repentina de los servicios, la detección es **inmediata**. Las consecuencias también son **inmediatas** porque la infraestructura ya no se puede usar. Los clientes rescindieron sus contratos inmediatamente, y por lo tanto, los ingresos se perdieron de inmediato.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Interrupción del servicio de TI y problemas de cumplimiento (SLAs incumplidos)

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** Aceptación de que esta situación permanece después de la reparación de las instalaciones y la sustitución de la infraestructura.
- **Compartir/transferir el riesgo:** Seguro contra la pérdida financiera por la infraestructura y las instalaciones
- **Mitigación del riesgo:** El consejo debe tomar en cuenta los reportes de auditoría. Las líneas y los recursos de comunicación deben ser redundantes y es necesario establecer rutas secundarias. Se debe construir un recinto especial y una mejora de las características del techo del centro de datos.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas e infraestructura

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de copias de respaldo	Las copias de respaldo están disponibles.	Bajo	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
BAI04.02	Evaluar el impacto en el negocio.	Identificar servicios importantes para la empresa, asignar servicios y recursos a los procesos de negocio, e identificar dependencias comerciales. Asegurarse de que el impacto de los recursos no disponibles sea totalmente comprendido y aceptado por los propietarios del negocio. Asegurarse de que, para funciones críticas del negocio, se puedan satisfacer los requisitos de disponibilidad de los SLA.	Medio	Alto	SÍ
DSS01.04	Gestionar los factores ambientales.	Mantener medidas de protección contra los factores ambientales. Instalar equipo y dispositivos especializados para monitorizr y controlar los factores ambientales.	Bajo	Alto	SÍ
DSS01.05	Gestionar las instalaciones.	Gestionar las instalaciones, incluyendo el equipo de suministro eléctrico y de comunicaciones, conformea las leyes y regulaciones, los requerimientos técnicos y de negocio, las especificaciones del proveedor, y las pautas de estado y seguridad.	Alto	Alto	SÍ
DSS04.03	Desarrollar e implementar una respuesta de continuidad del negocio.	Desarrollar un plan de continuidad del negocio (PCN) basado en la estrategia que documenta los procedimientos y elementos de información que permiten a la empresa continuar sus actividades críticas después de un incidente.	Alto	Alto	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gerente de continuidad del negocio	Responsable de los planes de PCN.		Bajo	Alto	SÍ
Jefe de operaciones de TI	Responsable de gestionar el entorno y las instalaciones de TI.		Alto	Medio	SÍ
Director de Informática (CIO)	Responsable de desarrollar e implementar una respuesta de continuidad del negocio.		Bajo	Alto	SÍ
Propietarios del proceso de negocio	Responsables de desarrollar e implementar una respuesta de continuidad del negocio.		Bajo	Alto	SÍ
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Las partes interesadas son conscientes de cómo identificar y responder ante amenazas.	Las personas están involucradas y son conscientes de cómo reaccionar cuando ocurre un incidente.		Alto	Alto	SÍ
La dirección del negocio se compromete a una colaboración multifuncional continua para permitir programas de continuidad del negocio eficientes y eficaces.	La empresa está comprometida y contribuye proactivamente a la mitigación del riesgo.		Bajo	Alto	SÍ
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Póliza de seguros	Seguro disponible en caso de desastres naturales.		Bajo	Medio	NO
Informes de evaluación de instalaciones	La empresa es consciente del estado y del riesgo de las instalaciones.		Alto	Bajo	SÍ
Acciones y comunicaciones de respuesta ante incidentes	Las personas son conscientes de cómo reaccionar cuando ocurre un incidente.		Bajo	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones					

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Servicios de monitorización y alerta	Notificación temprana de amenazas potenciales.	Medio	Bajo	NO
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gestión de riesgos de la información	Identificar y formular una respuesta al riesgo de información relacionado con desastres naturales.	Alto	Alto	SÍ
Comprensión técnica	Experiencia técnica sobre desastres naturales específicos y relevantes.	Medio	Medio	NO
Indicadores clave de riesgo (KRIs) relacionados con las metas de TI				
• *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos* • *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos* • *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI* • *(04) Frecuencia de actualización del perfil de riesgo* • *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI* • *(07) Porcentaje de partes interesadas del negocio satisfechas donde la prestación de servicios de TI cumple con los niveles de servicio acordados* • *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI* • *(14) Número de incidentes en procesos de negocio causados por la falta de disponibilidad de información* • *(14) Relación y extensión de las decisiones de negocio erróneas en las que la información errónea o no disponible fue un factor clave*				
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso				
• *(BAI04) Número de incidentes de disponibilidad* • *(BAI04) Número y porcentaje de incidencias de disponibilidad, rendimiento y capacidad sin resolver* • *(DSS01) Número de incidentes causados por problemas operativos* • *(DSS01) Proporción de eventos en comparación con el número de incidentes* • *(DSS01) Porcentaje de tipos de eventos operativos críticos cubiertos por sistemas de detección automática* • *(DSS04) Porcentaje de restauración exitosa y temprana de copias de respaldo o copias de medios alternativos* • *(DSS04) Porcentaje de medios de copia de respaldo transferidos y almacenados de forma segura* • *(DSS04) Número de sistemas de negocio críticos no cubiertos por el plan de continuidad del negocio* • *(DSS04) Número de ejercicios y pruebas que han alcanzado los objetivos de recuperación* • *(DSS04) Frecuencia de las pruebas de recuperación* • *(DSS04) Porcentaje de mejoras acordadas en el plan de continuidad del negocio que se han incorporado* • *(DSS04) Porcentaje de incidencias identificadas que se han abordado posteriormente en el plan de continuidad del negocio* • *(DSS04) Porcentaje de partes interesadas internas y externas que han recibido capacitación en continuidad del negocio* • *(DSS04) Porcentaje de incidencias identificadas que se han abordado posteriormente en los materiales de formación sobre continuidad del negocio*				

1905 Centro de datos en el río

Título del escenario de riesgo	Centro de datos en el río
Categoría del escenario de riesgo	19 Desastres naturales
Referencia del escenario de riesgo	1905

Escenario de riesgo
Una gran empresa de fabricación completó la adquisición de una empresa de fabricación que tiene su centro de datos principal en una planta que se encuentra a lo largo de un gran río. La adquisición se acababa de completar cuando hubo una inundación importante debido a tormentas fuertes. Incluso con los procesos de mitigación de bombas implementados, la planta se inundó rápidamente, incluyendo el centro de datos.

Esto resultó en daños graves al centro de datos. Además, debido a la pérdida de personal crítico, a que no se actualizó la lista de acceso a los archivos de respaldo de la compañía adquirida, y a que no se renovó el contrato con la capacidad de respaldo del fabricante adquirido, no hubo capacidad para recuperar fácilmente las instalaciones de TI dentro del plazo requerido por el negocio. No solo la planta ha sido impactada, sino que la capacidad de gestionar deudores, acreedores y personal se ha perdido hasta que las instalaciones de TI se puedan restaurar.

El plan de recuperación de desastres (PRD) cubre el equipo de fabricación y los sistemas relacionados con su recuperación, pero no cubre las instalaciones de TI.

Componentes del escenario de riesgo

Tipo de amenaza
El principal tipo de amenaza es un evento **natural**. Una naturaleza secundaria del evento es el **fallo** del **proceso** DSS04 *Gestionar la continuidad*, especialmente, no actualizar la lista de acceso de los archivos de respaldo y no renovar el contrato con la capacidad de respaldo del fabricante adquirido.

Agente
No todo tipo de amenaza requiere un agente, p. ej., fallas de equipos o causas naturales. Este evento tiene una causa natural, y debido a ello, no hay un agente. Para la falla del **proceso** DSS04 *Gestionar la continuidad*, el agente es **interno**, la persona responsable de la actualización del plan de continuidad del negocio (BCP) y de las capacidades DRP.

Evento
El evento es la **destrucción** de instalaciones (la planta), y una **interrupción** porque no había capacidad para recuperarse fácilmente en un plazo razonable. Además, se ha perdido la capacidad de gestionar los acreedores y al personal (**interrupción**) hasta que las operaciones se puedan restaurar.

Activo/Recurso (causa)
Los activos/recursos que conducen al impacto en el negocio son las **instalaciones** en la planta destruida, y el **proceso** DSS04 *Gestionar la continuidad*, que fue ejecutado ineficazmente.

Activo/Recurso (efecto)
Los activos/recursos afectados son diferentes **procesos de negocios**, así como las instalaciones que fueron **destruidas**.

Tiempo
Debido a que la tormenta ocurrió cuando la lista de acceso de los archivos de respaldo aún no se había actualizado, y cuando el contrato con la capacidad de respaldo del fabricante adquirido aún no se había renovado, el tiempo de ocurrencia del evento es **crítico**. Debido a que no hay capacidad para recuperarse fácilmente en un intervalo de tiempo razonable, la duración del evento es **extensa**. Ya que la inundación (derretimiento de la nieve y la lluvia fuerte) destruyó repentinamente la planta e interrumpió los servicios al mismo tiempo, la detección es **inmediata**. Las consecuencias también son **inmediatas** porque la planta destruida ya no se puede usar y tiene que ser reemplazada, reconstruida o reparada.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Destrucción de las instalaciones e interrupción del servicio

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** Seguro de las instalaciones.
- **Mitigación del riesgo:** La empresa necesita realizar una revisión inmediata de su PCN para incorporar todos los sistemas críticos y probar el plan siguiendo una revisión del proceso y método de recuperación.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de copias de respaldo	Las copias de respaldo están disponibles.	Bajo	Alto	SÍ
Política de continuidad del negocio y de recuperación de desastres	Validar la recuperabilidad de los datos.	Bajo	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
DSS01.04	Gestionar los factores ambientales.	Mantener medidas de protección contra los factores ambientales. Instalar equipo y dispositivos especializados para monitorizar y controlarlos factores ambientales.	Medio	Alto	SÍ
DSS01.05	Gestionar las instalaciones.	Gestionar las instalaciones, incluyendo el equipo de suministro eléctrico y comunicaciones, de forma alineada con las leyes y regulaciones, los requerimientos técnicos y del negocio, las especificaciones del proveedor, y las pautas de estado y seguridad.	Medio	Alto	SÍ
DSS04.01	Definir la política de continuidad del negocio, los objetivos y el alcance.	Definir la política de continuidad del negocio y el alcance alineado con los objetivos de la empresa y de las partes interesadas.	Medio	Alto	SÍ
DSS04.02	Mantener una estrategia de continuidad.	Evaluar las opciones de gestión de continuidad del negocio, y elegir una estrategia de continuidad viable y rentable para asegurar la recuperación y la continuidad de la empresa ante un desastre u otro incidente o interrupción mayor.	Medio	Alto	SÍ
DSS04.03	Desarrollar e implementar una respuesta de continuidad del negocio.	Desarrollar un plan de continuidad del negocio (PCN) basado en la estrategia de documentar los procedimientos y elementos de información que permiten a la empresa continuar sus actividades críticas después de un incidente.	Medio	Alto	SÍ
DSS04.04	Ejercitar, probar y revisar el PCN.	Probar los planes de continuidad de forma periódica para ejercitar los planes de recuperación ante resultados predeterminados, permitir que se desarrollen soluciones innovadoras, y ayudar a verificar a en el tiempo que el plan funcionará según lo esperado.	Medio	Alto	SÍ
DSS04.05	Revisar, mantener y mejorar el PCN.	Realizar de forma periódica una revisión de gestión de la capacidad de continuidad para asegurar su idoneidad, propiedad y efectividad de manera continua. Gestionar los cambios al plan de acuerdo con el proceso de control de cambios para garantizar que el plan de continuidad se mantenga actualizado y que refleje continuamente los requerimientos del negocio actuales.	Medio	Alto	SÍ
DSS04.06	Realizar capacitación en el PCN.	Proporcionar sesiones de capacitación periódicas a todas las partes internas y externas involucradas sobre los procedimientos y sus funciones y responsabilidades en caso de una interrupción.	Medio	Alto	SÍ
DSS04.07	Gestionar los planes de respaldo.	Mantener la disponibilidad de la información crítica para el negocio.	Medio	Alto	SÍ
DSS04.08	Realizar una evaluación post-reanudación .	Evaluar la idoneidad del PCN tras la reanudación con éxito de los procesos y servicios del negocio después de una interrupción.	Medio	Alto	SÍ

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gerente de continuidad del negocio	Responsable del PCN.	Bajo	Alto	SÍ
Jefe de operaciones de TI	Responsable de gestionar el entorno y las instalaciones de TI.	Alto	Medio	SÍ
Director de Informática (CIO)	Responsable de desarrollar e implementar una respuesta de continuidad del negocio.	Bajo	Alto	SÍ
Propietarios del proceso de negocio	Responsables de desarrollar e implementar una respuesta de continuidad del negocio.	Bajo	Alto	SÍ

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Las partes interesadas son conscientes de cómo identificar y responder ante amenazas	Las personas están involucradas y son conscientes de cómo reaccionar cuando ocurre un incidente.	Bajo	Alto	SÍ
La dirección del negocio se compromete a una colaboración multifuncional continua a fin de fomentar la puesta en marcha de programas de continuidad del negocio eficientes y efectivos.	El negocio está comprometido y contribuye proactivamente a la mitigación del riesgo.	Bajo	Alto	SÍ
Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Póliza de seguros	Seguro disponible en caso de desastres naturales.	Bajo	Alto	SÍ
Informes de evaluación de instalaciones	La empresa es consciente del estado y riesgo de las instalaciones.	Alto	Bajo	SÍ
Acciones y comunicaciones de respuesta ante incidentes	Las personas son conscientes de cómo reaccionar cuando ocurre un incidente.	Bajo	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Servicios de monitorización y alerta	Notificación temprana de amenazas potenciales.	Bajo	Alto	SÍ
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gestión de riesgos de la información	Identificar y formular una respuesta al riesgo de información relacionado con desastres naturales.	Alto	Alto	SÍ
Comprensión técnica	Experiencia técnica sobre desastres naturales específicos y relevantes.	Alto	Alto	SÍ

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos*
- *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos*
- *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI*
- *(04) Frecuencia de actualización del perfil de riesgo*
- *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI*
- *(11) Tendencia de resultados de la evaluación de capacidad*
- *(11) Niveles de satisfacción de la dirección de negocio y de TI con los costes y capacidades relacionadas con TI*
- *(14) Nivel de satisfacción del usuario empresarial con la calidad y puntualidad (o disponibilidad) de la información de gestión*
- *(14) Número de incidentes de procesos de negocio causados por la falta de disponibilidad de información*
- *(14) Relación y extensión de las decisiones de negocio erróneas en las que la información errónea o no disponible fue un factor clave*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(DSS01) Número de incidentes causados por problemas operativos*
- *(DSS01) Proporción de eventos en comparación con el número de incidentes*
- *(DSS01) Porcentaje de tipos de eventos operativos críticos cubiertos por sistemas de detección automática*
- *(DSS04) Porcentaje de servicios de TI que satisfacen los requisitos de tiempo de actividad*
- *(DSS04) Porcentaje de restauración exitosa y temprana de copias de respaldo o copias de medios alternativos*
- *(DSS04) Porcentaje de medios de copia de respaldo transferidos y almacenados de forma segura*
- *(DSS04) Número de sistemas de negocio críticos no cubiertos por el plan de continuidad del negocio*
- *(DSS04) Número de ejercicios y pruebas que han alcanzado los objetivos de recuperación*
- *(DSS04) Frecuencia de las pruebas de recuperación*
- *(DSS04) Porcentaje de mejoras acordadas en el plan de continuidad del negocio que se han incorporado*
- *(DSS04) Porcentaje de incidencias identificadas que se han abordado posteriormente en el plan de continuidad del negocio*
- *(DSS04) Porcentaje de partes interesadas internas y externas que han recibido capacitación en continuidad del negocio*
- *(DSS04) Porcentaje de incidencias identificadas que se han abordado posteriormente en los materiales de capacitación sobre continuidad del negocio*

1906 Impacto del ascenso de la capa freática

Título del escenario de riesgo	Impacto del ascenso de la capa freática
Categoría del escenario de riesgo	19 Desastres naturales
Referencia del escenario de riesgo	1906

Escenario de riesgo
Una empresa financiera global tiene varios centros de datos a nivel mundial, con uno en una ubicación de Europa central que fue construido hace 15 años. Toda la instalación del centro de procesado de datos es subterránea y a prueba de bombas, tiene seguridad física de varias capas, y regularmente se prueban los procesos del plan de continuidad del negocio (PCN) con sus otros centros de datos. El creciente uso de la tecnología en la banca, en las adquisiciones y en los procesos de negocio, conlleva que la capacidad es un desafío constante para la empresa.

Ocasionalmente, han aparecido humedades en el centro de datos, y su cantidad ha ido aumentando con el tiempo a pesar de que se han instalado deshumidificadores instalados para compensar esta situación. Con el tiempo, el nivel de humedad ha aumentado de forma constante y la falla de un deshumidificador derivó en una falla completa del centro de datos, lo cual requirió el reemplazo de una gran cantidad de equipo debido al daño causado por el agua.

Una revisión posterior detectó la existencia de una capa freática que asciende lentamente. Aunque no es crítico, la dependencia del centro de datos requiere una acción.

Componentes del escenario de riesgo

Tipo de amenaza
El principal tipo de amenaza es un evento **natural**. Una naturaleza secundaria del evento es un **fallo** de la infraestructura/equipo físico, los deshumidificadores.

Agente
No todo tipo de amenaza requiere un agente, p. ej., fallas de equipos o causas naturales. Este evento tiene una causa natural, y el tipo secundario es la falla de los deshumidificadores y no hay un agente.

Evento
El evento es una **interrupción** causada por la falla total del centro de datos y la **destrucción** del techo derivada de una fuga de agua, así como la **destrucción** de una gran parte del equipo debido al daño por agua.

Activo/Recurso (causa)
El activo/recurso que conduce al impacto en el negocio son las **instalaciones/el equipo**, la falla del deshumidificador.

Activo/Recurso (efecto)
Los activos/recursos afectados son diferentes **procesos de negocios**, y la **infraestructura** misma que fue destruida y debe ser reemplazada.

Tiempo
En el momento de la falla del deshumidificador, la humedad ya había estado aumentando con el paso del tiempo, por lo tanto, el tiempo de la ocurrencia del evento (falla del deshumidificador) es **crítico**.

Debido a que una revisión posterior detectó la existencia de una capa freática que asciende lentamente, aunque es **no crítica**, la dependencia del centro de datos requiere una acción, y esto puede requerir algún tiempo, por lo que la duración del evento se clasifica como **extensa**. Debido a que la humedad en el centro de datos dañó repentinamente algunos de los equipos e interrumpió los servicios al mismo tiempo, la detección es **inmediata**. Las consecuencias también son **inmediatas** porque el equipo destruido ya no se puede usar y tiene que ser reemplazado inmediatamente.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**N/A**	
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**P**	Interrupción del servicio de TI, daños al equipo.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** La alta dirección debe determinar si el riesgo puede ser aceptado y/o las acciones para mitigar el riesgo, incluyendo la reconfiguración o reemplazo del centro de datos. Esto significaría que solo se reemplaza el deshumidificador que falló, y el centro de datos se deja como está.
- **Compartir/transferir el riesgo:** Seguro del el equipo destruido.
- **Mitigación del riesgo:** La empresa debe considerar las implicaciones del cambio ambiental en el centro de datos y la capacidad del centro de datos para funcionar dentro de las circunstancias ambientales cambiantes. La empresa tendrá que considerar la viabilidad futura del centro de datos o cambiar la infraestructura y/o reequilibrar la carga a lo largo de la empresa.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Política de copias de respaldo	Las copias de respaldo están disponibles.	Bajo	Medio	NO
Política de continuidad del negocio y de recuperación de desastres	Validar la recuperabilidad de los datos.	Bajo	Medio	NO

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
DSS01.04	Gestionar los factores ambientales.	Mantener medidas de protección contra los factores ambientales. Instalar equipo y dispositivos especializados para monitorizar y controlar los factores ambientales.	Medio	Alto	SÍ
DSS01.05	Gestionar las instalaciones.	Gestionar las instalaciones, incluyendo el equipo de suministro eléctrico y comunicaciones, de forma alineada con las leyes y regulaciones, los requerimientos técnicos y del negocio, las especificaciones del proveedor, y las pautas de estado y seguridad.	Alto	Alto	SÍ
DSS04.03	Desarrollar e implementar una respuesta de continuidad del negocio.	Desarrollar un plan de continuidad del negocio (PCN) basado en la estrategia de documentar los procedimientos y elementos de información que permiten a la empresa continuar sus actividades críticas después de un incidente.	Bajo	Alto	SÍ
DSS04.04	Ejercitar, probar y revisar el BCP.	Probar los arreglos de continuidad de forma periódica para ejercitar los planes de recuperación ante resultados predeterminados, permitir que se desarrollen soluciones innovadoras y ayudar a verificar den el tiempo que el plan funcionará según lo esperado.	Bajo	Alto	SÍ
DSS05.05	Gestionar el acceso físico a los activos de TI.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a las instalaciones, edificios y áreas debe justificarse, autorizarse, registrarse y monitorizarse. Esto debe aplicarse a todas las personas que entren en las instalaciones, incluyendo personal, personal temporal, clientes, proveedores, visitantes y cualquier otro tercero.	Alto	Alto	SÍ

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gerente de continuidad del negocio	Responsable de los planes de PCN.	Bajo	Alto	SÍ
Jefe de operaciones de TI	Responsable de gestionar el entorno y las instalaciones de TI.	Alto	Medio	SÍ
Director de Informática (CIO)	Responsable de desarrollar e implementar una respuesta de continuidad del negocio.	Bajo	Alto	SÍ
Propietarios del proceso de negocio	Responsables de desarrollar e implementar una respuesta de continuidad del negocio.	Bajo	Alto	SÍ

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Las partes interesadas son conscientes de cómo identificar y responder ante amenazas.	Las personas están involucradas y son conscientes de cómo reaccionar cuando ocurre un incidente.	Alto	Alto	SÍ
La dirección del negocio se compromete a una colaboración multifuncional continua con el objetivo de fomentar la puesta en marcha de programas de continuidad del negocio eficientes y efectivos.	El negocio está comprometido y contribuye proactivamente a la mitigación del riesgo.	Bajo	Alto	SÍ

Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Póliza de seguros	Seguro disponible en caso de desastres naturales.	Bajo	Medio	NO
Informes de evaluación de instalaciones	La empresa es consciente del estado y riesgo de las instalaciones.	Alto	Bajo	SÍ
Acciones y comunicaciones para respuesta ante incidentes	Las personas son conscientes de cómo reaccionar cuando ocurre un incidente.	Bajo	Alto	SÍ

Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Servicios de monitorización y alerta	Notificación oportuna de amenazas potenciales.	Alto	Bajo	NO
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Gestión de riesgos de la información	Identificar y formular una respuesta al riesgo de información relacionado con desastres naturales.	Alto	Alto	SÍ
Comprensión técnica	Experiencia técnica sobre desastres naturales específicos y relevantes.	Medio	Medio	NO

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos*
- *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos*
- *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI*
- *(04) Frecuencia de actualización del perfil de riesgo*
- *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI*
- *(14) Número de incidentes de procesos de negocio causados por la falta de disponibilidad de información*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(DSS01) Número de incidentes causados por problemas operativos*
- *(DSS01) Proporción de eventos en comparación con el número de incidentes*
- *(DSS01) Porcentaje de tipos de eventos operativos críticos cubiertos por sistemas de detección automática*
- *(DSS04) Porcentaje de servicios de TI que satisfacen los requisitos de tiempo de funcionamiento.*
- *(DSS04) Número de sistemas de negocio críticos no cubiertos por el plan de continuidad del negocio*
- *(DSS04) Número de ejercicios y pruebas que han alcanzado los objetivos de recuperación*
- *(DSS04) Frecuencia de las pruebas de recuperación*
- *(DSS04) Porcentaje de mejoras acordadas en el plan de continuidad del negocio que se han incorporado*
- *(DSS04) Porcentaje de incidencias identificadas que se han abordado posteriormente en el plan de continuidad del negocio*
- *(DSS04) Porcentaje de partes interesadas internas y externas que han recibido capacitación en continuidad del negocio*
- *(DSS04) Porcentaje de incidencias identificadas que se han abordado posteriormente en los materiales de capacitación sobre continuidad del negocio*
- *(DSS05) Porcentaje de pruebas periódicas de dispositivos de seguridad ambiental*
- *(DSS05) Calificación promedio de las evaluaciones de seguridad física*
- *(DSS05) Número de incidentes relacionados con la seguridad física*
- *(DSS05) Número de incidentes relacionados con el acceso no autorizado a la información*

Página intencionalmente en blanco

20 Innovación

2001 Interoperabilidad de las actualizaciones de los sistemas

Título del escenario de riesgo	Interoperabilidad de las actualizaciones de los sistemas
Categoría del escenario de riesgo	20 Innovación
Referencia del escenario de riesgo	2001

Escenario de riesgo
Una gran empresa que está actualizando su solución de plataforma de canales de negocio para clientes externos no consideró los prerrequisitos de software necesarios para la actualización. Las versiones de los navegadores actualmente aprobados de la empresa no son compatibles con la nueva solución debido a problemas de seguridad (nuevas políticas no desarrolladas, maestros de instalación no modificados, etc.), y el navegador no se puede actualizar a la versión necesaria para la solución en un período adecuado de tiempo.

Debido a esta situación y a las penalizaciones contractuales existentes que se definen en el acuerdo de nivel de servicio (ANS) del proveedor de servicios, se debe establecer un proyecto de alta prioridad para solucionar esta incidencia utilizando máquinas virtuales hasta que los departamentos de seguridad y tecnología revisen la situación y tomen las medidas correctivas necesarias.

Debido a que los requerimientos adicionales del procesador y de la línea de comunicación no fueron considerados como parte de los requerimientos de planificación de capacidad del diseño original para las filiales, toda la actualización se ve comprometida.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** de los procesos APO04 *Gestionar la innovación* y BAI02 *Gestionar la definición de requerimientos.*

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **interno**, el Comité de Dirección (Programas/Proyectos).

Evento
El evento es un **diseño ineficaz** y/o **ejecución ineficaz** de los procesos APO04 *Gestionar la innovación* y BAI02 *Gestionar la definición de requerimientos*, y deriva en la **interrupción** del proyecto para actualizar la solución de plataforma de canales de negocio.

Activo/Recurso (causa)
Los activos/recursos que conducen al impacto en el negocio son principalmente los **procesos** APO04 *Gestionar la innovación* y BAI02 *Gestionar la definición de requerimientos*, y las personas y habilidades del Comité de Dirección (Programas/Proyectos).

Activo/Recurso (efecto)
Los activos/recursos afectados son los **procesos** de negocio soportados por la solución de plataforma de canales de negocio.

Tiempo
La duración del evento es **extensa** porque toda la actualización se retrasa durante bastante tiempo. El momento de la ocurrencia es **crítico** porque las filiales necesitan esta actualización para mejorar sus ventas. La detección del evento es **lenta**; no se detectó que las versiones del navegador no eran compatibles hasta que surgieron los problemas de seguridad. El tiempo transcurrido entre el evento y la consecuencia es **demorado** porque el retraso de tiempo es sustancial.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**P**	Oportunidad perdida de utilizar la tecnología para mejorar la eficiencia.
Entrega del proyecto y programa de TI	**S**	Retraso de tiempo en el proyecto.
Entrega del servicio y operaciones de TI	**S**	Las soluciones temporales afectan a la estabilidad operativa.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Proporcionar una infraestructura que pueda ser un habilitador para la innovación, como herramientas de colaboración para mejorar el trabajo entre sitios geográficos y divisiones. Analizar los intereses y requerimientos de las partes interesadas (seguridad de TI). Monitorizar el rendimiento individual del proyecto en relación con la entrega de las capacidades, calendario, logro de beneficios, costes, iesgos u otras métricas esperadas para identificar los impactos potenciales en el rendimiento del programa. Tomar medidas correctivas oportunas cuando se requieran. Definir e implementar una definición de requerimientos y un procedimiento de mantenimiento, así como un repositorio de requerimientos que sean apropiados para el tamaño, la complejidad, los objetivos y el riesgo de la iniciativa.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Principios de arquitectura	Los principios de arquitectura definen las reglas y pautas generales aplicables en el uso y desarrollo de todos los recursos y activos de TI para toda la empresa.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO04.01	Crear un entorno favorable a la innovación.	Crear un entorno que propicie la innovación, considerando cuestiones como la cultura, las recompensas, la colaboración, los foros de tecnología y los mecanismos para promover y recoger las ideas de los empleados.	Medio	Bajo	NO
APO04.02	Mantener un entendimiento del entorno de la empresa.	Trabajar con las partes interesadas para comprender sus desafíos. Mantener una comprensión adecuada de la estrategia empresarial y del entorno competitivo o de otras restricciones, de forma que se puedan identificar las oportunidades habilitadas por las nuevas tecnologías.	Medio	Medio	NO
APO04.04	Evaluar el potencial de las tecnologías emergentes y las ideas de innovación.	Analizar las tecnologías emergentes identificadas y/u otras sugerencias de innovación en TI. Trabajar con las partes interesadas para validar las suposiciones sobre el potencial de nuevas tecnologías e innovación.	Medio	Medio	NO
APO04.05	Recomendar iniciativas apropiadas adicionales.	Evaluar y monitorizar los resultados de las iniciativas que son “prueba de concepto”, y si son favorables, generar recomendaciones de iniciativas adicionales y obtener el apoyo de las partes interesadas.	Alto	Alto	SÍ
BAI01.03	Gestionar la participación de las partes interesadas.	Gestionar la participación de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna que llegue a todas las partes interesadas relevantes. Esto incluye planificar, identificar e involucrar a las partes interesadas y gestionar sus expectativas.	Alto	Alto	SÍ
BAI02.01	Definir y mantener los requerimientos funcionales y técnicos del negocio.	Basándose en el caso de negocio, identificar, priorizar, especificar y acordar los requerimientos de información empresariales, funcionales, técnicos y de control que cubran el alcance/la comprensión de todas las iniciativas necesarias para lograr los resultados esperados de la solución empresarial propuesta habilitada por TI.	Alto	Bajo	SÍ
BAI02.04	Obtener la aprobación de requerimientos y soluciones.	Coordinar las observaciones de las partes interesadas afectadas, y en etapas clave predeterminadas, obtener la aprobación y autorización del patrocinador del negocio o del propietario del producto para los requerimientos funcionales y técnicos, estudios de viabilidad, análisis de riesgos y soluciones recomendadas.	Alto	Alto	SÍ

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director General Ejecutivo (CEO)	Responsable de crear el entorno propicio para la innovación.	Medio	Bajo	NO
Comité de estrategia	Responsable de promover y monitorizar iniciativas para favorecer la innovación.	Medio	Medio	NO
Director de Informática (CIO)	Responsable de identificar las innovaciones basadas en tecnología y de evaluar su potencial.	Alto	Alto	SÍ
Grupo de innovación	Responsable de identificar las oportunidades de innovación y desarrollar casos de negocio para las iniciativas de innovación.	Alto	Alto	SÍ

Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Disposición para tomar riesgos	La innovación por definición trata de nuevas tecnologías y nuevas maneras de trabajar, generando tanto resistencia potencial como beneficios inciertos. Sin embargo, no tener esta actitud de disposición al riesgo, excluirá de antemano cualquier potencial de innovación.	Alto	Alto	SÍ
Apoyo de la alta gerencia para las iniciativas de innovación	Se requiere el apoyo de la alta gerencia para financiar las iniciativas de innovación y apoyarlas para superar la resistencia inicial.	Alto	Alto	SÍ
El fracaso es una actitud permitida	No todos los proyectos o iniciativas de innovación tendrán éxito, y se aceptará una cierta cantidad de fracasos como el precio a pagar por las iniciativas con éxito.	Alto	Medio	SÍ

Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Plan de innovación	Las innovaciones están diseñadas claramente para que puedan ser monitorizadas e incorporadas a los planes estratégicos de la empresa.	Alto	Alto	SÍ
Programa de reconocimiento	La innovación se debe recompensar adecuadamente, de acuerdo con un plan formalizado.	Bajo	Bajo	NO
Evaluación de las iniciativas de innovación	La evaluación formal de las iniciativas de innovación facilita la toma de decisiones ejecutivas.	Alto	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Liderazgo y comunicación	Aclarar los motivos de la arquitectura y las consecuencias potenciales.	Alto	Alto	SÍ
Habilidades de arquitectura	Desarrollar una arquitectura eficiente y efectiva alineada con los requerimientos del negocio.	Alto	Alto	SÍ

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(04) Porcentaje de procesos de negocio críticos, servicios de TI y programas empresariales habilitados por TI cubiertos por la evaluación de riesgos*
- *(04) Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos*
- *(04) Porcentaje de las evaluaciones de riesgo empresarial, incluyendo el riesgo relacionado con las TI*
- *(04) Frecuencia de actualización del perfil de riesgo*
- *(05) Porcentaje de inversiones habilitadas para TI en las que se supervisa el logro de beneficios durante todo el ciclo de vida económico*
- *(05) Porcentaje de servicios de TI donde se logran los beneficios esperados*
- *(05) Porcentaje de inversiones habilitadas para TI en las que los beneficios esperados se cumplen o exceden*
- *(08) Valor presente neto (VPN) que muestra el nivel de satisfacción empresarial de la calidad y utilidad de las soluciones tecnológicas*
- *(09) Nivel de satisfacción de los ejecutivos del negocio con la capacidad de respuesta de TI a los nuevos requerimientos*
- *(09) Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas*
- *(12) Número de cambios en los procesos de negocio que deben ser aplazados o revisados debido a problemas de integración tecnológica*
- *(12) Número de programas empresariales habilitados por TI retrasados o que incurren en costes adicionales debido a incidencias de integración tecnológica*
- *(12) Número de aplicaciones o infraestructuras críticas que operan en silos y no están integradas*
- *(13) Número de programas/proyectos ejecutados a tiempo y dentro del presupuesto*
- *(13) Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto*
- *(13) Número de programas que necesitan revisión significativa debido a defectos de calidad*
- *(13) Coste del mantenimiento de la aplicación frente al coste total de TI*
- *(17) Nivel de conocimiento y comprensión de los ejecutivos del negocio sobre las posibilidades de innovación en TI*
- *(17) Nivel de satisfacción de las partes interesadas con los niveles de conocimientos e ideas sobre innovación en TI*
- *(17) Número de iniciativas aprobadas como resultado de ideas innovadoras de TI*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(APO04) Percepciones y observaciones de las partes interesadas de la empresa respecto a la innovación en TI*
- *(APO04) Porcentaje de iniciativas implementadas que logran los beneficios previstos*
- *(APO04) Porcentaje de iniciativas implementadas con un claro vínculo a un objetivo empresarial*
- *(APO04) Observaciones y encuestas de las partes interesadas*
- *(BAI01) Porcentaje de partes interesadas efectivamente involucradas*
- *(BAI01) Nivel de satisfacción de las partes interesadas con la participación*
- *(BAI01) Porcentaje de partes interesadas que aprueban la necesidad empresarial, el alcance, el resultado previsto y el nivel de riesgo del proyecto*
- *(BAI01) Porcentaje de actividades alineadas con el alcance y los resultados esperados*
- *(BAI01) Frecuencia de las revisiones del estado del proyecto*
- *(BAI01) Porcentaje de desviaciones del plan abordadas*
- *(BAI01) Porcentaje de firmas de autorización de las partes interesadas para las revisiones etapa-puerta de los programas activos*
- *(BAI01) Porcentaje de beneficios esperados logrados*
- *(BAI01) Porcentaje de resultados con aceptación en primera instancia*
- *(BAI01) Nivel de satisfacción de las partes interesadas expresado en la revisión de cierre del proyecto*
- *(BAI02) Porcentaje de requerimientos revisados debido a la desalineación con las necesidades y expectativas de la empresa*
- *(BAI02) Nivel de satisfacción de las partes interesadas con los requerimientos*
- *(BAI02) Porcentaje de requerimientos satisfechos por la solución propuesta*

2002 Error de programación

Título del escenario de riesgo	Error de programación
Categoría del escenario de riesgo	20 Innovación
Referencia del escenario de riesgo	2002

Escenario de riesgo
Un programador comete un error de codificación que permite a personas obtener un acceso más allá de sus responsabilidades. El error de programación no es detectado por los procedimientos de garantía de la calidad (QA) y el código se implementa en producción. El error de programación en esta aplicación, que gestiona expedientes médicos, permite a todos los usuarios del sistema acceso abierto a información médica sensible e identificable del paciente. Este acceso puede derivar en una divulgación no autorizada e inapropiada (accidental o malintencionada) de información sensible, lo que generalmente resulta en una multa por parte de los reguladores locales debido a la violación de la privacidad de los datos, así como en una pérdida de confianza pública sobre la capacidad de la empresa para mantener información médica sensible de manera segura.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es una divulgación no autorizada e inapropiada **accidental** de información sensible.

Agente
El programador interno que comete el error de codificación y las personas **internas** que obtienen un acceso más allá de sus responsabilidades.

Evento
El evento es la **divulgación** de información sensible.

Activo/Recurso (causa)
Los activos/recursos que conducen al impacto en el negocio son personas, el programador y el equipo de QA, así como el **proceso** APO11 *Gestionar la calidad*, el cual no detectó el error de programación.

Activo/Recurso (efecto)
El activo/recurso es la **información** porque el error de programación proporciona acceso a datos sensibles de pacientes a los que el usuario no tiene derecho.

Tiempo
El momento es **crítico** porque la exposición potencial a los expedientes médicos es inmediata. La duración es **extensa**, la detección es **lenta** y el tiempo transcurrido es **demorado**. El error de programación puede pasar desapercibido durante un largo período de tiempo porque los usuarios que descubren que tienen acceso a expedientes a los que normalmente no pueden acceder tal vez no informen a la persona responsable de la seguridad de la información.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**P**	Eficacia de los procesos de negocio.
Entrega del proyecto y programa de TI	**N/A**	
Entrega del servicio y operaciones de TI	**S**	Problemas de seguridad y de cumplimiento

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** N/A
- **Mitigación del riesgo:** Implementar la gestión de cambios y QA.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Principios de arquitectura	Los principios de arquitectura definen las reglas y pautas generales aplicables en el uso y desarrollo de todos los recursos y activos de TI para toda la empresa.	Medio	Medio	NO

Habilitador del proceso

Referencia	Título Descripción	Efecto en la frecuencia	Efecto en el impacto	Control esencial	Control esencial
APO11.05	Integrar la gestión de la calidad en soluciones para el desarrollo y la prestación de servicios.	Incorporar prácticas relevantes de gestión de la calidad a la definición, monitorización y gestión continua del desarrollo de soluciones y la oferta de servicios.	Medio	Bajo	NO
BAI07.01	Establecer un plan de implementación.	Establecer un plan de implementación que cubra la conversión de sistemas y datos, los criterios de pruebas de aceptación, la comunicación, la capacitación, la preparación de lanzamientos, la puesta en producción, el apoyo a la producción inmediato, un plan de respaldo/vuelta atrás, y una revisión post-implementación. Obtener la aprobación de las partes relevantes.	Alto	Medio	SÍ

Habilitador del proceso *(cont.)*					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
BAI07.03	Pruebas de aceptación del plan.	Establecer un plan de pruebas basado en estándares de toda la empresa que definen roles, responsabilidades y criterios de entrada y salida. Asegurarse de que el plan sea aprobado por las partes relevantes.	Alto	Alto	SÍ
BAI07.05	Realizar pruebas de aceptación.	Probar los cambios de forma independiente de acuerdo con el plan de prueba definido antes de la migración al entorno operativo en vivo.	Alto	Alto	SÍ
BAI07.06	Pasar a producción y gestionar los lanzamientos.	Promover la solución aceptada al negocio y las operaciones. Cuando sea apropiado, ejecutar la solución como una implementación piloto o en paralelo con la solución antigua durante un período definido y comparar el comportamiento y los resultados. Si se producen problemas significativos, volver al entorno original basándose en el plan de respaldo/ vuelta atrás. Gestionar los lanzamientos de los componentes de la solución.	Alto	Medio	SÍ
BAI03.06	Realizar el QA.	Desarrollar, aprovisionar y ejecutar un plan de aseguramiento de calidad (QA) alineado con el sistema de gestión de calidad (QMS) para obtener la calidad especificada en la definición de los requerimientos y en las políticas y procedimientos de calidad de la empresa.	Alto	Medio	SÍ
Habilitador de estructuras organizacionales					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director General Ejecutivo (CEO)	Responsable de crear el entorno propicio para la innovación.		Medio	Medio	NO
Comité de estrategia	Responsable de promover y monitorizar iniciativas para favorecer la innovación.		Bajo	Bajo	NO
Director de Informática (CIO)	Responsable de identificar las innovaciones basadas en tecnología y de evaluar su potencial.		Medio	Medio	NO
Grupo de innovación	Responsable de identificar las oportunidades de innovación y desarrollar casos de negocio para las iniciativas de innovación.		Bajo	Bajo	NO
Habilitador de cultura, ética y comportamiento					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Disposición para tomar riesgos	La innovación por definición trata de nuevas tecnologías y nuevas maneras de trabajar, generando tanto resistencia potencial como beneficios inciertos. Sin embargo, no tener esta actitud de disposición al riesgo, excluirá de antemano cualquier potencial de innovación.		Medio	Bajo	NO
Apoyo de la alta gerencia para las iniciativas de innovación	Se requiere el apoyo de la alta gerencia para financiar las iniciativas de innovación y apoyarlas para superar la resistencia inicial.		Bajo	Bajo	NO
El fracaso es una actitud permitida	No todos los proyectos o iniciativas de innovación tendrán éxito, y se aceptará una cierta cantidad de fracasos como el precio a pagar por las iniciativas con éxito.		Medio	Medio	NO
Habilitador de información					
Referencia	**Contribución a la respuesta**		**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Plan de innovación	Las innovaciones están diseñadas claramente para que puedan ser monitorizadas e incorporadas a los planes estratégicos de la empresa.		Medio	Medio	NO
Programa de reconocimiento	La innovación se debe recompensar adecuadamente, de acuerdo con un plan acordado y formalizado.		Bajo	Bajo	NO
Evaluación de las iniciativas de innovación	La evaluación formal de las iniciativas de innovación facilita la toma de decisiones ejecutivas.		Medio	Medio	NO

Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Liderazgo y comunicación	Aclarar los motivos de la arquitectura y las consecuencias potenciales.	Medio	Medio	NO
Habilidades de arquitectura	Desarrollar una arquitectura eficiente y efectiva alineada con los requerimientos del negocio.	Medio	Medio	SÍ

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI

- *(07) Número de interrupciones del negocio debido a incidentes de servicios de TI*
- *(07) Porcentaje de partes interesadas del negocio satisfechas en que la prestación de servicios de TI cumple con los niveles de servicio acordados*
- *(07) Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de TI*
- *(13) Número de programas que necesitan revisión significativa debido a defectos de calidad*

Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso

- *(APO11) Calificación promedio de satisfacción de las partes interesadas para las soluciones y los servicios*
- *(APO11) Porcentaje de partes interesadas satisfechas con la calidad de TI*
- *(APO11) Porcentaje de proyectos revisados que cumplen con las metas y los objetivos de calidad deseados*
- *(APO11) Porcentaje de soluciones y servicios entregados con certificación formal*
- *(APO11) Número de defectos descubiertos antes de la producción*
- *(APO11) Número de procesos con un requerimiento de calidad definido*
- *(APO11) Número de procesos con un reporte formal de evaluación de la calidad*
- *(BAI03) Número de diseños de soluciones revisados debido a la desalineación con los requerimientos*
- *(BAI03) Tiempo necesario para aprobar que el producto de diseño ha cumplido con los requerimientos*
- *(BAI03) Número de errores encontrados durante la prueba*

2003 Detención de una adquisición

Título del escenario de riesgo	Detención de una adquisición
Categoría del escenario de riesgo	20 Innovación
Referencia del escenario de riesgo	2003

Escenario de riesgo
Para sus procesos administrativos, una compañía de seguros está utilizando plataformas de TI desarrolladas internamente desde los años 80 o 90. Por lo general, estas soluciones funcionan bastante bien y son fiables. Sin embargo, también son inflexibles. Por lo tanto, es muy lento, complejo y costoso lanzar nuevos productos de seguros al mercado.

La empresa planea adquirir una solución de una compañía de software relativamente pequeña. Los planes son reemplazar su vieja solución desarrollada internamente con este nuevo software estándar, que se convertirá en la nueva solución de seguros para la administración de reclamaciones. La implementación y personalización se realiza junto con la empresa de software. A la mitad del proyecto, se reconoce que éste no proporcionará los beneficios esperados y no cumplirá los requerimientos. El proyecto se detiene y se cancela el contrato con la empresa de software.

Debido a que el antiguo sistema heredado aún debe reemplazarse, hay diferentes opciones que la compañía de seguros puede considerar. Éstas varían desde una nueva solución estándar hasta un desarrollo interno completo. Sin embargo, la detención del proyecto conduce a un retraso de al menos uno o dos años, y la mayoría de los desarrollos hasta la fecha se pierden.

Componentes del escenario de riesgo

Tipo de amenaza
La naturaleza del evento es un **fallo** de los procesos APO04 *Gestionar la innovación* y BAI03 *Gestionar la identificación y el desarrollo de soluciones.*

Agente
El agente que genera la amenaza que explota una vulnerabilidad es **interno**, el Comité de Dirección (Programas/Proyectos).

Evento
El evento es un **diseño ineficaz** y/o **ejecución ineficaz** del proceso BAI03 *Gestionar la identificación y el desarrollo de soluciones.*

Activo/Recurso (causa)
El activo/recurso que conduce al impacto del negocio son las **personas** que eligieron esta solución estándar y decidieron contratar a la pequeña empresa de software; estas personas podrían ser el Comité Ejecutivo de Estrategia o el Comité de Dirección (Programas/Proyectos).

Activo/Recurso (efecto)
Los activos/recursos afectados son los **procesos** de negocio, la innovación empresarial y las personas que tienen que trabajar con los sistemas inflexibles.

Tiempo
La duración del evento es **extensa** ya que el proyecto detenido tiene que ser relanzado o incluso comenzado desde cero de nuevo. El momento de la ocurrencia es **crítico** ya que otras compañías de seguros ya tienen soluciones nuevas y más flexibles, y por lo tanto, son más competitivas. El evento se detecta después de un tiempo **moderado**, y el proyecto fue detenido y no se completó hasta el final, cuando se detectó que la solución no cumpliría con los requisitos. El tiempo transcurrido entre el evento y la consecuencia es **demorado** ya que el retraso del proyecto será de uno a dos años.

Tipo de riesgo

Habilitación del beneficio/valor de TI	**P**	Oportunidad perdida de utilizar la tecnología para mejorar la eficiencia, la efectividad y la flexibilidad.
Entrega del proyecto y programa de TI	**P**	Costes atados para inversiones.
	P	Retraso significativo en la ejecución del proyecto.
Entrega del servicio y operaciones de TI	**S**	Los sistemas antiguos e inflexibles pueden causar reducción del valor a la empresa.

Posibles respuestas al riesgo

- **Evasión del riesgo:** N/A
- **Aceptación del riesgo:** N/A
- **Compartir/transferir el riesgo:** Usar un proveedor de procesos de negocio para la administración de reclamaciones.
- **Mitigación del riesgo:** Prueba de concepto. Gestión clara de los requerimientos.

Mitigación del Riesgo Usando Habilitadores de COBIT 5

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Control esencial
Principios de arquitectura	Los principios de arquitectura definen las reglas y pautas generales aplicables en el uso y desarrollo de todos los recursos y activos de TI para toda la empresa.	Alto	Alto	SÍ

Habilitador del proceso					
Referencia	**Título Descripción**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**	**Control esencial**
APO04.02	Mantener un entendimiento del entorno de la empresa.	Trabajar con las partes interesadas para comprender sus desafíos. Mantener una comprensión adecuada de la estrategia empresarial y del entorno competitivo o de otras restricciones, de forma que se puedan identificar las oportunidades habilitadas por las nuevas tecnologías.	Alto	Alto	SÍ
APO04.03	Monitorizar y escanear el entorno tecnológico.	Monitorizar y escanear sistemáticamente el entorno externo de la empresa para identificar las tecnologías emergentes con el potencial de crear valor (p. ej., ejecutar la estrategia empresarial, optimizar costes, evitar la obsolescencia y habilitar de mejor manera los procesos empresariales y de TI). Monitorizar el mercado, el entorno competitivo, los sectores de la industria y las tendencias legales y regulatorias para poder analizar las tecnologías emergentes o las ideas de innovación en el contexto empresarial.	Medio	Bajo	NO
APO04.04	Evaluar el potencial de las tecnologías emergentes y las ideas de innovación.	Analizar las tecnologías emergentes identificadas y/u otras sugerencias de innovación en TI. Trabajar con las partes interesadas para validar las suposiciones sobre el potencial de nuevas tecnologías e innovación.	Medio	Bajo	NO
APO04.05	Recomendar iniciativas apropiadas adicionales.	Evaluar y monitorizar los resultados de las iniciativas que son “prueba de concepto”, y si son favorables, generar recomendaciones de iniciativas adicionales y obtener el apoyo de las partes interesadas.	Bajo	Medio	NO
APO04.06	Monitorizar la implementación y el uso de la innovación.	Monitorizar la implementación y el uso de las tecnologías emergentes y las innovaciones durante la integración, adopción y todo el ciclo de vida económico para garantizar que se obtengan los beneficios prometidos y para identificar las lecciones aprendidas.	Bajo	Alto	SÍ
BAI02.01	Definir y mantener los requerimientos funcionales y técnicos del negocio.	Basándose en el caso de negocio, identificar, priorizar, especificar y acordar los requerimientos de información empresariales, funcionales, técnicos y de control que cubran el alcance/la comprensión de todas las iniciativas necesarias para lograr los resultados esperados de la solución empresarial propuesta habilitada por TI .	Alto	Medio	SÍ
BAI02.02	Realizar un estudio de viabilidad y formular soluciones alternativas	Realizar un estudio de viabilidad de posibles soluciones alternativas, evaluar su viabilidad y seleccionar la opción preferida. Si es apropiado, implementar la opción seleccionada como piloto para determinar posibles mejoras.	Alto	Alto	SÍ
BAI02.03	Gestionar el riesgo de los requerimientos.	Identificar, documentar, priorizar y mitigar el riesgo funcional, técnico y de procesamiento de la información asociado con los requerimientos empresariales y la solución propuesta.	Medio	Medio	NO
BAI03.04	Obtener los componentes de la solución.	Adquirir componentes de la solución basados en el plan de adquisiciones de acuerdo con los requerimientos y los diseños detallados, los principios y estándares de la arquitectura, y los procedimientos generales de adquisiciones y contratos de la empresa, requerimientos de garantía de calidad (QA) y estándares de aprobación. Asegurarse de que el proveedor identifique y aborde todos los requerimientos legales y contractuales.	Medio	Medio	NO

Habilitador de estructuras organizacionales				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Director General Ejecutivo (CEO)	Responsable de crear el entorno propicio para la innovación.	Medio	Alto	SÍ
Comité de estrategia	Responsable de promover y monitorizar iniciativas para favorecer la innovación.	Alto	Alto	SÍ
Director de Informática (CIO)	Responsable de identificar las innovaciones basadas en tecnología y de evaluar su potencial.	Alto	Alto	SÍ
Grupo de innovación	Responsable de identificar las oportunidades de innovación y desarrollar casos de negocio para las iniciativas de innovación.	Medio	Alto	SÍ
Habilitador de cultura, ética y comportamiento				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Disposición para tomar riesgos	La innovación por definición trata de nuevas tecnologías y nuevas maneras de trabajar, generando tanto resistencia potencial como beneficios inciertos. Sin embargo, no tener esta actitud de disposición al riesgo, excluirá de antemano cualquier potencial de innovación.	Medio	Medio	NO
Apoyo de la alta gerencia para las iniciativas de innovación	Se requiere el apoyo de la alta gerencia para financiar las iniciativas de innovación y apoyarlas para superar la resistencia inicial.	Medio	Medio	NO
El fracaso es una actitud permitida	No todos los proyectos o iniciativas de innovación tienen éxito, y se aceptará una cierta cantidad de fracasos como el precio a pagar por las iniciativas de éxito.	Medio	Medio	NO
Habilitador de información				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Plan de innovación	Las innovaciones están diseñadas claramente para que puedan ser monitorizadas e incorporadas a los planes estratégicos de la empresa.	Alto	Alto	SÍ
Programa de reconocimiento	La innovación se debe recompensar adecuadamente, de acuerdo con un plan formalizado.	Bajo	Bajo	NO
Evaluación de las iniciativas de innovación	La evaluación formal de las iniciativas de innovación facilita la toma de decisiones ejecutivas.	Alto	Alto	SÍ
Habilitador de servicios, infraestructura y aplicaciones				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
N/A	N/A			
Habilitador de personas, habilidades y competencias				
Referencia	**Contribución a la respuesta**	**Efecto en la frecuencia**	**Efecto en el impacto**	**Control esencial**
Liderazgo y comunicación	Aclarar los motivos de la arquitectura y las consecuencias potenciales.	Alto	Alto	SÍ
Habilidades de arquitectura	Desarrollar una arquitectura eficiente y eficaz alineada con los requerimientos del negocio.	Alto	Alto	SÍ

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI
• *(05) Porcentaje de inversiones habilitadas para TI en las que se supervisa el logro de beneficios durante todo el ciclo de vida económico*
• *(05) Porcentaje de servicios de TI donde se logran los beneficios esperados*
• *(05) Porcentaje de inversiones habilitadas para TI en las que los beneficios afirmados se cumplen o exceden*
• *(08) Porcentaje de propietarios de procesos de negocio satisfechos con los productos y servicios de soporte de TI*
• *(08) Nivel de comprensión por parte del usuario empresarial de cómo las soluciones tecnológicas apoyan sus procesos*
• *(08) Valor presente neto (VPN) que muestra el nivel de satisfacción empresarial de la calidad y utilidad de las soluciones tecnológicas*
• *(09) Nivel de satisfacción de los ejecutivos del negocio con la capacidad de respuesta de TI a los nuevos requerimientos*
• *(09) Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas*
• *(09) Tiempo promedio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada*
• *(17) Nivel de conocimiento y comprensión de los ejecutivos del negocio sobre las posibilidades de innovación en TI*
• *(17) Nivel de satisfacción de las partes interesadas con los niveles de conocimientos e ideas sobre innovación en TI*
• *(17) Número de iniciativas aprobadas como resultado de ideas innovadoras de TI*
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso
• *(APO04) Aumento de la cuota de mercado o competitividad debido a innovaciones*
• *(APO04) Percepciones y observaciones de las partes interesadas de la empresa respecto a la innovación en TI*
• *(APO04) Porcentaje de iniciativas implementadas que logran los beneficios previstos*
• *(APO04) Porcentaje de iniciativas implementadas con un claro vínculo a un objetivo empresarial*
• *(APO04) Inclusión de objetivos relacionados con la innovación o tecnología emergente en los objetivos de rendimiento para el personal relevante*
• *(BAI03) Número de diseños de soluciones revisados debido a la desalineación con los requerimientos*
• *(BAI03) Tiempo necesario para aprobar que el producto de diseño ha cumplido con los requerimientos*

Apéndice 1
Plantilla de Análisis de Escenarios de Riesgo[10]

Este apéndice contiene una plantilla integral para el tratamiento de un escenario de riesgo, desde la concepción hasta la respuesta y monitorización, en apoyo a los procesos centrales de gestión de riesgos (APO12) de una empresa.

Plantilla del escenario de riesgo	
Título del escenario de riesgo	
Categoría del escenario de riesgo Descripción de alto nivel de la categoría del escenario	☐ 01 Establecimiento y mantenimiento del portafolio ☐ 02 Gestión del ciclo de vida del programa/proyectos ☐ 03-Toma de decisiones sobre inversiones en TI ☐ 04-Experiencia y habilidades en TI ☐ 05-Operaciones del personal ☐ 06-Información ☐ 07-Arquitectura ☐ 08-Infraestructura ☐ 09-Software ☐ 10-Propiedad empresarial de TI ☐ 11-Proveedores ☐ 12-Cumplimiento regulatorio ☐ 13-Geopolítica ☐ 14-Robo o destrucción de infraestructura ☐ 15-Malware ☐ 16-Ataques lógicos ☐ 17-Acción industrial ☐ 18-Medio ambiente ☐ 19-Actos de la naturaleza ☐ 20-Innovación
Escenario de riesgo Describa el escenario de riesgo/oportunidad, incluyendo un razonamiento sobre el impacto negativo y positivo del escenario. La descripción aclara el tipo de amenaza/vulnerabilidad e incluye los agentes, eventos, activos y cuestiones de tiempo.	
Componentes del escenario de riesgo	
Tipo de amenaza La naturaleza del evento	☐ Maliciosa ☐ Accidental ☐ Error ☐ Fallo ☐ Natural ☐ Requerimiento externo
Agente Quién o qué desencadena la amenaza que explota una vulnerabilidad	☐ Interno ☐ Externo ☐ Humano ☐ No humano
Evento Algo que sucede y que no se esperaba que sucediera, algo que no sucede y que se esperaba que sucediera, o un cambio en las circunstancias. Los eventos siempre tienen causas y suelen tener consecuencias. Una consecuencia es el resultado de un evento y tiene un impacto en los objetivos.	☐ Divulgación ☐ Interrupción ☐ Modificación ☐ Robo ☐ Destrucción ☐ Diseño ineficaz ☐ Ejecución ineficaz ☐ Reglas y regulaciones ☐ Uso inapropiado
Activo Un activo es algo de valor tangible o intangible que vale la pena proteger, incluyendo a personas, sistemas, infraestructura, finanzas y reputación.	☐ Proceso ☐ Personas y habilidades ☐ Estructura organizacional ☐ Infraestructura física ☐ Infraestructura de TI ☐ Información ☐ Aplicaciones
Recurso Un recurso es cualquier cosa que ayuda a alcanzar una meta.	☐ Proceso ☐ Personas y habilidades ☐ Estructura organizacional ☐ Infraestructura física ☐ Infraestructura de TI ☐ Información ☐ Aplicaciones

Adaptado de ISACA, *COBIT® 5 para Riesgos*, EE.UU., 2013, *www.isaca.org/cobit*, pp. 243-244.

Plantilla del escenario de riesgo *(cont.)*				
Tiempo	**Momento**	☐ No crítico	☐ Crítico	
	Duración	☐ Corta	☐ Moderada	☐ Extensa
	Detección	☐ Lenta	☐ Moderada	☐ Instantánea
	Tiempo transcurrido	☐ Inmediato	☐ Demorado	

Tipo de riesgo
Describa las consecuencias derivadas del evento. Incluya si el tipo de riesgo es primario o secundario.

Tipo de riesgo	P/S	Descripción del riesgo
Habilitación del beneficio/valor de TI		
Entrega del proyecto y programa de TI		
Entrega del servicio y operaciones de TI		

Posibles respuestas al riesgo

Evasión del riesgo:
Aceptación de riesgo:
Compartir/transferir el riesgo:
Mitigación del riesgo:

Mitigación del Riesgo Usando Habilitadores de COBIT 5 (consulte el Apéndice D en *COBIT 5 para Riesgos*)

Habilitador de principios, políticas y marco de trabajo

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Esencial Control

Habilitador del proceso

Referencia	Contribución a la respuesta	Efecto En la frecuencia	Efecto En el impacto	Esencial Control

Habilitador de estructuras organizacionales

Referencia	Contribución a la respuesta	Efecto En la frecuencia	Efecto En el impacto	Esencial Control

Habilitador de cultura, ética y comportamiento

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Esencial Control

Habilitador de información

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Esencial Control

Habilitador de servicios, infraestructura y aplicaciones

Referencia	Contribución a la respuesta	Efecto en la frecuencia	Efecto en el impacto	Esencial Control

Habilitador de personas, habilidades y competencias

Referencia	Contribución a la respuesta	Efecto En la frecuencia	Efecto En el impacto	Esencial Control

Indicadores clave de riesgo (KRIs) relacionados con las metas de TI
• •
Indicadores clave de riesgo (KRIs) relacionados con las metas del proceso
• •

Página intencionalmente en blanco

Apéndice 2
Glosario

Término	Explicación
Activo	Algo de valor tangible o intangible que vale la pena proteger, incluyendo a personas, sistemas, infraestructura, finanzas y reputación.
Amenaza	Cualquier cosa (por ejemplo, un objeto, una sustancia, un ser humano) que es capaz de actuar contra un activo de una manera que pueda dañarlo.
Análisis de riesgos	1. Un proceso por el cual se calculan la frecuencia y la magnitud de los escenarios de riesgo de TI. 2. Los pasos iniciales de la gestión de riesgos: El análisis del valor de los activos para el negocio, la identificación de las amenazas a esos activos y la evaluación de la vulnerabilidad de cada activo a esas amenazas.
Análisis del impacto en el negocio (BIA)	Evaluar la criticidad y la sensibilidad de los activos de información. Es un ejercicio que determina el impacto que tendría en una empresa perder el soporte de algún recurso; establece el escalamiento de dicha pérdida con el paso del tiempo; identifica los recursos mínimos necesarios para recuperarse; y prioriza la recuperación de procesos y del sistema de soporte.
Apetito de riesgo	Cantidad de riesgo, a un nivel amplio, que una entidad está dispuesta a aceptar en busca de su misión.
Consolidación de riesgos	El proceso de integración de las evaluaciones de riesgos a nivel corporativo para obtener una visión completa del riesgo global para la empresa.
Cultura de riesgos	El conjunto de valores y creencias compartidas que gobierna las actitudes hacia la asunción de riesgos, la atención y la integridad, y determina la forma en que se reportan y discuten abiertamente los riesgos y las pérdidas.
Declaración del riesgo	Una descripción de las condiciones actuales que pueden derivar en la pérdida; y una descripción de la pérdida. Fuente: Software Engineering Institute (SEI). Para que un riesgo sea comprensible, debe expresarse claramente. Tal declaración debe incluir una descripción de las condiciones actuales que pueden derivar en la pérdida; y una descripción de la pérdida.
Escenario de riesgos de TI	La descripción de un evento relacionado con TI que puede derivar en un impacto en el negocio.
Evaluación del riesgo	Un proceso utilizado para identificar y evaluar los riesgos y sus efectos potenciales.
Evento	Algo que sucede en un lugar y/o momento específico.
Evento de amenaza	Cualquier evento durante el cual un elemento/agente de amenaza actúa en contra de un activo de una manera que tiene el potencial de derivar directamente en un daño.
Evento de pérdida	Cualquier evento durante el cual un evento de amenaza causa una pérdida.
Evento de vulnerabilidad	Cualquier evento durante el cual se produce un aumento significativo en la vulnerabilidad. Tenga en cuenta que este aumento en la vulnerabilidad puede derivar de cambios en las condiciones de control o de cambios en la capacidad/fuerza de la amenaza.
Factor de riesgo	Una condición que puede influir en la frecuencia y/o magnitud y, en última instancia, en el impacto que los eventos/escenarios relacionados con TI tienen en el negocio.
Frecuencia	Es la medida de la tasa por la cual ocurren los eventos en un determinado período de tiempo.
Gestión de riesgos empresariales (ERM)	La disciplina por la cual una empresa en cualquier industria evalúa, controla, explota, financia y monitorea el riesgo de todas las fuentes con el propósito de aumentar el valor de la empresa, a corto y largo plazo, para sus grupos de interés.
Impacto en el negocio	El efecto neto, positivo o negativo, del logro de los objetivos del negocio.
Incidente relacionado con TI	Un evento relacionado con TI que causa un impacto en el negocio operativo, de desarrollo y/o estratégico.
Indicador clave de riesgo (KRI)	Un subconjunto de los indicadores clave de riesgo altamente relevantes y que tienen una alta probabilidad de predecir o de indicar un riesgo importante.
Indicador de demora	Métricas para el logro de metas: Un indicador relacionado con el resultado o resultado de un habilitador, es decir, este indicador solo está disponible después de los hechos o eventos.
Indicador de riesgo	Una métrica capaz de demostrar que la empresa está sujeta o tiene una alta probabilidad de estar sujeta a un riesgo que excede el apetito de riesgo definido.
Indicador líder	Métricas para la aplicación de buenas prácticas: Un indicador relacionado con el funcionamiento de un habilitador, es decir, este indicador proporcionará una indicación sobre el posible resultado del habilitador.
Magnitud	Una medida de la gravedad potencial de la pérdida o la ganancia potencial de los eventos/escenarios ocurridos.
Mapa de riesgos	Una herramienta (gráfica) para clasificar y mostrar el riesgo por rangos definidos de frecuencia y magnitud.
Meta del negocio	La traducción de la misión de la empresa de una declaración de intención a objetivos de rendimiento y resultados.
Objetivo de negocio	Un desarrollo adicional de las metas empresariales en objetivos tácticos y resultados deseados.
Perfil de riesgo de TI	Una descripción del riesgo general (identificado) al que la empresa es expuesta.
Problema de riesgo (TI)	1. Una instancia de un riesgo de TI. 2. Una combinación de condiciones de control, valor y amenaza que imponen un nivel notable de riesgo de TI.

Término	Explicación
Registro de riesgos de TI	Un repositorio de los atributos clave de riesgos de TI potenciales y conocidos. Los atributos pueden incluir nombre, descripción, propietario, frecuencia esperada/real, magnitud potencial/real, impacto en el negocio potencial/real y disposición.
Respuesta al riesgo	Evasión del riesgo, aceptación del riesgo, compartir/transferir el riesgo, mitigación del riesgo, lo que conduce a una situación en la que la mayor cantidad de riesgo residual futuro (riesgo actual con la respuesta al riesgo definida e implementada) como sea posible (normalmente dependiendo de los presupuestos disponibles) cae dentro de los límites de apetito de riesgo.
Riesgo (negocio)	Una situación probable con una frecuencia y una magnitud de la pérdida (o ganancia) inciertas.
Riesgo de TI	El riesgo de negocio asociado con el uso, la propiedad, la operación, la participación, la influencia y la adopción de TI dentro de una empresa.
Riesgo residual	El riesgo restante después de que la gerencia ha implementado una respuesta al riesgo.
Tipo de evento	Para el propósito de gestión de riesgos de TI,[11] uno de los tres posibles tipos de eventos: evento de amenaza, evento de pérdida y evento de vulnerabilidad.
Tolerancia al riesgo	El nivel aceptable de variación que la gerencia está dispuesta a permitir para cualquier riesgo en particular mientras la empresa persigue sus objetivos.
Vulnerabilidad	Una debilidad en el diseño, implementación, operación o control interno de un proceso que podría exponer al sistema a amenazas adversas provenientes de eventos de amenazas.

[11] Poder diferenciar de manera consistente y efectiva los diferentes tipos de eventos que contribuyen al riesgo es un elemento crítico en el desarrollo de buenas métricas relacionadas con el riesgo y de decisiones bien informadas. A menos que se reconozcan y apliquen estas diferencias categóricas, las métricas resultantes pierden significado y, como resultado, las decisiones basadas en esas métricas son mucho más propensas a tener fallas.

Apéndice 3
Procesos para el Gobierno y Gestión de la TI de la Empresa

Figura 18: Modelo de referencia del proceso COBIT 5

Fuente: COBIT® 5, ISACA, EE.UU., 2012, figura 16

Procesar	Práctica de gobierno o gestión de COBIT 5
EDM01 Asegurar el establecimiento y el mantenimiento del marco de gobierno	**EDM01.01: Evaluar el sistema de gobierno.** Identificar e involucrarse continuamente con las partes interesadas de la empresa, documentar una comprensión de los requisitos y hacer un juicio sobre el diseño actual y futuro del gobierno de TI empresarial.
	EDM01.02: Orientar el sistema de gobierno. Informar a los líderes y obtener su apoyo, aprobación y compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de TI en línea con los principios de diseño de gobierno acordados, los modelos de toma de decisiones y los niveles de autoridad. Definir la información requerida para la toma de decisiones informadas.
	EDM01.03: Monitorizar el sistema de gobierno. Monitorizar la efectividad y el desempeño del gobierno de TI de la empresa. Evaluar si el sistema de gobierno y los mecanismos implementados (incluyendo las estructuras, los principios y los procesos) están operando de forma efectiva y ofrecen una supervisión apropiada de TI.

Procesar	Práctica de gobierno o gestión de COBIT 5
EDM02 Asegurar la entrega de beneficios	**EDM02.01: Evaluar la optimización de valor.** Evaluar continuamente la cartera de inversiones, servicios y activos habilitados por TI con el fin de determinar la probabilidad de alcanzar los objetivos de la empresa y entregar un valor a un coste razonable. Identificar y hacer un juicio sobre cualquier cambio en la dirección que debe ofrecerse a la gerencia para optimizar la creación de valor.
	EDM02.02: Dirigir la optimización del valor. Dirigir los principios y las prácticas de gestión de valor para permitir una obtención óptima de valor con las inversiones habilitadas para TI durante todo su ciclo de vida económico.
	EDM02.03: Monitorizar la optimización del valor. Monitorizar las metas y métricas clave para determinar la medida en que el negocio está generando el valor y los beneficios esperados para la empresa a través de las inversiones y los servicios habilitados por TI. Identificar problemas significativos y considerar acciones correctivas.
EDM03 Asegurar la optimización del riesgo	**EDM03.01: Evaluar la gestión de riesgos.** Examinar y analizar continuamente el efecto del riesgo sobre el uso actual y futuro de TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado, y que el riesgo para el valor de la empresa relacionado con el uso de las TI sea identificado y administrado.
	EDM03.02: Dirigir la gestión de riesgos. Dirigir el establecimiento de prácticas de gestión de riesgos para ofrecer una seguridad razonable de que las prácticas de gestión de riesgos de TI son apropiadas para asegurarse de que el riesgo de TI actual no sobrepase el apetito al riesgo del consejo de dirección.
	EDM03.03: Monitorizar la gestión de riesgos Monitorizar las metas y las métricas clave de los procesos de gestión de riesgos y establecer cómo las desviaciones o los problemas se identificarán, rastrearán y se informarán para su solución.
EDM04 Asegurar la optimización de recursos	**EDM04.01: Evaluar la gestión de recursos.** Examinar y analizar continuamente la necesidad actual y futura de recursos relacionados con TI, las opciones de recursos (incluyendo estrategias de adquisición), y principios de asignación y gestión para satisfacer las necesidades de la empresa de la manera óptima.
	EDM04.02: Dirigir la gestión de recursos. Asegurar la adopción de principios de gestión de recursos para permitir un uso óptimo de los recursos de TI durante todo su ciclo de vida económica.
	EDM04.03: Monitorizar la gestión de recursos. Monitorizar las metas y las métricas clave de los procesos de gestión de recursos y establecer cómo las desviaciones o los problemas se identificarán, rastrearán y se informarán para su solución.
EDM05 Asegurar la transparencia de las partes interesadas	**EDM05.01: Evaluar los requerimientos de informes a las partes interesadas.** Examinar y analizar continuamente los requerimientos actuales y futuros de comunicación y presentación de informes a las partes interesadas, incluyendo tanto requisitos obligatorios de informes (p. ej., regulatorios) como comunicaciones a otras partes interesadas. Establecer los principios para la comunicación.
	EDM05.02: Dirigir la comunicación y presentación de informes a las partes interesadas. Garantizar el establecimiento de comunicaciones e informes efectivos a las partes interesadas, incluyendo mecanismos para asegurar la calidad y la integridad de la información, la supervisión de los informes obligatorios, y creando una estrategia de comunicación para las partes interesadas.
	EDM05.03: Monitorizar la comunicación con las partes interesadas. Monitorizar la efectividad de la comunicación con las partes interesadas. Evaluar los mecanismos para garantizar la precisión, confiabilidad y efectividad, y evaluar si se están cumpliendo los requerimientos de las diferentes partes interesadas.

Procesar	Práctica de gobierno o gestión de COBIT 5
APO01 Gestionar el marco de gestión de TI	**APO01.01: Definir la estructura organizativa.** Establecer una estructura organizacional interna y extendida que refleje las necesidades del negocio y las prioridades de TI. Establecer las estructuras de gestión requeridas (p. ej., comités) que permitan que la toma de decisiones de gestión se lleve a cabo de la manera más eficaz y eficiente.
	APO01.02: Establecer roles y responsabilidades. Establecer, acordar y comunicar los roles y responsabilidades del personal de TI, así como de otras partes interesadas con responsabilidades de TI de la empresa, que reflejen claramente las necesidades y los objetivos de TI generales del negocio, y la autoridad, responsabilidades y rendición de cuentas del personal relevante.
	APO01.03: Mantener los habilitadores del sistema de gestión. Mantener los habilitadores del sistema de gestión y el entorno de control para las TI empresariales, y asegurarse de que estén integrados y alineados con la filosofía de gobierno y gestión y el estilo operativo de la empresa. Estos habilitadores incluyen la comunicación clara de expectativas/requerimientos. El sistema de gestión debe fomentar la cooperación y el trabajo en equipo entre las divisiones, promover el cumplimiento y la mejora continua, y manejar las desviaciones del proceso (incluyendo los fracasos).
	APO01.04: Comunicar los objetivos y la dirección de la gerencia. Comunicar concientización y comprensión de los objetivos y la dirección de TI a las partes interesadas apropiadas y los usuarios en toda la empresa.
	APO01.05: Optimizar la ubicación de la función de TI. Colocar la capacidad de TI en la estructura organización general para reflejar un modelo empresarial relevante a la importancia de las TI dentro de la empresa, específicamente, su criticidad para la estrategia empresarial y el nivel de dependencia operativa en las TI. La línea jerárquica del CIO debe ser proporcional a la importancia de las TI dentro de la empresa.
	APO01.06: Definir la propiedad de la información (datos) y del sistema. Definir y mantener las responsabilidades de propiedad de información (datos) y sistemas de información. Asegurarse de que los propietarios tomen decisiones acerca de clasificar la información y los sistemas y protegerlos de acuerdo con esta clasificación.
	APO01.07: Gestionar la mejora continua de los procesos. Evaluar, planificar y ejecutar la mejora continua de los procesos y su madurez para garantizar que sean capaces de cumplir con los objetivos empresariales, de gobernanza, gestión y control. Considerar la guía de implementación del proceso COBIT, los estándares emergentes, los requerimientos de cumplimiento, las oportunidades de automatización, y la retroalimentación de los usuarios del proceso, el equipo del proceso y otras partes interesadas. Actualizar el proceso y considerar los impactos en los habilitadores de procesos.
	APO01.08: Mantener el cumplimiento con las políticas y los procedimientos. Implementar procedimientos para mantener el cumplimiento y medir el rendimiento de las políticas y otros habilitadores del marco de control, y hacer cumplir las consecuencias del incumplimiento o desempeño inadecuado. Dar seguimiento a las tendencias y el rendimiento y considerarlos en el futuro diseño y mejora del marco de control.
APO02 Gestionar la estrategia	**APO02.01: Comprender la dirección de la empresa.** Considerar el entorno empresarial actual, así como los procesos de negocio, la estrategia empresarial y los objetivos futuros. También considerar el entorno externo de la empresa (impulsores de la industria, regulaciones relevantes y bases de la competencia).
	APO02.02: Evaluar el entorno, las capacidades y el desempeño actuales. Evaluar el rendimiento de las capacidades internas actuales del negocio y de TI, así como los servicios de TI externos, y desarrollar una comprensión de la arquitectura empresarial en relación con TI. Identificar los problemas que se están experimentando actualmente y desarrollar recomendaciones en áreas que podrían beneficiarse con una mejora. Considerar los diferenciadores y las opciones de proveedores de servicios, y el impacto financiero y los costos y beneficios potenciales de usar servicios externos.
	APO02.03: Definir las capacidades objetivo de TI. Definir las capacidades objetivo del negocio y de TI, así como los servicios de TI requeridos. Esto debe basarse en el entendimiento del entorno y los requerimientos de la empresa; la evaluación de los procesos comerciales actuales y el entorno y los problemas de TI; y considerando los estándares de referencia, las mejores prácticas y las tecnologías emergentes validadas o las propuestas de innovación.
	APO02.04: Llevar a cabo un análisis de brechas. Identificar las brechas entre los entornos actuales y objetivos, y considerar la alineación de los activos (las capacidades que apoyan los servicios) con los resultados del negocio para optimizar la inversión y la utilización de la base de activos internos y externos. Considerar los factores críticos de éxito para apoyar la ejecución de la estrategia.
	APO02.05: Definir el plan estratégico y mapa de ruta. Crear un plan estratégico que defina, en cooperación con las partes interesadas relevantes, cómo las metas relacionadas con TI contribuirán a las metas estratégicas de la empresa. Incluir la manera en que la TI soportará los programas de inversión, procesos empresariales, servicios de TI y activos de TI habilitados por TI. Dirigir al equipo de TI para definir las iniciativas que se necesitarán para cerrar las brechas, la estrategia de aprovisionamiento y las medidas que se usarán para monitorizar el logro de las metas, y después priorizar las iniciativas y combinarlas en una hoja de ruta de alto nivel.
	APO02.06: Comunicar la dirección y estrategia de TI. Crear concientización y comprensión de los objetivos y la dirección del negocio y de TI, tal como se capturaron en la estrategia de TI, mediante la comunicación con las partes interesadas y los usuarios apropiados en toda la empresa.

Procesar	Práctica de gobierno o gestión de COBIT 5
APO03 Gestionar la arquitectura empresarial	**APO03.01: Desarrollar la visión de arquitectura empresarial.** La visión de la arquitectura ofrece una descripción preliminar de alto nivel de la línea de referencia y las arquitecturas objetivo, cubriendo los dominios de negocio, de información, de datos, de aplicación y de tecnología. La visión de la arquitectura ofrece al patrocinador una herramienta clave para promover los beneficios de las capacidades propuestas a las partes interesadas de la empresa. La visión de la arquitectura describe cómo la nueva capacidad cumplirá con las metas y los objetivos empresariales estratégicos, y abordará las preocupaciones de las partes interesadas cuando se implemente.
	APO03.02: Definir la arquitectura de referencia. La arquitectura de referencia describe las arquitecturas actuales y objetivo para los dominios de negocio, información, datos, aplicación y tecnología.
	APO03.03: Seleccionar oportunidades y soluciones. Racionalizar las brechas entre las arquitecturas de referencia y objetivo, tomando tanto las perspectivas de negocio como técnicas, y agruparlas lógicamente en paquetes de trabajo del proyecto. Integrar el proyecto con todos los programas de inversión habilitados por TI relacionados para asegurarse de que las iniciativas arquitectónicas estén alineadas con, y habilitar estas iniciativas como parte de, un cambio empresarial general. Hacer de este un esfuerzo colaborativo con las partes interesadas clave del negocio y de TI para evaluar la disposición de transformación de la empresa, e identificar oportunidades, soluciones y todas las restricciones de implementación.
	APO03.04: Definir la implementación de la arquitectura. Crear un plan de implementación y migración viable alineado con las carteras de programas y proyectos. Asegurar de que el plan esté estrechamente coordinado para garantizar que la entrega de valor y que los recursos necesarios estén disponibles para completar el trabajo necesario.
	APO03.05: Proporcionar servicios de arquitectura empresarial. La prestación de servicios de arquitectura empresarial dentro de la empresa incluye orientación y monitorización de proyectos de implementación, formalización de formas de trabajar a través de contratos de arquitectura y medición y comunicación de la creación de valor agregado y monitorización del cumplimiento.
APO04 Gestionar la innovación	**APO04.01: Crear un entorno favorable a la innovación.** Crear un entorno que propicie la innovación, considerando cuestiones como la cultura, las recompensas, la colaboración, los foros de tecnología y los mecanismos para promover y capturar las ideas de los empleados.
	APO04.02: Mantener un entendimiento del entorno de la empresa. Trabajar con las partes interesadas relevantes para entender sus desafíos. Mantener una comprensión adecuada de la estrategia empresarial y del entorno competitivo o de otras restricciones, de forma que se puedan identificar las oportunidades habilitadas por las nuevas tecnologías.
	APO04.03: Monitorizar y escanear el entorno tecnológico. Monitorizar y escanear sistemáticamente el entorno externo de la empresa para identificar las tecnologías emergentes con el potencial de crear valor (p. ej., ejecutar la estrategia empresarial, optimizar costos, evitar la obsolescencia y habilitar de mejor manera los procesos empresariales y de TI). Monitorizar el mercado, el entorno competitivo, los sectores de la industria y las tendencias legales y regulatorias para poder analizar las tecnologías emergentes o las ideas de innovación en el contexto empresarial.
	APO04.04: Evaluar el potencial de las tecnologías emergentes y las ideas de innovación. Analizar las tecnologías emergentes identificadas y/u otras sugerencias de innovación en TI. Trabajar con las partes interesadas para validar las suposiciones sobre el potencial de nuevas tecnologías e innovación.
	APO04.05: Recomendar iniciativas apropiadas adicionales. Evaluar y monitorizar los resultados de las iniciativas que son prueba de concepto y, si son favorables, generar recomendaciones para promover las iniciativas y obtener el apoyo de las partes interesadas.
	APO04.06: Monitorizar la implementación y el uso de la innovación. Monitorizar la implementación y el uso de las tecnologías emergentes y las innovaciones durante la integración, adopción y todo el ciclo de vida económica para garantizar que se obtengan los beneficios prometidos y para identificar las lecciones aprendidas.

Procesar	Práctica de gobierno o gestión de COBIT 5
APO05 Gestionar la cartera	**APO05.01: Establecer el objetivo de la mezcla de inversión.** Revisar y asegurar que las estrategias y los servicios actuales de la empresa y de TI sean claros. Definir una mezcla de inversiones apropiada con base en el coste, la alineación con la estrategia, y las medidas financieras como el coste y el ROI anticipado durante todo el ciclo de vida económico, el grado de riesgo y el tipo de beneficio para los programas en la cartera. Ajustar las estrategias empresariales y de TI cuando sea necesario.
	APO05.02: Determinar la disponibilidad y las fuentes de fondos. Determinar posibles fuentes de fondos, diferentes opciones de financiamiento y las implicaciones de las fuentes de financiamiento en las expectativas de retorno de inversión.
	APO05.03: Evaluar y seleccionar programas para financiar. Basándose en los requerimientos generales de la mezcla de la cartera de inversión, evaluar y establecer prioridades de los casos de negocio del programa, y tomar decisiones sobre las propuestas de inversión. Asignar fondos e iniciar los programas.
	APO05.04: Monitorizar, optimizar e informar sobre el rendimiento de la cartera de inversión. Monitorizar y optimizar de forma periódica el rendimiento de la cartera de inversión y los programas individuales durante todo el ciclo de vida de las inversiones.
	APO05.05: Mantener las carteras. Mantener las carteras de los programas y proyectos de inversión, servicios de TI y activos de TI.
	APO05.06: Gestionar el logro de beneficios. Monitorizar los beneficios de ofrecer y mantener servicios y capacidades de TI apropiados, con base en el caso de negocio acordado y actual.
APO06 Gestionar el presupuesto y los costos	**APO06.01: Gestión de finanzas y contabilidad.** Establecer y mantener un método para contabilizar todos los costes y la depreciación relacionados con TI como una parte integral de los sistemas financieros de la empresa y crear una tabla para contabilizar y administrar las inversiones y los costes de TI. Capturar y asignar los costes reales, analizar las variaciones entre las previsiones y los costes reales, y realizar informes usando los sistemas de medición financiera de la empresa.
	APO06.02: Establecer prioridades para la asignación de recursos. Implementar un proceso de toma de decisiones para establecer prioridades sobre la asignación de recursos y reglas para las inversiones discrecionales por unidades del negocio individuales. Incluir el posible uso de proveedores de servicios externos y considerar las opciones de compra, desarrollo y alquiler.
	APO06.03: Crear y mantener presupuestos. Preparar un presupuesto que refleje las prioridades de inversión y que apoye los objetivos estratégicos basados en la cartera de programas habilitados por TI y los servicios de TI.
	APO06.04: Modelar y asignar los costes. Establecer y usar un modelo de costes de TI basado en la definición del servicio, asegurando que esta asignación de costes para servicios sea identificable, medible y predecible, para fomentar el uso responsable de los recursos, incluyendo aquellos proporcionados por proveedores de servicios. Revisar y comparar periódicamente la idoneidad del modelo de costes/recargos para mantener su relevancia e idoneidad para las actividades empresariales y de TI en evolución.
	APO06.05: Gestionar los costes. Implementar un proceso de gestión de costes que compare los costes actuales con los presupuestos. Es necesario monitorizar e informar sobre los costes, y en caso de desviaciones, identificarlos de forma oportuna, así como su impacto sobre los procesos empresariales y los servicios analizados.
APO07 Gestionar los recursos humanos	**APO07.01: Mantener una dotación de personal suficiente y adecuada.** Evaluar los requerimientos de personal de forma periódica o ante cambios mayores en los entornos empresariales, operativos o de TI para garantizar que la empresa cuente con suficientes recursos humanos para apoyar las metas y los objetivos empresariales. La dotación de personal incluye tanto los recursos internos como externos.
	APO07.02: Identificar al personal clave de TI. Identificar al personal clave de TI mientras se minimiza la dependencia en una sola persona que realice una función de trabajo crítica a través de la captura de conocimientos (documentación), compartir los conocimientos, planificar la sucesión y tener un respaldo de personal.
	APO07.03: Mantener las habilidades y las competencias del personal. Definir y administrar las habilidades y las competencias del personal necesario. Verificar periódicamente que el personal cuente con las competencias necesarias para realizar sus funciones con base en su educación, capacitación y/o experiencia, y verificar que estas competencias se mantengan usando programas de cualificación y certificación cuando sea apropiado. Dar a los empleados oportunidades de aprendizaje continuas para mantener sus conocimientos, habilidades y competencias al nivel requerido para alcanzar las metas empresariales.

Procesar	Práctica de gobierno o gestión de COBIT 5
APO07 Gestionar los recursos humanos *(cont.)*	**APO07.04: Evaluar el rendimiento laboral de los empleados.** Realizar evaluaciones de rendimiento oportunas de manera periódica de acuerdo con los objetivos individuales derivados de las metas empresariales, los estándares establecidos, las responsabilidades específicas del trabajo, y el marco de habilidades y competencias. Los empleados deben recibir asesoramiento sobre el rendimiento y la conducta cuando sea apropiado.
	APO07.05: Planificar y rastrear el uso de recursos de TI y humanos. Comprender y rastrear la demanda actual y futura de recursos humanos empresariales y de TI con responsabilidades para las TI empresariales. Identificar las carencias y proporcionar comentarios sobre los planes de adquisiciones, y los procesos de reclutamiento empresarial y de TI.
	APO07.06: Gestionar al personal contratado. Asegurar que los consultores y el personal contratado que dan soporte a la empresa con habilidades de TI conozcan y cumplan con las políticas de la organización y con los requerimientos contractuales acordados.
APO08 Gestionar las relaciones	**APO08.01: Entender las expectativas de negocio.** Comprender los problemas y objetivos actuales del negocio, así como las expectativas que se tienen de TI. Asegurarse que se comprendan, gestionen y comuniquen los requerimientos, y que su estado se acepte y apruebe.
	APO08.02: Identificar oportunidades, riesgos y limitaciones para que TI mejore el negocio. Identificar oportunidades potenciales para que TI sea un habilitador del rendimiento empresarial mejorado.
	APO08.03: Gestionar la relación comercial. Gestionar la relación con los clientes (representantes comerciales). Asegurar que las funciones y las responsabilidades de las relaciones se definan y asignen, y que se facilite la comunicación.
	APO08.04: Coordinar y comunicar. Trabajar con las partes interesadas y coordinar la entrega extremo a extremo de los servicios y soluciones de TI que se ofrecen al negocio.
	APO08.05: Proporcionar información para la mejora continua de los servicios. Mejorar y evolucionar continuamente los servicios habilitados por TI, y la entrega de servicios para la empresa, para alinearse con los requerimientos tecnológicos y empresariales cambiantes.
APO09 Gestionar los acuerdos de servicio	**APO09.01: Identificar servicios de TI.** Analizar los requerimientos del negocio y la forma en la que los servicios habilitados por TI y los niveles de servicio apoyan los procesos del negocio. Analizar y acordar los servicios y niveles de servicio potenciales con el negocio, y compararlos con la cartera actual de servicios para identificar opciones nuevas o modificadas de servicios o de nivel de servicio.
	APO09.02: Catalogar los servicios habilitados por TI. Definir y mantener uno o más catálogos de servicios para grupos objetivo relevantes. Publicar y mantener servicios en vivo habilitados por TI en los catálogos de servicios.
	APO09.03: Definir y preparar acuerdos de servicio. Definir y preparar acuerdos de servicio basados en las opciones de los catálogos de servicio. Incluyen acuerdos operativos internos.
	APO09.04: Monitorizar y reportar los niveles de servicio. Monitorizar los niveles de servicio, informar sobre los logros e identificar tendencias. Ofrecer la información gerencial apropiada para ayudar a la gestión del rendimiento.
	APO09.05: Revisar los acuerdos y los contratos de servicio. Realizar revisiones periódicas de los acuerdos de servicio y revisarlos cuando sea necesario.
APO10 Gestionar los proveedores	**APO10.01: Identificar y evaluar los contratos y relaciones con los proveedores.** Identificar proveedores y contratos asociados, y clasificarlos en tipo, importancia y criticidad. Establecer criterios de evaluación para el proveedor y el contrato, y evaluar la cartera general de proveedores y contratos actuales y alternativos.
	APO10.02: Seleccionar proveedores. Seleccionar proveedores de acuerdo a una práctica justa y formal para garantizar el mejor ajuste viable basado en los requerimientos especificados. Los requerimientos deben optimizarse con la participación de los proveedores potenciales.
	APO010.03: Gestionar los contratos y las relaciones con los proveedores. Formalizar y gestionar la relación con el proveedor para cada uno de los proveedores. Gestionar, mantener y supervisar los contratos y la prestación de servicios. Asegurarse de que los contratos nuevos o modificados cumplan con los estándares de la empresa y con los requerimientos legales y regulatorios. Tratar las disputas contractuales.
	APO010.04: Gestionar el riesgo con los proveedores. Identificar y gestionar el riesgo relacionado con los proveedores para proporcionar continuamente una prestación de servicios segura, eficiente y eficaz.
	APO010.05: Monitorizar el rendimiento y el cumplimiento del proveedor. Revisar periódicamente el rendimiento general de los proveedores, el cumplimiento con los requerimientos contractuales, el valor del dinero y abordar los problemas identificados.

Procesar	Práctica de gobierno o gestión de COBIT 5
APO11 Gestionar la calidad	**APO011.01: Establecer un sistema de gestión de calidad (QMS).** Establecer y mantener un QMS que proporciona un enfoque estándar, formal y continuo para la gestión de calidad de la información, habilitando así la tecnología y los procesos del negocio que están alineados con los requerimientos del negocio y la gestión de la calidad empresarial.
	APO011.02: Definir y gestionar los estándares, prácticas y procedimientos de calidad. Identificar y mantener los requerimientos, estándares, procedimientos y prácticas para los procesos clave para guiar a la empresa en alcanzar los QMS acordados. Esto debe estar en línea con los requerimientos del marco de control de TI. Considerar la certificación para los procesos clave, unidades organizacionales, productos o servicios.
	APO011.03: Enfocar la gestión de la calidad en los clientes. Enfocar la gestión de la calidad en los clientes al determinar sus requerimientos y asegurando la alineación con las prácticas de gestión de la calidad.
	APO011.04: Realizar el monitorización, control y revisiones de calidad. Monitorizar la calidad de los procesos y los servicios de forma continua, tal como se define en el QMS. Definir, planificar e implementar medidas para monitorizar la satisfacción del cliente con la calidad, así como con el valor que ofrece el QMS. La información recolectada debe ser utilizada por los propietarios del proceso para mejorar la calidad.
	APO011.05: Integrar la gestión de la calidad a soluciones para el desarrollo y la prestación de servicios. Incorporar prácticas relevantes de gestión de la calidad a la definición, monitorización y gestión continua del desarrollo de soluciones y la oferta de servicios.
	APO011.06: Mantener una mejora continua. Mantener y comunicar periódicamente un plan de calidad general que promueva la mejora continua. Éste debe incluir la necesidad y los beneficios de la mejora continua. Recolectar y analizar datos sobre el QMS y mejorar su efectividad. Corregir los incumplimientos para evitar la recurrencia. Promover una cultura de calidad y mejora continua.
APO12 Gestionar el riesgo	**APO012.01: Recolectar datos.** Identificar y recolectar datos relevantes para habilitar una identificación, análisis y reporte efectivos de los riesgos relacionados con TI.
	APO12.02: Analizar el riesgo Desarrollar información útil para soportar decisiones sobre riesgos que consideran la relevancia para el negocio de los factores de riesgo.
	APO12.03: Mantener un perfil de riesgo. Mantener un inventario de los riesgos conocidos y los atributos de riesgo (incluyendo la frecuencia esperada, el impacto potencial y las respuestas), y de recursos relacionados, capacidades y actividades de control actuales.
	APO12.04: Expresar el riesgo. Proporcionar información sobre el estado actual de las exposiciones y oportunidades relacionadas con TI de manera oportuna a todas las partes interesadas requeridas para obtener una respuesta apropiada.
	APO12.05: Definir un portafolio de acción de gestión de riesgos. Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como una cartera.
	APO12.06: Responder al riesgo. Responder de manera oportuna con medidas eficaces para limitar la magnitud de la pérdida de los eventos relacionados con TI.
APO13 Gestionar la seguridad	**APO013.01: Establecer y mantener un sistema de gestión de seguridad de la información (ISMS).** Establecer y mantener un ISMS que proporcione un enfoque estándar, formal y continuo para la gestión de seguridad de la información, habilitando así la tecnología segura y los procesos del negocio que estén alineados con los requerimientos del negocio y la gestión de la seguridad empresarial.
	APO013.02: Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información. Mantener un plan de seguridad de la información que describe cómo se deben manejar los riesgos de seguridad de la información y cómo se debe alinear con la estrategia y la arquitectura empresariales. Asegurarse de que las recomendaciones para implementar mejoras a la seguridad se basen en casos de negocio aprobados e implementados como una parte integral del desarrollo de servicios y soluciones, y que después se operen como una parte integral de la operación del negocio.
	APO013.03: Monitorizar y revisar el ISMS. Mantener y comunicar periódicamente la necesidad y los beneficios de una mejora continua de seguridad de la información. Recolectar y analizar datos sobre el ISMS, y mejorar la efectividad del ISMS. Corregir los incumplimientos para evitar la recurrencia. Promover una cultura de seguridad y mejora continua.

Procesar	Práctica de gobierno o gestión de COBIT 5
BAI01 Gestionar programas y proyectos	**BAI01.01: Mantener un enfoque estándar para la gestión de programas y proyectos.** Mantener un enfoque estándar para la gestión de programas y proyectos que permita la evaluación del gobierno y la gestión, así como las actividades de gestión de toma de decisiones y de entrega, enfocadas en el logro de valor y de las metas (requerimientos, riesgos, costes, calendario, calidad) para el negocio de forma consistente.
	BAI01.02: Iniciar un programa. Iniciar un programa para confirmar los beneficios esperados y obtener la autorización para proceder. Esto incluye acordar el apoyo a los programas, confirmar el mandato del programa mediante la aprobación del caso de negocio conceptual, asignando una junta directiva o un comité para el programa, produciendo el resumen del programa, revisando y actualizando el caso comercial, desarrollando un plan de objetivos de beneficios y obteniendo la aprobación de los patrocinadores para proceder.
	BAI01.03: Gestionar la participación de las partes interesadas. Gestionar la participación de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna que llegue a todas las partes interesadas relevantes. Esto incluye planificar, identificar e involucrar a las partes interesadas y gestionar sus expectativas.
	BAI01.04: Desarrollar y mantener el plan del programa. Formular un programa que establezca las bases iniciales y una posición para la ejecución exitosa al formalizar el alcance del trabajo que debe alcanzarse, e identificar los entregables que satisfarán las metas y producirán valor. Mantener y actualizar el plan del programa y el caso de negocio durante todo el ciclo de vida económica del programa, asegurando la alineación con los objetivos estratégicos y reflejando el estado actual y la información actualizada que se obtiene diariamente.
	BAI01.05: Lanzar y ejecutar el programa. Lanzar y ejecutar el programa para adquirir y dirigir los recursos necesarios para lograr las metas y beneficios del programa tal como se define en el plan del programa. De acuerdo con los criterios de revisión de aprobación o publicación, prepararse para las revisiones de aprobación, iteración o publicación para informar sobre el avance del programa y poder presentar argumentos para la financiación hasta la siguiente revisión de aprobación o publicación.
	BAI01.06: Monitorizar, controlar e informar sobre los resultados del programa. Monitorizar y controlar el programa (entrega de la solución) y el rendimiento de la empresa (valor/resultado) en comparación con el plan durante todo el ciclo de vida económica de la inversión. Informar sobre este rendimiento al Comité de Dirección del programa y a los patrocinadores.
	BAI01.07: Establecer e iniciar proyectos dentro de un programa. Definir y documentar la naturaleza y el alcance del proyecto para confirmar y desarrollar con las partes interesadas un entendimiento común del alcance del proyecto y cómo se relaciona con otros proyectos dentro del programa general de inversiones habilitadas para TI. La definición debe ser aprobada formalmente por los patrocinadores del programa y el proyecto.
	BAI01.08: Planificar proyectos. Establecer y mantener un plan de proyecto formal, integrado y aprobado (que cubra los recursos del negocio y de TI) para guiar la ejecución y el control del proyecto durante la vida útil del proyecto. El alcance de los proyectos debe definirse claramente y vincularse al desarrollo o mejora de las capacidades del negocio.
	BAI01.09: Gestionar programas y proyectos de calidad. Preparar y ejecutar un plan de gestión de la calidad, procesos y prácticas, alineadas con el QMS que describe el programa y el enfoque de calidad hacia el proyecto y cómo se implementará. Todas las partes relevantes deben evaluar y aceptar formalmente el plan, y después deben incorporarse al programa integrado y a los planes del proyecto.
	BAI01.10: Gestionar el programa y el riesgo del proyecto. Eliminar o minimizar el riesgo específico asociado con los programas y proyectos mediante un proceso sistemático de planificación, identificación, análisis, respuesta y monitorización, y controlando las áreas o eventos que tienen el potencial de ocasionar un cambio no deseado. Establecer y registrar centralmente el riesgo al que se enfrenta el programa y el proyecto.
	BAI01.11: Monitorizar y controlar proyectos. Medir el rendimiento del proyecto en comparación con los criterios clave de rendimiento del proyecto, como el calendario, la calidad, el coste y el riesgo. Identificar las desviaciones de las expectativas. Evaluar el impacto de las desviaciones en el proyecto y en el programa general, y reportar los resultados a las partes interesadas clave.
	BAI01.12: Gestionar los recursos del proyecto y los paquetes de trabajo. Gestionar los paquetes de trabajo del proyecto estableciendo requerimientos formales para autorizar y aceptar paquetes de trabajo, y asignando y coordinando los recursos del negocio y de TI apropiados.
	BAI01.13: Cerrar un proyecto o iteración. Al final de cada proyecto, liberación o iteración, requerir a las partes interesadas del proyecto que determinen si el proyecto, liberación o iteración han dado los resultados y el valor previstos. Identificar y comunicar las actividades pendientes necesarias para lograr los resultados del proyecto y los beneficios del programa previstos, e identificar y documentar las lecciones aprendidas para su uso en futuros proyectos, lanzamientos, iteraciones y programas.
	BAI01.14: Cerrar un programa. Retirar el programa de la cartera de inversiones activas cuando exista el acuerdo de que se ha alcanzado el valor deseado o cuando está claro que no se alcanzará dentro de los criterios de valor establecidos para el programa.

Procesar	Práctica de gobierno o gestión de COBIT 5
BAI02 Gestionar la definición de requerimientos	**BAI02.01: Definir y mantener los requerimientos funcionales y técnicos del negocio.** Basándose en el caso de negocio, identificar, priorizar, especificar y acordar los requerimientos de información de negocio, funcionales, técnicos y de control que cubren el alcance/la comprensión de todas las iniciativas necesarias para lograr los resultados esperados de la solución empresarial habilitada para TI propuesta.
	BAI02.02: Realizar un estudio de viabilidad y formular soluciones alternativas. Realizar un estudio de viabilidad de posibles soluciones alternativas, evaluar su viabilidad y seleccionar la opción preferida. Si es apropiado, implementar la opción seleccionada como piloto para determinar posibles mejoras.
	BAI02.03: Gestionar el riesgo de los requerimientos. Identificar, documentar, priorizar y mitigar el riesgo funcional, técnico y de procesamiento de la información asociado con los requerimientos empresariales y la solución propuesta.
	BAI02.04: Obtener la aprobación de requerimientos y soluciones. Coordinar la retroalimentación de las partes interesadas afectadas y, en etapas clave predeterminadas, obtener la aprobación y la autorización del patrocinador del negocio o del propietario del producto de los requerimientos funcionales y técnicos, estudios de viabilidad, análisis de riesgos y soluciones recomendadas.
BAI03 Gestionar la identificación y creación de soluciones	**BAI03.01: Diseño de soluciones de alto nivel.** Desarrollar y documentar diseños de alto nivel usando técnicas acordadas de desarrollo con las etapas apropiadas o técnicas ágiles y rápidas. Asegurar la alineación con la estrategia de TI y la arquitectura empresarial. Volver a evaluar y actualizar los diseños cuando se presenten problemas significativos durante las fases de diseño detallado o construcción, o conforme evoluciona la solución. Asegurarse de que las partes interesadas participen activamente en el diseño y la aprobación de cada versión.
	BAI03.02: Diseñar componentes detallados para la solución. Desarrollar, documentar y elaborar diseños detallados progresivamente usando técnicas acordadas de desarrollo ágiles y rápidas, o técnicas con las fases apropiadas, abordando todos los componentes (procesos de negocio y controles automatizados y manuales relacionados, apoyando las aplicaciones de TI, los servicios de infraestructura y los productos de tecnología, así como a los socios/proveedores). Asegurarse de que el diseño detallado incluya los SLA y OLA internos y externos.
	BAI03.03: Desarrollar los componentes de la solución. Desarrollar progresivamente los componentes de la solución de acuerdo con los diseños detallados siguiendo métodos de desarrollo y estándares de documentación, requerimientos de aseguramiento de calidad (QA) y estándares de aprobación. Asegurarse que se aborden todos los requerimientos de control en los procesos de negocio, apoyando las aplicaciones de TI y los servicios de infraestructura, los servicios y productos de tecnología, y los socios/proveedores.
	BAI03.04: Obtener los componentes de la solución. Adquirir componentes de la solución basados en el plan de adquisiciones de acuerdo con los requerimientos y los diseños detallados, los principios y estándares de la arquitectura, y los procedimientos generales de adquisiciones y contratos de la empresa, requerimientos de QA y estándares de aprobación. Asegurarse de que el proveedor identifique y aborde todos los requerimientos legales y contractuales.
	BAI03.05: Construir soluciones. Instalar y configurar las soluciones e integrarlas con las actividades de los procesos de negocio. Implementar medidas de control, seguridad y auditabilidad durante la configuración, y durante la integración del hardware y el software de infraestructura, para proteger los recursos y asegurar la disponibilidad y la integridad de los datos. Actualizar el catálogo de servicios para reflejar las soluciones nuevas.
	BAI03.06: Realizar el aseguramiento de calidad (QA). Desarrollar, aprovisionar y ejecutar un plan de QA alineado con el QMS para obtener la calidad especificada en la definición de los requerimientos y las políticas y procedimientos de calidad de la empresa.
	BAI03.07: Prepararse para las pruebas de la solución. Establecer un plan de pruebas y los entornos requeridos para probar los componentes de la solución individuales e integrados, incluyendo los procesos de negocio, y los servicios, las aplicaciones y la infraestructura de soporte.
	BAI03.08: Ejecutar pruebas de la solución. Ejecutar pruebas continuamente durante el desarrollo, incluyendo pruebas de control, de acuerdo con el plan de pruebas definido y las prácticas de desarrollo en el entorno apropiado. Incluir a los propietarios de los procesos de negocio y a los usuarios finales en el equipo de pruebas. Identificar, registrar y priorizar los errores y los problemas que se identificaron durante las pruebas.
	BAI03.09: Gestionar los cambios de los requerimientos. Rastrear el estado de requerimientos individuales (incluyendo todos los requerimientos rechazados) durante el ciclo de vida del proyecto, y gestionar la aprobación de cambios de los requerimientos.
	BAI03.10: Mantener soluciones. Desarrollar y ejecutar un plan para el mantenimiento de los componentes de la solución y la infraestructura. Incluir revisiones periódicas en comparación con las necesidades del negocio y los requerimientos operativos.
	BAI03.11: Definir servicios de TI y mantener la cartera de servicios. Definir y acordar las opciones nuevas o modificadas de servicios de TI o de nivel de servicio. Documentar las definiciones de servicio y las opciones de nivel de servicio nuevas o modificadas en la cartera de servicios.

Procesar	Práctica de gobierno o gestión de COBIT 5
BAI04 Gestionar la disponibilidad y capacidad	**BAI04.01: Evaluar la disponibilidad, el rendimiento y la capacidad actuales, y crear una línea de referencia.** Evaluar la disponibilidad, el rendimiento y la capacidad de servicios y recursos para asegurarse de que exista una capacidad y rendimiento con un coste justificable disponibles para dar apoyo a las necesidades del negocio y que cumplan con los SLA. Crear líneas de referencia de disponibilidad, rendimiento y capacidad para la comparación en el futuro.
	BAI04.02: Evaluar el impacto en el negocio. Identificar servicios importantes para la empresa, asignar servicios y recursos a los procesos de negocio, e identificar dependencias comerciales. Asegurarse de que el impacto de los recursos no disponibles sea totalmente acordado y aceptado por el cliente. Asegurarse de que, para funciones del negocio vitales, se puedan satisfacer los requisitos de disponibilidad de los SLA.
	BAI04.03: Planificar los requerimientos de los servicios nuevos o modificados. Planificar y priorizar las implicaciones de disponibilidad, rendimiento y capacidad de las necesidades cambiantes del negocio y los requisitos de servicio.
	BAI04.04: Monitorizar y revisar la disponibilidad y capacidad. Monitorizar, medir, analizar, reportar y revisar la disponibilidad, rendimiento y capacidad. Identificar desviaciones de las líneas de referencia establecidas. Revisar los reportes de análisis de tendencias que identifican problemas y variaciones significativos, iniciando acciones cuando sea necesario, y asegurándose que se le dé seguimiento a todos los problemas pendientes.
	BAI04.05: Investigar y abordar las cuestiones de disponibilidad, rendimiento y capacidad. Abordar las desviaciones al investigar y resolver los problemas de disponibilidad, rendimiento y capacidad identificados.
BAI05 Gestionar la habilitación del cambio organizacional	**BAI05.01: Establecer el deseo de cambiar.** Comprender el alcance y el impacto del cambio concebido y la preparación/voluntad de las partes interesadas para el cambio. Identificar acciones que motiven a las partes interesadas a aceptar y querer que el cambio funcione exitosamente.
	BAI05.02: Formar un equipo de implementación eficaz. Establecer un equipo de implementación eficaz reuniendo a los miembros apropiados, generando confianza y estableciendo los objetivos comunes y las medidas de eficacia.
	BAI05.03: Comunicar la visión deseada. Comunicar la visión deseada para el cambio en el idioma de los afectados por el mismo. La alta gerencia debe realizar la comunicación, y debe incluir la justificación y los beneficios del cambio, los impactos de no hacer el cambio, así como la visión, la hoja de ruta y la participación necesaria de las distintas partes interesadas.
	BAI05.04: Empoderar a los participantes e identificar las victorias a corto plazo. Empoderar a aquellos con roles de implementación al asegurarse de que sus responsabilidades sean asignadas, se les proporcione capacitación, y al alinearse a las estructuras organizacionales y los procesos de RR.HH. Identificar y comunicar las victorias a corto plazo que pueden alcanzarse y que son importantes desde la perspectiva de habilitar cambios.
	BAI05.05: Habilitar las operaciones y el uso. Planificar e implementar todos los aspectos técnicos, operativos y de uso, de forma que todas las personas involucradas en el futuro estado del entorno puedan ejercer sus responsabilidades.
	BAI05.06: Incorporar nuevos enfoques. Integrar nuevos enfoques rastreando los cambios implementados, evaluando la efectividad de la operación y el plan de uso, y mantener una concientización constante mediante una comunicación regular. Tomar las medidas correctivas que sean apropiadas, las cuales pueden incluir la obligación al cumplimiento.
	BAI05.07: Mantener los cambios. Mantener los cambios mediante una capacitación efectiva del nuevo personal, campañas continuas de comunicación, compromiso permanente de la alta gerencia, monitorización de la adopción y compartir las lecciones aprendidas en toda la empresa.
BAI06 Gestionar los cambios	**BAI06.01: Evaluar, priorizar y autorizar solicitudes de cambio.** Evaluar todas las solicitudes de cambio para determinar el impacto en los procesos de negocio y servicios de TI; y evaluar si el cambio afectará negativamente al entorno operativo y presentará riesgos inaceptables. Asegurarse de que los cambios se registren, prioricen, categoricen, evalúen, autoricen, planifiquen y programen.
	BAI06.02: Gestionar cambios de emergencia. Gestionar cuidadosamente los cambios de emergencia para minimizar futuros incidentes y asegurarse de que el cambio esté controlado y se realice de forma segura. Verificar que los cambios de emergencia sean evaluados adecuadamente y autorizados después del cambio.
	BAI06.03: Rastrear y reportar el estado de los cambios. Mantener un sistema de rastreo y reportes para documentar los cambios rechazados, comunicar el estado de los cambios aprobados y en proceso, y los cambios finalizados. Asegurarse de que los cambios aprobados se implementen según lo previsto.
	BAI06.04: Cerrar y documentar los cambios. Siempre que se implementen cambios, actualizar acordemente la documentación de la solución y del usuario, así como los procedimientos afectados por el cambio.

Procesar	Práctica de gobierno o gestión de COBIT 5
BAI07 Gestionar la aceptación de cambios y la transición	**BAI07.01: Establecer un plan de implementación.** Establecer un plan de implementación que cubra la conversión de sistemas y datos, los criterios de pruebas de aceptación, la comunicación, la capacitación, la preparación de lanzamientos, la promoción a producción, el apoyo a la producción temprana, un plan de respaldo/ abandono, y una revisión postimplementación. Obtener la aprobación de las partes relevantes.
	BAI07.02: Planificar la conversión de procesos del negocio, sistemas y datos. Prepararse para la migración de los procesos del negocio, los datos de servicios de TI y la infraestructura como parte de los métodos de desarrollo empresariales, incluyendo pistas de auditoría y un plan de recuperación si la migración falla.
	BAI07.03: Pruebas de aceptación del plan. Establecer un plan de pruebas basado en estándares de toda la empresa que definen roles, responsabilidades y criterios de entrada y salida. Asegurarse de que el plan sea aprobado por las partes relevantes.
	BAI07.04: Establecer un entorno de pruebas. Definir y establecer un entorno de pruebas seguro y representativo del entorno planificado para el proceso de negocio y las operaciones de TI, el rendimiento y la capacidad, la seguridad, los controles internos, las prácticas operativas, los requerimientos de calidad y privacidad de datos, y las cargas de trabajo.
	BAI07.05: Realizar pruebas de aceptación. Probar los cambios de forma independiente de acuerdo con el plan de prueba definido antes de la migración al entorno operativo en vivo.
	BAI07.06: Pasar a producción y gestionar los lanzamientos. Promover la solución aceptada al negocio y las operaciones. Cuando sea apropiado, ejecutar la solución como una implementación piloto o en paralelo con la solución antigua durante un período definido y comparar el comportamiento y los resultados. Si se producen problemas significativos, volver al entorno original basándose en el plan de respaldo/retiro. Gestionar los lanzamientos de los componentes de la solución.
	BAI07.07: Realizar una revisión post-implementación. Proporcionar apoyo temprano a los usuarios y las operaciones de TI por un período de tiempo acordado para abordar los problemas y ayudar a estabilizar la nueva solución.
	BAI07.08: Proporcionar apoyo a la producción temprana. Realizar una revisión postimplementación para confirmar los resultados, identificar las lecciones aprendidas y desarrollar un plan de acción. Evaluar y verificar el rendimiento y los resultados reales del servicio nuevo o cambiado, en comparación con el rendimiento y los resultados previstos (el servicio esperado por el usuario o el cliente).
BAI08 Gestionar el conocimiento	**BAI08.01: Fomentar y facilitar una cultura de intercambio de conocimientos.** Idear e implementar un esquema para fomentar y facilitar una cultura de intercambio de conocimientos.
	BAI08.02: Identificar y clasificar las fuentes de información. Identificar, validar y clasificar diversas fuentes de información interna y externa requeridas para permitir el uso y la operación eficientes de los procesos de negocio y de los servicios de TI.
	BAI08.03: Organizar y contextualizar la información en conocimiento. Organizar información basándose en criterios de clasificación. Identificar y crear relaciones significativas entre los elementos de información y permitir el uso de la información. Identificar a los propietarios y definir e implementar niveles de acceso a los recursos de conocimiento.
	BAI08.04: Utilizar y compartir conocimientos. Transmitir los recursos de conocimiento disponibles a las partes interesadas relevantes, y comunicar cómo estos recursos pueden utilizarse para abordar diferentes necesidades (p. ej., resolución de problemas, aprendizaje, planificación estratégica y toma de decisiones).
	BAI08.05: Evaluar y retirar la información. Medir el uso y evaluar la popularidad y relevancia de la información. Retirar la información obsoleta.
BAI09 Gestionar los activos	**BAI09.01: Identificar y registrar los activos actuales.** Mantener un registro actualizado y preciso de todos los activos de TI requeridos para entregar servicios y garantizar la alineación con la gestión de configuración y la gestión financiera.
	BAI09.02: Gestionar activos críticos. Identificar activos críticos para la provisión de la capacidad de servicio, y tomar acciones para maximizar su confiabilidad y disponibilidad para soportar las necesidades del negocio.
	BAI09.03: Gestionar el ciclo de vida del activo. Gestionar los activos, desde la adquisición hasta su eliminación, para que éstos se usen con la mayor eficacia y eficiencia como sea posible, y se puedan contabilizar y proteger físicamente.
	BAI09.04: Optimizar los costes de los activos. Revisar periódicamente la base de activos global para identificar maneras de optimizar los costos y mantener la alineación con las necesidades del negocio.
	BAI09.05: Gestionar licencias. Gestionar licencias de software de modo que se mantenga el número óptimo de licencias para soportar los requerimientos del negocio, y que el número de licencias poseídas sea suficiente para cubrir el software instalado en uso.

Procesar	Práctica de gobierno o gestión de COBIT 5
BAI10 Gestionar la configuración	**BAI10.01: Establecer y mantener un modelo de configuración.** Establecer y mantener un modelo lógico de servicios, activos e infraestructura, y cómo registrar los elementos de configuración (CI) y la relación entre éstos. Incluir los CI que se consideran necesarios para gestionar los servicios de forma efectiva y proporcionar una descripción confiable única de los activos en un servicio.
	BAI10.02: Establecer y mantener un repositorio de configuración y una línea de referencia. Establecer y mantener un repositorio de gestión de la configuración y crear líneas de referencias controladas de la configuración.
	BAI10.03: Mantener y controlar los elementos de configuración. Mantener un repositorio actualizado de los elementos de configuración completándolo con cambios.
	BAI10.04: Generar informes del estado y de la configuración. Definir y generar informes de configuración sobre los cambios de estado de los elementos de configuración.
	BAI10.05: Verificar y revisar la integridad del repositorio de configuración. Revisar periódicamente el repositorio de configuración y verificar su integridad y precisión en comparación con la meta deseada.
DSS01 Gestionar las operaciones	**DSS01.01: Realizar procedimientos operativos.** Mantener y realizar procedimientos operativos y tareas operativas de forma confiable y consistente.
	BAI01.02: Gestionar servicios subcontratados de TI. Gestionar la operación de los servicios de TI subcontratados para mantener la protección de la información empresarial y la confiabilidad de la provisión del servicio.
	DSS01.03: Monitorizar la infraestructura de TI. Monitorizar la infraestructura de TI y los eventos relacionados. Almacenar suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examinación de las secuencias temporales de las operaciones y de las otras actividades que rodean o apoyan las operaciones.
	DSS01.04: Gestionar el ambiente. Mantener medidas de protección contra los factores ambientales. Instalar equipo y dispositivos especializados para monitorizar y controlar el ambiente.
	DSS01.05: Gestionar las instalaciones. Gestionar las instalaciones, incluyendo el equipo de suministro eléctrico y comunicaciones, en línea con las leyes y regulaciones, los requerimientos técnicos y del negocio, las especificaciones del proveedor, y las pautas de salud y seguridad.
DSS02 Gestionar las solicitudes e incidentes de servicio	**DSS02.01: Definir esquemas de clasificación de incidentes y solicitudes de servicio.** Definir esquemas de clasificación de incidentes y solicitudes de servicio.
	DSS02.02: Registrar, clasificar y priorizar las peticiones y los incidentes. Identificar, registrar y clasificar las peticiones de servicio y los incidentes, y asignar una prioridad con base en los acuerdos de servicio críticos para el negocio.
	DSS02.03: Verificar, aprobar y resolver peticiones de servicio. Seleccionar los procedimientos apropiados para peticiones, y verificar que las solicitudes de servicio cumplan con los criterios de solicitud definidos. Obtener aprobación, si se requiere, y cumplir con las peticiones .
	DSS02.04: Investigar, diagnosticar y asignar incidentes. Identificar y registrar los síntomas de los incidentes, determinar las causas posibles y asignarlos para su resolución.
	DSS02.05: Resolver y recuperarse de los incidentes. Documentar, aplicar y probar las soluciones o remedios identificados, y realizar acciones de recuperación para restaurar el servicio relacionado con TI.
	DSS02.06: Gestionar las peticiones e incidentes de servicio. Verificar una satisfactoria resolución del incidente y/o finalización de la petición, y cerrar.
	DSS02.07: Rastrear el estado y producir informes. Rastrear, analizar e informar regularmente sobre las tendencias de incidentes y cumplimiento de las peticiones para proporcionar información para una mejora continua.
DSS03 Gestionar los problemas	**DSS03.01: Identificar y clasificar los problemas.** Definir e implementar criterios y procedimientos para reportar los problemas identificados, incluyendo la clasificación, categorización y priorización del problema.
	DSS03.02: Investigar y diagnosticar problemas. Investigar y diagnosticar problemas usando a expertos en la materia para evaluar y analizar las causas raíz.
	DSS03.03: Presentar los errores conocidos. Tan pronto como se identifiquen las causas raíz de los problemas, crear registros de los problemas conocidos y una solución apropiada, e identificar soluciones potenciales.
	DSS03.04: Resolver y cerrar los problemas. Identificar e iniciar soluciones sostenibles que aborden la causa raíz, presentando solicitudes de cambio a través del proceso de gestión de cambios establecido si se requiere para resolver los errores. Asegurarse de que el personal afectado sea consciente de las acciones que se tomaron y de los planes desarrollados para evitar que ocurran incidentes en el futuro.
	DSS03.05: Realizar una gestión proactiva de los problemas. Recolectar y analizar datos operacionales (especialmente los registros de incidentes y de cambios) para identificar las tendencias emergentes que puedan indicar problemas. Registrar los expedientes de los problemas para permitir su evaluación.

Procesar	Práctica de gobierno o gestión de COBIT 5
DSS04 Gestionar la continuidad	**DSS04.01: Definir la política de continuidad del negocio, los objetivos y el alcance.** Definir la política de continuidad del negocio y el alcance alineado con los objetivos de la empresa y de las partes interesadas.
	DSS04.02: Mantener una estrategia de continuidad. Evaluar las opciones de gestión de continuidad del negocio, y elegir una estrategia de continuidad viable y rentable para asegurar la recuperación y la continuidad de la empresa ante un desastre u otro incidente o interrupción mayor.
	DSS04.03: Desarrollar e implementar una respuesta de continuidad del negocio. Desarrollar un plan de continuidad del negocio (BCP) basado en la estrategia que documente los procedimientos y la información en preparación para su uso en un incidente con el fin de permitir que la empresa continúe con sus actividades críticas.
	DSS04.04: Ejercitar, probar y revisar el BCP. Probar los arreglos de continuidad de forma periódica para ejercitar los planes de recuperación ante resultados predeterminados, para permitir que se desarrollen soluciones innovadoras, y para ayudar a verificar a través del tiempo que el plan funcionará tal como está previsto.
	DSS04.05: Revisar, mantener y mejorar el plan de continuidad. Realizar, en intervalos regulares, una revisión gerencial de la capacidad de continuidad para asegurarse de que su idoneidad, propiedad y efectividad sean continuas. Gestionar los cambios al plan de acuerdo con el proceso de control de cambios para asegurarse de que el plan de continuidad se mantenga actualizado y que refleje continuamente los requerimientos del negocio actuales.
	DSS04.06: Realizar una capacitación en el plan de continuidad. Proporcionar sesiones de capacitación periódicas a todas las partes internas y externas involucradas sobre los procedimientos y sus funciones y responsabilidades en caso de una interrupción.
	DSS04.07: Administrar los arreglos de respaldo. Mantener la disponibilidad de la información crítica para el negocio.
	DSS04.08: Realizar revisiones después de la reanudación. Evaluar la idoneidad del BCP tras la reanudación exitosa de los procesos y servicios del negocio después de una interrupción.
DSS05 Gestionar los servicios de seguridad	**DSS05.01: Proteger contra malware.** Implementar y mantener medidas de prevención, detección y corrección (especialmente parches de seguridad y control de virus actualizados) en toda la empresa para proteger los sistemas de información y la tecnología contra malware (p. ej., virus, gusanos, spyware, spam).
	DSS05.02: Gestionar la seguridad de la red y las conexiones. Usar medidas de seguridad y procedimientos de gestión relacionados para proteger la información a través de todos los métodos de conectividad.
	DSS05.03: Gestionar la seguridad de los terminales. Asegurarse de que los terminales (p. ej., laptop, computadora de escritorio, servidor y otros dispositivos o software móviles o de red) estén asegurados a un nivel igual o superior al de los requerimientos de seguridad definidos para la información procesada, almacenada o transmitida.
	DSS05.04: Gestionar la identidad del usuario y el acceso lógico. Asegurarse de que todos los usuarios tengan derechos de acceso a la información de acuerdo con sus requerimientos del negocio, y que haya coordinación con las unidades del negocio que gestionan sus propios derechos de acceso en los procesos de negocio.
	DSS05.05: Gestionar el acceso físico a los activos de TI. Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a las instalaciones, edificios y áreas debe justificarse, autorizarse, registrarse y monitorizarse. Esto debe aplicarse a todas las personas que entren en las instalaciones, incluyendo personal, personal temporal, clientes, proveedores, visitantes y cualquier otro tercero.
	DSS05.06: Gestionar documentos sensibles y dispositivos de salida. Establecer protecciones físicas apropiadas, prácticas de contabilización y gestión de inventario para activos de TI sensibles, como formularios especiales, instrumentos negociables, impresoras para fines especiales o tokens de seguridad.
	DSS05.07: Monitorizar la infraestructura para detectar eventos relacionados con la seguridad. Usar herramientas de detección de intrusos, monitorizar la infraestructura para detectar accesos no autorizados y asegurarse de que cualquier evento se integre a la monitorización general de eventos y a la gestión de incidentes.

Procesar	Práctica de gobierno o gestión de COBIT 5
DSS06 Gestionar los controles de procesos de negocio	**DSS06.01: Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales.** Evaluar y monitorizar continuamente la ejecución de las actividades de los procesos de negocio y los controles relacionados, basándose en el riesgo empresarial, para asegurarse de que los controles de procesamiento estén alineados con las necesidades del negocio.
	DSS06.02: Controlar el procesamiento de información. Operar la ejecución de las actividades de los procesos de negocio y los controles relacionados, basándose en el riesgo empresarial, para garantizar que el procesamiento de información sea válido, completo, preciso, oportuno y seguro (p. ej., refleja el uso comercial legítimo y autorizado).
	DSS06.03: Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización. Gestionar las funciones del negocio, responsabilidades, niveles de autoridad y segregación de funciones necesarias para apoyar los objetivos de proceso del negocio. Autorizar el acceso a cualquier activo de información relacionado con los procesos de información del negocio, incluyendo aquellos bajo custodia del negocio, TI y terceros. Esto asegura que la empresa sepa dónde están los datos y quién está manejando los datos en su nombre.
	DSS06.04: Gestionar errores y excepciones. Gestionar las excepciones y los errores del proceso de negocio, y facilitar su corrección. Incluir el escalamiento de los errores del proceso de negocio, las excepciones y la ejecución de las acciones correctivas definidas. Esto ofrece una garantía de la precisión e integridad de los procesos de información del negocio.
	DSS06.05: Asegurar la trazabilidad de los eventos de información y la rendición de cuentas. Asegurarse que la información del negocio pueda rastrearse hasta el evento del negocio que la originó y a las partes responsables. Esto permite la trazabilidad de la información durante su ciclo de vida y los procesos relacionados. Esto ofrece la seguridad de que la información que impulsa al negocio es confiable y que se ha procesado de acuerdo con objetivos definidos.
	DSS06.06: Asegurar los activos de información. Asegurar los activos de información a los que tiene acceso el negocio a través de métodos aprobados, incluyendo información en formato electrónico (como métodos que crean nuevos activos en cualquier forma, dispositivos de medios portátiles, aplicaciones de usuario y dispositivos de almacenamiento), información en forma física (como documentos originales o informes de salida) e información en tránsito. Esto beneficia al negocio al ofrecer una protección de extremo a extremo para la información.
MEA01 Monitorizar, evaluar y valorar el desempeño y la conformidad	**MEA01.01: Establecer un enfoque de monitorización.** Involucrar a las partes interesadas para establecer y mantener un enfoque de monitorización para definir los objetivos, el alcance y el método para medir la solución del negocio, la entrega de servicios y la contribución a los objetivos de la empresa. Integrar este enfoque con el sistema de gestión de desempeño corporativo.
	MEA01.02: Establecer los objetivos de rendimiento y cumplimiento. Trabajar con las partes interesadas para definir, revisar periódicamente, actualizar y aprobar los objetivos de rendimiento y cumplimiento dentro del sistema de medición de desempeño.
	MEA01.03: Recolectar y procesar los datos de rendimiento y cumplimiento. Recolectar y procesar datos oportunos y precisos alineados con los enfoques de la empresa.
	MEA01.04: Analizar y reportar sobre el rendimiento. Revisar y reportar periódicamente sobre el rendimiento en comparación con los objetivos, usando un método que ofrezca una visión sucinta y completa del rendimiento de TI y que se adapte al sistema de monitorización de la empresa.
	MEA01.05: Asegurar la implementación de acciones correctivas. Ayudar a las partes interesadas a identificar, iniciar y rastrear las acciones correctivas para abordar las anomalías.

Procesar	Práctica de gobierno o gestión de COBIT 5
MEA02 Monitorizar, evaluar y valorar el sistema de control interno	**MEA02.01: Monitorizar los controles internos.** Monitorizar, comparar y mejorar continuamente el entorno de control de TI y el marco de control para alcanzar los objetivos organizacionales.
	MEA02.02: Revisar la eficacia de los controles del proceso de negocio. Revisar la operación de los controles, incluyendo una revisión de la monitorización y la evidencia de las pruebas, para asegurarse de que los controles en los procesos del negocio operen de forma efectiva. Incluir actividades para mantener evidencia de la operación efectiva de los controles a través de mecanismos como pruebas periódicas de los controles, monitorización continua de los controles, evaluaciones independientes, centros de comando y control, y centros de operaciones de la red. Esto le da al negocio seguridad sobre la efectividad de los controles para cumplir con los requerimientos relacionados con las responsabilidades comerciales, regulatorias y sociales.
	MEA02.03: Realizar autoevaluaciones de control. Recomendar a la gerencia y a los propietarios de los procesos que asuman una propiedad positiva de la mejora del control a través de un programa continuo de autoevaluación para evaluar la integridad y la efectividad del control de la gestión sobre los procesos, políticas y contratos.
	MEA02.04: Identificar y comunicar las deficiencias de control. Identificar las deficiencias de control y analizar e identificar su causa raíz subyacente. Escalar las deficiencias de control e informar a las partes interesadas.
	MEA02.05: Asegurar que los proveedores de aseguramiento sean independientes y estén calificados. Asegurar que las entidades que realizan el aseguramiento sean independientes de la función, grupos u organizaciones en el alcance. Las entidades que realizan el aseguramiento deben demostrar una actitud y apariencia apropiadas, competencia en las habilidades y el conocimiento necesario para realizar el aseguramiento, y apegarse a los códigos de ética y a los estándares profesionales.
	MEA02.06: Planificar las iniciativas de aseguramiento. Planificar iniciativas de aseguramiento basadas en los objetivos del negocio y en las prioridades estratégicas, el riesgo inherente, las restricciones de recursos y un conocimiento suficiente de la empresa.
	MEA02.07: Alcance de las iniciativas de aseguramiento. Definir y acordar con la gerencia el alcance de la iniciativa de aseguramiento, basándose en los objetivos de aseguramiento.
	MEA02.08: Ejecutar las iniciativas de aseguramiento. Ejecutar la iniciativa de aseguramiento planificada. Reportar los hallazgos identificados. Ofrecer opiniones positivas del aseguramiento cuando sea apropiado, así como recomendaciones de mejora relacionadas con el desempeño operacional identificado, el cumplimiento externo y el riesgo residual del sistema de control interno.
MEA03 Monitorizar, evaluar y valorar el cumplimiento con los requerimientos externos	**MEA03.01: Identificar los requerimientos de cumplimiento externos.** Identificar y monitorizar de forma continua los cambios en las leyes y regulaciones locales e internacionales, así como otros requerimientos externos que se deben cumplir desde una perspectiva de TI.
	MEA03.02: Optimizar la respuesta a los requerimientos externos. Revisar y ajustar las políticas, los principios, los estándares, los procedimientos y las metodologías para asegurarse que se aborden y comuniquen los requerimientos legales, regulatorios y contractuales. Considerar los estándares de la industria, códigos de buenas prácticas y pautas de mejores prácticas para la adopción y adaptación.
	MEA03.03: Confirmar el cumplimiento externo. Confirmar el cumplimiento de las políticas, los principios, los estándares, los procedimientos y las metodologías con los requerimientos legales, regulatorios y contractuales.
	MEA03.04: Obtener garantía del cumplimiento externo. Obtener y reportar la garantía del cumplimiento y adeherncia a las políticas, principios, estándares, procedimientos y metodologías. Confirmar que las acciones correctivas para abordar las brechas en el cumplimiento se cierren de manera oportuna.

Página intencionalmente en blanco