

COBIT®



para Riesgos

COBIT®
5
AN ISACA® FRAMEWORK

ISACA®

Con más de 110.000 asociados en 180 países, ISACA (www.isaca.org) ayuda a las empresas y los líderes de Tecnologías de la Información a maximizar el valor y gestionar los riesgos relacionados con la Tecnología de Información. Fundada en 1969, ISACA, asociación independiente y sin ánimo de lucro, es defensora de los profesionales que intervienen en la seguridad de la información, el aseguramiento, la gestión de riesgos y el gobierno. Estos profesionales se basan en ISACA como fuente confiable de información y conocimiento tecnológico, de la comunidad, las normas y la certificación. La asociación, que cuenta con 200 capítulos en todo el mundo, mejora y valida las habilidades y conocimientos críticos para el negocio mediante los siguientes credenciales respetados mundialmente: Auditor Certificado de Sistemas de información: Certified Information Systems Auditor (CISA®), Gerente Certificado de Seguridad de Información: Certified Information Security Manage (CISM®), Certificado en el gobierno empresarial de las Tecnologías de la Información: Certified in the Governance of Enterprise IT (CGEIT®) y Certificado en Control de Riesgo y Sistemas de Información: Certified in Risk and Information Systems Control™ (CRISC™). ISACA desarrolló también y actualiza continuamente COBIT®, un marco empresarial que ayuda a las empresas, con independencia del sector y de su ubicación geográfica, a gobernar y administrar su información y tecnología.

Renuncia:

ISACA ha diseñado esta publicación, COBIT® 5 para Riesgos (el ‘Trabajo’), principalmente como recurso educativo para los profesionales de aseguramiento. ISACA no afirma que el uso de cualquier parte del Trabajo asegure un resultado exitoso. No debe considerarse que el Trabajo incluye toda la información, procedimientos y pruebas adecuadas, ni que excluya otro tipo de información, procedimientos y pruebas razonablemente dirigidos a obtener los mismos resultados. Al determinar la conveniencia de cualquier información, procedimiento o prueba, los profesionales de aseguramiento deben aplicar su propio juicio profesional a las circunstancias específicas presentadas por los sistemas particulares o por el entorno de tecnologías de la información.

Reserva de Derechos

© 2013 ISACA. Todos los derechos reservados. Para obtener instrucciones de uso, consulte www.isaca.org/COBITuse.

ISACA

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

Comentarios: www.isaca.org/cobit

Participar en el Centro de Conocimiento de ISACA: www.isaca.org/knowledge-center

Sigue a ISACA en Twitter: <https://twitter.com/ISACANews>

Únete a ISACA en LinkedIn: ISACA (Oficial), <http://linkd.in/ISACAOOfficial>

Me gusta ISACA en Facebook: www.facebook.com/ISACAHQ

COBIT® 5 for Risk

ISBN 978-1-60420-556-5

ISACA®

With more than 110,000 constituents in 180 countries, ISACA (www.isaca.org) helps business and IT leaders maximize value and manage risk related to information and technology. Founded in 1969, the non-profit, independent ISACA is an advocate for professionals involved in information security, assurance, risk management and governance. These professionals rely on ISACA as the trusted source for information and technology knowledge, community, standards and certification. The association, which has 200 chapters worldwide, advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) credentials. ISACA also developed and continually updates COBIT®, a business framework that helps enterprises in all industries and geographies govern and manage their information and technology.

Disclaimer

ISACA has designed and created COBIT® 5 for Risk (the ‘Work’) primarily as an educational resource for assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Reservation of Rights

© 2013 ISACA. All rights reserved. For usage guidelines, see www.isaca.org/COBITuse.

ISACA

3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA

Phone: +1.847.253.1545

Fax: +1.847.253.1443

Email: info@isaca.org

Web site: www.isaca.org

Provide Feedback: www.isaca.org/cobit

Participate in the ISACA Knowledge Center: www.isaca.org/knowledge-center

Follow ISACA on Twitter: <https://twitter.com/ISACANews>

Join ISACA on LinkedIn: ISACA (Official), <http://linkd.in/ISACAOOfficial>

Like ISACA on Facebook: www.facebook.com/ISACAHQ

COBIT® 5 for Risk

AGRADECIMIENTOS

ISACA quiere reconocer la labor de:

Fuerza de trabajo de CobiT para Riesgos

Steven A. Babb, CGEIT, CRISC, ITIL, Betfair, Reino Unido, Presidente

Evelyn Anton, CISA, CISM, CGEIT, CRISC, Uruguay

Jean-Louis Bleicher, CRISC, Francia

Derek Oliver, Ph.D., CISA, CISM, CRISC, FBCS, FISM, MInstISP, Ravenswood Consultants Ltd., Reino Unido

Steve Reznik, CISA, ADP Inc., Estados Unidos

Gladys Rouissi, CISA, ANZ Bank, Australia

Alok Tuteja, CGEIT, CRISC, Mazrui Holdings LLC, Emiratos Árabes Unidos

Equipo de Desarrollo

Floris Ampe, CISA, CGEIT, CRISC, CIA, ISO 27000, PwC, Bélgica

Stefanie Grijp, PwC, Bélgica

Bart Peeters, CISA, PwC, Bélgica

Dirk Steuperaert, CISA, CGEIT, CRISC, ITIL, IT In Balance BVBA, Bélgica

Sven Van Hoorebeeck, PwC, Bélgica

Participantes en el taller

Elza Adams, CISA, CISSP, PMP, IBM, Estados Unidos

Yalcin Gerek, CISA, CGEIT, CRISC, TAC, Turquía

Jimmy Heschl, CISA, CISM, CGEIT, Bwin.party Digital Entertainment Plc, Austria

Mike Hughes, CISA, CGEIT, CRISC, 123 Consultants GRC Ltd., Reino Unido

Jack Jones, CISA, CISM, CRISC, CISSP, Risk Management Insight, Estados Unidos

Andre Pitkowski, CGEIT, CRISC, APIT Informatica Ltd, Brasil

Eduardo Ritegno, CISA, CRISC, Banco de la Nacion Argentina, Argentina

Robert Stroud, CGEIT, CRISC, CA Technologies, Estados Unidos

Nicky Tiesenga, CISA, CISM, CGEIT, CRISC, IBM, Estados Unidos

Revisores Expertos

Elza Adams, CISA, CISSP, PMP, IBM, Estados Unidos

Mark Adler, CISA, CISM, CGEIT, CRISC, CIA, CRP, CFE, CISSP, Wal-Mart Stores Inc., Estados Unidos

Michael Berardi, CISA, CGEIT, CRISC, Bank of America, Estados Unidos

Peter R. Bitterli, CISA, CISM, CGEIT, Bitterli Consulting AG, Suiza

Sushil Chatterji, CGEIT, CMC, CEA, Edutech Enterprises, Singapur

Frank Cindrich, CGEIT, CIPP/G, CIPP/US, Deloitte and Touche, LLP, Estados Unidos

Diego Patricio del Hoyo, Westpac Banking Corporation, Australia

Michael Dickson, CISA, CISM, CRISC, CPA, GBQ Partners, Estados Unidos

AnnMarie DonVito, CISA, CISSP, ISSAP, ISO 27001 Lead Auditor, PRINCE2 Practitioner, ITIL Foundation V3, Deloitte AG, Suiza

Ken Doughty, CISA, CRISC, CRMA, ANZ, Australia

Urs Fischer, CRISC, CISA, CPA (Swiss), Fischer IT GRC Consulting and Training, Suiza

Shawna Flanders, CISA, CISM, CRISC, CSSGB, PSCU, Estados Unidos

Joseph Fodor, CISA, CPA, Ernst and Young LLP, Estados Unidos

Yalcin Gerek, CISA, CGEIT, CRISC, TAC, Turquía

J. Winston Hayden, CISA, CISM, CGEIT, CRISC, Sudáfrica

Mike Hughes, CISA, CGEIT, CRISC, 123 Consultants GRC Ltd., UK Duc Huynh, CISA, ANZ Wealth, Australia

Monica Jain, CGEIT, Southern California Edison (SCE), Estados Unidos

Waleed Khalid, CISA, MetLife, Reino Unido

John W. Lainhart, IV, CISA, CISM, CGEIT, CRISC, CIPP/G, CIPP/US, IBM Global Business Services, Estados Unidos

Debbie Lew, CISA, CRISC, Ernst and Young LLP, Estados Unidos

Marcia Maggiore, CISA, CRISC, Consultor en TI, Argentina

Lucio Augusto Molina Focazio, CISA, CISM, CRISC, Consultor independiente, Colombia

Anthony Noble, CISA, Viacom Inc., Estados Unidos

Abdul Rafeq, CISA, CGEIT, A.Rafeq and Associates, India

Salomon Rico, CISA, CISM, CGEIT, Deloitte, México

Eduardo Ritegno, CISA, CRISC, Banco de la Nacion Argentina, Argentina

AGRADECIMIENTOS (CONT.)

Revisores Expertos (cont.)

Paras Kesharichand Shah, CISA, CGEIT, CRISC, Vital Interacts, Australia
Mark Stacey, CISA, FCA, BG Group plc, Reino Unido
Robert Stroud, CGEIT, CRISC, CA Technologies, Estados Unidos
Greet Volders, CGEIT, Voquals N.V., Bélgica
John A. Wheeler, CRISC, Gartner, Estados Unidos
Tichaona Zororo, CISA, CISM, CGEIT, CRISC, CIA, CRMA, EGIT | Enterprise Governance of IT (PTY) LTD, Sudáfrica

Consejo de Administración de ISACA

Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Presidente Internacional
Allan Boardman, CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, Reino Unido, Vicepresidente
Juan Luis Carselle, CISA, CGEIT, CRISC, RadioShack, México, Vicepresidente
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, España, Vicepresidente
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, Estados Unidos, Vicepresidente
Vittal Raj, CISA, CISM, CGEIT, CFE, CIA, CISSP, FCA, Kumar and Raj, India, Vicepresidente
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management Inc., Estados Unidos, Vicepresidente
Marc Vael, Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Bélgica, Vicepresidente
Gregory T. Grocholski, CISA, The Dow Chemical Co., Estados Unidos, antiguo Presidente Internacional
Kenneth L. Vander Wal, CISA, CPA, Ernst and Young LLP (retirado), Estados Unidos, antiguo Presidente Internacional
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Grecia, Director
Krysten McCabe, CISA, The Home Depot, Estados Unidos, Director
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, BRM Holdich, Australia, Director

Junta de Expertos

Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Grecia, Presidente
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., Países Bajos
Steven A. Babb, CGEIT, CRISC, Betfair, Reino Unido
Thomas E. Borton, CISA, CISM, CRISC, CISSP, Cost Plus, Estados Unidos
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, Estados Unidos
Anthony P. Noble, CISA, Viacom, Estados Unidos
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, Reino Unido

Comité del Marco

Steven A. Babb, CGEIT, CRISC, Betfair, Reino Unido, Presidente
David Cau, Francia
Sushil Chatterji, Edutech Enterprises, Singapur
Frank Cindrich, CGEIT, CIPP/G, CIPP/US, Deloitte and Touche, LLP, Estados Unidos
Joanne T. De Vita De Palma, The Ardent Group, Estados Unidos
Jimmy Heschl, CISA, CISM, CGEIT, Bwin.party Digital Entertainment Plc, Austria
Katherine McIntosh, CISA, Central Hudson Gas and Electric Corp., Estados Unidos
Andre Pitkowski, CGEIT, CRISC, APIT Informatica, Brasil
Paras Kesharichand Shah, CISA, CGEIT, CRISC, Vital Interacts, Australia

Y un reconocimiento especial por el apoyo financiero al:

Capítulo de Los Ángeles

Equipo de traducción ISACA Barcelona:

Gonzalo Cuatrecasas, MBA, CISA, CISM, CGEIT
Inma González Gallo, MBA
Juan Dávila R., CISA, CISM, CRISC, ISO27001LA, ISO22301LA
Carles Mateu, CISA
Xavier Vila, Eur Ing, CISA, CISM, CRISC, ISO27001LA, ASITF
Salvador Simarro, CISA, 27001LA
Joan Figueras Tugas, CISA
Miguel Ángel Martínez Ayuso, MBA, CISA, CISM, CGEIT
Ramon Codina, CISM

AGRADECIMIENTOS (CONT.)

Equipo de traducción ISACA Barcelona (cont.)

Daniel Agudo García, CISA, CISM, CISSP, OPST, ISO27001, PMP
César Grasa Bello, CISA
Jordi Brinquez, CISA, ISO 27001LA
Rafael Estevan, CISA, CERT-CC
Xavier Rubiralta Costa, CISA, CISM, CGEIT, CRISC
Isidre Fàbregues, CISA
Marta Bernat Masat, CLSP
Antonio González Ortiz, CISA, CIA, CISM
José Manuel Valdés César, CISA, CRISC, ITIL Service Manager
Enric Güell, CISA
Gemma Déler, CISA, CGEIT, PMP, ISO27001, ITIL
Josep Lluís Masmitjà, CISA
Enric Gómez, CISA
Ignacio Guimaran, CISA, CISM, CRISC
Jacqueline Nolte-Pfleiderer, CISA
Albert Lladó, MBA, CISA, CISM, CGEIT, CRISC, ISO27001LA, ISO22301LA
Carlos Bachmaier, CGEIT, CRISC, CISA, CISM, ISO27001LA
Laia Segarra, asesora lingüística, Auren

Equipo de traducción América Latina:

Juan Dávila R., CISA, CISM, CRISC, ISO27001LA, ISO22301LA, Perú
Luis Gómez Nina, CPA, CRISC, República Dominicana
Edgar Morrobert, CISA, CRISC, República Dominicana
Hernando Peña, PMP, ITIL FC, ISO27001 LA, Colombia
Jorge Arturo Pérez Morales, CISM, México
Franco Rigante, CISA, CRISC, PMP, Argentina
Claudia Deprati, CISA, CRISC, Argentina
Stanley Velando, CISA, CRISC, Perú
Evelyn Anton, CISA, CISM, CRISC, CGEIT, Uruguay
Fernando Izquierdo Duarte, CISA. Colombia
Pablo Caneo, CISA, CGEIT, CRISC, ITIL, Chile
Marcela Pallero, Argentina
María Patricia Prandini, CISA, CRISC, Argentina
Lenin Espinosa, CISA, CRISC, ISO 27001 LA, Ecuador
Sergio Molanphy Palma, CISM, CRISC, Chile
Alfonso Mateluna Concha, CISA, CISM, CRISC, CISSP, Chile
Lolita E. Vargas De Leon, CPA, CISA, CIA, Puerto Rico

TABLA DE CONTENIDOS

Lista de Figuras	9
Resumen Ejecutivo	11
Introducción	11
Terminología	11
Factores impulsores de la Gestión de Riesgos	12
Ventajas del uso de esta publicación	12
Público objetivo de esta publicación	12
Información para el uso de esta publicación	14
Requisito previo de Conocimiento	16
Sección 1. Riesgo y Gestión de Riesgos	17
Capítulo 1. Objetivo de Gobierno: Creación de Valor	17
Capítulo 2. Riesgo	19
Capítulo 3. Alcance de esta Publicación	21
3.1 Perspectivas sobre riesgos con COBIT 5	21
3.2 Alcance de <i>COBIT 5 para Riesgos</i>	22
Capítulo 4. Aplicar los Principios de COBIT 5 a la Gestión de Riesgos	25
4.1 Satisfacer las necesidades de las partes interesadas	25
4.2 Cubrir la empresa de extremo-a-extremo	26
4.3 Aplicar un marco de referencia único e integrado	26
4.4 Posibilitar un enfoque holístico	26
4.5 Separar el Gobierno de la Gestión	27
Section 2A. Perspectiva de la Función de Riesgos	29
Capítulo 1. Introducción a los Catalizadores	29
1.1 Introducción	29
1.2 Dimensiones del modelo genérico de catalizadores	29
1.3 <i>COBIT 5 para Riesgos</i> y los catalizadores	30
Capítulo 2. Catalizador: Principios, Políticas y Marcos de Referencia	31
2.1 El modelo de Principios, Políticas y Marcos de Referencia	31
2.2 Perspectiva de la función de riesgos: Principios y Políticas relativas al gobierno y gestión del riesgo	32
Capítulo 3. Catalizador: Procesos	35
3.1 El Modelo de Procesos	35
3.2 Perspectiva de la función de riesgos: procesos que apoyan la gestión de riesgos	36
Capítulo 4. Catalizador: Estructuras Organizativas	39
4.1 El modelo de Estructuras Organizativas	39
4.2 Perspectiva de la función de riesgos: gobierno –y gestión– del riesgo relacionado con la Estructura Organizativa	40
Capítulo 5. Catalizador: Cultura, Ética y Conducta	43
5.1 El modelo de Cultura, Ética y Conducta	43
5.2 Perspectiva de la función de riesgos: gobierno –y gestión– del riesgo relacionado con la Cultura y Conducta	44
Capítulo 6. Catalizador: Información	47
6.1 El modelo de Información	47
6.2 Perspectiva de la función de riesgos: Información relacionada con el gobierno –y gestión– del riesgo	50
Capítulo 7. Catalizador: Servicios, Infraestructura y Aplicaciones	53
7.1 El modelo de Servicios, Infraestructura y Aplicaciones	53
7.2 Perspectiva de la función de riesgos: Servicios, Infraestructura y Aplicaciones relacionados con el gobierno –y gestión– del riesgo	54

Capítulo 8. Catalizador: Personas, Habilidades y Competencias	57
8.1 El modelo de Personas, Habilidades y Competencias	57
8.2 Perspectiva de la función de riesgos: Habilidades y Competencias relacionadas con el gobierno –y gestión– del riesgo	58
Sección 2B. La Perspectiva de la Gestión de Riesgos y el Uso de los Catalizadores de COBIT 5	61
Capítulo 1. Procesos Principales de Riesgos	61
Capítulo 2. Escenarios de Riesgo	63
2.1 Introducción	63
2.2 Flujo de trabajo en el desarrollo de escenarios de riesgo	64
2.3 Factores de riesgo	64
2.4 Estructura de escenarios de riesgos de TI	66
2.5 Temas principales durante el desarrollo y uso de escenarios de riesgo	68
Capítulo 3. Escenarios Genéricos de Riesgo	71
Capítulo 4. Agregación de Riesgos	79
4.1 ¿Por qué la agregación de riesgos?	79
4.2 Enfoque hacia la agregación de riesgos	79
Capítulo 5. Respuesta al Riesgo	85
5.1 Definiciones	85
5.2 Flujo y opciones de respuesta al riesgo	85
5.3 Selección y priorización de respuesta al riesgo	87
5.4 Guía en la selección y priorización de respuesta al riesgo	89
Sección 3. ¿Cómo se Alinea esta Publicación con otros Estándares?	91
Capítulo 1. ISO 31000 y COBIT 5 para Riesgos	91
1.1 ISO 31000:2009 Principios y directrices para la gestión de riesgos	91
Capítulo 2. ISO/IEC 27005 y COBIT 5 para Riesgos	95
2.1 ISO/IEC 27005:2011—Tecnología de Información—Técnicas de seguridad—Gestión de seguridad de información	95
Capítulo 3. COSO ERM y COBIT 5 para Riesgos	99
3.1 COSO ERM—Marco de referencia integrado	99
Capítulo 4. Comparación con Fuentes de Referencia de Riesgo del Mercado	103
4.1 Comparaciones de vocabulario: COBIT 5 para Riesgos vs. ISO Guide 73 y COSO ERM	103
Apéndices	
Apéndice A. Glosario	111
Apéndice B. Detalle de los Catalizadores para el Gobierno y la Gestión de los Riesgos	113
B.1 Catalizador: Principios, Políticas y Marcos de referencia	113
B.2. Catalizador: Procesos	117
B.3. Catalizadores: Estructuras Organizativas	149
B.4. Catalizadores: Cultura, Ética y Conducta	157
B.5. Catalizador: Información	159
B.6. Catalizadores: Servicios, Infraestructura y Aplicaciones	200
B.7. Catalizador: Gente, Habilidades y Competencias	203
Apéndice C. Principales Procesos de Gestión de Riesgos en COBIT 5	205
Apéndice D. El uso de Catalizadores de COBIT 5 para Reducir los Escenarios de Riesgo en TI	217
Introducción	217
Apéndice E. Comparativa de Riesgos de TI con COBIT 5	257
Apéndice F. Plantilla Exhaustiva para Escenarios de Riesgos	263

LISTA DE FIGURAS

Figura 1—COBIT 5 Familia de Productos COBIT 5	11
Figura 2— <i>COBIT 5 para Riesgos</i> Público objetivo y Beneficios	13
Figura 3— <i>COBIT 5 para Riesgos</i>	15
Figura 4—Objetivo de Gobierno: Creación de valor	17
Figura 5—Categorías de riesgo de TI	19
Figura 6—Dualidad del riesgo	20
Figura 7—Interrelaciones del riesgo inherente, corriente y residual	20
Figura 8— Dos perspectivas sobre riesgos	21
Figura 9—Ilustración de las dos perspectivas sobre riesgos	22
Figura 10—Alcance de <i>COBIT 5 para Riesgos</i>	23
Figura 11—Principios de COBIT 5	25
Figura 12—Catalizadores de COBIT 5	26
Figura 13—Catalizadores de COBIT 5: Genéricos	29
Figura 14—Catalizadores de COBIT 5: Principios, Políticas y Marcos de referencia	31
Figura 15—Principios para la gestión de riesgos	33
Figura 16—Ejemplos de políticas de riesgo	33
Figura 17—Catalizador: Procesos	35
Figura 18—Procesos de soporte de la función de riesgos	37
Figura 19—Procesos clave de soporte de la función de riesgos	37
Figura 20—Otros procesos de soporte para la función de riesgos	38
Figura 21—Catalizador: Estructuras organizativas	39
Figura 22—Principales estructuras organizativas	40
Figura 23—Líneas de defensa contra el riesgo	40
Figura 24—Otras estructuras relevantes para el riesgo	41
Figura 25—Catalizador: Cultura, Ética y Conducta	43
Figura 26—Comportamientos relevantes para el gobierno y la gestión del riesgo	44
Figura 27—Catalizador: Información	47
Figura 28—Elementos de información que apoyan el gobierno y la gestión del riesgo	50
Figura 29—Catalizador: Servicios, Infraestructura y Aplicaciones	53
Figura 30—Servicios relacionados con la gestión de riesgos	54
Figura 31—Catalizador: Personas, Habilidades y Competencias	57
Figura 32—Conjuntos de habilidades y competencias para la gestión de riesgos	58
Figura 33—Procesos principales de riesgo	61
Figura 34—Panorama de escenarios de riesgo	63
Figura 35—Factores de riesgo	65
Figura 36—Estructura de escenarios de riesgo	67
Figura 37—Principales áreas de enfoque en la técnica de escenarios de riesgo	68
Figura 38—Ejemplos de escenarios de riesgos	71
Figura 39—Agregación de mapas de riesgos—Riesgos independientes	82
Figura 40—Agregación de mapas de riesgos—Riesgos compartidos	82
Figura 41—Definición de términos de riesgos	85
Figura 42—Flujo de respuesta al riesgo	86
Figura 43—Flujo de la priorización de la respuesta al riesgo	88
Figura 44—ISO 31000 Principios de la gestión de riesgos cubiertos por <i>COBIT 5 para Riesgos</i>	91
Figura 45—ISO 31000 Marco de referencia para la gestión de riesgos cubierto por <i>COBIT 5 para Riesgos</i>	92
Figura 46—ISO 31000 Procesos de gestión de riesgos cubiertos por <i>COBIT 5 para Riesgos</i>	93

Figura 47—Proceso de gestión de riesgos de seguridad de la información	95
Figura 48—ISO/IEC 27005 Pasos de proceso cubiertos por <i>COBIT 5 para Riesgos</i>	96
Figura 49—Componentes COSO ERM cubiertos por <i>COBIT 5 para Riesgos</i>	99
Figura 50—Comparación de las definiciones de ISO Guide 73 con las de <i>COBIT 5 para Riesgos</i>	103
Figura 51—Comparación de las definiciones en COSO ERM y <i>COBIT 5 para Riesgos</i>	106
Figura 52—Principios del riesgo	113
Figura 53—Ejemplo de tabla de contenidos de una política de riesgos	113
Figura 54—Aspectos acerca de la vigencia que deben ser identificados en una política de riesgos	114
Figura 55—Procesos de Soporte a las Funciones Clave de Riesgo	117
Figura 56—Comité de la Gestión del Riesgo de la empresa /ERM)	149
Figura 57—Grupo del Riesgo de la empresa	152
Figura 58—Función del Riesgo	154
Figura 59—Departamento de Auditoría	155
Figura 60—Departamento de Cumplimiento Normativo	156
Figura 61—Perfil de riesgo	159
Figura 62—Plantilla de entrada del registro de riesgos	163
Figura 63—Plan de comunicación del riesgo	165
Figura 64—Informe de riesgo	168
Figura 65—Programa de Sensibilización de Riesgo	170
Figura 66—Mapa de Riesgos	172
Figura 67—Universo de Riesgo, Apetito y Tolerancia	174
Figura 68—Capacidad de Riesgo, Apetito de Riesgo y Riesgo Real	176
Figura 69—¿Qué es un Indicador Clave de Riesgo?	178
Figura 70—Ejemplos de ICR	182
Figura 71—Problemas y factores de riesgo emergente	183
Figura 72—Taxonomía del riesgo	186
Figura 73—Análisis del impacto en la empresa	188
Figura 74—Eventos de riesgo	191
Figura 75—Risk and Control Activity Matrix (RCAM)	194
Figura 76—Evaluación del Riesgo	197
Figura 77—Servicios de Asesoría de Riesgos de Programa/Proyecto	200
Figura 78—Servicios de Gestión de Incidencias	200
Figura 79—Servicios de Asesoría de Arquitectura	201
Figura 80—Servicios de Inteligencia de Riesgos	201
Figura 81—Servicios de Gestión de Riesgos	201
Figura 82—Servicios de Gestión de Crisis	202
Figura 83—Gestor del riesgo	203
Figura 84—Analista del riesgo	204
Figura 85—Procesos de Gestión de Riesgos Principales	205

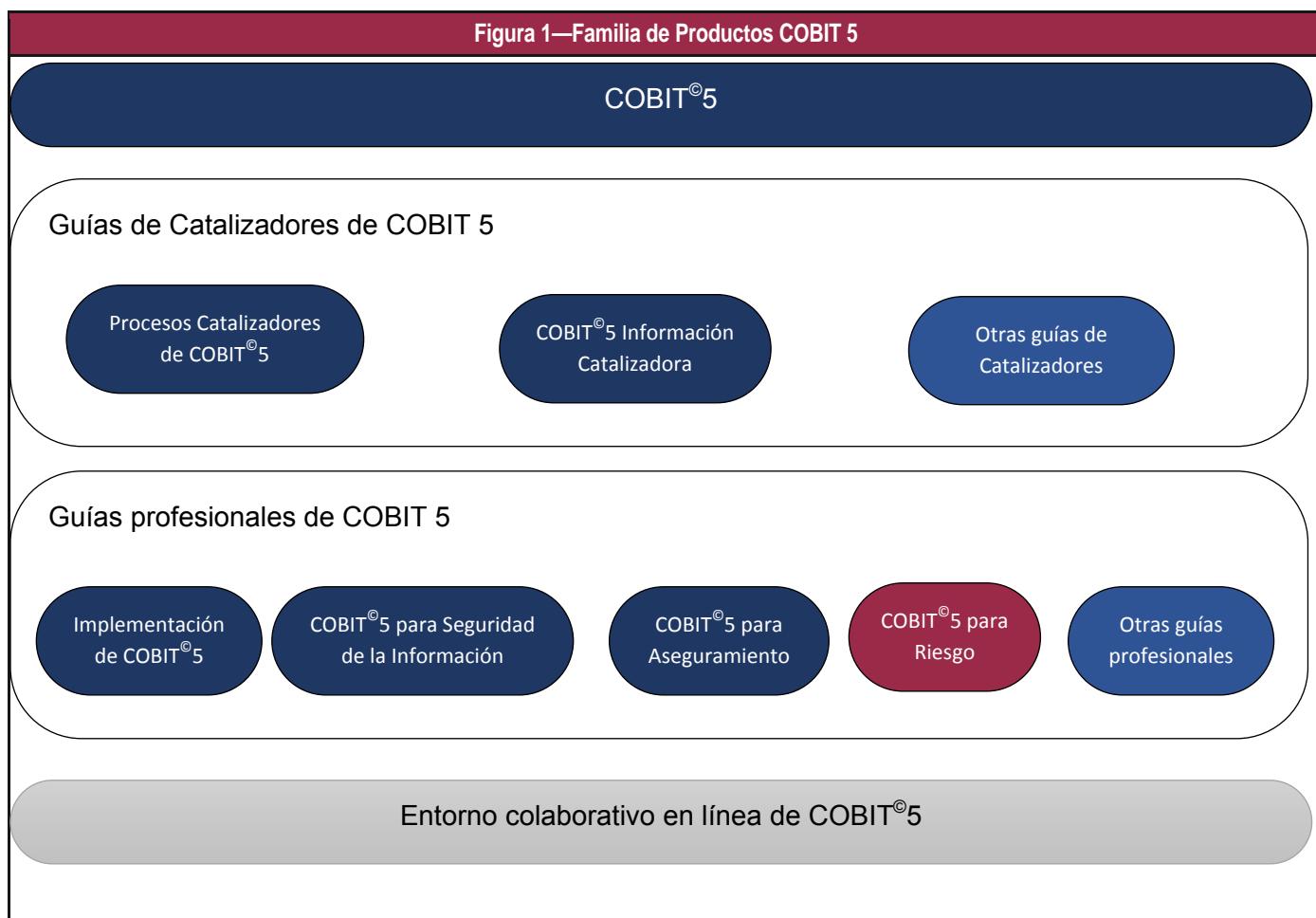
RESUMEN EJECUTIVO

Introducción

La información es un recurso fundamental para todas las empresas. Desde el momento de la información se crea hasta el en que se destruye, la tecnología juega un papel importante en la contención, distribución y análisis de la información. La tecnología es cada vez más avanzada y se ha hecho omnipresente en las empresas y los entornos social, público y empresarial.

COBIT 5 ofrece un marco integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de la tecnología de información en la empresa (TI). En pocas palabras, COBIT 5 ayuda a las empresas a crear valor óptimo a partir de las TI mediante el mantenimiento de un equilibrio entre la obtención de beneficios y la optimización de los niveles de riesgo y del uso de recursos. COBIT 5 facilita el gobierno y gestión de la TI en forma integral para toda la empresa, teniendo en cuenta el negocio extremo a extremo y las áreas funcionales de la responsabilidad TI y teniendo en cuenta los intereses relacionados con las TI de las partes interesadas tanto internas como externas.

COBIT 5 para Riesgos, destacado en la figura 1, se basa en el marco COBIT 5, centrándose en el riesgo y proporcionando una orientación más detallada y práctica a los profesionales de riesgo y otras partes interesadas en cualquier nivel de la empresa.



Terminología

COBIT 5 para Riesgos analiza los riesgos relacionados con TI. El capítulo 2 de la sección 1, define lo que se entiende por riesgos relacionados con las TI. Sin embargo, para facilitar la lectura, el término ‘riesgo’ se usa a lo largo de toda la publicación para referirse a los riesgos relacionados con TI. La orientación y los principios explicados en esta publicación son aplicables a cualquier tipo de empresa, tanto si opera en un contexto comercial como si no, en el sector privado o del sector público, o tanto si se trata de una empresa pequeña, mediana o grande.

COBIT 5 para Riesgos presenta dos perspectivas en el uso de COBIT en un contexto de riesgo: la función de riesgo y la gestión de riesgos. La **perspectiva de la función de riesgo** se centra en lo que se necesita para construir y mantener la función de riesgo en la empresa. La **perspectiva de la gestión de riesgos** se centra en los procesos básicos de gobierno y gestión del riesgo para optimizar el riesgo y en cómo identificar, analizar, responder y reportar sobre el riesgo a diario. Estas perspectivas se explican en detalle en el capítulo 2 de la sección 1: Riesgo; en la sección 2ª, La Perspectiva de la Función del Riesgos; y la sección 2B, La perspectiva de la Gestión de Riesgos y uso de los Catalizadores de COBIT 5.

Factores impulsores de la Gestión de Riesgos

Los principales impulsores de la gestión del riesgo en sus distintas formas incluyen la necesidad de mejorar de los resultados del negocio, la toma de decisiones y la estrategia global al proporcionar:

- A las partes interesadas opiniones fundamentadas y consistentes sobre la situación actual de riesgo en toda la empresa
- Orientación sobre la forma de gestionar el riesgo dependiendo del apetito/aversión al riesgo por parte de la empresa
- Orientación para configurar la cultura de riesgo adecuada en la empresa
- Siempre que sea posible, evaluaciones cuantitativas de riesgos que permiten a las partes interesadas considerar el coste de la mitigación y los recursos necesarios versus la exposición a pérdidas

Para ello, esta publicación:

- Proporciona orientación para el uso del marco de trabajo de COBIT 5 en el establecimiento de las funciones de gobierno y de gestión de riesgos en la empresa
- Proporciona orientación y un enfoque estructurado para el uso de los principios de COBIT 5 para gobernar y administrar los riesgos TI
- Muestra cómo COBIT 5 para el Riesgo se alinea con otras normas pertinentes

Ventajas del uso de esta publicación

Usar COBIT 5 para Riesgos aumenta las capacidades relacionadas con el riesgo de la empresa proporcionando beneficios tales como:

- Una identificación más precisa del riesgo y la medida del éxito en el tratamiento del mismo
- Una mejor comprensión del impacto del riesgo en la empresa
- Guía de extremo a extremo sobre cómo gestionar el riesgo, incluyendo un amplio conjunto de medidas
- El conocimiento de cómo sacar provecho de las inversiones relacionadas con las prácticas de gestión de riesgos de TI
- La comprensión de cómo una gestión de riesgos TI eficiente optimiza el valor, junto con la eficacia y eficiencia de los procesos de negocio, la mejora de la calidad y la reducción de costes y residuos
- Las oportunidades para integrar la gestión de riesgos TI con las estructuras para el riesgo y el cumplimiento en la empresa
- La mejora en la comunicación y el entendimiento entre todas las partes interesadas (internas y externas) gracias al uso de un marco común mundialmente aceptado y sostenible y el lenguaje para evaluación y respuesta al riesgo
- Promover la responsabilidad sobre los riesgos y su aceptación en toda la empresa
- Un perfil de riesgo completo, identificando la exposición total al riesgo de la empresa y facilitando una mejor utilización de sus recursos
- Mejorar la conciencia del riesgo en toda la empresa

Público objetivo de esta publicación

El público objetivo de *COBIT 5 para Riesgos* es amplio tal y como son las razones para la adopción y el uso del marco y los beneficios que cada uno encuentre en esta publicación dependiendo de su rol y función en la empresa. Los roles y las funciones que aparecen en la **figura 2** se consideran partes interesadas en la gestión del riesgo. Estas partes interesadas no se refieren necesariamente a los individuos, sino a los roles y funciones dentro de la empresa o en su entorno.

Figura 2—COBIT 5 para Riesgos. Público Objetivo y Beneficios	
Rol/Función	Beneficio/Razón para Adoptar y Adaptar COBIT 5 para Riesgos
Junta Directiva y Ejecutiva	<ul style="list-style-type: none"> Mejor comprensión de sus responsabilidades y roles con respecto a la gestión de riesgos TI y de la implicación de los riesgos TI con los objetivos estratégicos de la empresa Mejor comprensión de cómo optimizar el uso de TI para la ejecución exitosa de la estrategia
Responsables/Directores de Función del riesgo y riesgo empresarial en la estructura para la gestión del riesgo empresarial (ERM: <i>Enterprise Risk Management</i>)	Ayuda en la gestión de riesgos de TI, de acuerdo con los principios generalmente aceptados del ERM e incorporando los riesgos TI en el riesgo empresarial
Los gestores de riesgos operacionales	<ul style="list-style-type: none"> Vinculación de su marco de riesgos a COBIT 5 para Riesgos Identificación de las pérdidas operacionales o el desarrollo de indicadores de riesgo (KRI: Key Risk Indicators)
Gestión de TI	Mejor comprensión de cómo identificar y gestionar los riesgos de TI y cómo comunicarlos a los que toman decisiones de negocios
Gestores de los servicios TI	Mejora de su punto de vista sobre el riesgo operacional, que debe encajar en el marco general de gestión de riesgos TI
Continuidad del negocio	Alineamiento con el ERC, al ser la evaluación del riesgo un aspecto clave de su responsabilidad
Seguridad TI	Posicionar el riesgo para la seguridad entre las demás categorías de riesgos TI
Seguridad de la información	Posicionar el riesgo TI en la estructura de gestión de riesgos de la información de la empresa
Director Financiero (CFO: <i>Chief financial officer</i>)	Mejorar la visibilidad de los riesgos TI y de sus implicaciones financieras en inversión y gestión de carteras
Responsables de gobierno de la empresa	Ayuda en su revisión y el seguimiento de las responsabilidades de gobierno y otros roles de gobierno TI
Gestor de Negocio	La comprensión y gestión de los riesgos TI - uno de los muchos elementos de riesgo de negocio, todo lo cual debe ser gestionado en forma consistente
Los auditores internos	Mejora del análisis de riesgo en apoyo de los planes e informes de auditoría
Cumplimiento	Soporte en el rol de asesores clave en la función de riesgos en relación con los requisitos de cumplimiento y su impacto potencial sobre la empresa
El abogado general	Soporte en el papel de asesor clave para la función de riesgo en los riesgos relacionados con la regulación y su impacto potencial o implicaciones legales
Reguladores	Mediante su evaluación de la aproximación a la gestión de riesgos IT en la empresa regulada y el impacto del riesgo en los requisitos reglamentarios
Auditores externos	Orientación adicional sobre los niveles de exposición para establecer una opinión sobre la calidad del control interno
Aseguradoras	Soporte en el momento de establecer una cobertura de seguro adecuada para TI y en la búsqueda del acuerdo sobre los niveles de exposición
Agencias de calificación	En colaboración con las aseguradoras, referencia para evaluar y calificar objetivamente cómo gestiona la empresa los riesgos TI
Contratistas y subcontratistas TI	<ul style="list-style-type: none"> Mejor alineación de la utilidad y garantía de los servicios prestados Comprendión de las responsabilidades aparecidas en la evaluación de riesgos

Nota: La guía y principios proporcionados en esta publicación son aplicables a todas las empresas, independientemente de su tamaño, sector y naturaleza.

Información para el uso de esta publicación

COBIT 5 para Riesgos se dirige a las preguntas y cuestiones fundamentales sobre la gestión de riesgos TI. La **Figura 3** muestra estas preguntas y explica cómo y dónde *COBIT 5 para Riesgos*, si están dentro del alcance de esta guía, es de ayuda.

COBIT 5 para Riesgos se refiere a los siete facilitadores de COBIT 5:

- Principios, políticas y marcos
- Procesos
- Estructuras organizativas
- Cultura, Ética y Conducta
- Información
- Servicios, Infraestructura y Aplicaciones
- Personas, Habilidades y Competencias

El carácter único de cada empresa dará lugar a que estos facilitadores se implementen de forma diferente para gestionar el riesgo de manera óptima. Esta guía ofrece una visión en profundidad explicando cada concepto de COBIT 5 desde la perspectiva de la función de riesgo y usando orientación y ejemplos adicionales.

Para guiar al lector a través de la colección completa de información, *COBIT 5 para Riesgos* se divide en tres secciones y seis apéndices. A continuación se presenta una breve descripción de cada sección y cómo estas secciones se interconectan.

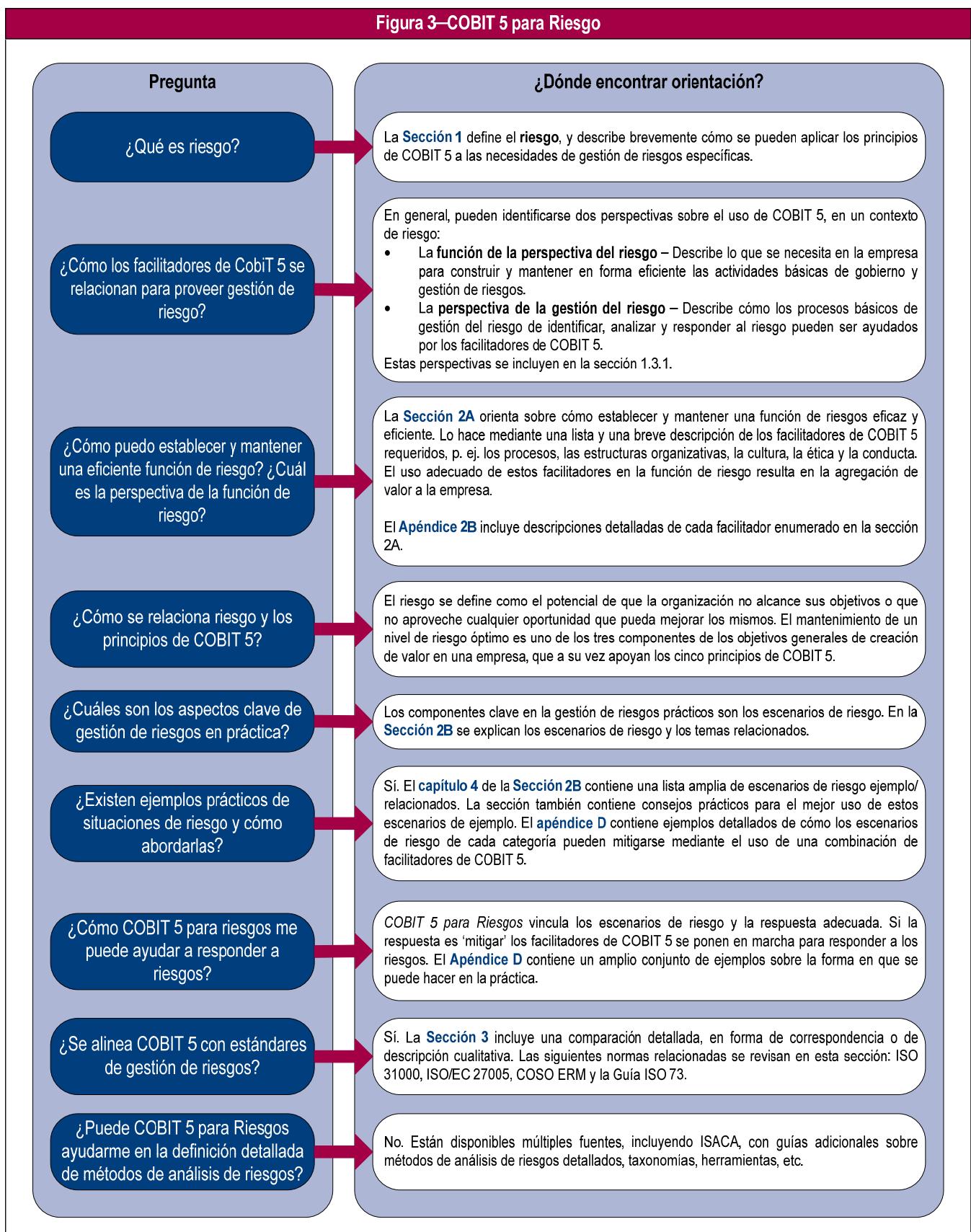
Sección 1 – Trata del riesgo y de su gestión describiendo brevemente cómo se pueden aplicar los principios de COBIT 5 en las necesidades específicas de gestión de riesgos. Esta sección ofrece al lector un punto de referencia que se sigue en el resto del documento.

Sección 2 –Trata del uso de los facilitadores de COBIT 5 en la práctica de la gestión del riesgo. El Gobierno de las TI de la empresa (GEIT: *Governance of enterprise IT*) es sistémico y se apoya en un conjunto de facilitadores. En esta sección, se presentan los dos puntos de vista sobre la manera de aplicar los facilitadores de COBIT 5. En los apéndices se proporciona una guía detallada de estos facilitadores.

Sección 2A - Describe los facilitadores COBIT 5 que se necesitan para construir y mantener la función de riesgo.

Sección 2B - Describe cómo los facilitadores de COBIT 5 son de ayuda en procesos básicos de gestión del riesgos (identificación, análisis y respuesta). Esta sección ofrece también algunos escenarios de riesgo genéricos.

Sección 3 -presenta la alineación de *COBIT 5 para Riesgos* con las normas y prácticas de TI o de ERM relevantes incluyendo COSO ERM, ISO 31000, ISO / IEC 27005 y la Guía ISO 73. Esta sección incluye también una comparación entre *COBIT 5 para Riesgos* y estas normas.



Apéndices - Contienen el glosario y la guía detallada de los facilitadores introducidos en la sección 2:

- **Apéndice A** – Glosario
- **Apéndice B** – Información detallada de los facilitadores para el gobierno y gestión de riesgos:
 - B.1 – Principios, políticas y marcos
 - B.2 – Procesos
 - B.3 – Estructuras organizativas
 - B.4 – Cultura, Ética y Conducta
 - B.5 – Información
 - B.6 – Servicios, Infraestructura y Aplicaciones
 - B.7 – Personas, Habilidades y Competencias
- **Apéndice C** – Descripción detallada de los procesos básicos de gestión de riesgos
- **Apéndice D** – Guía de escenarios de riesgo, contiene un amplio conjunto de ejemplos sobre cómo mitigarlos usando los facilitadores COBIT 5
- **Apéndice E** – Comparación entre COBIT 5 para Riesgos y el anterior Risk IT Framework
- **Apéndice F** – Plantilla para la descripción del escenario de riesgo

Requisito previo de Conocimiento

COBIT 5 para Riesgos se basa en COBIT 5. La mayoría de los conceptos claves de COBIT 5 se tratan en esta publicación, sin embargo, la comprensión previa de COBIT 5 y sus facilitadores acelerará la comprensión de esta guía.

Si los lectores desean conocer los conceptos de COBIT 5 más allá de lo que se requiere para la gestión del riesgo, deben consultar el marco COBIT 5.

COBIT 5 para Riesgos también se refiere al *Modelo de Evaluación de Procesos de COBIT (PAM: Process Assessment Model): Usando COBIT 5* y a los procedimientos de COBIT 5 allí descritos. Si desea saber más acerca de los procesos de COBIT 5, p. ej. para implementar o mejorar algunos de ellos como parte de la respuesta al riesgo, debe consultar la publicación *COBIT 5: Procesos Catalizadores*.

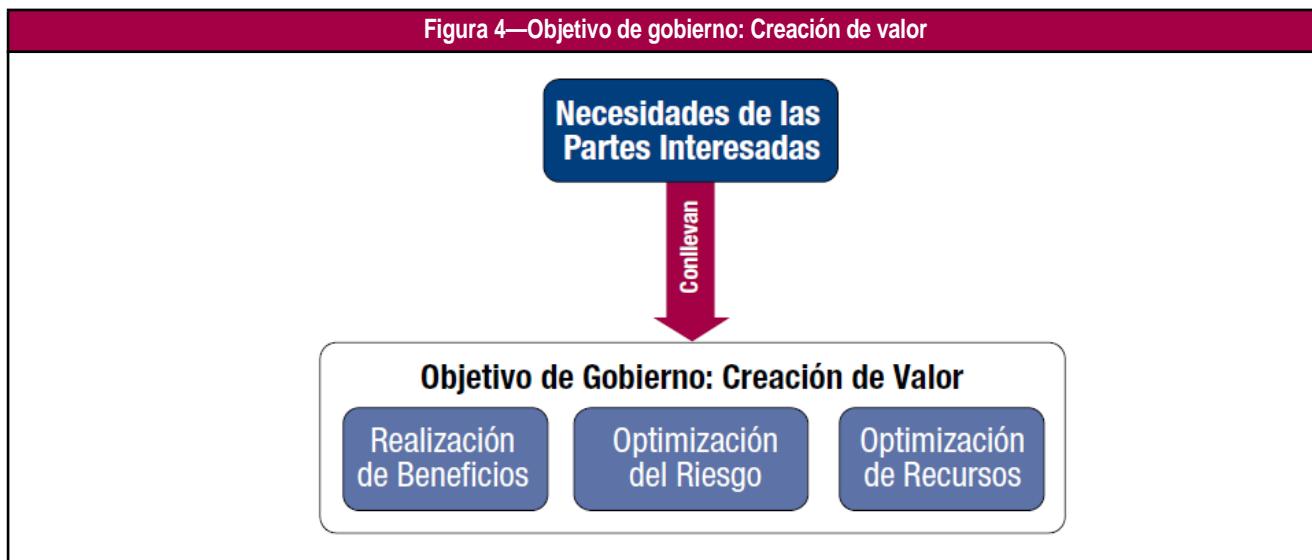
El conjunto de productos COBIT 5 incluye también un modelo de madurez de procesos basado en la norma reconocida internacionalmente ISO/IEC 15504 para la evaluación de procesos de ingeniería del software. Aunque el modelo de evaluación de procesos no es requisito previo para el conocimiento de *COBIT 5 para Riesgos*, los lectores pueden utilizar éste para evaluar el desempeño de cualquiera de los procesos de gobierno o de gestión e identificar las áreas de mejora.

SECCIÓN 1. RIESGO Y GESTIÓN DE RIESGOS

CAPÍTULO 1 OBJETIVO DE GOBIERNO: CREACIÓN DE VALOR

Las empresas existen para crear valor para sus accionistas. En consecuencia, cualquier empresa, sea comercial o no, tendrá a la creación de valor como objetivo de gobierno.

La creación de valor significa la obtención de beneficios a un costo óptimo de recursos **mientras se optimiza el riesgo** (**figura 4**). Los beneficios pueden tomar varias formas, p.ej., financieras para las empresas comerciales o de servicios públicos para entidades gubernamentales.



Las empresas pueden tener muchas partes interesadas, y la “creación de valor” puede significar cosas diferentes, y a veces conflictivas, para cada uno de ellos. El gobierno trata acerca de la negociación y la decisión entre los intereses de las diferentes partes interesadas sobre el valor.

El componente de optimización del riesgo en la creación de valor muestra que:

- La optimización del riesgo es parte esencial de cualquier sistema de gobierno.
- La optimización del riesgo no puede ser vista de forma aislada, es decir, las acciones tomadas como parte de la gestión de riesgos impactarán en la realización de beneficios y en la optimización del uso de recursos.

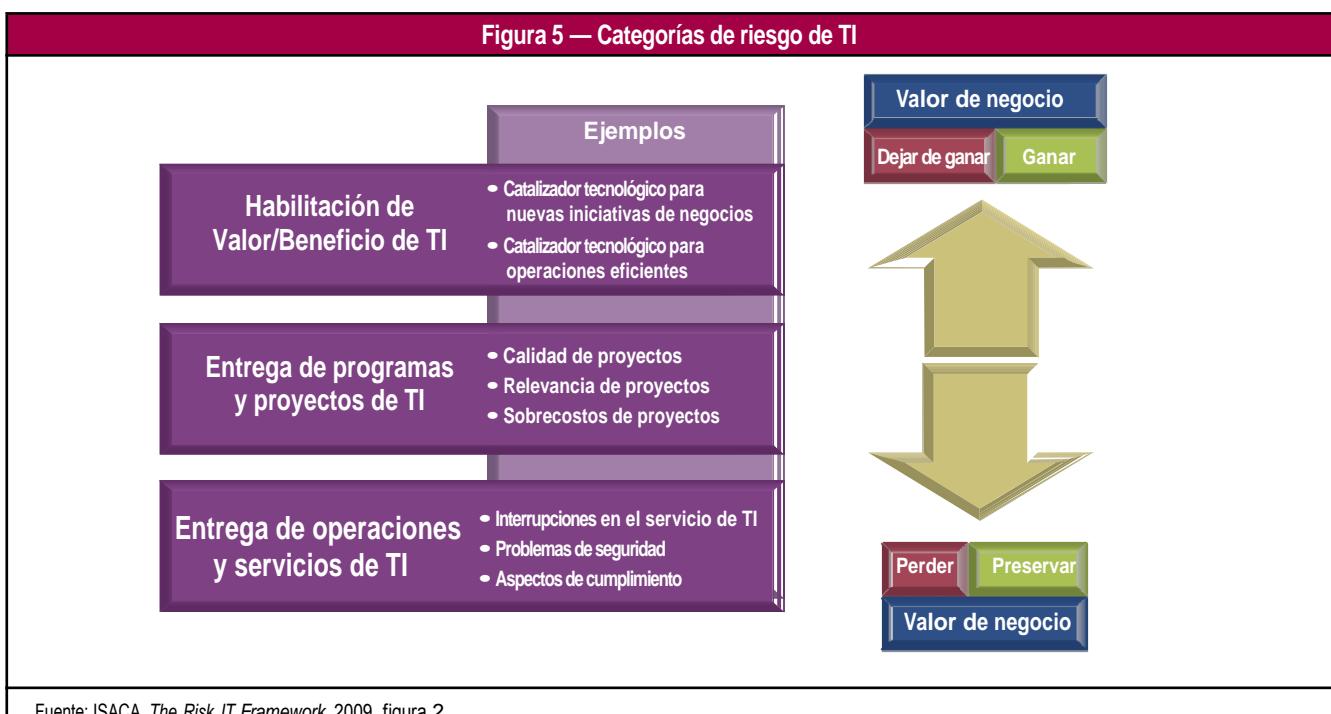
Página dejada en blanco intencionadamente

CAPÍTULO 2

RIESGO

El riesgo es definido generalmente como una combinación de la probabilidad de un evento y sus consecuencias (ISO Guide 73). Las consecuencias se reflejan en que no se logren los objetivos de la empresa. *COBIT 5 para Riesgos* define el riesgo de TI como un riesgo de negocio, específicamente, el riesgo de negocio asociado con el uso, la propiedad, operación, involucramiento, influencia y adopción de las TI en una empresa. El riesgo de TI consiste de eventos relacionados a TI que potencialmente podrían impactar al negocio. El riesgo de TI puede darse con una frecuencia e impacto inciertos, generando desafíos en el logro de las metas y los objetivos estratégicos.

El riesgo de TI existe siempre, así sea o no detectado y reconocido por una organización.



Los riesgos de TI pueden ser categorizados como sigue:

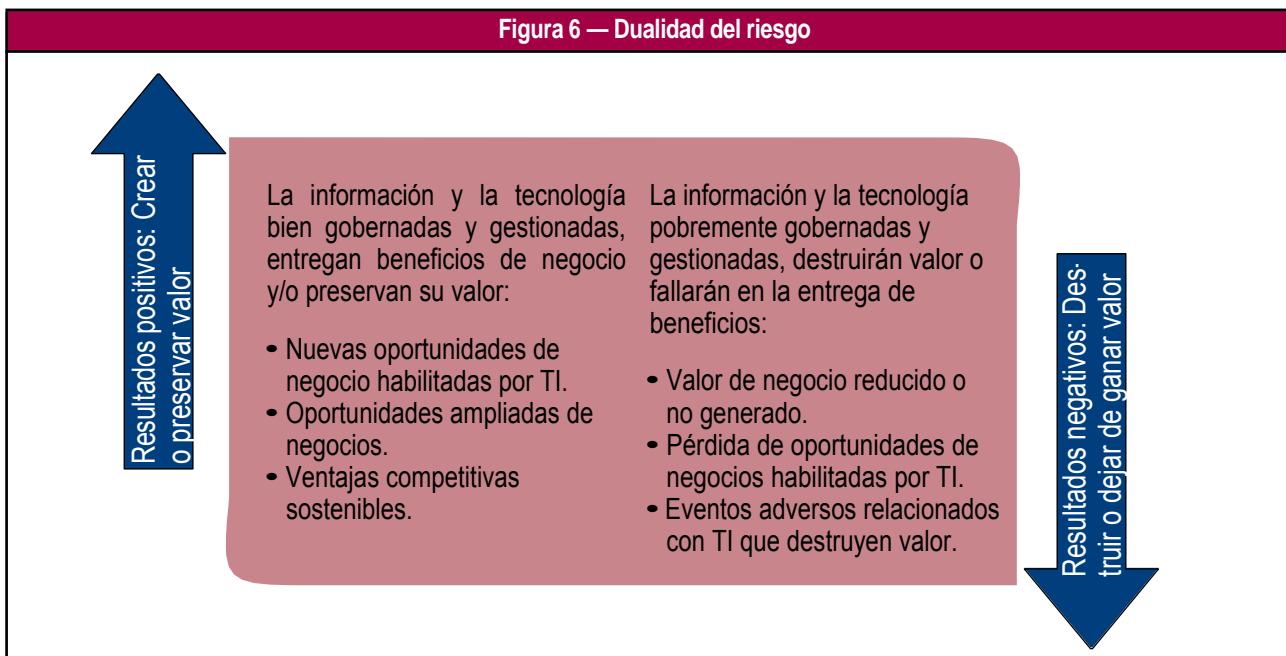
- **Riesgo en la habilitación de valor/beneficio de TI:** Asociado con las oportunidades perdidas de utilización de la tecnología con el fin de mejorar la eficiencia o efectividad de los procesos de negocio, o como un habilitador para nuevas iniciativas de negocio.
- **Riesgo en la entrega de programas y proyectos de TI:** Asociado con la contribución de TI a soluciones de negocio nuevas o mejoradas, generalmente bajo la forma de programas y proyectos que forman parte de portafolios de inversión.
- **Riesgo en la entrega de operaciones y servicios de TI:** Asociado con todos los aspectos del negocio como el desempeño normal de sistemas y servicios de TI, los que pueden destruir o reducir el valor para la empresa.

La **figura 5** muestra que para todas las categorías de riesgos decrecientes de TI (valores de negocio “Dejar de ganar” y “Perder”), existe un equivalente creciente (“Ganar” y “Preservar”). Por ejemplo:

- **Entrega de servicios:** Si se fortalecen las prácticas de entrega de servicios de TI, la empresa puede beneficiarse, p.ej., estando lista para absorber volúmenes de transacciones o porcentajes de mercado adicionales.
- **Entrega de proyectos:** La entrega exitosa de proyectos de TI proporciona nuevas funcionalidades de negocio.

Es importante mantener en mente esta dualidad creciente/decreciente de los riesgos (ver **figura 6**), durante todas las decisiones relacionadas con el riesgo. Por ejemplo, las decisiones deberían considerar:

- La exposición que puede resultar si un riesgo no es mitigado versus el beneficio obtenido si la exposición a la pérdida asociada es reducida a un nivel aceptable.
- El beneficio potencial que puede acumularse si se toman las oportunidades versus los beneficios perdidos si se renuncian a las mismas.



No siempre se puede evitar el riesgo. Hacer negocios se trata de tomar riesgos en forma consistente con el apetito de riesgo; es decir, muchas propuestas de negocio requieren tomar riesgos de TI para lograr la propuesta de valor y concretar las metas y los objetivos organizacionales, y dicho riesgo debería ser gestionado pero no necesariamente evitado.

Cuando se referencia al riesgo en *COBIT 5 para Riesgos*, se refiere al riesgo **corriente**. Raramente se utiliza el concepto de riesgo inherente en *COBIT 5 para Riesgos*. La **figura 7** muestra cómo se interrelacionan el riesgo inherente, corriente y el residual. Teóricamente, *COBIT 5 para Riesgos* se focaliza en el riesgo corriente porque, en la práctica, eso es lo que se utiliza.



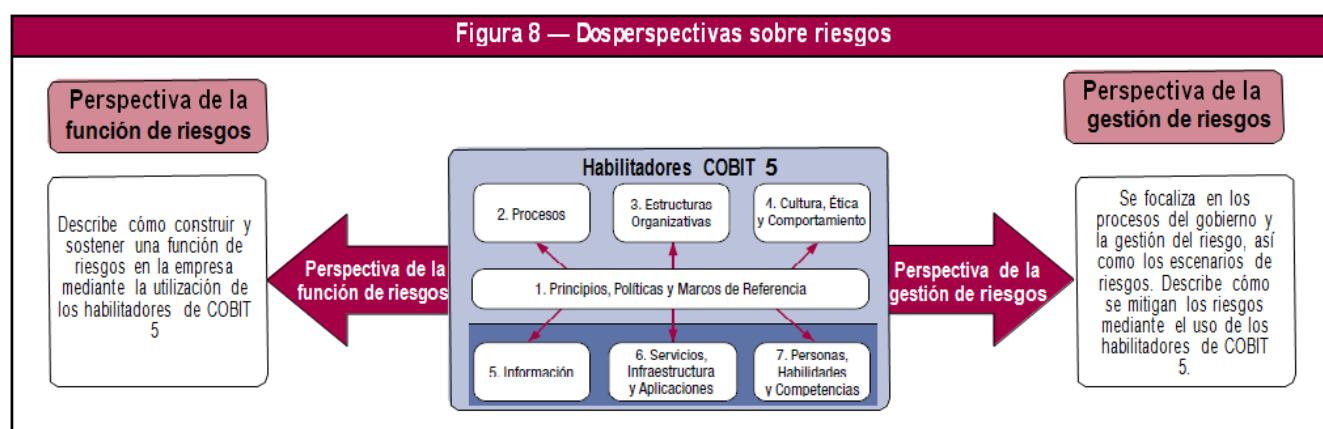
CAPÍTULO 3

ALCANCE DE ESTA PUBLICACIÓN

3.1 Perspectivas sobre riesgos con COBIT 5

La **figura 8** muestra las siguientes dos perspectivas sobre la forma de utilizar COBIT 5 en un contexto de riesgo:

- **Perspectiva de la función de riesgos:** Describe lo que se necesita en una organización para construir y sostener actividades principales de gobierno y gestión del riesgo en forma efectiva y eficiente.
- **Perspectiva de la gestión de riesgos:** Describe cómo el proceso principal de gestión de riesgos, para la identificación, análisis, respuesta y reporte sobre los riesgos puede ser apoyado por los catalizadores de COBIT 5.



La perspectiva de la función de riesgos

COBIT 5 es un marco de referencia de extremo a extremo que considera a la optimización del riesgo como un objetivo clave de valor. COBIT 5 considera al gobierno y a la gestión del riesgo como parte del gobierno y gestión global de TI en la organización.

Para cada habilitador, la perspectiva de función de riesgos describe cómo contribuye a la función global de gobierno y gestión del riesgo. Por ejemplo:

- Se requieren procesos para definir y sostener la función de riesgos, el gobierno y la gestión del riesgo: EDM01, APO01, etc.
- Se requieren flujos de información para el gobierno y la gestión del riesgo: El universo de riesgos, el perfil de riesgo, etc.
- Se requieren estructuras organizativas para el gobierno y la gestión del riesgo: Comité ERM, la función de riesgos, etc.

Los capítulos 2 al 8 de la Sección 2A contienen ejemplos para cada habilitador, ejemplos que se detallan en el apéndice B.

La perspectiva de la gestión de riesgos

Esta perspectiva comprende el gobierno y la gestión, es decir, cómo identificar, analizar y responder al riesgo, y cómo utilizar el marco COBIT 5 para dicho propósito. Esta perspectiva requiere implementar procesos principales del riesgo (EDM03 *Asegurar la optimización del riesgo* y APO12 *Gestionar el riesgo*). Estos procesos se describen en detalle en el apéndice C.

El riesgo es representado por los escenarios de riesgo. Se ha hecho un vínculo y comparación desde la perspectiva de gestión de riesgos hacia los catalizadores de COBIT 5 para ilustrar la forma en que el marco COBIT 5 puede ayudar a las organizaciones en el gobierno y la gestión de los riesgos identificados.

Ilustración de las dos perspectivas de riesgo

La **figura 9** ilustra las dos perspectivas sobre riesgo en un ejemplo de una empresa puesta en marcha, mostrando las fases de definición del riesgo, y las respectivas acciones de ambas perspectivas en cada fase.

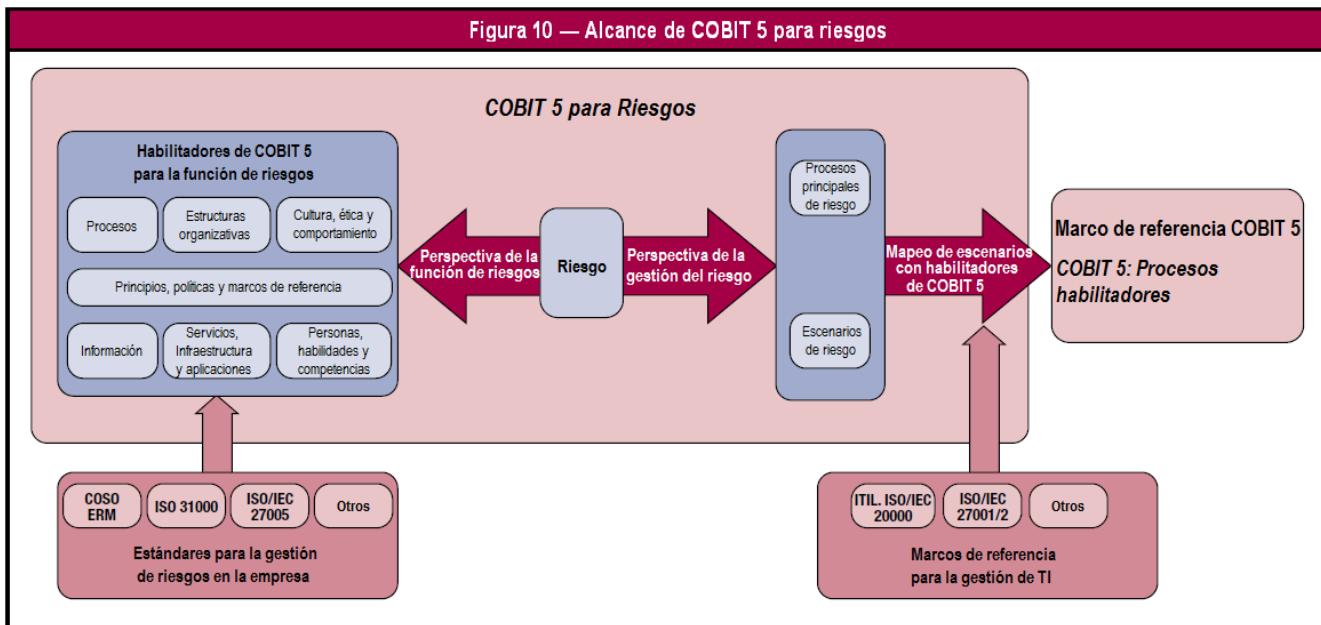
Figura 9—Ilustración de las dos perspectivas sobre riesgos		
Fase	Perspectiva de la función de riesgos: Uso de los catalizadores de COBIT 5 para definir y sostener una función efectiva del riesgo	Perspectiva de la gestión de riesgos: Uso de COBIT 5 para identificar, analizar, responder y reportar sobre el riesgo
Establecimiento de la función de riesgos	<p>La empresa define estructuras organizativas, entre otras, la función de riesgos, y asigna responsabilidades relacionadas al riesgo a algunos roles existentes, p.ej., el Director General Ejecutivo (CEO) y el Consejo Directivo.</p> <p>La empresa define un presupuesto para la función de riesgos, asigna responsabilidades y la obligación de rendir cuenta a personas con las habilidades relevantes, etc.</p>	
Establecimiento del proceso de gestión de riesgos	<p>La empresa define y mantiene un proceso de gobierno del riesgo, es decir, el proceso EDM03 de COBIT 5, en el contexto de un marco de gestión de riesgos, que incluye el establecimiento de los niveles de apetito y tolerancia al riesgo, la promoción de una cultura consciente del riesgo, el monitoreo del perfil del riesgo, etc.</p> <p>La empresa define e implementa un proceso de gestión de riesgos, es decir, el proceso APO12 de COBIT 5.</p> <p>Se elabora una política de gestión de riesgos.</p>	<p>La empresa ejecuta los procesos definidos (EDM03 y APO12), que están apoyados por los catalizadores que han sido implementados.</p> <p>Basado en tales procesos y en el apetito de riesgo definido, por ejemplo, la empresa determina que la calidad de sus aplicaciones de software y que la seguridad del hardware y software son aspectos clave de riesgo que requieren acciones apropiadas.</p> <p>La empresa responde al riesgo, es decir, ejecuta la práctica de proceso APO12.06 de COBIT 5. Esta respuesta requiere la implementación de todas las acciones de respuesta al riesgo, previamente definidas y aprobadas. En la práctica, estas acciones de respuesta al riesgo consisten de varios de los catalizadores de COBIT 5, aplicadas al ambiente general de TI.</p>
Gestión de riesgos en operaciones		<p>En respuesta a los aspectos identificados de calidad del software, la empresa implementa y/o mejora lo siguiente:</p> <ul style="list-style-type: none"> • Los procesos APO09 y APO10 para gestionar proveedores y acuerdos de servicios con proveedores. • El proceso APO11 para gestionar la calidad del desarrollo del software. • Todos los procesos en el dominio BAI (Construir, adquirir e implementar). • El proceso DSS01 para proporcionar operaciones de TI. • El proceso DSS04 para proporcionar continuidad de negocio. <p>Adicionalmente, se definen e implementan los otros catalizadores relacionados, p.ej., la información, las políticas, las estructuras organizativas, etc.</p> <p>En respuesta a los aspectos de seguridad, la empresa implementa y/o mejora lo siguiente:</p> <ul style="list-style-type: none"> • El proceso APO13 para gestionar la seguridad. • El proceso DSS05 para gestionar los servicios de seguridad. <p>Adicionalmente, se definen, implementan y reportan los otros catalizadores relacionados, p.ej., la información, las políticas, las estructuras organizativas, etc.</p>

3.2 Alcance de COBIT 5 para Riesgos

La **figura 10** muestra el alcance de *COBIT 5 para Riesgos* y cómo se relaciona con otros documentos de ISACA que, en forma conjunta, brindan una guía completa sobre el gobierno y la gestión del riesgo sobre TI de la empresa. La **figura 10** muestra que *COBIT 5 para Riesgos*:

- Se focaliza en la aplicación de los catalizadores de COBIT 5 hacia el riesgo, a través de la perspectiva de la función de riesgos, es decir, cómo utilizar los catalizadores de COBIT 5 para asegurar una función efectiva y eficiente de gobierno y gestión del riesgo.
- Ofrece una guía de alto nivel sobre cómo identificar, analizar y responder al riesgo, a través de la aplicación de los procesos principales de gestión de riesgos en COBIT 5 y mediante el uso de escenarios de riesgos.

- Está alineada con fuentes de referencia de ERM en el mercado (estándares, marcos de referencia y guías prácticas) y con las iniciativas ERM. *COBIT 5 para Riesgos* incluye vínculos y comparaciones con las mayores fuentes de referencia del mercado.
- Ofrece un vínculo entre los escenarios de riesgos y los catalizadores de COBIT 5 que pueden ser utilizados para mitigar los riesgos. También se pueden utilizar otros marcos de gestión de TI para dicho propósito, como ITIL e ISO/IEC 27001/2; sin embargo, en esta guía no se incluyen vínculos/mapeos detallados.

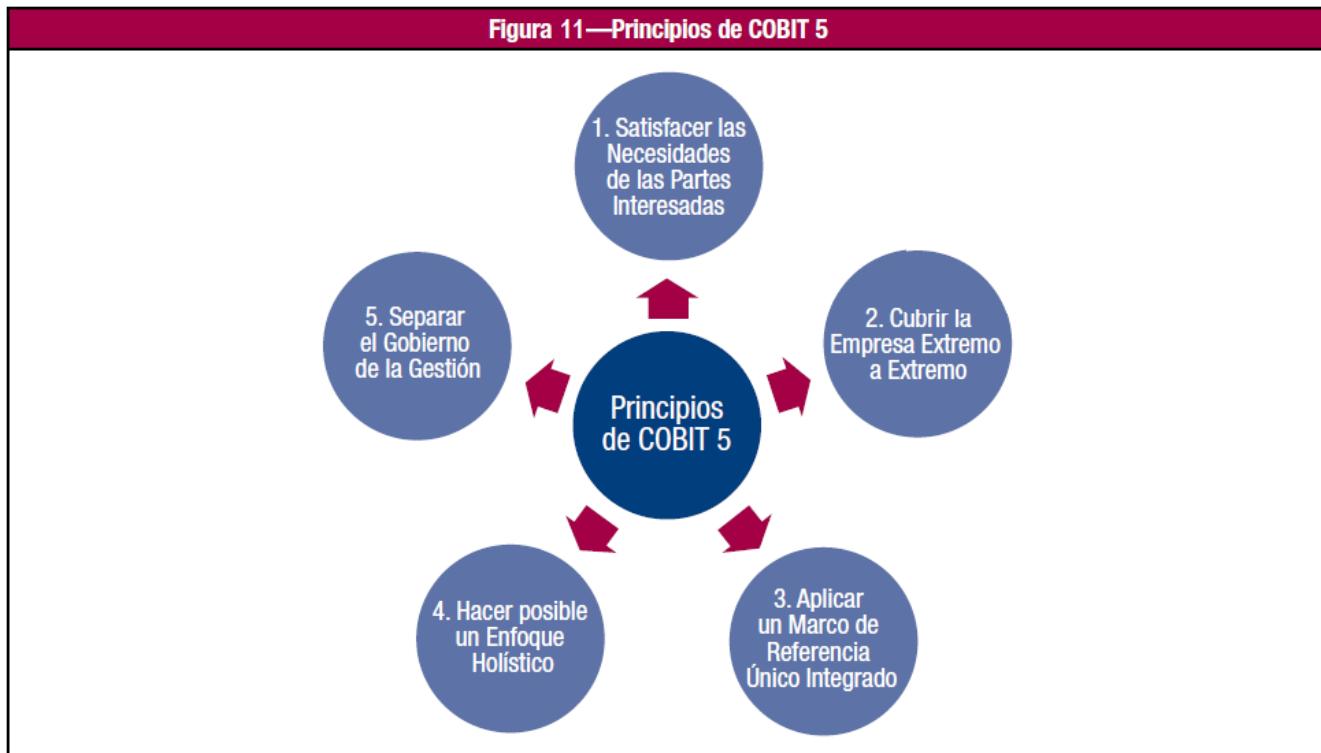


Página dejada en blanco intencionadamente

CAPÍTULO 4

APLICAR LOS PRINCIPIOS DE COBIT 5 A LA GESTIÓN DE RIESGOS

COBIT 5 se basa en cinco principios, tal como se muestra en la **figura 11**.



COBIT 5 para Riesgos aplica estos principios a los riesgos de la siguiente manera:

1. **Satisfacer las necesidades de las partes interesadas:** El propósito del gobierno y la gestión de riesgos es ayudar a garantizar que los objetivos de la empresa se logren a través de la cascada de metas. La optimización del riesgo es uno de los tres componentes del objetivo general de creación de valor para la empresa.
2. **Cubrir la empresa de Extremo-a-Extremo:** *COBIT 5 para Riesgos* cubre todos los catalizadores de gobierno y de gestión en su alcance y describe todas las fases requeridas de gobierno y gestión de riesgos.
3. **Aplicar un marco de referencia único e integrado:** *COBIT 5 para Riesgos* se alinea con todos los principales marcos y estándares de gestión de riesgos.
4. **Posibilitar un enfoque holístico:** *COBIT 5 para Riesgos* identifica todos los elementos interrelacionados de los catalizadores que son requeridos para proporcionar el gobierno y la gestión de riesgos en forma adecuada, presentando un enfoque holístico y sistemático hacia el riesgo.
5. **Separar el gobierno de la gestión:** COBIT 5 distingue entre el gobierno del riesgo y las actividades de la gestión de riesgos.

4.1 Satisfacer las necesidades de las partes interesadas

Uno de los objetivos básicos de cualquier empresa es asegurar niveles de exposición óptimos, por tanto, ofrecer una adecuada gestión de riesgos es una preocupación de las partes interesadas, tanto internas como externas. La **figura 2** (véase la sección “Audiencia objetivo” del Resumen Ejecutivo de esta publicación), enumera las principales partes interesadas para la gestión de riesgos y se explica su interés en ella.

4.2 Cubrir la empresa de extremo-a-extremo

COBIT 5 integra GEIT en el gobierno corporativo, de la siguiente manera:

- Cubre todas las funciones y procesos dentro de la organización. COBIT 5 no se centra sólo en la función de TI, sino que trata la información y las tecnologías relacionadas como activos que requieren ser gestionados por todos en la empresa, como cualquier otro activo.
- Considera que todos los catalizadores de gobierno y gestión relacionados con las TI están de extremo a extremo en toda la organización, es decir, que incluye a todo y a todos, internos y externos, que son relevantes para el gobierno y la gestión de la información y las TI relacionadas.

Para aplicar este principio al riesgo, *COBIT 5 para Riesgos* se orienta a todas las partes interesadas, funciones y procesos de la organización, que son relevantes para el gobierno y la gestión de riesgos.

4.3 Aplicar un marco de referencia único e integrado

Muchos de los estándares y las mejores prácticas relacionadas con TI ofrecen orientación sobre un subconjunto de actividades relacionadas con TI. COBIT 5 ofrece una cobertura completa de la empresa, proporcionando una base para integrar efectivamente otros marcos, estándares y prácticas. Sirve como una fuente consistente y consolidada de orientación en un lenguaje común y no técnico. COBIT 5 se alinea con otros estándares y marcos relevantes, por lo tanto permite a la empresa utilizarlo como el marco general de gobierno y gestión de TI.

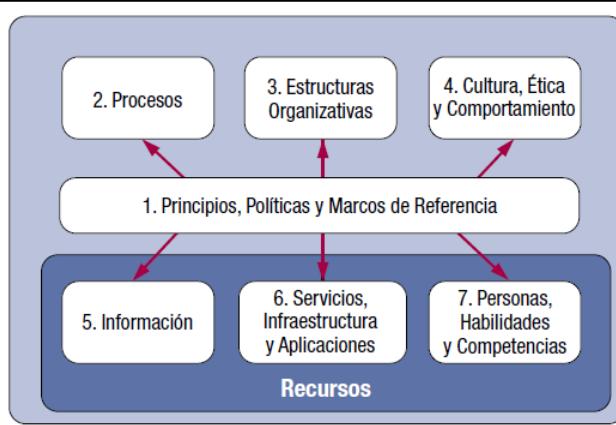
Más específicamente, *COBIT 5 para Riesgos* reúne conocimientos previos, dispersos en otros marcos de ISACA, tales como COBIT, BMIS (Business Model for Information Security), Risk IT y Val IT, con la orientación de otros estándares importantes relacionados con riesgos, tales como ISO 31000, ISO/IEC 27005 y COSO ERM.

El marco de referencia *Risk IT* fue publicado en 2009 por ISACA, incluyendo una guía de soporte para profesionales. Las prácticas de *Risk IT* están mapeadas con las prácticas de gobierno y de gestión de COBIT 5 en el apéndice A de *Cobit 5 Procesos Catalizadores*. *COBIT 5 para Riesgos* presenta dos perspectivas sobre el riesgo: la función de riesgos y la gestión de riesgos, para ayudar aún más a los profesionales de ERM.

4.4 Posibilitar un enfoque holístico

El gobierno y la gestión eficientes y efectivos de TI en una empresa, requieren un enfoque holístico, considerando que interactúan varios componentes. COBIT 5 define un conjunto de catalizadores que apoyan la implementación de un sistema integral de gobierno y gestión de TI en la empresa. Los catalizadores son factores que influyen, individual y colectivamente para el éxito del gobierno y la gestión de TI. Los catalizadores son impulsados por la cascada de metas de COBIT 5, es decir, las metas de alto nivel de la empresa y las metas relacionadas con TI definen lo que los diferentes catalizadores deberían lograr. El marco COBIT 5 define siete categorías de catalizadores (**figura 12**).

Figura 12—Habilitadores de COBIT 5



Las siete categorías de catalizadores también se aplican a la gestión de riesgos. Los catalizadores apoyan la implementación del gobierno y la gestión del riesgo sobre TI, como se muestra en los siguientes ejemplos:

1. **Principios, políticas y marcos de referencia:** Principios, políticas y enfoques de cumplimiento del riesgo;
2. **Procesos:** Los procesos principales del riesgo en los dominios EDM (Evaluar, Dirigir y Supervisar) y APO (Alinear, Planificar y Organizar), así como la aplicación de muchos otros procesos a la función de riesgos;
3. **Estructuras organizativas:** El comité ERM, el Director de Riesgos (CRO);
4. **Cultura, ética y comportamiento:** El comportamiento de toda la empresa, de la gerencia y de los profesionales de riesgos responsables de la gestión de riesgos;
5. **Información:** Perfiles de riesgo, escenarios de riesgo, mapas de riesgo;
6. **Servicios, infraestructura y aplicaciones:** Servicios consultivos en riesgos emergentes;
7. **Personas, habilidades y competencias:** Certificación CRISC, competencias técnicas y en gestión de riesgos.

En la Sección 2A se discuten todos los catalizadores interrelacionados necesarios para implementar adecuadamente el gobierno y la gestión de riesgos, presentando un enfoque holístico y sistémico hacia el riesgo.

4.5 Separar el Gobierno de la Gestión

COBIT 5 hace una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren estructuras organizativas diferentes y sirven para diferentes propósitos.

Gobierno

El gobierno asegura que se evalúen las necesidades, condiciones y las opciones de las partes interesadas para determinar que se alcanzan los objetivos corporativos acordados, en forma equilibrada, estableciendo la dirección a través de la priorización y la toma de decisiones, supervisando el desempeño, cumplimiento y avance respecto a la dirección y objetivos acordados.

En la mayoría de las empresas, el gobierno es responsabilidad del consejo directivo bajo el liderazgo de su presidente.

Buen gobierno significa que la optimización de riesgos forma parte de los mecanismos de gobierno implementados y que se incluye la información sobre riesgos en el proceso de toma de decisiones. Al mismo tiempo, la función de riesgos requiere ser gobernada, es decir, proporcionándole dirección y supervisión. En *COBIT 5 para Riesgos*, el proceso EDM03 asegura la optimización del riesgo y es apoyado por los catalizadores relacionados.

Gestión

La gestión planifica, construye, ejecuta y supervisa las actividades alineadas con la dirección establecida por el órgano de gobierno para alcanzar los objetivos corporativos.

En la mayoría de las empresas, la gestión es responsabilidad de la dirección ejecutiva, bajo el liderazgo del Director General Ejecutivo (CEO).

En *COBIT 5 para Riesgos*, el proceso APO12 *Gestionar el riesgo*, conjuntamente con los catalizadores, permiten a la empresa construir, ejecutar y supervisar una eficiente y efectiva función de gestión de riesgos.

Página dejada en blanco intencionadamente

SECCIÓN 2A. PERSPECTIVA DE LA FUNCIÓN DE RIESGOS

CAPÍTULO 1 INTRODUCCIÓN A LOS CATALIZADORES

1.1 Introducción

Esta sección describe la forma en que los catalizadores de COBIT5, presentados en la sección anterior, pueden ser aplicados en situaciones prácticas y cómo pueden utilizarse para implementar un efectivo y eficiente gobierno y gestión de riesgos en la empresa.

Todos los catalizadores definidos en COBIT 5 tienen un conjunto de dimensiones comunes (**figura 13**), las cuales:

- Proporcionan una forma sencilla y estructurada de trabajar con los catalizadores.
- Permiten la gestión de las complejas interacciones entre los catalizadores.
- Facilitan la obtención de resultados exitosos a partir de los catalizadores.

Error! Not a valid link.

1.2 Dimensiones del modelo genérico de catalizadores

Las cuatro dimensiones comunes de los catalizadores son:

- **Partes interesadas:** Cada habilitador tiene partes interesadas que desempeñan un rol activo y/o tienen interés en el habilitador. Por ejemplo, para el habilitador de Procesos, varias partes ejecutan actividades del proceso y/o tienen un interés en los resultados del proceso; y para el habilitador de Estructuras Organizativas, las partes interesadas, cada una con sus propios roles e intereses, son parte de las estructuras. Las partes interesadas pueden ser internas o externas, con sus propias necesidades e intereses, algunas veces conflictivos entre sí. Las necesidades e intereses de los grupos de interés se traducen en metas corporativas, que a su vez se traducen en metas de TI para la empresa.
- **Metas:** Cada habilitador tiene metas, las cuales son resultados esperados. Los catalizadores proporcionan valor por el logro de estas metas. Las metas del habilitador son el paso final en la cascada de metas de COBIT 5. Las metas pueden dividirse a su vez en las siguientes categorías:
 - Calidad intrínseca: Medida en que los catalizadores proporcionan resultados precisos, objetivos y confiables.
 - Calidad contextual: Medida en que los resultados de los catalizadores se ajustan al propósito, dado el contexto en el que operan. Por ejemplo, los resultados deben ser relevantes, completos, vigentes, apropiados, consistentes, comprensibles, ágiles y fáciles de usar.
 - Accesibilidad y seguridad: Medida en que los resultados de los catalizadores están accesibles y disponibles cuando se necesitan, y seguros, es decir, que el acceso esté restringido a quienes están autorizados y lo necesiten.
- **Ciclo de vida:** Cada habilitador tiene un ciclo de vida, desde el inicio, pasando por su vida útil / operativa, hasta su eliminación. La identificación, evaluación, mitigación, monitoreo y reporte de los riesgos, son parte de este ciclo de vida. Las siguientes son las fases del ciclo de vida:
 - Planificar (incluye el desarrollo conceptual y la selección).
 - Diseñar.
 - Construir / adquirir / crear / implementar.
 - Utilizar / operar.
 - Evaluar / monitorear.
 - Actualizar / eliminar.
- **Buenas prácticas:** Se pueden definir buenas prácticas para cada uno de los catalizadores. Las buenas prácticas apoyan el logro de las metas del habilitador y brindan ejemplos o sugerencias de cómo implementar mejor el habilitador y los productos o entradas y salidas requeridos. Una vez que las buenas prácticas son adaptadas adecuadamente e integradas con éxito en la empresa, pueden llegar a ser las mejores prácticas para la empresa, a través del seguimiento y supervisión adecuada a las necesidades cambiantes del negocio.

1.3 COBIT 5 para Riesgos y los catalizadores

COBIT 5 para Riesgos proporciona orientación específica relacionada con todos los catalizadores:

1. **Principios, políticas y marcos de referencia** para riesgos.
2. **Procesos**, incluyendo actividades y detalles específicos de la función de riesgo.
3. **Estructuras organizativas** específicas para riesgos.
4. En términos de **cultura, ética y comportamiento**, los factores determinantes en el éxito del gobierno del riesgo.
5. **Información** de tipos específicos de riesgos para facilitar el gobierno y la gestión del riesgo en la organización.
6. Respecto a **servicios, infraestructura y aplicaciones**, las capacidades de servicios requeridas para ofrecer funciones relacionadas a riesgos en la organización.
7. Para **personas, habilidades y competencias**, se requieren habilidades y competencias específicas para riesgos.

Los capítulos siguientes exponen los siete catalizadores y su lugar en la gestión de riesgos. Cada capítulo comienza con una descripción del modelo del habilitador basado en el modelo genérico presentado en este capítulo; sin embargo, se adiciona información específica de la gestión de riesgos para cada uno de los catalizadores según sea necesario. Por eso, aunque todos los modelos se parecen entre sí, éstos son diferentes y cada uno debe ser estudiado cuidadosamente.

El apéndice B contiene la descripción específica de riesgos de los componentes de los catalizadores y una guía detallada respecto a estos.

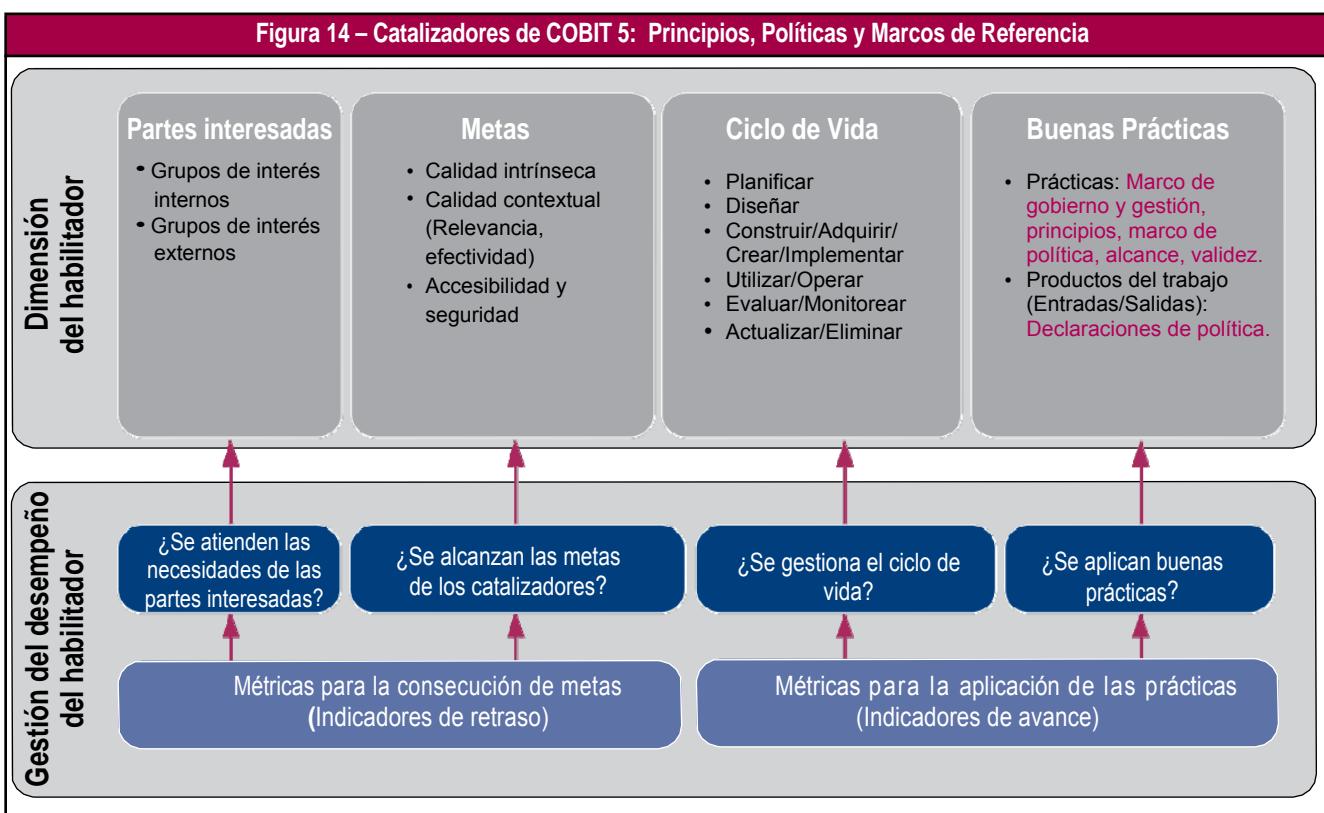
CAPÍTULO 2

CATALIZADOR: PRINCIPIOS, POLÍTICAS Y MARCOS DE REFERENCIA

Este capítulo contiene una guía, desde la perspectiva de la función de riesgos, sobre cómo los principios, políticas y marcos de referencia pueden habilitar el gobierno y la gestión de riesgos en una empresa. Este capítulo trata los siguientes temas:

- El modelo de Principios, Políticas y Marcos de Referencia.
- Una selección de principios, políticas y marcos de referencia que son relevantes para el gobierno y la gestión de riesgos.
- El apéndice B.1 ofrece una descripción de la información detallada por cada aspecto de los principios, políticas y marcos de referencia.

2.1 El modelo de Principios, Políticas y Marcos de Referencia



El modelo de principios, políticas y marcos de referencia (ver **figura 14**) muestra:

- **Partes interesadas:** Pueden ser internas o externas a la empresa. Incluyen al consejo directivo, la gerencia ejecutiva, directores de cumplimiento, gerentes de riesgos, auditores internos y externos, proveedores de servicios, clientes y reguladores. Sus intereses están divididos, algunas partes interesadas definen y establecen las políticas, mientras que otras tienen que alinearse a ellas y cumplirlas.

- **Metas y métricas:** Los principios, políticas y marcos de referencia son instrumentos para comunicar las reglas de la empresa, en apoyo de los objetivos de gobierno y los valores de la empresa, según lo definido por el consejo directivo y la gerencia ejecutiva.

Los principios requieren:

- Ser limitados en número.
- Usar un lenguaje simple, que expresen los valores fundamentales de la empresa de la forma más clara posible.

Las políticas proporcionan una guía detallada sobre cómo poner en práctica los principios e influyen en la forma en que la toma de decisiones se alinea con los principios. Las buenas políticas son:

- Efectivas: Logran el propósito declarado.
- Eficientes: Aseguran que los principios se implementen en la forma más eficiente.
- No intrusivas: Parecen lógicas para quienes tienen que cumplirlas, es decir, no crean resistencia innecesaria.
- Alineadas: Están alineadas con la estrategia general de la empresa.

Acceso a las políticas: ¿Existe un mecanismo que proporcione un fácil acceso a las políticas para todas las partes interesadas? En otras palabras, ¿las partes interesadas saben dónde encontrar las políticas?

- **Ciclo de vida:** Las políticas tienen un ciclo de vida en el que apoyan el logro de las metas definidas. Los marcos de referencia son claves porque proporcionan una estructura para definir guías consistentes. Por ejemplo, un marco de política proporciona la estructura con la cual se puede crear y mantener un conjunto de políticas coherentes, y también proporciona una referencia de navegación sencilla dentro de las políticas individuales y entre ellas.
- **Buenas prácticas:**
 - Las buenas prácticas requieren que las políticas sean parte de un marco general de gobierno y de gestión, proporcionando una estructura (jerárquica) a la que deberían ceñirse todas las políticas y actuando de enlace con los principios subyacentes. Como parte del marco de política, se requiere describir los siguientes aspectos:
 - Alcance y validez.
 - Roles y responsabilidades de las partes interesadas.
 - Las consecuencias de incumplir la política.
 - Los medios para el manejo de excepciones.
 - La manera en la cual el cumplimiento de la política será verificado y medido.
 - Los marcos de gobierno y de gestión generalmente reconocidos pueden proporcionar una valiosa orientación sobre las declaraciones vigentes que deben incluirse en las políticas.
 - Las políticas deben estar alineadas con el apetito de riesgo de la empresa. Las políticas son un componente clave del sistema de control interno de la organización, cuyo propósito es gestionar y contener el riesgo. Como parte de las actividades de gobierno del riesgo, se define el apetito de riesgo, que debe estar reflejado en las políticas. Una empresa aversa al riesgo tiene políticas más estrictas que una empresa más proclive al riesgo.
 - Las políticas necesitan ser revisadas y actualizadas a intervalos regulares para asegurar su relevancia con las prácticas y requerimientos del negocio.

2.2 Perspectiva de la función de riesgos: principios y políticas relativas al gobierno y gestión del riesgo

El propósito de esta sección es identificar y exponer los principios y las políticas requeridas para construir y mantener un gobierno y gestión de riesgos de TI, efectivo y eficiente en la empresa.

Los principios de riesgos (ver **figura 15**) se centran en proporcionar un enfoque sistemático, oportuno y estructurado para la gestión de riesgos, lo cual contribuirá a resultados consistentes, comparables y fiables. Los principios de riesgo formalizan y estandarizan la implementación de las políticas de riesgo, las cuales se analizan en la sección 2.2.2. El apéndice B.1 contiene descripciones detalladas de los principios de riesgo.



Las políticas proporcionan una guía más detallada sobre cómo poner en práctica los principios y cómo influirán en la toma de decisiones. No todas las políticas relevantes están escritas y bajo propiedad de la función de riesgos de TI. Esta publicación describe una serie de políticas relacionadas con riesgos, y se especifica el componente de política dentro de la empresa.

En la **figura 16** se muestran ejemplos de políticas de riesgos de TI, incluyendo ejemplos de políticas sobre las operaciones que deberían ser considerados para una completa gestión de riesgos de TI. Dependiendo del tamaño y naturaleza de la organización, estas pueden ser políticas en sí mismas o secciones dentro de las políticas existentes. Para mayor eficiencia en las operaciones, es necesario mantener estas políticas en sintonía con la política de riesgos.

Figura 16—Ejemplos de políticas de riesgo

Políticas	Descripción
Política principal de riesgos de TI	Define a nivel estratégico, táctico y operativo, cómo se requiere gobernar y gestionar el riesgo en una empresa, en cumplimiento de sus objetivos de negocio. Esta política traduce el gobierno corporativo en principios y políticas de gobierno del riesgo y elabora actividades de gestión de riesgos.
Política de seguridad de información	Establece pautas de comportamiento en la protección de la información corporativa y de los sistemas e infraestructuras asociadas. Los requerimientos de negocio en materia de seguridad y almacenamiento son más dinámicos que la gestión de riesgos de TI, por lo que, por razones de efectividad, su gobierno requiere ser manejado por separado del gobierno de riesgos de TI. Sin embargo, por eficiencia operativa, es necesario mantener la política de seguridad de la información en sintonía con la política de riesgos de TI.
Política de gestión de crisis	Al igual que la seguridad de TI, la gestión de redes y la seguridad de datos, la gestión de crisis de TI es una de las políticas de nivel operativo que debe considerarse para la gestión completa de riesgos de TI. Establece las directrices sobre cómo actuar en situaciones de crisis y detalla la secuencia en la cual se enfrenta cada una de las áreas de riesgo (clave) identificadas.
Política de gestión de la entrega de servicios de TI por terceros	Establece las directrices para la gestión de riesgos relacionados con los servicios de terceros. Establece un marco de referencia de expectativas de comportamiento y las precauciones de seguridad tomadas por terceros proveedores de servicios para gestionar el riesgo relacionado con la prestación del servicio.

Figura 16—Ejemplos de políticas de riesgo (cont.)

Política	Descripción
Política de continuidad de negocio	Contiene el compromiso y la visión de la gerencia sobre: <ul style="list-style-type: none"> • Análisis de impacto en el negocio (BIA). • Planes de contingencia de negocios con recuperación confiable. • Requerimientos de recuperación para los sistemas críticos. • Umbralas y procedimientos definidos para contingencias. • Manejo de escalamiento de incidentes. • Plan de recuperación de desastres (DRP). • Entrenamiento y pruebas.
Política de gestión de programas/proyectos	Se ocupa de la gestión de los riesgos vinculados a los programas y proyectos. Detalla la posición y las expectativas de la gerencia respecto a la gestión de programas y proyectos. Además, se encarga de la rendición de cuentas, metas y objetivos respecto al desempeño, presupuesto, análisis de riesgos, reporte y mitigación de eventos adversos durante la ejecución de programas y proyectos.
Política de recursos humanos (RH)	Detalla lo que pueden esperar los empleados de la organización y lo que espera la organización de los empleados, detallando el comportamiento aceptable e inaceptable de los empleados y, al hacerlo, gestiona el riesgo que está relacionado con el comportamiento de las personas.
Política del riesgo de fraude	Se refiere a la protección de pérdidas o daños a la marca de la empresa, la reputación y los activos, resultantes de incidentes de fraude o inconducta. La política ofrece orientación a todos los empleados acerca del reporte de cualquier actividad sospechosa y formas de manejar la información sensible y las evidencias. Ayuda a fomentar una cultura antifraude y crear conciencia sobre el riesgo.
Política de cumplimiento	Explica el proceso de evaluación sobre el cumplimiento de requerimientos regulatorios, contractuales e internos. Enumera los roles y responsabilidades de las diferentes actividades del proceso y proporciona orientación sobre las métricas que se utilizarán para medir el cumplimiento.
Política de ética	Define elementos esenciales de interacción entre las personas de una organización, así como la forma en que van a interactuar con cualquier consumidor o cliente al que atienden.
Política de gestión de la calidad	Detalla la visión de la gerencia sobre los objetivos de calidad de la organización, el nivel aceptable de calidad y las obligaciones de los departamentos específicos para asegurar la calidad.
Política de gestión del servicio	Proporciona dirección y orientación para asegurar la gestión e implementación efectiva de todos los servicios de tecnología de la información para satisfacer los requerimientos del negocio y de los clientes, en un marco de medición del desempeño. Además se ocupa de la gestión de riesgos relacionados con servicios de TI. El marco de referencia ITIL V3 ofrece orientación detallada sobre la gestión del servicio y la optimización de los riesgos relacionados con los servicios.
Política de gestión de cambios	Comunica la intención de la gerencia de que los cambios en la tecnología de información de la empresa sean gestionados e implementados de forma que se minimice el riesgo e impacto para las partes interesadas. La política contiene información sobre los activos a los cuales aplica y el proceso establecido de gestión de cambios estándar.
Política de delegación de autoridad	Detalla: <ul style="list-style-type: none"> • La autoridad que el consejo directivo conserva estrictamente para sí. • Los principios generales de delegación de autoridad. • Un calendario de la delegación de autoridad (incluyendo límites claros). • Una definición clara de las estructuras organizativas a las que el consejo directivo delega su autoridad.
Política de denuncias	Debe: <ul style="list-style-type: none"> • Animar a los empleados a plantear inquietudes y preguntas. • Ofrecer los medios para que los empleados planteen inquietudes con absoluta confianza. • Asegurar que los empleados recibirán una respuesta a las inquietudes planteadas y ser capaz de escalar las inquietudes si ellos no quedan satisfechos con las respuestas. • Asegurar que los empleados están protegidos cuando se plantean problemas y que no teman represalias.
Política de control Interno	El propósito es: <ul style="list-style-type: none"> • Comunicar los objetivos del control interno de la gerencia. • Establecer estándares para el diseño y operación del sistema de control interno de la empresa para reducir la exposición a todos los riesgos que enfrenta.
Política de propiedad intelectual (PI)	El propósito es asegurar que todos los riesgos relacionados con el uso, propiedad, venta y distribución de los productos del esfuerzo creativo relacionados con TI de los empleados de una empresa; por ejemplo, el desarrollo de software, es detallado de manera apropiada desde el inicio de cualquier esfuerzo.
Política de privacidad de los datos	Una declaración o documento que revela las formas en que una parte reúne, utiliza, divulga y gestiona los datos personales. La información personal puede ser cualquier cosa que puede utilizarse para identificar a un individuo, incluyendo, pero no limitándose a, el nombre, la dirección, fecha de nacimiento, estado civil, información de contacto, número y fecha de expiración de la identificación, registros financieros, información de crédito, historial médico, destino de viajes, e intención de adquirir bienes y servicios. La política define la forma en que una empresa recolecta, almacena y libera la información personal que recopila. La política informa al cliente de la información específica que se recoge, y si se mantiene confidencial, se comparte con socios comerciales, o se vende a otras firmas o empresas. Además, la política asegura el cumplimiento del marco legal relevante en relación con la protección de datos.

CAPÍTULO 3

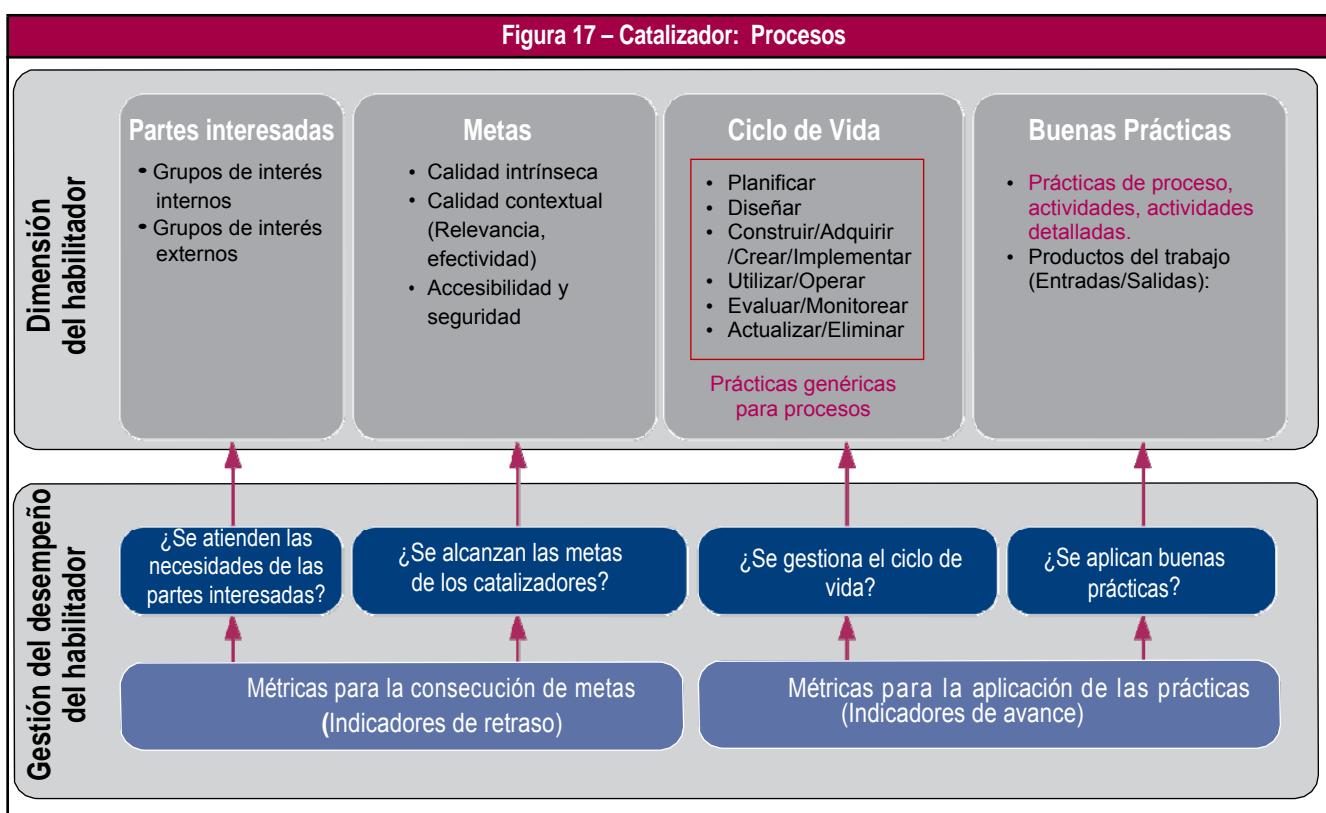
CATALIZADOR: PROCESOS

Este capítulo contiene una guía sobre cómo los procesos pueden habilitar el gobierno y la gestión del riesgo en una empresa (la perspectiva de la función de riesgos). Para este propósito, se tratan los siguientes temas:

- El modelo de procesos.
- Una lista de todos los procesos relevantes para el gobierno y la gestión del riesgo. Esta lista es un subconjunto de los procesos de COBIT 5 descritos en *COBIT 5: Procesos Catalizadores*, y está agrupada en dos categorías:
 - Procesos clave de soporte para el gobierno y la gestión del riesgo.
 - Otros procesos de soporte para el gobierno y la gestión del riesgo.
- Nota:** Estos procesos no incluyen los procesos principales de la gestión de riesgos (EDM03 y APO12, es decir, describiendo el análisis de riesgo y la respuesta al riesgo, que están descritos en la sección 2B de esta guía y en el apéndice C).
- La descripción de la información detallada para cada proceso. El apéndice B.2 incluye la información detallada vigente.

3.1 El modelo de Procesos

Un proceso se define como “el conjunto de prácticas, influenciadas por las políticas y procedimientos de una empresa, que reciben entradas de varias fuentes (incluyendo otros procesos), manipulan las entradas y generan salidas (p. ej., productos y servicios)”.



El modelo de procesos (**figura 17**) muestra:

- **Partes interesadas:** Los procesos tienen partes interesadas internas y externas, con sus propios roles; las partes interesadas y sus niveles de responsabilidad están documentados en las matrices RACI (*Responsible, Accountable, Consulted, Informed*). Las partes interesadas externas incluyen a los clientes, socios de negocio, accionistas y reguladores. Las partes interesadas internas incluyen al consejo directivo, la gerencia, el staff y los voluntarios.
- **Metas:** Las metas de los procesos se definen como ‘una declaración que describe el resultado deseado del proceso. El resultado puede ser un artefacto, un cambio de estado significativo o una mejora significativa en la capacidad de otros procesos’. Son parte de la cascada de metas, es decir, que las metas del proceso apoyan las metas relacionadas con TI, que, a su vez, apoyan las metas de la empresa. Las metas del proceso pueden ser categorizadas en:
 - Metas intrínsecas: ¿El proceso tiene calidad intrínseca? ¿Es preciso y está alineado con las buenas prácticas?
 – ¿Cumple con las reglas internas y externas?
 - Metas contextuales: ¿El proceso ha sido personalizado y adaptado a la situación específica de la empresa?
 – ¿El proceso es relevante, entendible y fácil de aplicar?
 - Metas de accesibilidad y seguridad: El proceso se mantiene confidencial cuando así se lo requiere, y es conocido y accesible por aquellos que lo necesitan.
- **Ciclo de vida:** Cada proceso tiene un ciclo de vida. Está definido, creado, operado, monitoreado y ajustado/actualizado o desechado. Las prácticas genéricas de procesos tales como las definidas en el modelo de evaluación de procesos de COBIT (PAM), basado en el estándar ISO/IEC 15504, pueden ayudar en la definición, ejecución, monitoreo y optimización de procesos.
- **Buenas prácticas:** *COBIT 5: Procesos Catalizadores* contiene un modelo de referencia de procesos, en el que se describen las buenas prácticas internas de procesos en niveles crecientes de detalle: prácticas, actividades y actividades detalladas. En esta publicación, esta buena práctica no se repite; sólo se desarrolla orientación específica de riesgo en caso de ser relevante.

3.2 Perspectiva de la función de riesgos: Procesos que apoyan la gestión de riesgos

El propósito de esta sección es identificar y discutir todos los procesos de COBIT 5 requeridos para construir y sostener el gobierno y la gestión del riesgo en la empresa, de forma efectiva y eficiente. En otras palabras, enumera todos los procesos que van a apoyar la función de riesgos.

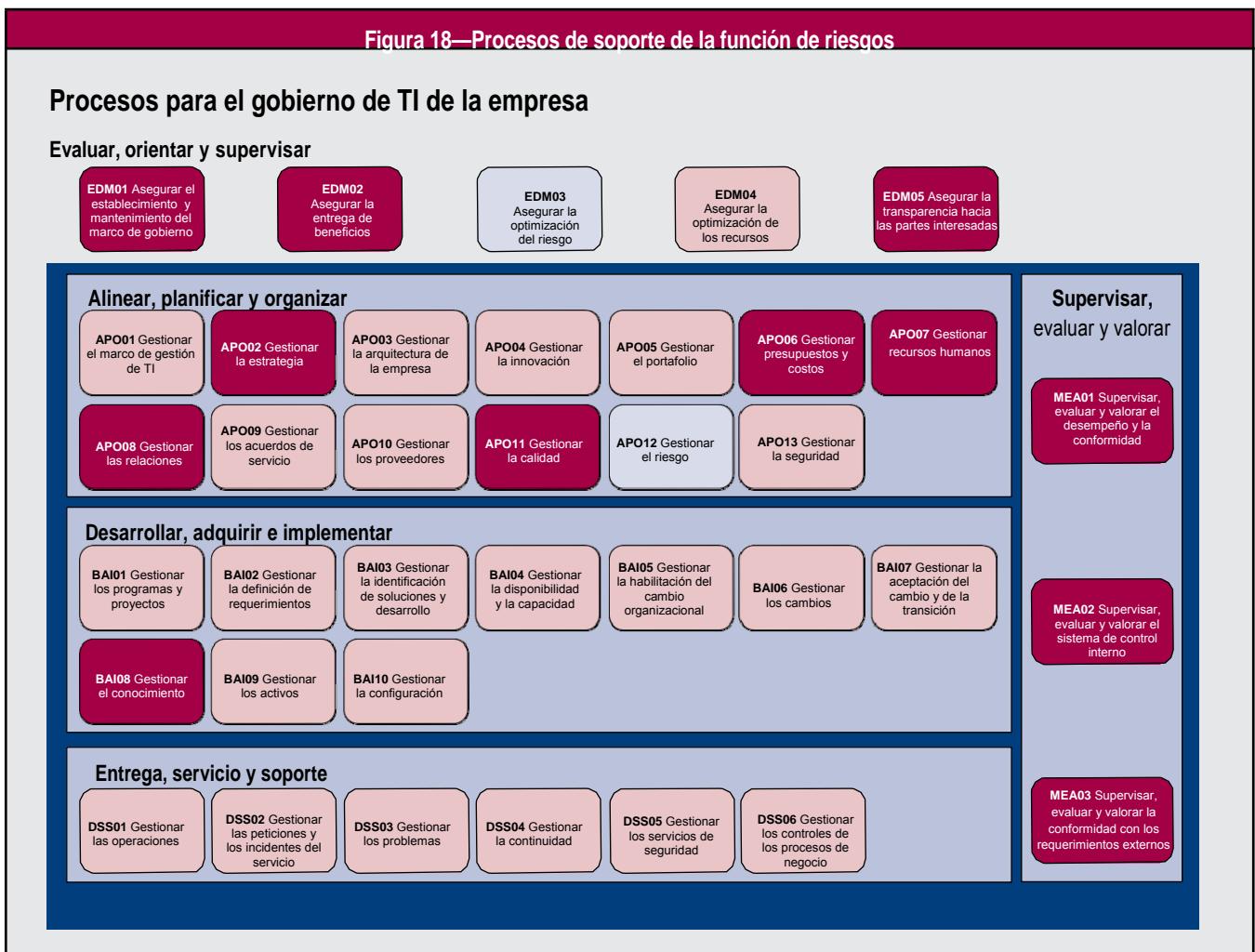
Estos procesos no incluyen los procesos principales (EDM03 y APO12) para el gobierno y la gestión del riesgo, los que se describen con detalle en la sección 2B de esta guía.

La información detallada de procesos y específica de riesgo para los procesos de COBIT 5 incluye:

- **Metas y métricas del proceso:** Por cada proceso, se incluye un número limitado de metas de proceso específicos de riesgo, y para cada meta de proceso, se lista un número limitado de ejemplos de métricas específicas de riesgo, reflejando la clara relación entre metas y métricas.
- **Descripción detallada de las prácticas del proceso:** Esta descripción contiene, para cada práctica:
 - Entradas y salidas (productos) específicas de riesgo, con indicación de origen y destino.
 - Actividades del proceso específicas de riesgo.

La **figura 18** resalta los procesos clave que soportan COBIT 5 (mostrados en rosa oscuro), así como los otros procesos de soporte (mostrados en rosa claro). Los párrafos que siguen a la figura 18 ofrecen una breve descripción de cada proceso de soporte, el motivo por el cual es importante y las salidas claves.

Nota: Los procesos principales del riesgo (mostrados en celeste) están detallados en el capítulo 1 de la sección 2B.



Los procesos listados en la **figura 19** son procesos clave de soporte de la función de riesgos en la empresa.

Figura 19—Procesos clave de soporte de la función de riesgos

Identificación del proceso	Descripción	Productos específicos de riesgo
EDM01 Asegurar el establecimiento y mantenimiento del marco de gobierno.	El gobierno y la gestión de los riesgos requieren el establecimiento de un marco adecuado de gobierno para implementar estructuras, principios, procesos y prácticas.	Principios guía del gobierno del riesgo.
EDM02 Asegurar la entrega de beneficios.	Este proceso se focaliza en el manejo del valor que genera la función de riesgos.	Acciones para mejorar la entrega de valor del riesgo.
EDM05 Asegurar la transparencia hacia las partes interesadas.	La función de riesgos de una empresa, requiere de la medición transparente del desempeño y la conformidad, con metas y métricas aprobadas por las partes interesadas.	Evaluación de los requisitos del informe de riesgos.
APO02 Gestionar la estrategia.	La estrategia de gestión de riesgos de TI debe estar bien definida y alineada con el enfoque ERM.	Estrategia de la gestión de riesgos.
APO06 Gestionar presupuestos y costos.	La función de riesgos debe presupuestarse.	Requisitos financieros y presupuestarios.
APO07 Gestionar los recursos humanos.	La gestión de riesgos requiere una cantidad adecuada de personas, habilidades y experiencia.	Marco de competencias de recursos humanos.
APO08 Gestionar las relaciones.	Mantener las relaciones entre la función de riesgos y el negocio.	Plan de comunicación de la gestión de riesgos.
APO11 Gestionar la calidad.	La calidad es un componente que no debe omitirse en la gestión efectiva de riesgos. Los entregables de la función de riesgos debieran ser tratados siguiendo el sistema de gestión de calidad de la empresa.	Revisión de la calidad de los entregables de la función de riesgos.
BAI08 Gestionar el conocimiento.	La función de riesgos requiere el conocimiento necesario para apoyar al personal en sus actividades.	<ul style="list-style-type: none"> Clasificación de la información de la función de riesgos. Control de acceso sobre dicha información. Reglas para desechar la información.

Figura 19—Procesos clave de soporte de la función de riesgos (cont)

Identificación del proceso	Descripción	Productos específicos de riesgo
MEA01 Supervisar, evaluar y valorar el desempeño y la conformidad.	El riesgo es un aspecto clave en la supervisión, evaluación y valoración del negocio y de TI.	Métricas y objetivos para la supervisión del riesgo.
MEA02 Supervisar, evaluar y valorar el sistema de control interno.	Los controles internos son claves para la supervisión y contención del riesgo para evitar que el riesgo se materialice.	Resultados de la supervisión y revisión del control interno.
MEA03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos.	El cumplimiento de las leyes, normas y requerimientos contractuales representa un riesgo que debe ser supervisado, evaluado y valorado en línea con la estrategia de la empresa.	Informe de problemas de incumplimiento y sus causas.

Los otros procesos de soporte, enumerados en la **figura 20**, no se describen en más detalle en esta guía. La guía de procesos estándar de COBIT 5 se incluye en *COBIT 5: Procesos Catalizadores*.

Figura 20—Otros procesos de soporte para la función de riesgos

Identificación del proceso	Descripción
EDM04 Asegurar la optimización de los recursos.	La función de riesgos necesita optimizar la utilización de sus recursos.
APO01 Gestionar el marco de gestión de TI.	La función de gestión de riesgos apoya al marco de gestión de TI.
APO03 Gestionar la arquitectura empresarial.	La función de riesgos debería utilizar la arquitectura de la empresa como fuente de información clave para apoyar la evaluación de riesgos.
APO04 Gestionar la innovación.	La función de riesgos siempre debería estar buscando nuevas metodologías, tecnologías y herramientas que puedan apoyar al gobierno y la gestión del riesgo en la empresa.
APO05 Gestionar el portafolio.	El portafolio de riesgos de los sistemas debe ser gestionado y considerado como una fuente principal de información.
APO09 Gestionar los acuerdos de servicio.	La función de riesgos puede hacer uso de proveedores de servicios (internos o externos), p.ej., una función de riesgos de TI compartida.
APO10 Gestionar los proveedores.	La función de riesgo puede hacer uso de proveedores de servicios (internos o externos), p.ej., una función de riesgos de TI compartida.
APO13 Gestionar la seguridad.	La función de riesgos tiene requerimientos de seguridad que se necesita gestionar.
BAI01 Gestionar los programas y proyectos.	Será necesario implementar un nuevo software de gestión de riesgos.
BAI02 Gestionar la definición de requisitos.	Será necesario desarrollar los requisitos del nuevo software de gestión de riesgos.
BAI03 Gestionar la identificación y la construcción de soluciones.	El nuevo sistema de gestión de riesgos necesitará soluciones de identificación y construcción.
BAI04 Gestionar la disponibilidad y la capacidad.	Será necesario gestionar la disponibilidad y capacidad del nuevo software de gestión de riesgos.
BAI05 Gestionar la habilitación del cambio organizativo.	El nuevo software de gestión de riesgos necesitará la gestión del cambio.
BAI06 Gestionar los cambios.	El software de gestión de riesgos necesitará la definición de un proceso de cambios.
BAI07 Gestionar la aceptación del cambio y de la transición.	El sistema de gestión de riesgos necesitará la definición de un proceso de aceptación de usuario.
BAI09 Gestionar los activos.	La función de riesgos debe estar involucrada en la gestión de sus activos de TI.
BAI10 Gestionar la configuración.	La función de riesgos debe gestionar su configuración de TI en conjunto con el departamento de TI.
DSS01 Gestionar las operaciones.	La función de riesgos debe gestionar las herramientas y aplicaciones de TI que soportan sus operaciones diarias.
DSS02 Gestionar las peticiones y los incidentes del servicio.	La función de riesgos necesita hacer un seguimiento de los requerimientos de servicio e incidentes de sus activos de TI.
DSS03 Gestionar los problemas.	La función de riesgos necesita hacer un seguimiento de los problemas relacionados con sus activos de TI.
DSS04 Gestionar la continuidad.	La función de riesgos debe gestionar su propia continuidad de negocio.
DSS05 Gestionar los servicios de seguridad.	La función de riesgos necesita cumplir con las políticas de seguridad relacionadas con sus activos de TI.
DSS06 Gestionar los controles de los procesos de negocio.	La función de riesgos necesita gestionar los controles de procesos de negocio relacionados con sus activos de TI.

CAPÍTULO 4

CATALIZADOR: ESTRUCTURAS ORGANIZATIVAS

Este capítulo contiene una guía sobre cómo las estructuras organizativas pueden habilitar el gobierno y la gestión del riesgo en una empresa (perspectiva de la función de riesgos). Para este propósito, se tratan los siguientes temas:

- El modelo de Estructuras Organizativas.
- Una lista de todas las estructuras organizativas relevantes para el gobierno y la gestión de riesgos. Esta lista es un subconjunto extendido de la lista de roles de COBIT 5 en *COBIT 5: Procesos Catalizadores*, y está agrupado en dos categorías de estructuras que son:
 - Principales estructuras organizativas relacionadas con el gobierno y la gestión del riesgo.
 - Estructuras organizativas de apoyo.
- Una descripción de la información detallada para cada estructura organizativa. El apéndice B.3 incluye la información detallada vigente.

4.1 El modelo de Estructuras Organizativas

Error! Not a valid link.

El modelo de Estructuras Organizativas (**figura 21**) muestra:

- **Partes interesadas:** Pueden ser internas o externas a la empresa. Estas partes interesadas incluyen a los miembros individuales de las estructuras, otras estructuras, entidades organizacionales, clientes, proveedores y reguladores. Sus roles varían e incluyen la toma de decisiones, influenciar y asesorar. Los intereses de cada una de las partes interesadas también varían, es decir, ¿qué interés tienen ellos en las decisiones tomadas por la estructura?
- **Metas:** Las metas incluyen tener un mandato propio, principios de operación bien definidos y la aplicación de otras buenas prácticas. El resultado de este habilitador debería incluir numerosas actividades y decisiones útiles.
- **Ciclo de vida:** Una estructura organizativa tiene un ciclo de vida. Es creada, existe, es adaptada, y finalmente, puede ser disuelta. Durante su inicio, tiene que definirse un mandato, es decir, una razón y propósito para su existencia.
- **Buenas prácticas:** Se puede distinguir un número de buenas prácticas para las estructuras organizativas, tales como:
 - Principios operativos: Disposiciones prácticas sobre cómo opera la estructura, tales como la frecuencia de reuniones, documentación y reglas de mantenimiento.

- Decisiones: La dirección basada en riesgos considera el procesamiento de entradas relevantes y los resultados esperados o requeridos.
- Ámbito de control: Límites del derecho a las decisiones de la estructura organizativa.
- Niveles de autoridad/decisión: Las decisiones que la estructura está autorizada a tomar.
- Delegación de autoridad: La autoridad de la estructura para delegar un subconjunto de sus derechos de decisión a otras estructuras que le reportan.
- Procedimientos de escalamiento: La ruta de escalamiento para una estructura, el cual describe las acciones requeridas en caso de problemas en la toma de decisiones.

4.2 Perspectiva de la función de riesgos: Gobierno –y gestión– del riesgo relacionado con la Estructura Organizativa

El propósito de esta sección es identificar y discutir todas las estructuras/roles organizacionales que se requieren para construir y sostener el gobierno y la gestión del riesgo en la empresa, de forma efectiva y eficiente. Las estructuras y los roles principales son aquellos que invierten la mayor parte de su tiempo en el gobierno y la gestión del riesgo. Los roles de soporte apoyan al gobierno y la gestión del riesgo solo en una pequeña parte de su trabajo total.

La **figura 22** define las principales estructuras organizativas que soportan la función de la gestión de riesgos:

Figura 22–Principales estructuras organizativas	
Rol/Estructura	Definición/Descripción
Comité de Gestión de Riesgo Corporativo (ERM)	Es el grupo de ejecutivos corporativos que es responsable de la colaboración y consenso a nivel corporativo requeridos para soportar las actividades y decisiones de ERM. Este comité es considerado para ser la segunda línea de defensa contra las manifestaciones del riesgo. Se puede establecer un Consejo de Riesgos de TI para considerar los riesgos de TI con mayor detalle y asesorar al comité de ERM. Los miembros de este comité son usualmente miembros del consejo directivo y está liderado por el CEO.
Grupo de Riesgo Corporativo	El grupo de riesgo corporativo considera al riesgo con mayor detalle y asesora al comité de ERM. El grupo de riesgo corporativo es un conjunto de recursos de TI y de negocios que ofician como facilitadores del programa de gestión de riesgos, manteniendo los registros y los perfiles de riesgo de la empresa. Ellos son considerados la primera línea de defensa contra las manifestaciones del riesgo.
Función de Riesgos	El oficial senior de mayor rango de la empresa quien es responsable de todos los aspectos de la gestión de riesgos a través de toda la empresa, incluyendo asumir la dirección del Comité de ERM. Se puede establecer una función de Oficial de Riesgos de TI para atender estos riesgos.
Departamento de Auditoría	Es la función corporativa responsable de proporcionar reportes de auditoría interna sobre los riesgos asociados con las brechas identificadas en los controles mientras se revisa el desempeño ¹ . Es considerada la tercera línea de defensa, por tanto, es posible convocar a un representante al Comité de ERM.
Departamento de Cumplimiento	Es la función corporativa responsable de identificar los riesgos corporativos relacionados con regulaciones, mandatos legales, políticas y estándares internos.

Las estructuras organizativas de la **figura 22** también pueden ser relacionadas con el modelo de las “tres líneas de defensa”, como se muestra en la **figura 23**.



¹ Para una descripción detallada del “Departamento de Auditoría”, referirse al apéndice B.3.

SECCIÓN 2A, CAPÍTULO 4

HABILITADOR: ESTRUCTURAS ORGANIZATIVAS

En el modelo de las tres líneas de defensa², el control gerencial es la primera línea de defensa en la gestión de riesgos. Los diferentes controles del riesgo y actividades de supervisión del cumplimiento establecidas por la gerencia son la segunda línea de defensa, y el aseguramiento independiente es la tercera línea de defensa. Cada una de estas tres líneas cumple un rol distinto dentro del amplio marco de trabajo del gobierno corporativo:

- Como primera línea de defensa, los gerentes operacionales gestionan sus propios riesgos. Ellos también son responsables de la implementación de acciones correctivas en los procesos y controles con deficiencias.
- En la práctica, una sola línea de defensa puede a menudo ser inadecuada. La gerencia establece varias funciones de gestión de riesgos y cumplimiento para ayudar a construir y/o monitorear la primera línea de controles de defensa.
- Los auditores internos proveen al equipo de gobierno y gerencia senior de un aseguramiento comprehensivo basado en los más altos niveles de independencia y objetividad dentro de la empresa. Este alto nivel de independencia no se observa en la segunda línea de defensa. La auditoría interna también proporciona aseguramiento sobre la manera en la cual la primera y segunda línea de defensa logran gestionar los riesgos.

Aunque ni los equipos de gobierno ni la gerencia senior están considerados dentro de las tres líneas de defensa del modelo, ellos constituyen las partes interesadas primariamente servidas por las líneas de defensa, y además son los que están mejor posicionados para ayudar a asegurar que el modelo de las tres líneas de defensa se refleje en los procesos de control y gestión de riesgos de la empresa.

En forma colectiva, la gerencia senior y los equipos de gobierno tienen la responsabilidad y la obligación de rendir cuentas en el establecimiento de los objetivos de la empresa, definiendo estrategias para lograr esos objetivos y estableciendo estructuras de gobierno y procesos para la mejor gestión de riesgos en el logro de tales objetivos.

Se pueden encontrar roles/estructuras adicionales que tienen cierto efecto en la gestión de riesgos; aunque no están directamente involucrados en la gestión de riesgos, son partes interesadas relevantes en este proceso. La **figura 24** enumera otros roles y estructuras relevantes, proporcionando una breve descripción de lo que cada uno hace para apoyar la función de riesgos.

Figura 24—Otras estructuras relevantes para el riesgo

Rol/Estructura	Definición/Descripción	Rol en el proceso de riesgo
Consejo Directivo	El grupo de los más altos ejecutivos senior y no ejecutivos de la empresa, quienes son responsables del gobierno corporativo y tienen control global sobre los recursos.	<ul style="list-style-type: none"> • Supervisa el impacto del riesgo corporativo sobre los objetivos corporativos³ y toma decisiones sobre el riesgo para proteger el valor de los accionistas a un óptimo costo de los recursos. • Establece el tono directivo respecto a la gestión y la concientización del riesgo.
CEO	El ejecutivo senior de más alto nivel en la empresa, a cargo de la gerencia general de la empresa.	Ofrece apoyo ejecutivo y colabora en las decisiones de gestión de riesgos.
Comité estratégico (Ejecutivo de TI)	Un grupo de ejecutivos senior designados por el consejo directivo para asegurar que dicho consejo se mantenga involucrado e informado de las principales decisiones y aspectos relacionados con TI. El comité es responsable de la gestión del portafolio de inversiones habilitadas por TI, así como los servicios y activos de TI, asegurando la entrega de valor y la gestión de los riesgos. El comité es normalmente dirigido por un miembro del consejo directivo y no por el ejecutivo en jefe de información (CIO).	Proactivo en la gestión de los riesgos relacionados con el portafolio de las inversiones de TI.
Oficial en jefe de Operaciones (COO)	El ejecutivo senior de más alto nivel de la empresa que es responsable de las operaciones de la empresa.	Consultor en riesgo operacional.
Ejecutivo de negocios	Un miembro de la gerencia senior que es responsable de la operación de una unidad de negocio específica o subsidiaria. Esto incluye a propietarios de las líneas de negocio clave y jefes de departamentos tales como: ventas, marketing, recursos humanos, manufactura, etc.	<ul style="list-style-type: none"> • Consultor en riesgos relacionados con líneas de negocio o departamentos. • Acepta la propiedad de riesgos asignados y reporta sobre los avances en la mitigación.
Oficial en jefe de Tecnología CIO/CTO	El ejecutivo senior de más alto nivel en la empresa que es responsable de alinear las TI con las estrategias de negocio y responsable de dar cuenta por la planificación, recursos y gestión de la entrega de servicios y soluciones de TI para soportar los objetivos de la empresa.	Consultor en aspectos técnicos y acciones sobre el riesgo.

² Fuente: Instituto de Auditoría Interna (IIA); *IIA Position Paper: The Three Lines of Defense en Effective Risk Management and Control*, USA, 2013

³ Para más información en el rol del Consejo Directivo en la supervisión de riesgos, ver “Risk Governance: Balancing Risk and Rewards” reporte del Blue Ribbon Commission, National Association of Corporate Directors (NACD), 2009

Figura 24—Otras estructuras relevantes para el riesgo (cont.)

Rol/Estructura	Definición/Descripción	Rol en el proceso de riesgo
Propietario de proceso de negocio	Una persona responsable por el desempeño de un proceso en el logro de sus objetivos, aprobando cambios y logrando mejoras en el proceso. En general, un propietario de proceso de negocio debe estar en un adecuado nivel en la empresa y tener autoridad para asignar recursos hacia las actividades de gestión de riesgos específicos del proceso.	<ul style="list-style-type: none"> Consultor en riesgos relacionados a procesos de negocio. Acepta la propiedad de riesgos asignados y reporta sobre los avances en la mitigación.
Oficial en jefe de Seguridad de la Información (CISO)	El ejecutivo senior de más alto nivel en la empresa que es responsable de la seguridad de la información de la empresa en todas sus formas.	<ul style="list-style-type: none"> Consultor en riesgos de seguridad. Coordina respuestas a incidentes.
Oficial en jefe de Finanzas (CFO)	El ejecutivo senior de más alto nivel en la empresa que es responsable de todos los aspectos de la gestión financiera, incluyendo el riesgo y los controles financieros y las cuentas fiables y precisas.	Consultor en los niveles aceptables de exposición a pérdidas, la importancia de los factores de riesgo y sobre los costos de las opciones de respuesta al riesgo.
Gerente de Continuidad del Negocio	Una persona que gestiona, diseña y/o evalúa la capacidad de la continuidad del negocio de la empresa para asegurar que las funciones críticas de la empresa continuarán operando luego de eventos de interrupción.	Consultor en interrupciones de las operaciones de la empresa.
Propietario de los procesos (servicios) de TI	Una persona líder que es responsable y rinde cuentas sobre los procesos de TI y/o los servicios proporcionados.	<ul style="list-style-type: none"> Consultor en riesgos relacionados a los procesos o servicios de TI Acepta la propiedad de los riesgos asignados y reporta sobre los avances en la mitigación.
Gerente de Servicios	Una persona que gestiona el desarrollo, implementación, evaluación y la administración en marcha de productos y servicios existentes y nuevos para un cliente específico, usuario o grupo de clientes.	Consultor en la gestión de servicios relacionados a riesgos.
Director de Recursos Humanos	El ejecutivo senior de más alto nivel en la empresa que es responsable de la planificación y políticas con respecto a los recursos humanos de la empresa.	Consultor sobre aspectos y acciones del riesgo respecto de los recursos humanos.
Oficial de Privacidad	Una persona que es responsable de monitorear el riesgo e impacto de leyes sobre privacidad en la empresa, así como guiar y coordinar la implementación de políticas y actividades para asegurar que se cumplan las directivas de privacidad.	Consultor sobre aspectos clave relacionados al monitoreo del riesgo e impacto en el negocio de leyes y políticas de privacidad.
Comité directivo para programas y proyectos	Un grupo de partes interesadas y expertos quienes son responsables de guiar los programas y proyectos, incluyendo la gestión y monitoreo de planes, asignación de recursos, entrega de beneficios y valor, así como la gestión de riesgos en programas y proyectos.	Articula los riesgos asociados con programas y proyectos.
Oficial en jefe de Seguros	El ejecutivo senior de más alto nivel en la empresa que está a cargo de gestionar las políticas sobre seguros.	Consultor en transferir/compartir riesgos.
Procurador	La función que vincula y gestiona a proveedores y los procesos asociados, tales como contratos y la cadena completa de valor.	<ul style="list-style-type: none"> Consultor y asesor en la gestión de riesgos de terceros. Negocia los términos de los contratos para gestionar los riesgos y la gestión del desempeño.

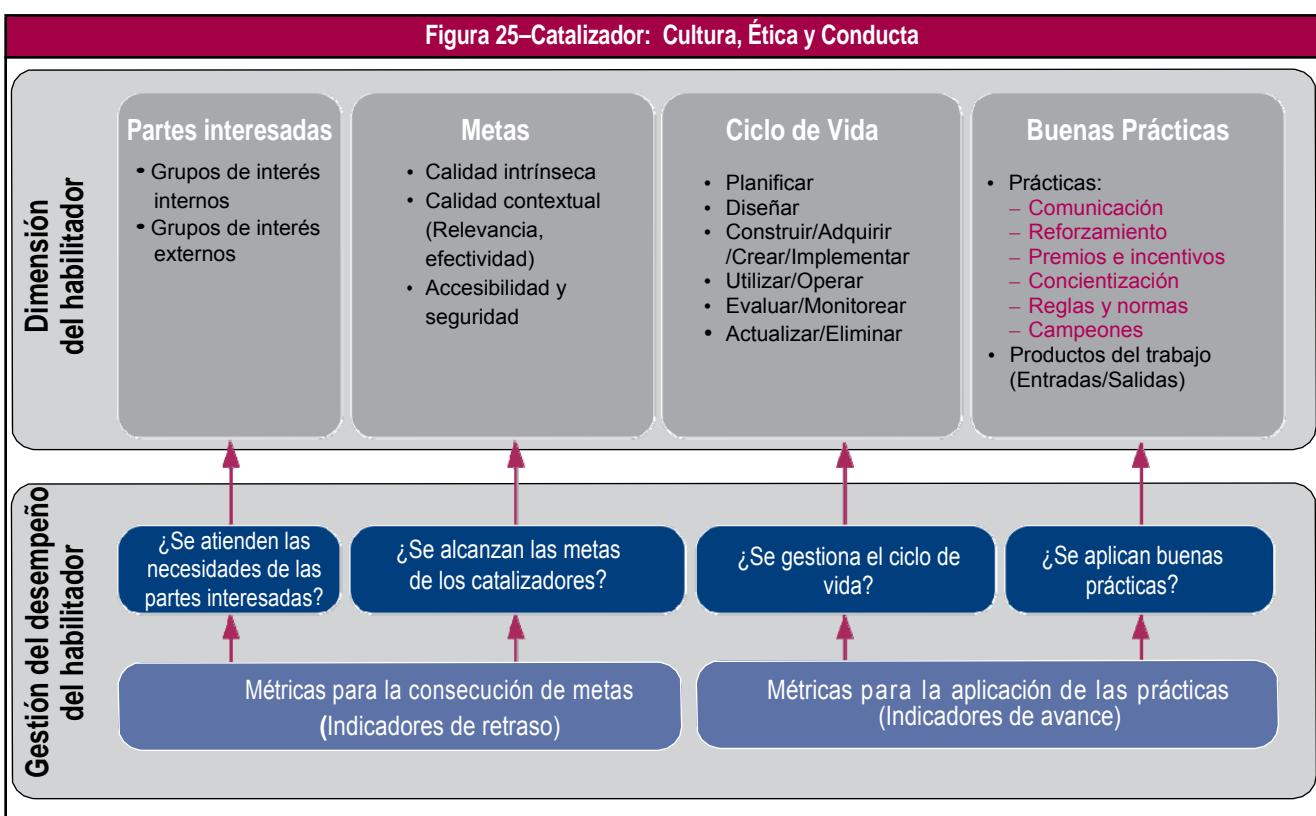
CAPÍTULO 5

CATALIZADOR: CULTURA, ÉTICA Y CONDUCTA

Este capítulo contiene una guía sobre cómo la cultura y el comportamiento pueden habilitar el gobierno y la gestión del riesgo en una empresa (perspectiva de la función de riesgos). Para este propósito, se tratan los siguientes temas:

- El modelo de Cultura, Ética y Conducta.
- Un listado de comportamientos seleccionados que son relevantes para el logro del gobierno y gestión del riesgo.
- Una descripción de la información detallada para cada elemento de comportamiento. El apéndice B.4 incluye la información detallada vigente.

5.1 El modelo de Cultura, Ética y Conducta



El modelo de Cultura, Ética y Conducta (**figura 25**) muestra:

- **Partes interesadas:** Pueden ser internas o externas a la empresa. Las partes interesadas internas incluyen a toda la empresa. Las externas incluyen a los reguladores, los auditores externos o cuerpos de supervisión. Los intereses son de dos tipos: algunas partes interesadas como los oficiales de cumplimiento legal, gerentes de riesgo, gerentes de RRHH y comités de remuneraciones deben definir, implementar y reforzar comportamientos deseables; mientras que otras tienen que alinearse con las reglas y normas definidas.
- **Metas:** Las metas de la cultura, ética y comportamiento se relacionan con:
 - Ética organizacional, determinada por los valores que la empresa privilegia y quiere ser reconocida.
 - Ética individual, determinada por los valores personales de cada individuo en la empresa y que dependen, en gran medida, de factores externos tales como la religión, factores étnicos, socioeconómicos, geográficos y experiencias personales.
 - Comportamientos individuales, que colectivamente determinan la cultura de una empresa. Muchos factores, como los externos ya mencionados, las relaciones interpersonales en las empresas, los objetivos y las ambiciones personales, también influyen en los comportamientos. Algunos tipos de comportamientos que pueden ser relevantes en este contexto incluyen:
 - Conducta hacia la toma de riesgos: ¿Cuánto riesgo siente la empresa que puede absorber y cuál riesgo está dispuesta a tomar?

- Conducta hacia el seguimiento de políticas: ¿En qué medida las personas adoptarán y/o cumplirán la política?
- Conducta hacia resultados negativos: ¿Cómo enfrenta la empresa a los resultados negativos, como por ejemplo, eventos de pérdida u oportunidades perdidas? ¿Aprenderá de ellos y tratará de ajustarse, o se echarán culpas sin tratar la causa raíz?
- **Ciclo de vida:** La cultura organizacional, postura ética y comportamientos individuales, etc., tienen sus ciclos de vida. Comenzando desde una cultura existente, una empresa puede identificar los cambios que se necesitan y trabajar en su implementación. Se pueden utilizar varias herramientas descritas en las buenas prácticas.
- **Buenas prácticas:** Las buenas prácticas para crear, fomentar y mantener comportamientos deseados en toda la empresa incluyen:
 - Comunicación de los comportamientos deseados y de los valores corporativos subyacentes, a través de toda la empresa.
 - Concientización del comportamiento deseado, reforzado por el comportamiento ejemplar de la alta gerencia y otros campeones.
 - A menudo, como parte del programa de reconocimiento y recompensa de RRHH, se establecen incentivos que fomentan el comportamiento deseado y medidas disuasivas que desalientan el comportamiento no deseable.
 - Re-evaluaciones de expectativas, influencias y cambios en el comportamiento e informes del comportamiento existente versus el comportamiento que percibe la gerencia.
 - Reglas y normas que ofrecen mayor orientación sobre el comportamiento organizacional deseado, y que vinculan claramente a los principios y políticas que una empresa pone en práctica.

5.2 Perspectiva de la función de riesgos: Gobierno –y gestión– del riesgo relacionado con la Cultura y Conducta.

El propósito de esta sección es identificar elementos de cultura y comportamiento relevantes que se requieren para construir y sostener el gobierno y la gestión del riesgo en la empresa, de forma efectiva y eficiente, que contribuyan a establecer y mantener una cultura consciente de los riesgos en todos los niveles de la empresa. En otras palabras, se enumeran comportamientos relevantes que apoyan a la función de riesgos. Los comportamientos deseables son clasificados de acuerdo a tres niveles dentro de la empresa:

- General (toda la empresa).
- Profesionales de riesgo.
- Gerencia.

Para cada comportamiento se listan la meta u objetivo clave, los criterios adecuados o los resultados deseados (**figura 26**).

Figura 26—Comportamientos relevantes para el gobierno y la gestión del riesgo

Conducta	Objetivo clave / Criterio adecuado / Resultado
Conducta General	
Tiene una cultura consciente del riesgo y del cumplimiento, incluyendo la identificación proactiva y el escalamiento de riesgos.	Debe definir un enfoque de gestión de riesgos y el apetito de riesgo. Se debe establecer la política de tolerancia cero hacia el incumplimiento de requisitos legales y regulatorios.
Tiene políticas definidas que han sido comunicadas y que guían el comportamiento.	Todo el personal comprende e implementa los requerimientos de la empresa, según se define en las políticas.
Muestra un comportamiento positivo hacia el escalamiento de problemas o de resultados negativos.	Aquellos que denuncian problemas son vistos como una contribución positiva a la empresa. Se evita la “cultura de la culpa”. El personal comprende la necesidad de la concientización del riesgo y de reportar posibles debilidades.
Reconoce el valor del riesgo.	El personal comprende la importancia para la empresa de mantener una conciencia del riesgo y el valor que la gestión de riesgos agrega a su rol.
Tiene una cultura transparente y participativa como un foco importante.	La comunicación es abierta y transparente, de modo que no se omitan los hechos, no se tergiversen o no se entiendan. Se evita el impacto negativo de agendas ocultas.
Se muestra respeto mutuo.	Se fomenta la colaboración de las partes interesadas y de los asesores de riesgos. Las personas son respetadas como profesionales y son tratados como expertos en sus roles.
El negocio acepta la propiedad del riesgo.	Las prácticas de riesgos están incorporadas a través de toda la empresa. Las responsabilidades son claras y se aceptan. Los riesgos de negocios relativos a TI son asumidos por el negocio y no son vistos como la responsabilidad del área de TI o de la función de riesgos.
Permite la aceptación del riesgo como una opción válida.	La gerencia entiende la probabilidad y consecuencias del impacto de la aceptación del riesgo. Se ha determinado que el impacto esté dentro de los márgenes de apetito de riesgo de la empresa.

SECCIÓN 2A, CAPÍTULO 5
HABILITADOR: CULTURA, ÉTICA Y COMPORTAMIENTO

Figura 26—Comportamientos relevantes para el gobierno y la gestión del riesgo (cont.)

Conducta	Objetivo clave / Criterio adecuado / Resultado
Conducta del profesional de riesgos (cont.)	
Demuestra esfuerzo en entender qué riesgo aplica a cada parte interesada y cómo impacta a sus objetivos.	Los profesionales de riesgos comprenden la realidad comercial del impacto del riesgo. Esto puede incluir requerimientos competitivos, operativos, regulatorios y de cumplimiento. Si bien puede haber riesgos comunes a ciertas industrias, cada empresa es única en términos de cómo estos tipos de riesgo impactan a los objetivos específicos de la empresa.
Crean conciencia y entendimiento de la política de riesgos.	El alineamiento entre la capacidad de riesgo, el apetito de riesgo y la política de la empresa, puede llevar a estrategias efectivas de riesgo.
Colaboración y comunicación en ambos sentidos durante la evaluación de riesgos.	La evaluación de riesgos es fundamentalmente precisa, completa y considera las necesidades de las partes interesadas.
El apetito de riesgo es claro y comunicado de manera oportuna a las partes interesadas relevantes.	Las partes interesadas gestionan el riesgo de forma más efectiva y hay un adecuado alineamiento con los objetivos y la estrategia organizacional.
Las políticas reflejan el apetito y la tolerancia al riesgo.	Los empleados y la gerencia operan dentro de la tolerancia al riesgo. Las líneas de negocio aplican formalmente la tolerancia y el apetito de riesgo en sus prácticas diarias. Existe un proceso claro para proponer y hacer cambios a los niveles de apetito de riesgo, con la consideración y aprobación de la alta gerencia.
La cultura de la empresa apoya las prácticas efectivas de riesgo.	Las partes interesadas entienden el riesgo desde la perspectiva de portafolio común (producto, proceso) y aplica la toma de decisiones basado en el riesgo en las prácticas diarias.
Se utilizan KRIs como indicadores de alerta temprana.	Los KRIs se asocian con métricas válidas y pueden ser usados como indicadores de fallas de procesos o controles. Las métricas de KRI están disponibles y se pueden acceder para reportes periódicos relacionados con los objetivos.
Se actúa ante indicadores de riesgo o eventos que caen fuera de los niveles de apetito y tolerancia al riesgo.	Los indicadores de riesgo están vinculados a la respuesta de riesgo de la gerencia y a las actividades de remediación.
Conducta de la gerencia	
La gerencia senior establece la dirección y demuestra visible y genuino apoyo a las prácticas de riesgo.	Se mantiene la calidad de las prácticas de gestión de riesgos mediante el apoyo genuino de la gerencia senior.
La gerencia articula con todas las partes interesadas relevantes para acordar acciones y seguimiento de los planes de acción.	Las partes interesadas correctas están apropiadamente involucradas para asegurar la oportuna resolución de problemas y el logro de los planes de negocio.
Se obtiene un compromiso genuino y se asignan recursos para la ejecución de las acciones.	El personal está empoderado en la ejecución de acciones requeridas por las decisiones de gestión de riesgos.
La gerencia alinea las políticas y las acciones con el apetito de riesgo.	La gerencia toma decisiones apropiadas de riesgo en cumplimiento con las políticas. Los ingresos ajustados al riesgo están en línea con las expectativas de la gerencia.
La gerencia supervisa proactivamente el riesgo y el avance de los planes de acción.	Los planes de remediación se completan dentro de los márgenes de tiempo esperados y tienen un impacto positivo en los objetivos de la empresa.
Las tendencias de riesgo son informadas a la gerencia.	El reporte oportuno de las tendencias de riesgo ayuda a la gestión proactiva del riesgo y evita la pérdida de oportunidades.
La gestión efectiva del riesgo es recompensada.	Se reconoce a las buenas prácticas de riesgo. Se establecen las metas de desempeño de los empleados y las estructuras de recompensa, a fin de estimular las prácticas efectivas de gestión de riesgos y una ejecución apropiada de las acciones de mitigación.

El apéndice B4 incluye una descripción detallada acerca de cómo los aspectos culturales, tales como la comunicación, reglas, incentivos, recompensas y sensibilización pueden influir en estos comportamientos.

Página dejada en blanco intencionadamente

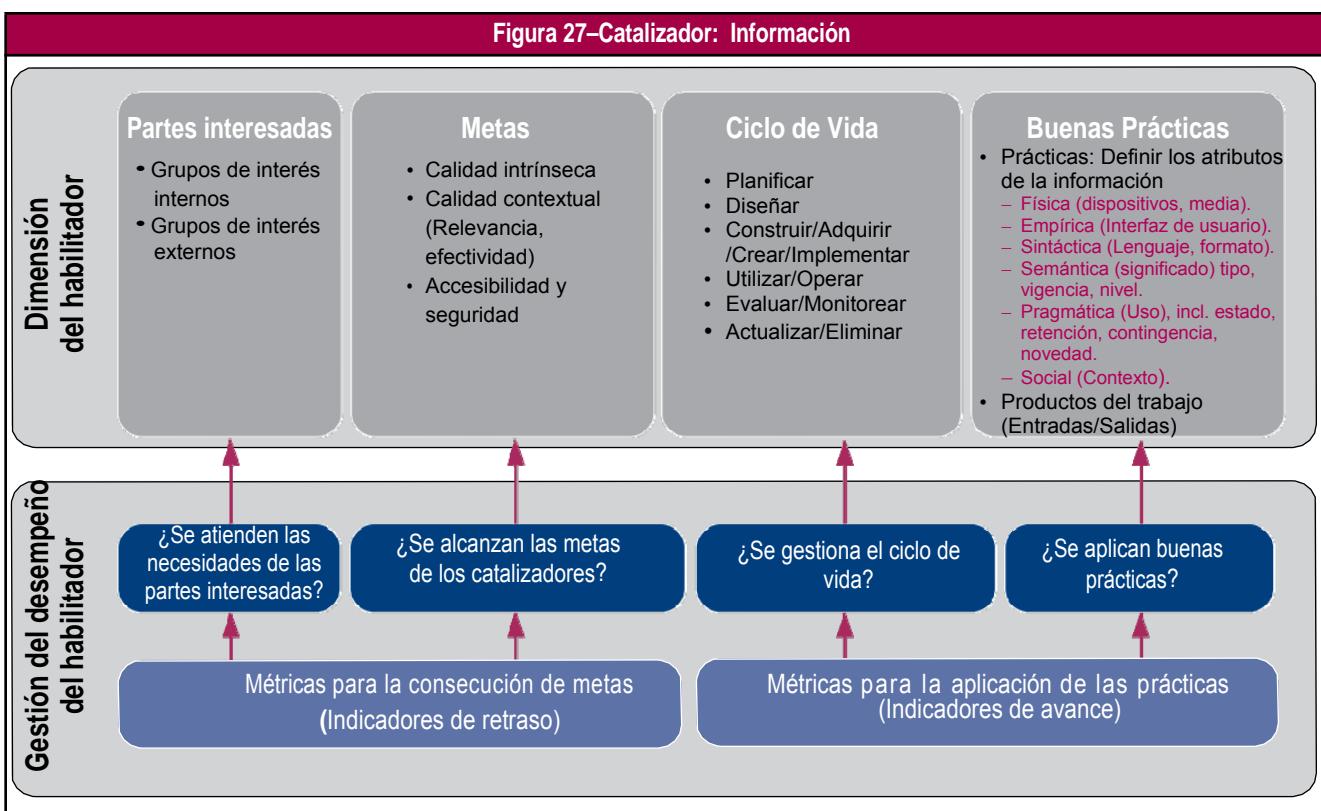
CAPÍTULO 6

CATALIZADOR: INFORMACIÓN

Este capítulo contiene una guía sobre cómo los elementos de la información pueden habilitar el gobierno y la gestión del riesgo en una empresa (perspectiva de la función de riesgos). Para este propósito, se tratan los siguientes temas:

- El modelo de Información.
- Un listado de elementos de seleccionados de la información que son relevantes para el gobierno y gestión del riesgo.
- Una descripción de la información detallada para cada ítem de la información. El apéndice B.5 incluye la información detallada vigente.

6.1 El modelo de Información



El modelo de Información (**figura 27**) muestra:

- **Partes interesadas:** Pueden ser internas o externas a la empresa. El modelo genérico también sugiere que además de identificar a las partes interesadas, también se necesita identificar sus intereses (es decir, ¿Por qué a ellos les importa o están interesados en la información?) Puede haber diferentes categorías de roles relativos a la información, que van desde propuestas detalladas (por ejemplo, datos específicos o roles de información tales como arquitecto, propietario, administrador, fideicomisario, proveedor, beneficiario, modelador, gerente de calidad, gerente de seguridad) hasta propuestas más generales, por ejemplo, diferenciando entre generadores, custodios y consumidores de la información, de la siguiente forma:
 - El generador de la información es responsable de crear la información.
 - El custodio de la información es responsable de almacenar y mantener la información.
 - El consumidor de la información es responsable de utilizar la información.

Estas categorías se refieren a actividades específicas respecto a los recursos de información. Las actividades dependen de la fase del ciclo de vida de la información, por tanto, para encontrar una categoría de roles con un nivel apropiado de granularidad para el modelo de Información, se pueden utilizar las dimensiones del ciclo de vida de la información. Esto significa que los roles de las partes interesadas relativas a la información, por ejemplo, los planificadores, receptores y usuarios de la información, pueden estar definidos en términos de las fases del ciclo de vida de la información. Al mismo tiempo, esto significa que la dimensión de las partes

interesadas relativas a la información no es independiente; cada fase del ciclo de vida tiene diferentes partes interesadas.

Mientras los roles relevantes dependan de las fases del ciclo de vida de la información, las partes interesadas pueden relacionarse con metas de la información.

- **Metas:** Las metas de la Información se subdividen en **tres sub-dimensiones de calidad:**

- Calidad intrínseca: La medida en la cual los valores de los datos están en consonancia con los valores vigentes o verdaderos. Esto incluye:
 - Precisión: Medida en la cual la información es correcta y confiable.
 - Objetividad: Medida en la cual la información no es ambigua, sin prejuicios e imparcial.
 - Credibilidad: Medida en la cual la información se considera como verídica y creíble.
 - Reputación: Medida en la cual la información está bien considerada en términos de su origen o contenido.
 - Calidad conceptual y representativa: La medida en la cual la información es aplicable a las tareas de los usuarios, está presentada de manera clara y comprensible, reconociendo que la calidad de la información depende del contexto de uso. Esto incluye:
 - Relevancia: Medida en que la información es aplicable y útil.
 - Completa: Medida en la cual no hay información faltante y ésta es de profundidad y amplitud suficiente.
 - Vigencia: Medida en la cual la información está suficientemente actualizada.
 - Cantidad apropiada de información: Medida en la cual el volumen de información es apropiado.
 - Representación concisa: Medida en la cual la información está representada de manera compacta.
 - Representación consistente: Medida en la cual la información se presenta en un mismo formato.
 - Interpretable: Medida en la cual la información está expresada en idiomas, símbolos y unidades apropiadas y con definiciones claras.
 - Comprensible: Medida en la cual la información resulta fácil de comprender.
 - Facilidad de manipulación: Medida en la cual la información es fácil de manejar y aplicar a diferentes tareas.
 - Calidad de la accesibilidad y seguridad: Medida en la cual la información está accesible y disponible, lo que incluye:
 - Disponibilidad/Oportunidad: Medida en la cual la información está disponible cuando es requerida y es fácil y rápidamente recuperable.
 - Acceso restringido: Medida en la cual la información se restringe apropiadamente a las partes autorizadas.
- **Ciclo de vida:** Se debe considerar el ciclo de vida completo de la información, pudiéndose requerir diversos enfoques para las distintas fases del ciclo de vida. El habilitador “Información” distingue las siguientes fases:
 - Planificar: La fase en que se prepara la creación y uso de los recursos de información. Las actividades en esta fase se refieren a la identificación de objetivos, el planeamiento de la arquitectura de información y el desarrollo de estándares y definiciones, p.ej., definiciones de datos y procedimientos de captura de datos.
 - Diseñar: Definición de los requerimientos de información para la gestión de los riesgos.
 - Construir/Adquirir/Crear/Implementar: Fase en la que se adquieren los recursos de información. Las actividades en estas fases incluyen la creación de registros de datos, la compra de datos y la carga de archivos externos.
 - Utilizar/Operar, lo cual incluye:
 - Almacenar: Fase en la cual se mantiene la información en formato electrónico (archivos electrónicos, bases de datos o repositorios de datos), físico (documentos impresos) o incluso en la memoria humana.
 - Compartir: Fase en la cual la información está disponible para su uso a través de métodos de distribución. Las actividades en esta fase abarcan los procesos involucrados en obtener la información para colocarla en lugares donde pueda ser accedida y utilizada, p.ej., distribución de documentos por correo electrónico. Para información en formato electrónico, esta fase puede superponerse con la fase de almacenamiento, p.ej., compartir información a través del acceso a la base de datos, servidores de archivos y documentos, etc.
 - Utilizar: Fase en la cual la información es utilizada para lograr las metas. Las actividades en esta fase se refieren a todo tipo de uso de la información. (p.ej., la toma de decisiones gerenciales, la ejecución de procesos automatizado) y pueden también incluir actividades tales como recuperación de información y conversión de información de un formato a otro.

La información es un habilitador para el gobierno corporativo, por lo tanto, el uso de la información como se define en el modelo de Información, puede entenderse en función de los propósitos para las partes interesadas del gobierno de la empresa cuando necesitan la información al asumir sus funciones, realizan sus actividades e

interactúan con los demás. La interacción entre las partes interesadas requiere flujos de información cuyos propósitos se indican en el esquema: Rendición de cuentas, delegación, monitoreo, establecimiento de la dirección, alineamiento, ejecución y control.

- **Evaluación/Monitoreo:** Fases en la que se asegura que los recursos de información continúan trabajando correctamente, p.ej., para ser valiosa. Las actividades en esta fase incluyen el mantener la información actualizada al igual que otros tipos de actividades de gestión de la información, p.ej., ampliación, depuración, consolidación, eliminación de información duplicada en los repositorios de datos.
- **Actualizar/Eliminar:** Fase en que el recurso de información es descartado cuando ya no es utilizado. Las actividades se refieren al archivamiento o a la destrucción de la información.
- **Buenas prácticas:** El concepto de información es entendida de manera diferente en disciplinas diferentes como la economía, la teoría de la comunicación, ciencias de la información, sistemas de información y gestión del conocimiento, por lo tanto, no hay una definición universalmente acordada respecto a lo que es la información. La naturaleza de la información puede, sin embargo, ser aclarada al definir y describir sus propiedades.

Se propone un esquema para estructurar las diferentes propiedades de la información, compuesto de seis niveles o capas para definir y describir las propiedades de la información. Estos seis niveles presentan un continuo de atributos, que van desde el mundo físico de la información, donde los atributos están relacionados con tecnologías de la información y medios de comunicación para capturar, almacenar, procesar, distribuir y presentar información al mundo social respecto a su uso, comprensión y acción. Se pueden asignar las siguientes descripciones a las capas y atributos de la información:

- Capa del mundo físico: El mundo en el que todos los fenómenos pueden ser observados de forma empírica:
 - Medio de la información: El atributo que identifica el soporte físico de la información, por ejemplo, papel, señales eléctricas, ondas de sonido, entre otros.
- Capa empírica: La observación empírica de los signos utilizados para codificar la información y su distinción entre sí y del ruido de fondo:
 - Canal de acceso a la información: El atributo que identifica al canal de acceso de la información, por ejemplo, interfaces de usuario.
- Capa sintáctica: Las reglas y principios para construir frases en lenguajes naturales o artificiales. La sintaxis se refiere al formato de la información.
 - Código/Lenguaje: Atributo que identifica el formato/lenguaje de representación utilizado para la codificación de la información y las reglas para la combinación de los símbolos del lenguaje para formar estructuras sintácticas.
- Capa semántica: Las reglas y principios para construir el significado de las estructuras sintácticas. La semántica se refiere al significado de la información.
 - Tipo de información: Atributo que identifica el tipo de información, por ejemplo, información financiera vs no-financiera, origen interno vs externo, pronosticada vs valores observados, valores planificados vs realizados, entre otros.
 - Vigencia de la información: Atributo que identifica el horizonte temporal al cual se refiere la información, es decir, información sobre el pasado, el presente o el futuro.
 - Nivel de la información: Atributo que identifica el grado de detalle de la información, por ejemplo, las ventas por año, trimestre, mes.
- Capa pragmática: Las reglas y estructuras para la construcción de estructuras mayores del lenguaje que cumplan propósitos específicos en la comunicación humana. La pragmática se refiere a la utilización de la información.
 - Período de retención: Atributo que identifica el periodo de retención de la información antes de ser destruida.
 - Estado de la información: Atributo que identifica si la información es operativa o histórica.
 - Novedad: Atributo que identifica si la información crea nuevos conocimientos o confirma los existentes, es decir, información vs confirmación.
 - Contingencia: Atributo que identifica la información que se requiere para preceder a esta información (para que sea considerada como información).
- Capa del mundo social: El mundo que se construye socialmente a través de la utilización de estructuras de lenguaje en el nivel pragmático de la semiótica, por ejemplo, los contratos, las leyes y la cultura.
 - Contexto: Atributo que identifica el contexto en el que la información tiene sentido, se utiliza, tiene un valor, etc., por ejemplo, el contexto cultural y el contexto de dominio del sujeto.

6.2 Perspectiva de la función de riesgos: Información relacionada con el gobierno –y gestión– del riesgo.

El propósito de esta sección es identificar todos los elementos de la información que se requieren para construir y sostener el gobierno y la gestión del riesgo en la empresa, de forma efectiva y eficiente. En otras palabras, se enumeran elementos de la información que apoyarán a la función y a la evaluación de riesgos.

La **figura 28** enumera elementos que conforman las fuentes de información relacionada con los riesgos de la empresa.

Figura 28—Elementos de información que apoyan el gobierno y la gestión del riesgo

Elemento de información	Definición/Descripción
Perfil de riesgo	<p>Es una descripción del riesgo global identificado al cual está expuesta la empresa. Un perfil de riesgo consiste de:</p> <ul style="list-style-type: none"> • Registro de riesgos: <ul style="list-style-type: none"> – Escenario de riesgos. – Análisis de riesgos. • Plan de acción de riesgos. • Evento de pérdida (histórica y vigente). • Factor de riesgo. • Hallazgos en evaluaciones independientes.
Registro de riesgos (universo de riesgos) [parte del perfil de riesgo].	<p>Un registro de riesgos provee información detallada sobre:</p> <ul style="list-style-type: none"> • Cada riesgo identificado, así como el dueño del riesgo, detalles de los escenarios y supuestos. • Partes interesadas afectadas. • Causas/indicadores. • Información sobre la puntuación detallada, es decir, la calificación de los riesgos en el análisis de riesgos. • Información detallada sobre la respuesta al riesgo (p.ej., el dueño de la acción) y el estado de la respuesta al riesgo (p.ej., el plazo para la acción). • Proyectos relacionados. • Nivel de tolerancia al riesgo <p>Esto también puede ser definido como el universo de riesgos.</p>
Escenarios de riesgo [parte del registro de riesgos].	<p>Un escenario de riesgo es una descripción detallada de los riesgos relacionados de TI que pueden conducir a un impacto en la empresa, cuando ocurra. Incluye elementos tales como:</p> <ul style="list-style-type: none"> • Actor. • Tipo de amenaza. • Evento. • Activos/recurso. • Tiempo. <p>Estos elementos son explicados con más detalle en la sección 2B del Capítulo 2.</p>
Resultado del análisis de riesgos [parte del registro de riesgos].	<p>El análisis de escenarios de riesgos es una técnica para hacer el riesgo más comprensible y para permitir la evaluación y el análisis apropiado de los riesgos. El resultado del análisis de riesgo consiste en la frecuencia e impacto estimados, formas de pérdidas y las opciones para reducir la frecuencia e impacto en los escenarios.</p>
Plan de acción de riesgos [parte del perfil de riesgo].	<p>El plan de acción de riesgos provee un marco para documentar el orden de prioridades en el cual se deben implementar las acciones individuales y cómo deben ser implementadas. Un plan de acción debería ser discutido con las partes interesadas apropiadas y documentarse claramente:</p> <ul style="list-style-type: none"> • Escenarios de riesgos que serán mitigados mediante acciones identificadas. • Causa raíz del escenario (Análisis de causa/raíz [RCA]). • Las razones para seleccionar las opciones de acción basadas en los criterios de evaluación del control. • Aquellos que son responsables de aprobar el plan y quienes son responsables por implementar el plan. • Acciones propuestas. • Requerimientos de recursos, incluyendo contingencias. • Medidas de desempeño y restricciones. • Costo vs beneficio de reducción del riesgo. • Requerimientos de reportes y monitoreo. • Cronograma y tiempos.
Evento de pérdida [parte del perfil de riesgo].	<p>Un evento de riesgo que resulta en una pérdida. Por ejemplo, errores en procesamiento/tiempos de los sistemas pueden resultar en una pérdida económica o en una posición negativa. Incluye información de causa/raíz y costos reales de eventos que afectaron a la empresa de acuerdo a los estándares de formas de perdidas establecidos.</p>

Figura 28—Elementos de información que apoyan el gobierno y la gestión del riesgo (cont.)

Elemento de información	Definición/Descripción
Factor de riesgo [parte del perfil de riesgo]	<p>Un factor de riesgo es una condición que puede influenciar la frecuencia e impacto y, finalmente, el impacto de los eventos y escenarios de TI en la empresa.</p> <p>Los factores de riesgos también pueden ser interpretados como factores causales del escenario que se está materializando, debido a vulnerabilidades o debilidades. Estos factores incluyen:</p> <ul style="list-style-type: none"> • Contexto externo. • Contexto interno. • Competencias en gestión de riesgos. • Competencias relacionadas con TI.
Hallazgos de evaluaciones independientes [parte del perfil de riesgo].	El reporte de auditoría que contiene los hallazgos de evaluaciones, las que deben ser consideradas durante las actividades de identificación y análisis de riesgos.
Plan de comunicación de riesgos	Un plan de comunicación de riesgos es usado para definir la frecuencia, los tipos y los repositorios de información acerca del riesgo. El objetivo principal es reducir el exceso de información no relevante (evitando el ruido de riesgo).
Reporte de riesgos	Un reporte de riesgos cubre la información sobre el perfil de riesgo vigente, incluyendo el mapa de riesgo, el tablero de riesgo, el estado actual de la respuesta al riesgo, riesgo emergente y tendencias. Además, identifica los diez primeros elementos de riesgo, que pueden ser estratégicos, tácticos u operativos, que requieren de enfoque de gestión. Este reporte es adaptado a los requerimientos del repositorio.
Programa de concientización de riesgos	Un programa de concientización de riesgos es un plan formal y claramente definido, enfoque estructurado y un conjunto de actividades y procedimientos relacionados, con el objetivo de lograr y mantener una cultura consciente de los riesgos.
Mapa de riesgos	El mapa de riesgo es una técnica muy simple, común e intuitiva para presentar el riesgo. El riesgo se traza en un diagrama de dos dimensiones (frecuencia e impacto). La representación del mapa de riesgo es poderosa y proporciona una completa e inmediata vista sobre los riesgos y las áreas aparentes para la acción. Además, permite definir zonas de color que indican bandas de apetito de significancia en modo gráfico.
Universo de riesgos	El universo de riesgos está compuesto por todos los riesgos relacionados a la empresa, incluyendo aquellos que se desconocen ⁴ y que podrían tener un impacto, ya sea positivo o negativo, en la habilidad de una empresa para lograr su misión (o visión) a largo plazo.
Apetito de riesgo	Apetito de riesgo es el nivel de riesgo en diferentes aspectos que una empresa está dispuesta a aceptar en pos del cumplimiento de su misión (o visión).
Tolerancia al riesgo⁵	Tolerancia al riesgo es el nivel aceptable de variación que la gerencia está dispuesta a permitir para un riesgo en particular, en el cumplimiento de sus objetivos.
Indicadores clave de riesgo (KRIs).	<p>Un indicador de riesgo es una métrica capaz de mostrar que la empresa está sujeta a, o tiene una alta probabilidad de estar sujeta a un riesgo que excede el apetito de riesgo definido.</p> <p>Un indicador clave de riesgo (KRI) se diferencia por ser altamente relevante y poseer una alta probabilidad para predecir o indicar un riesgo importante.</p>
Problemas y factores de riesgos emergentes	Consiste en información sobre la inminente o probable combinación de controles, valor y condiciones de amenaza que constituyen un notable nivel de futuros riesgos de TI.
Taxonomía de los riesgos.	Trata de proporcionar una comprensión clara de las terminologías y escalas a ser usadas entre las partes interesadas al discutir y comunicar los riesgos. La taxonomía debería ser comunicada y utilizada a través de toda la empresa.
Reporte de Análisis de Impacto al Negocio (BIA)	El reporte que resulta del BIA tiene el propósito de desarrollar un entendimiento común de los procesos de negocio que son específicos para cada unidad de negocios, calificar el impacto en el caso de la ocurrencia de un riesgo y es crítico para la supervivencia de una empresa.
Evento de riesgo	Un evento de riesgo es algo que ocurre en un lugar y/o tiempo específico que puede afectar la ejecución apropiada de las funciones de negocio. Pueden ser divididos en amenazas, vulnerabilidades y pérdidas.
Matriz de riesgo y actividades de control.	La matriz de riesgo y actividades de control es un documento que contiene elementos identificados de riesgo, su ranking, actividades de control, diseño y efectividad operativa.
Evaluación de riesgos.	Una evaluación de riesgos es el proceso utilizado para identificar y calificar o cuantificar el riesgo y sus efectos potenciales.

⁴ Riesgo desconocido es el riesgo al cual la empresa no sabe que está expuesta. Esta definición es compatible con las definiciones del modelo COSO ERM, las que son equivalentes a las definiciones de ISO 31000 en ISO Guide 73.

⁵ Esta definición es compatible con las definiciones del modelo COSO ERM, las que son equivalentes a las definiciones de ISO 31000 en ISO Guide 73.

Página dejada en blanco intencionadamente

CAPÍTULO 7

CATALIZADOR: SERVICIOS, INFRAESTRUCTURA Y APLICACIONES

Este capítulo contiene una guía sobre cómo los servicios, infraestructura y aplicaciones pueden habilitar el gobierno y la gestión del riesgo en una empresa (perspectiva de la función de riesgos). Para este propósito, se tratan los siguientes temas:

- El modelo de Servicios, Infraestructura y Aplicaciones.
- Un listado de servicios seleccionados que son relevantes para la implementación del gobierno y gestión del riesgo.
- Una descripción de la información detallada para cada servicio. El apéndice B.6 incluye la información detallada vigente.

7.1 El modelo de Servicios, Infraestructura y Aplicaciones



El modelo de Servicios, Infraestructura y Aplicaciones (**figura 29**) muestra:

- **Partes interesadas:** Las partes interesadas de las capacidades (el término combinado para servicios, infraestructura y aplicaciones) del servicio pueden ser internas y externas. Los servicios pueden ser entregados por entidades internas o externas, como áreas internas de TI, gerentes de operaciones, proveedores de outsourcing. Los usuarios de los servicios también pueden ser internos (usuarios de negocio) y externos (socios, clientes, proveedores, etc.) Se necesita identificar los intereses de cada uno, y focalizarse en la entrega adecuada de servicios o en la recepción de los servicios requeridos a los proveedores.
- **Metas:** Las metas de la capacidad del nivel de servicio son expresadas en términos de servicios (aplicaciones, infraestructura y tecnología) y niveles de servicios, considerando cuales servicios y niveles de servicios son más económicos para la empresa. Una vez más, las metas se relacionan con los servicios y la forma en que estos son provistos, así como sus resultados, es decir, la contribución a procesos del negocio soportados de forma exitosa.
- **Ciclo de vida:** Las capacidades de servicio tienen un ciclo de vida. Las capacidades de servicio planificadas o futuras son típicamente descritas en una arquitectura objetivo, que cubre los bloques de construcción, tales como aplicaciones futuras y el modelo de infraestructura objetivo; además describe los enlaces y las relaciones entre estos bloques de construcción.

Las capacidades de servicio vigentes que son utilizadas u operadas para entregar servicios de TI, son descritas en una arquitectura de línea base. Dependiendo del marco de tiempo de la arquitectura objetivo, se puede definir una arquitectura de transición, la cual muestra la empresa en estados incrementales entre la arquitectura de línea base y la objetivo.

- **Buenas prácticas:** Las buenas prácticas para las capacidades de servicio incluyen:
 - Definición de principios de arquitectura: Los principios de arquitectura son directrices generales que gobiernan la implementación y el uso de recursos relacionados con TI en la empresa. Los siguientes son ejemplos de potenciales principios de arquitectura:
 - Recurso: Los componentes comunes de una arquitectura deberían ser utilizados cuando se diseñan e implementan soluciones como parte de las arquitecturas objetivo o de transición.
 - Comprar vs. Construir: Las soluciones deben ser compradas a menos que haya una razón fundamental y aprobada para ser desarrolladas internamente.
 - Simplicidad: La arquitectura de la empresa debería ser diseñada y mantenida tan simple como sea posible, sin dejar de cumplir los requisitos de la empresa.
 - Agilidad: La arquitectura de la empresa debería incorporar agilidad para satisfacer las necesidades cambiantes del negocio de forma efectiva y eficiente.
 - Apertura: La arquitectura de la empresa debería aprovechar los estándares abiertos de la industria.
 - Definición de puntos de vista de arquitectura: La definición de empresa de los puntos de vista más apropiados de la arquitectura para satisfacer las necesidades de las diferentes partes interesadas. Estos son los modelos, catálogos y matrices utilizados para describir las arquitecturas de línea base, transición u objetivo; por ejemplo, se podría describir una arquitectura de aplicación a través de un diagrama de interfaz de aplicación, el cual muestre las aplicaciones utilizadas (o planificadas) y las interfaces entre ellas.
 - Repositorio de arquitectura: Tener un repositorio de arquitectura que pueda ser utilizado para almacenar diferentes tipos de resultados de arquitecturas, incluyendo principios y estándares de arquitectura, modelos de referencia de arquitectura, y otros entregables de arquitectura, y define los bloques de construcción de servicios tales como:
 - Aplicaciones, proporcionando funcionalidad de negocio.
 - Infraestructura tecnológica, incluyendo hardware, software e infraestructura de red.
 - Infraestructura física.
 - Niveles de servicio que son definidos y entregados por los proveedores de servicio.

Existen buenas prácticas externas para marcos de referencia de arquitectura y capacidades de servicio. Estas son directrices, plantillas o estándares que pueden ser utilizados para agilizar la creación de entregables de arquitectura. Entre los ejemplos se incluyen:

- TOGAF (www.opengroup.org/togaf) proporciona un Modelo de Referencia Técnica y un Modelo de Referencia de Infraestructura de Información Integrada.
- ITIL ofrece una guía completa sobre cómo diseñar y operar servicios.

7.2 Perspectiva de la función de riesgos: Servicios, Infraestructura y Aplicaciones relacionados con el gobierno –y gestión– del riesgo.

El propósito de esta sección es identificar y discutir todos los servicios, infraestructura y aplicaciones que se requieren para construir y sostener una gestión efectiva y eficiente del riesgo en la empresa. En otras palabras, se enumeran todos los servicios y aplicaciones que soportan la función de gestión de riesgos.

Los servicios son un conjunto de funciones que el proceso de gestión de riesgos necesita para proporcionar, incluyendo el compromiso de las partes interesadas, la identificación, el análisis, reporte y priorización del riesgo. La **figura 30** identifica y describe servicios, infraestructura y aplicaciones que proporciona el proceso de gestión de riesgos.

Figura 30—Servicios relacionados con la gestión de riesgos	
Servicios y aplicaciones de soporte	Descripción
Servicios	
Servicios de asesoramiento en riesgos de programa/proyecto.	Función que ayuda a asegurar que la estrategia del negocio nueva o cambiante, los procesos y la tecnología mantengan un nivel optimizado de riesgo.
Servicios de gestión de incidentes.	Función que ayuda a la empresa a manejar de manera rentable, las pérdidas que pueden materializarse por incidentes.

Figura 30—Servicios relacionados con la gestión de riesgos (cont.)

Servicios y aplicaciones de soporte	Descripción
Servicios de asesoramiento de arquitectura.	Función que proporciona la guía de expertos para ayudar a asegurar que el negocio, los datos y la arquitectura tecnológica soportan los objetivos de gestión de riesgos de la empresa.
Servicios de inteligencia de riesgo.	Función que proporciona inteligencia tanto táctica como estratégica sobre amenazas, vulnerabilidades y activos para dar soporte a las decisiones de riesgo en la empresa.
Servicios de gestión de riesgos.	Función que proporciona la guía de expertos en riesgo para apoyar el desarrollo y el soporte a los programas de gestión de riesgos en la empresa.
Servicios de gestión de crisis.	El conjunto de personas, organizaciones, procesos y tecnología que ayudan a responder en cualquier tipo de crisis, incluyendo aquellos que requieren la activación del plan de continuidad del negocio (BCP).
Infraestructura	
Fuentes de datos.	Los recursos que proporcionan oportunamente los datos del ambiente de riesgo que soportan procesos de minería de datos y analítica de riesgos.
Infraestructura para repositorios de conocimiento.	Los recursos necesarios para almacenar inteligencia de fuentes internas y externas, p.ej., big data.
Arquitectura de integración de inteligencia.	Los recursos que proporcionan un medio para conectarse a fuentes de datos en tiempo real, p.ej., proveedores de SIM (System Insight Manager); repositorios de conocimiento, p.ej., las herramientas de gestión del riesgo corporativo (ERM); y aplicaciones analíticas de riesgos, para proporcionar soporte oportuno
Aplicaciones	
Herramientas de gobierno, riesgo y cumplimiento (GRC).	Un subconjunto de herramientas GRC que permiten recopilar, analizar, gestionar y reportar los riesgos, incluyendo potenciales tableros de control o cuadros de mando (BSC), según los defina la empresa. Estas herramientas tienen como objetivo comunicar el riesgo en un orden priorizado, de manera que la información clave se puede extraer de un solo vistazo. La matriz de riesgos (mapa de riesgos) es una de estas herramientas, la cual permite a la empresa reconocer los elementos más críticos de riesgo en el repositorio y qué tan lejos están del apetito de riesgo.
Herramientas para análisis.	Herramientas cualitativas y/o cuantitativas para apoyar la toma de decisiones bien informadas de riesgo.
Herramientas para comunicar/reportar los riesgos.	Estas herramientas tienen como objetivo comunicar los hallazgos de la gestión de riesgos.
Repositorios de conocimiento.	Conjunto de repositorios para gestionar la información utilizada para facilitar el análisis de la gestión de riesgos y el proceso en general.
Herramientas de continuidad del negocio.	Estas herramientas tienen como objetivo ayudar a gestionar el análisis de riesgos, por ejemplo, un análisis de impacto al negocio (BIA) y actividades relacionadas en un contexto de gestión de riesgos.

Página dejada en blanco intencionadamente

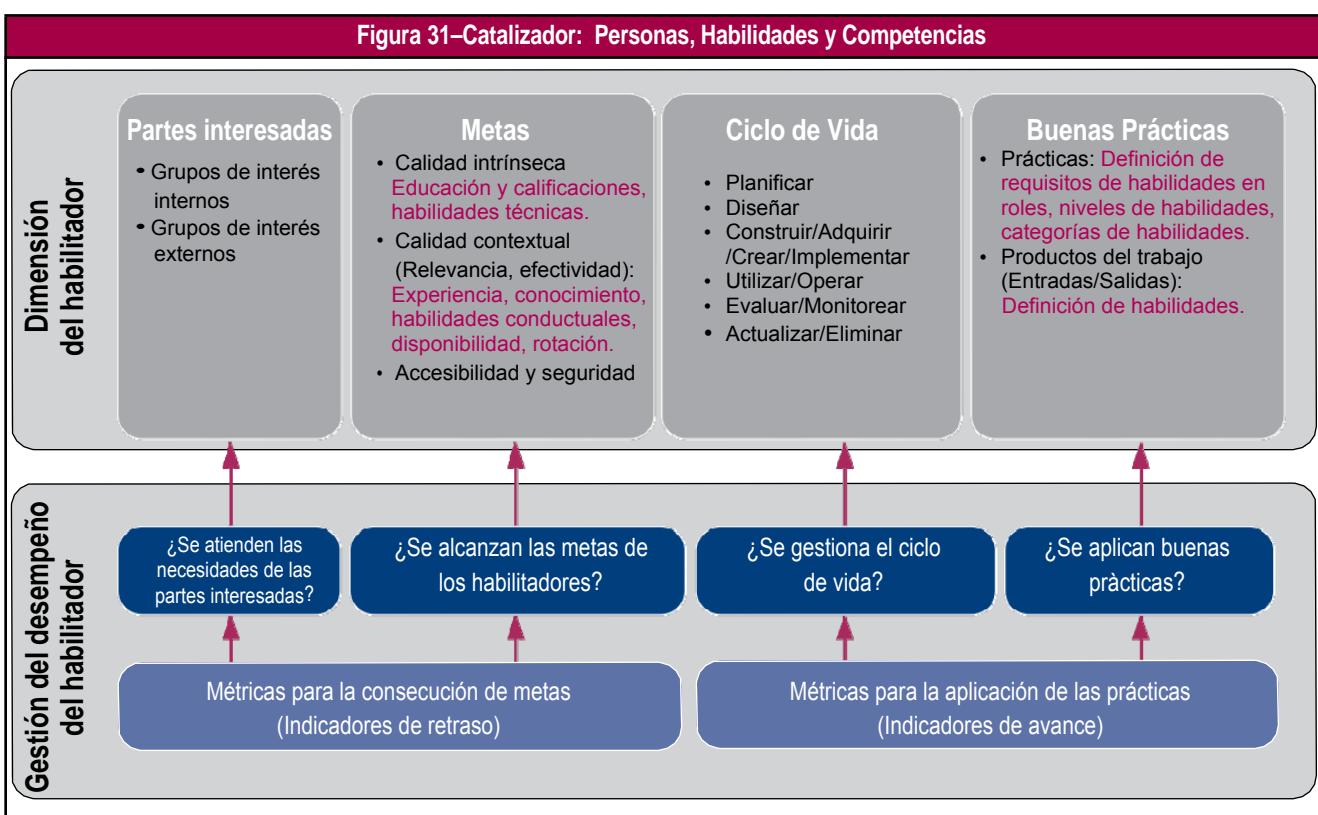
CAPÍTULO 8

CATALIZADOR: PERSONAS, HABILIDADES Y COMPETENCIAS

Este capítulo contiene una guía sobre cómo las personas, habilidades y competencias pueden habilitar el gobierno y la gestión del riesgo en una empresa (perspectiva de la función de riesgos). Para este propósito, se tratan los siguientes temas:

- El modelo de las Personas, Habilidades y Competencias.
- Una lista de conjuntos de habilidades que son relevantes para la implementación del gobierno y gestión del riesgo.
- Una descripción de los conjuntos de habilidades que se consideran relevantes para un analista de riesgos y un gerente de riesgos. El apéndice B.7 incluye la información detallada.

8.1 El modelo de Personas, Habilidades y Competencias



El modelo de Personas, Habilidades y Competencias (**figura 31**) muestra:

- **Partes interesadas:** Las partes interesadas de las habilidades y competencias son internas y externas. Las diferentes partes interesadas pueden asumir roles diferentes (gerentes de negocios, gerentes de proyectos, socios, competidores, reclutadores, entrenadores, desarrolladores, especialistas técnicos de TI, etc.) y cada rol requiere un conjunto distinto de habilidades. Esta sección discute los conjuntos de habilidades del analista de riesgos y del gerente de riesgos.
- **Metas:** Las metas para las habilidades y competencias están relacionadas con la educación y los niveles de calificación, habilidades técnicas, niveles de experiencia, conocimiento y habilidades conductuales requeridos para proporcionar y ejecutar actividades de los procesos de forma exitosa, roles organizacionales, etc. Las metas para las personas incluyen los niveles correctos de disponibilidad de personal y una tasa de rotación.
- **Ciclo de vida:** Las habilidades y competencias tienen un ciclo de vida. Una empresa tiene que conocer cuál es su base vigente de habilidades y planificar las que necesitan obtener. Esto está influenciado, entre otros factores, por la estrategia y las metas de la empresa. Las habilidades necesitan ser desarrolladas (p.ej., a través de entrenamiento), o adquiridas (p.ej., a través de reclutamiento) y desplegadas en los diferentes roles de la estructura organizativa. Las habilidades pueden necesitar ser eliminadas, por ejemplo, si una actividad es automatizada o externalizada.

Periódicamente, puede ser sobre una base anual, la empresa necesita evaluar la base de habilidades para entender su evolución, lo cual alimentará el proceso de planificación para el siguiente periodo. Esta evaluación también puede alimentar el proceso de recompensa y reconocimiento de los recursos humanos.

- **Buenas prácticas:** Las buenas prácticas para las habilidades y competencias incluye el definir la necesidad de requisitos objetivo de habilidades para cada rol jugado por las diferentes partes interesadas. Esto se puede describir a través de diferentes niveles de habilidades en diferentes categorías. Para cada nivel apropiado de habilidades en cada categoría, se debería tener una definición de la capacidad. Las categorías de habilidades tienen correspondencia con las actividades relacionadas con TI, p.ej., la gestión de la información y el análisis de negocio.

8.2 Perspectiva de la función de riesgos: Habilidades y competencias relacionadas con el gobierno –y gestión– del riesgo

El propósito de esta sección es identificar y describir todos los conjuntos de habilidades y competencias que se requieren para construir y sostener una gestión efectiva y eficiente del riesgo en la empresa. En otras palabras, se enumeran todos los conjuntos de habilidades y competencias necesarias para soportar la función de riesgos (**figura 32**).

Figura 32— Conjuntos de habilidades y competencias para la gestión de riesgos

Conjunto de habilidades y competencias	Descripción
Habilidades de liderazgo	La gestión de riesgos habitualmente involucra muchas partes interesadas con diferencias de opiniones y valores que deben ser dirigidos para alcanzar resultados de negocio efectivos, requiriendo liderazgo efectivo en la gestión de riesgos. Las habilidades de liderazgo incluyen un liderazgo proactivo que establezca una dirección clara y alineada con los resultados del negocio y la determinación para asegurar que las políticas implementadas entregan la disposición efectiva del riesgo. Las habilidades de liderazgo también requieren la capacidad para trabajar efectivamente con todas las partes interesadas para demostrar un escalamiento y una comunicación efectivos. Por último, el riesgo requiere ser gestionado de una manera rentable.
Capacidad analítica	La creciente complejidad de los negocios y la necesidad de cumplir con las regulaciones para cada industria específica, requiere que los analistas de riesgo tengan la capacidad de descomponer el riesgo en factores de riesgo que puedan evitar el logro de las metas y evaluar esos factores de riesgo. Esta creciente complejidad de requisitos de negocio, legales y regulatorios, demanda habilidades analíticas para descifrarlos. Para poder analizar el riesgo por partes e identificar dónde está la falla y, por consiguiente, juntar las partes de una manera útil y entendible, se requiere que el analista de riesgo enfoque metódicamente el tema y/o tenga una mentalidad estructurada.
Pensamiento crítico	Habilidad para hacer juicios profesionales acerca del valor de la información adicional y determinar si el nivel de análisis alcanzado es suficiente. También es necesaria la habilidad para documentar y calificar supuestos y articular escenarios de riesgo.
Habilidades interpersonales	Un atributo clave de los profesionales de riesgo es su habilidad para obtener información oportuna y precisa y para comunicarse con las partes interesadas, quienes tienen diferentes enfoques y objetivos. El profesional de riesgo utiliza lenguaje no técnico de forma efectiva, de modo que el mensaje sea significativo para todas las partes interesadas y demuestra un entendimiento esencial de las metas y prioridades del negocio.
Comunicación	El riesgo debe comunicarse a las partes interesadas quienes tienen diferentes enfoques y objetivos. El gerente o analista de riesgo debería tener la capacidad para comunicar el riesgo, los factores de riesgo y la exposición a pérdidas relacionadas, en el contexto, lenguaje y prioridad de la parte interesada relevante. El gerente o analista de riesgo es capaz de involucrar a todas las partes interesadas de forma significativa, utilizando nomenclatura consistente y brindando ejemplos para el contexto.
Influencia	Los profesionales de riesgo requieren habilidades de persuasión bien desarrolladas para ayudar en la adopción de prácticas de riesgo en toda la empresa y demostrar el valor a las partes interesadas.
Pensamiento lateral	El riesgo debe ser abordado de forma diferenciada dependiendo del tipo de riesgo. Se deberían aprovechar las ideas y las técnicas de otras disciplinas.
Entendimiento técnico	El nivel de las habilidades y competencias técnicas depende del rol dentro de la función de riesgos. Para entender las vulnerabilidades de los sistemas de TI y las amenazas que las explotan, se necesita tener un entendimiento básico de los componentes que constituyen los sistemas de TI y cómo se interconectan física y lógicamente entre ellos.
Concientización organizacional y de negocio	Para permitir que la empresa planifique, comunique y ejecute sus procesos de gestión de riesgos de forma efectiva, se debe documentar y mantener actualizados los puntos de contacto organizacionales, las unidades de negocio, las metas, los roles y las responsabilidades de los funcionarios y las rutas de escalamiento.

Figura 32— Conjuntos de habilidades y competencias para la gestión de riesgos (cont.)

Conjunto de habilidades y competencias	Descripción
Experiencia en riesgos	La experiencia en fuentes de amenazas, escenarios de amenazas, vulnerabilidades e impacto sobre el negocio, es crítica para el éxito. Esta habilidad se refiere al entendimiento de la naturaleza básica y la composición del riesgo, así como también a la mejora continua para mantener el ritmo frente a la naturaleza dinámica de las amenazas, vulnerabilidades e impactos en el ambiente moderno de negocios.
Capacitación y entrenamiento	La gestión de riesgos es una parte de los roles de la empresa. Para confirmar los niveles apropiados de experiencia y práctica en riesgos, la empresa requiere capacidades a través de capacitación y entrenamiento efectivos de las partes interesadas. Los programas de entrenamiento deben estar basados en niveles variados de concientización del riesgo. La habilidad para entregar programas específicos de entrenamiento es esencial para la actualización exitosa y la sostenibilidad de las prácticas de riesgo. Se deben implementar programas de entrenamiento para asegurar que las personas sean efectivas en sus roles.

Todas estas son habilidades generales relevantes para la gestión de riesgos en la empresa. Cada función o rol requiere una combinación de varias de estas habilidades. Como ejemplo, en el anexo B.7 se presentan perfiles detallados de un analista de riesgos y un gerente de riesgos. Esos ejemplos deben ser interpretados como una guía general sobre la experiencia común, el conocimiento y la pericia para esos perfiles. No son requisitos específicos para el rol.

Página dejada en blanco intencionadamente

SECCIÓN 2B

LA PERSPECTIVA DE LA GESTIÓN DE RIESGOS Y EL USO DE LOS CATALIZADORES DE COBIT 5

Esta sección comprende:

- Los procesos principales de la gestión de riesgos, utilizados para implementar la gestión efectiva y eficiente de riesgos en la empresa, para soportar la entrega de valor a las partes interesadas.
- Escenarios de riesgo, es decir, los elementos de información clave que se necesitan para identificar, analizar y responder al riesgo. Los escenarios de riesgo son la representación tangible y evaluable de los riesgos.
- La forma en que los catalizadores de COBIT 5 pueden ser utilizados para responder a escenarios de riesgo inaceptable.

CAPÍTULO 1 PROCESOS PRINCIPALES DE RIESGOS

Los procesos principales del gobierno y la gestión de riesgos están descritos en los procesos de COBIT 5 EDM03 *Asegurar la optimización del riesgo* y APO12 *Gestionar el riesgo* (**figura 33**). Estos procesos comprenden las actividades principales de la función de riesgos que se tratan en la sección 2A. Ellos brindan soporte a la empresa en la obtención de los objetivos corporativos y del valor para las partes interesadas, en tanto se optimizan los recursos y los riesgos.

Figura 33—Procesos principales del riesgo	
Procesos COBIT 5	Razonamiento
EDM03 Asegurar la optimización del riesgo	<p>Este proceso abarca el entendimiento, la articulación y la comunicación del apetito y tolerancia al riesgo de la empresa, y asegura la identificación y gestión del riesgo asociado al valor de la empresa que está relacionado con el uso de TI y su impacto. Las metas de este proceso son:</p> <ul style="list-style-type: none">• Definir y comunicar los umbrales de riesgo y asegurar que se conozcan los riesgos clave relacionados con TI.• Gestionar de una manera efectiva y eficiente a los riesgos críticos de la empresa relacionados con TI.• Asegurar que los riesgos de la empresa relacionados con TI no excedan su apetito de riesgo.
APO12 Gestionar el riesgo	<p>Este proceso abarca la continua identificación, evaluación y reducción del riesgo relacionado con TI dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la empresa. La gestión de riesgos de la empresa relacionado con TI debería ser integrada al ERM global. Se deberían balancear los costos y beneficios de gestionar el riesgo de la empresa relacionado con TI mediante:</p> <ul style="list-style-type: none">• La recolección de datos apropiados asociados al análisis de riesgos.• Manteniendo el perfil de riesgo de la empresa y articulando los riesgos.• Definiendo el portafolio de acciones de la gestión de riesgos y respondiendo al riesgo.

El anexo C describe con mayor detalle a estos procesos principales y sus actividades.

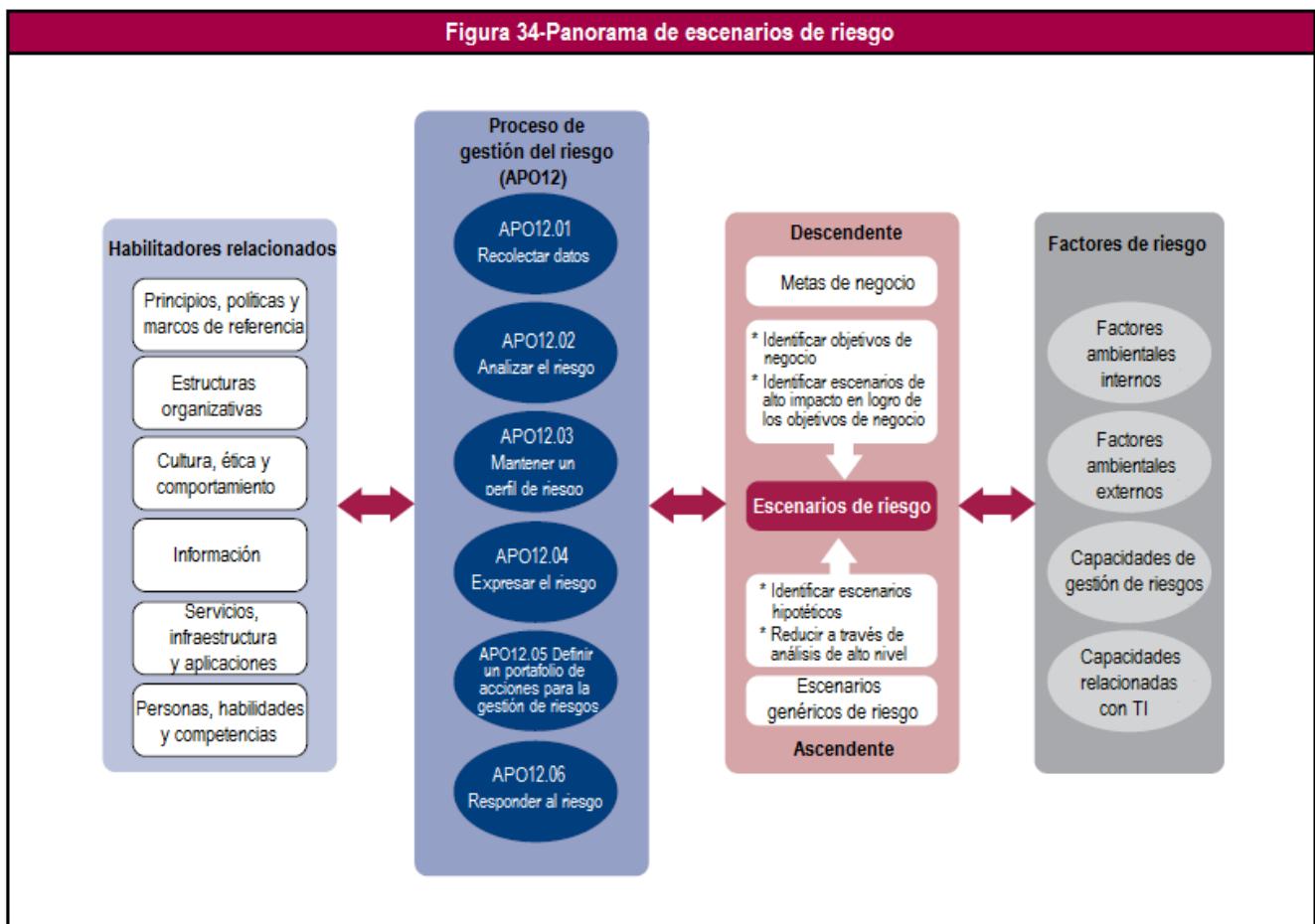
Página dejada en blanco intencionadamente

CAPÍTULO 2

ESCENARIOS DE RIESGO

2.1 Introducción

Un elemento de información clave que se utiliza en el proceso principal de la gestión de riesgos APO12 es el uso de escenarios de riesgo (**figura 34**).



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

El proceso principal de la gestión de riesgos requiere que los riesgos sean identificados, analizados y que se actúe al respecto. Los escenarios de riesgo que están bien desarrollados, soportan estas actividades y las hacen realistas y relevantes para la empresa.

La **figura 34** también muestra que los escenarios de riesgo se pueden derivar a través de dos mecanismos diferentes:

- Un enfoque descendente, donde se comienza desde los objetivos generales de la empresa y se realiza un análisis de los escenarios de riesgo de TI más relevantes y probables que impactan a los objetivos de la empresa. Si los criterios de impacto utilizados durante el análisis de riesgos 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 realidad individual de la empresa.

Los enfoques son complementarios y deberían ser utilizados de forma simultánea. De hecho, los escenarios de riesgo deben ser relevantes y estar vinculados a los riesgos reales del negocio. Por otro lado, el uso de un conjunto de ejemplos de escenarios de riesgo genéricos podría ayudar a identificar el riesgo y reducir la posibilidad de pasar por alto a los escenarios de riesgo comunes e importantes, y puede ofrecer una referencia completa para los riesgos de TI. Sin

embargo, se necesita considerar los elementos de riesgo específicos y los requerimientos críticos de negocio para cada empresa en los escenarios de riesgo de la empresa.

Nota: No confiar demasiado en la lista de ejemplos de los escenarios de riesgo genéricos. La lista, aunque es bastante completa, amplia y cubre la mayoría de los elementos de riesgo potencial, necesita 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 predefinidos de riesgos de TI. Más bien, se recomienda que la lista sea utilizada como base para el desarrollo de escenarios específicos y relevantes.

2.2 Flujo de trabajo en el desarrollo de escenarios de riesgo

En la práctica se sugiere el siguiente enfoque:

- Utilizar la lista de ejemplos de escenarios de riesgo genéricos (ver **figura 38** del capítulo 3) para definir un conjunto manejable de los escenarios de riesgo a la medida de la empresa. Para determinar un conjunto manejable de escenarios, una empresa puede empezar por considerar escenarios que ocurren comúnmente en su industria, área o proceso, los escenarios que representan las fuentes de amenazas que se incrementan en número o gravedad, y escenarios que involucren los requisitos legales y regulatorios aplicables al negocio. Otro enfoque podría ser identificar las unidades de negocio de alto riesgo y evaluar uno o dos procesos de operación de alto riesgo en cada unidad, incluyendo los componentes de TI que habilitan a ese proceso. Además, algunas situaciones menos comunes deberían estar incluidas en los escenarios.
- Efectuar una validación respecto de los objetivos de negocio de la entidad. ¿Los escenarios de riesgo seleccionados abordan los impactos potenciales en el logro de los objetivos estratégicos de la organización?
- Afinar los escenarios seleccionados sobre la base de la validación anterior, detallándolos a un nivel acorde con la criticidad de la entidad.
- Reducir el número de escenarios a un **conjunto manejable**. “Manejable” no significa un número fijo, sino que debería estar alineado con la importancia global (tamaño) y la criticidad de la unidad. No existe una regla general, pero si los escenarios poseen un alcance razonable y realista, la empresa debería esperar el desarrollo de por lo menos algunas docenas de escenarios.
- Mantener todos los escenarios en una lista para que puedan ser re-evaluados en el siguiente proceso de validación y que se puedan incluir para un análisis detallado, si se vuelven relevantes en un cierto tiempo.
- Incluir un evento no específico en los escenarios, p.ej., un incidente no cubierto en otros escenarios.

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

La organización también puede considerar la evaluación de los escenarios que tienen la probabilidad de ocurrir en forma simultánea. Con frecuencia esto se conoce como prueba de "estrés" y de hecho, implica la combinación de múltiples escenarios y la comprensión de lo que sería el impacto adicional, si ocurriera juntos.

2.3 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 diferente naturaleza y se pueden clasificar en dos categorías principales:

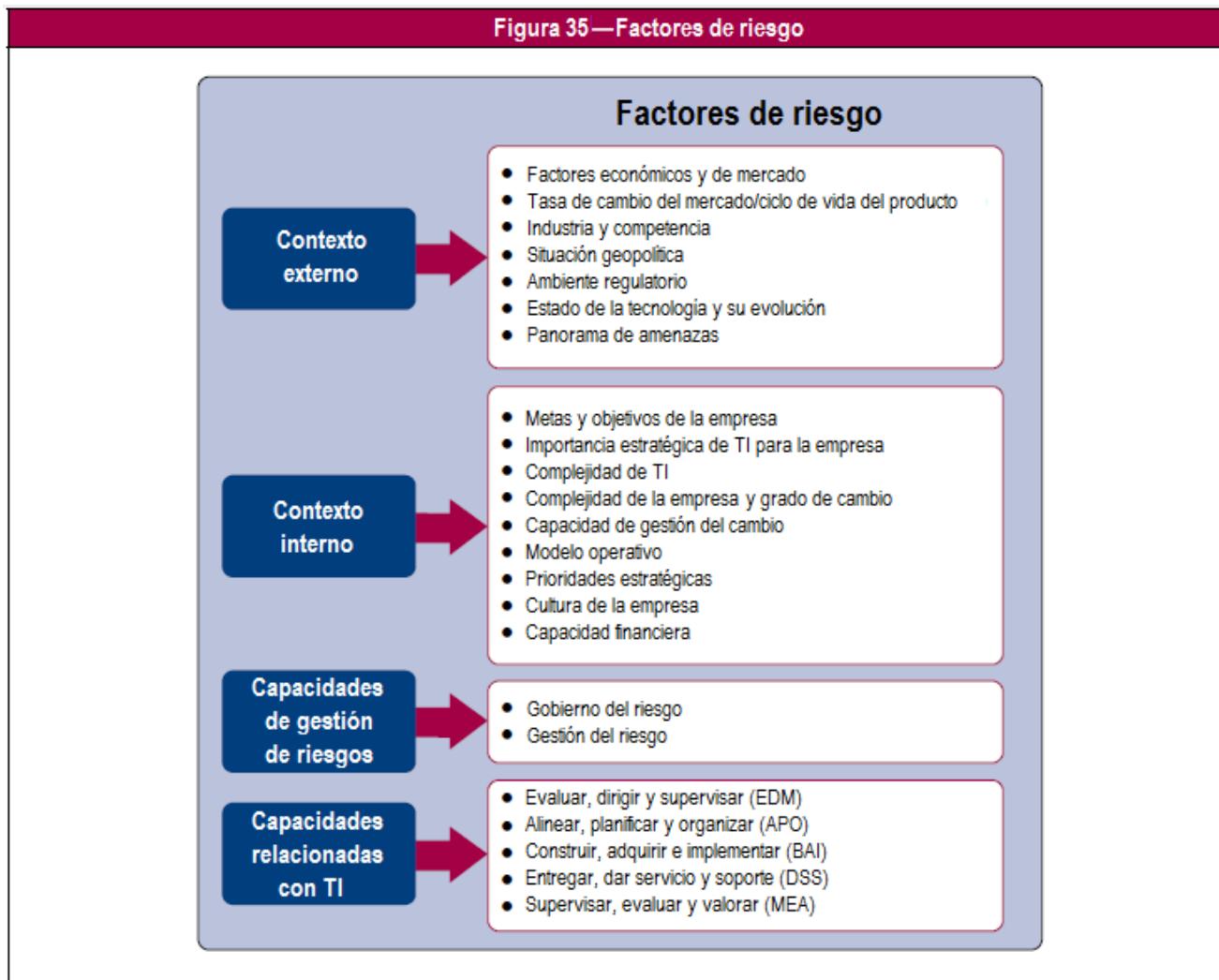
- **Factores de contexto:** Se pueden dividir en factores internos y externos, siendo la diferencia el grado de control que una empresa tiene sobre ellos:
 - Factores contextuales internos: En gran medida, están bajo el control de la empresa, a pesar de que no siempre son fáciles de cambiar.
 - Factores contextuales externos: En gran medida, están fuera del control de la empresa.
- **Capacidades:** ¿Qué tan efectiva y eficiente es la empresa en una serie de actividades relacionadas con TI? Estas pueden ser distinguidas en línea con el marco COBIT 5:
 - Capacidades de gestión de riesgos de TI: Indica el nivel de madurez de la empresa en la ejecución de los procesos de gestión de riesgos.
 - Capacidades relacionadas con TI: Indica la capacidad de los catalizadores de COBIT 5 relacionados con TI.

La importancia de los factores de riesgo se encuentra en la influencia que tienen sobre el riesgo. Estos factores tienen una influencia considerable sobre la frecuencia y el impacto en los escenarios de TI y deberían ser tomados en cuenta

durante cada análisis de riesgos. Los factores de riesgo también pueden interpretarse como factores causales del escenario que se materializa, o también como vulnerabilidades o debilidades. Estos términos son utilizados frecuentemente en otros marcos de gestión de riesgos.

El análisis de escenarios no sólo debería basarse en experiencias pasadas y en eventos conocidos, sino que también se debe considerar posibles circunstancias futuras.

La Figura 35 muestra factores de riesgo, los cuales son tratados con más detalle en los siguientes párrafos.



Contexto externo

Los factores contextuales de riesgo de TI, es decir, aquellas circunstancias que pueden incrementar la frecuencia o el impacto de un evento y que no siempre pueden ser controlados directamente por la empresa, incluyen:

- **Factores de mercado y económicos:** El sector de la industria en que opera la empresa; es decir, las capacidades y los requisitos de TI en el sector financiero son diferentes de la operación en el sector de manufactura. Se pueden incluir otros factores económicos, p.ej., nacionalizaciones, fusiones, adquisiciones y consolidaciones.
- **Tasa de cambio del mercado en el que opera la empresa:** ¿Los modelos de negocio están cambiando fundamentalmente? ¿El producto o servicio está al final de un momento importante del ciclo de vida?
- **Ambiente competitivo:** En el cual opera la empresa.
- **Situación geopolítica:** ¿La ubicación geográfica está sujeta a desastres naturales frecuentes? ¿El contexto político local y el contexto económico en general representan un riesgo adicional?
- **Ambiente regulatorio:** ¿La empresa está sujeta a nuevas regulaciones relacionadas con TI o más estrictas, o a otras regulaciones que afecten a TI? ¿Hay otros requisitos de cumplimiento más allá de la regulación, p.ej., específicos de la industria, contractuales?
- **Estado tecnológico y evolución:** ¿La empresa está utilizando el estado del arte de la tecnología? y, más importante, ¿qué tan rápido están evolucionando las tecnologías más relevantes?

- **Escenario de amenazas:** ¿Cómo están evolucionando las amenazas relevantes en términos de frecuencia de ocurrencia y nivel de capacidad?

Contexto interno

Los factores de riesgo interno incluyen:

- **Metas y objetivos de la empresa:** ¿Cuáles son las necesidades de las partes interesadas y cómo podrían verse impactadas por los riesgos?
- **Importancia estratégica de TI en la empresa:** ¿TI es un diferenciador estratégico, un habilitador funcional o una función de soporte?
- **Complejidad de TI:** ¿TI es altamente compleja (es decir, de arquitectura compleja, fusiones recientes) o TI es simple, estandarizada y efectivamente integrada?
- **Complejidad de la empresa** (incluyendo la dispersión geográfica y la cobertura de la cadena de valor, p.ej., en el sector de manufactura): ¿La empresa fabrica y distribuye piezas y/o también realiza actividades de ensamblaje?
- **Grado de cambio:** ¿Qué grado de cambios está experimentando la empresa?
- **Capacidad de gestión del cambio:** ¿Hasta qué punto la empresa es capaz de un cambio organizacional?
- **Filosofía de la gestión de riesgos:** ¿Cuál es la filosofía de riesgo de la empresa (aversa o tolerante al riesgo) y relacionado con ésta, cuáles son los valores de la empresa?
- **Modelo operativo:** El grado en que la empresa opera de manera independiente o está vinculada con sus clientes/proveedores, el grado de centralización/descentralización.
- **Prioridades estratégicas:** ¿Cuáles son las prioridades estratégicas de la empresa?
- **Cultura empresarial:** ¿La cultura existente en la empresa requiere cambiar para poder enfrentar de manera efectiva la gestión de riesgos?
- **Capacidad financiera:** La capacidad de la empresa para proporcionar apoyo financiero para mejorar y mantener el ambiente de TI, en tanto optimiza el riesgo.

Capacidad de gestión de riesgos

La capacidad de gestión de riesgos es un indicador de lo bien que la empresa ejecuta los procesos principales de gestión de riesgos y los catalizadores relacionados. Esto puede ser medido usando un cuadro de mando de riesgos. Entre mejor es el desempeño de los catalizadores, más efectivo es el programa de gestión de riesgos. Este factor se correlaciona con la capacidad de la empresa para reconocer y detectar el riesgo y los eventos adversos, por lo que no se debe descuidar. La capacidad de gestión de riesgos es un elemento muy significativo en la frecuencia e impacto de los eventos de riesgos en una empresa, ya que es responsable de las decisiones de riesgo para la gerencia (o por la falta de decisión), así como también de la presencia, ausencia y/o efectividad de los controles que existen en una empresa.

Capacidad relacionada a TI

Las capacidades relacionadas con TI se asocian con el nivel de capacidad de los procesos de TI y el resto de los catalizadores. El modelo genérico de catalizadores en COBIT 5 contiene un modelo de desempeño de catalizadores que soporta las evaluaciones de la capacidad. Un nivel de madurez elevado en relación con los diferentes catalizadores es equivalente a altas capacidades asociadas de TI, las cuales pueden tener una influencia positiva en:

- Reducción de la frecuencia de eventos, p.ej., un buen proceso de desarrollo de software para entregar software estable y de alta calidad, o tener buenas medidas de seguridad para reducir el número de incidentes de seguridad.
- Reducción del impacto en el negocio cuando los eventos ocurren, p.ej., tener un buen plan de BCP/DRP en caso de desastres.

2.4 Estructura de escenarios de riesgos de TI

Un escenario de riesgo de TI es una descripción de un evento relacionado con TI que, en caso de ocurrir, puede conducir a un impacto en el negocio. Para que los escenarios de riesgo estén completos y sean utilizables para fines de un análisis de riesgos, deben contener los siguientes componentes, como se muestra en la **figura 36**:

- **Actor:** Lo que genera la amenaza que aprovecha una vulnerabilidad. Los actores pueden ser internos o externos y pueden ser humanos o no humanos:
 - Los actores internos están dentro de la empresa, p.ej., el personal, los contratistas.
 - Los actores externos incluyen externos, competidores, reguladores, el mercado.No todos los tipos de amenazas requieren un actor, p.ej., fallas o causas naturales.
- **Tipo de amenaza** (la naturaleza del evento): ¿Es malicioso? Si no es así, ¿es accidental o se trata de la falla de un proceso bien definido? ¿Es un fenómeno natural?

- **Evento:** ¿Es la revelación de información confidencial, la interrupción de un sistema o de un proyecto, el robo o la destrucción? También incluye el diseño inefectivo de los sistemas y procesos, el uso inadecuado, los cambios en las normas y regulaciones que impactarán materialmente sobre el sistema, la ejecución inefectiva de los procesos, p.ej., los procedimientos de gestión de cambios, procedimientos de adquisición, procesos de priorización de proyectos.
- **Activo/recurso:** Recurso sobre el cual actúa el escenario. Un activo es cualquier elemento de valor para la empresa que puede ser afectado por el evento y dar lugar a un impacto en el negocio. Un recurso es cualquier cosa que ayude a lograr los objetivos de TI. Los activos y recursos pueden ser idénticos, p.ej., el hardware es un recurso importante porque todas las aplicaciones de TI lo usan, y al mismo tiempo, es un activo porque tiene un cierto valor para la empresa. Los activos/recursos incluyen:
 - Personas y habilidades.
 - Estructuras organizativas.
 - Procesos de TI, p.ej., modelados como los procesos COBIT 5, o procesos de negocio.
 - Infraestructura física, instalaciones, equipo, etc.
 - Infraestructura de TI, incluyendo hardware, infraestructura de redes y middleware.
 - Otros componentes de arquitectura de la empresa, 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 taller de autos local o la intranet del grupo de desarrollo de software. Los recursos críticos probablemente atraerán a un gran número de ataques o una mayor atención en caso de falla, por lo que la frecuencia de los escenarios relacionados probablemente será más alta. Se necesita habilidad, experiencia y la comprensión a fondo de las dependencias, para entender la diferencia entre un activo crítico y un activo no-crítico.

- **Tiempo:** Dimensión, donde lo siguiente podría ser descrito, si es relevante para el escenario:
 - La duración del evento, p.ej., un corte de energía prolongado de un servicio o del centro de datos.
 - El momento (¿Se produce el evento en un momento crítico?)
 - Detección (¿La detección es inmediata o no?)
 - El tiempo que transcurre entre el evento y la consecuencia (¿Hay una consecuencia inmediata, p.ej., una falla en la red, caída inmediata, o una consecuencia posterior, como p.ej., una arquitectura incorrecta de TI con altos costos acumulados a lo largo de un periodo de varios años?)

Es importante ser consciente de las diferencias entre los eventos de pérdida, eventos de amenazas y eventos de vulnerabilidad. Cuando un escenario de riesgo se materializa, se produce un evento de pérdida. El evento de pérdida ha sido desencadenado por un evento de amenaza (tipo de amenaza y eventos en la **figura 36**). La frecuencia del evento de amenaza que conduce a un evento de pérdida es influenciada por los factores de riesgo o la vulnerabilidad. La vulnerabilidad es generalmente un estado y puede ser aumentado o disminuido por eventos de vulnerabilidad, p.ej., el debilitamiento de los controles o por la fortaleza de las amenazas. **No se debería mezclar estos tres tipos de eventos en una gran "lista de riesgos".**



El capítulo 3 contiene un conjunto de escenarios genéricos de riesgos de TI que se construyen de acuerdo con el modelo descrito en los párrafos anteriores. El conjunto de escenarios genéricos contiene ejemplos de resultados negativos, pero también ejemplos en los que un riesgo, cuando se gestiona bien, puede conducir a un resultado positivo.

2.5 Temas principales durante el desarrollo y uso de escenarios de riesgo

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

La construcción de un conjunto completo de escenarios significa, en teoría, que debería combinarse cada valor posible de cada componente. Luego, cada combinación debería ser evaluada para determinar su relevancia y realismo, y en caso de ser relevante, ser documentada en el registro de riesgos. En la práctica, esto no es posible porque rápidamente se podría generar un número inviable de diferentes escenarios de riesgo. El número de escenarios que se desarrollarán y analizarán debe mantenerse relativamente pequeño con el fin de que siga siendo manejable.

La **figura 37** muestra algunas de las principales áreas de enfoque y aspectos que abordar cuando se utiliza la técnica de escenarios de riesgo.

Figura 37—Principales áreas de enfoque en la técnica de escenarios de riesgo	
Enfoque/Aspectos	Guía resumen
Mantener la vigencia de los escenarios de riesgo y sus factores.	Los factores de riesgo y la empresa cambian a través del tiempo, por lo que los escenarios cambiarán también con el tiempo, en el transcurso de un proyecto o con la evolución de la tecnología. Por ejemplo, es esencial que la función de riesgos desarrolle un cronograma de revisión y que el CIO trabaje con las gerencias de negocio para revisar y actualizar los escenarios relevantes e importantes. La frecuencia de este ejercicio depende del perfil de riesgo global de la empresa y se debe hacer por lo menos una vez al año, o cuando se produzcan cambios importantes.
Utilizar los escenarios de riesgo genéricos como punto de partida, aplicando más detalle donde y cuando sea necesario.	Una técnica de mantener un 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 justificarlos con el perfil de riesgo sólo en los niveles más operativos de la empresa. Los supuestos hechos al agrupar o generalizar deben ser bien entendidos por todos y adecuadamente documentados, ya que pueden ocultar ciertos escenarios o crear confusión cuando se confronte con la respuesta a los riesgos. Por ejemplo, si una "amenaza interna" no está bien definida en un escenario, puede que no sea claro si esta amenaza incluye miembros privilegiados y no privilegiados. Las diferencias entre estos aspectos del escenario pueden ser críticas cuando se trata de comprender la frecuencia y el impacto de los eventos, así como las oportunidades de mitigación.
El número de escenarios debe ser representativo y debe reflejar la realidad y la complejidad de la empresa.	La gestión de riesgos ayuda a hacer frente a la enorme complejidad de los entornos de TI actuales, dando prioridad a la acción potencial de acuerdo a su valor en la reducción del riesgo. La gestión de riesgos implica reducir la complejidad, no generarla; por tanto, este es otro motivo para trabajar con un número manejable de escenarios de riesgo, sin olvidar que el número de escenarios definido tiene que reflejar con exactitud a la realidad empresarial y su complejidad.
La taxonomía de riesgos debería reflejar la realidad y la complejidad de la empresa.	Debería haber un número suficiente de escalas de escenarios de riesgo que reflejen la complejidad de la empresa y el grado de exposición al que la empresa está expuesta. Las escalas potenciales podrían ser "baja", "media", "alta" o una escala numérica que califique la importancia del riesgo de 0 a 5. Las escalas deben estar alineadas en toda la empresa para asegurar una puntuación coherente.
Utilizar una estructura de escenarios genéricos de riesgo para simplificar el reporte de los riesgos	Del mismo modo, para efectos de reportar los riesgos, las entidades no deberían informar sobre todos los escenarios específicos y detallados, pero sí podrían hacerlo a través de la estructura de riesgos genéricos. Por ejemplo, un área de negocio puede haber tomado el escenario genérico 15 (calidad del proyecto), traducido en cinco escenarios de sus principales proyectos, luego, conducir un análisis de riesgos para cada escenario, y consolidar o resumir los resultados para el reporte con el título del escenario genérico "calidad del proyecto".

Figura 37—Principales áreas de enfoque en la técnica de escenarios de riesgo (cont.)

Enfoque/Aspectos	Guía resumen
Asegurar las personas y las habilidades adecuadas y requeridas para el desarrollo de escenarios de riesgos relevantes.	<p>Para el desarrollo de escenarios de riesgos relevantes y manejables se requiere:</p> <ul style="list-style-type: none"> Pericia y experiencia, para no pasar por alto los escenarios relevantes y no considerar escenarios altamente irreales⁶ o irrelevantes, que es importante evitarlos para utilizar adecuadamente los recursos limitados. Se debe prestar un poco de atención a las situaciones que son muy poco frecuentes e impredecibles, pero que podrían tener un impacto catastrófico sobre la empresa. Una comprensión completa del contexto, lo que incluye el entorno de TI (p.ej., la infraestructura y sus componentes, las aplicaciones y sus interdependencias), el ambiente global de negocios, y una comprensión de cómo y qué entornos de TI apoyan el ambiente de la empresa para entender el impacto en el negocio. La intervención y los puntos de vista comunes de todas las partes involucradas; la alta dirección que tiene el poder de decisión; la gerencia, que tiene el mejor panorama del impacto en el negocio; el área de TI, que entiende lo que puede salir mal con ella misma; y la gerencia de riesgos, que puede moderar y estructurar el debate entre las partes. El proceso de desarrollo de escenarios generalmente se beneficia de un enfoque o taller de tormenta de ideas, en donde por lo general se requiere una evaluación de alto nivel para reducir el número de escenarios a un número manejable, pero relevante y representativo.
Utilizar el proceso de construcción de escenarios de riesgo para obtener aceptación y credibilidad.	El análisis de escenarios no es sólo un ejercicio analítico hecho por "analistas de riesgo". Un beneficio adicional importante del análisis de escenarios es el logro de la aceptación y credibilidad de las áreas de la empresa, líneas de negocio, gerencia de riesgos, TI, finanzas, cumplimiento, entre otros. Ganar la aceptación y credibilidad 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 construcción de escenarios.	Además de coordinarse con la gerencia, se recomienda que se incluya en los debates a personal selecto que esté familiarizado con las operaciones detalladas, en los casos donde aplique, pues ellos están más familiarizados con las vulnerabilidades de la tecnología y de los procesos que pueden ser explotadas.
No orientarse sólo hacia escenarios raros y extremos.	En el desarrollo de escenarios, no hay que enfocarse sólo en los eventos más desfavorables, ya que rara vez se materializan, mientras que los incidentes menos severos son más frecuentes.
Deducir escenarios complejos a partir de escenarios simples mostrando el impacto y las dependencias.	<p>Los escenarios simples, una vez desarrollados, deberían ser profundizados hacia escenarios más complejos, mostrando impactos en cascada y/o fortuitos y reflejando las dependencias. Por ejemplo:</p> <ul style="list-style-type: none"> Un escenario donde se tiene una falla importante de hardware se puede combinar con el escenario de un Plan de Recuperación ante Desastres (DRP) inadecuado. Un escenario de falla de software importante puede provocar la corrupción de la bases de datos y en combinación con la gestión deficiente de copias de respaldo, puede generar consecuencias graves, o al menos consecuencias de una magnitud diferente a la de una falla de software por sí sola. Un escenario de un evento externo importante puede conducir a un escenario de apatía interna.
Considerar la posibilidad de riesgos sistémicos y de contagio.	<p>Se debe prestar atención a los escenarios de riesgos sistémicos y/o de contagio:</p> <ul style="list-style-type: none"> Sistémico: Algo sucede con un socio comercial importante, que afecta a un gran grupo de empresas en un área o industria. Un ejemplo sería un sistema nacional de control del tráfico aéreo que está fuera de operación por un período prolongado de tiempo, p.ej., seis horas, afectando el tráfico aéreo en gran escala. Contagioso: Eventos que ocurren con varios de los socios de negocio de la empresa en un plazo de tiempo muy corto. Un ejemplo podría ser un centro de información que puede estar totalmente preparado para cualquier tipo de emergencia por tener medidas muy sofisticadas de recuperación de desastres, pero cuando ocurre una catástrofe, encuentra que no hay transacciones enviadas por sus proveedores y por lo tanto, se encuentra temporalmente fuera del negocio.
Utilizar la construcción de escenarios para mejorar la concientización para la detección de riesgos.	<p>El desarrollo de escenarios también ayuda a tratar el tema de detección, alejándose de una situación en la que una empresa "no sabe lo que no sabe". El enfoque de colaboración para el desarrollo de escenarios ayuda en la identificación de los riesgos a los que la empresa, hasta entonces, no se habría dado cuenta de que estaba expuesta (y por lo tanto nunca se le hubiera ocurrido poner en marcha cualquier contramedida). Después de identificar el conjunto completo de los elementos de riesgo durante la generación de escenarios, el análisis de riesgos evalúa la frecuencia y el impacto de los escenarios.</p> <p>Las preguntas que deben formularse, incluyen:</p> <ul style="list-style-type: none"> ¿La empresa podrá detectar que el escenario de riesgo se ha materializado? ¿La empresa detectará que algo malo ha ocurrido para que pueda reaccionar de manera adecuada? <p>La generación de escenarios y el pensamiento creativo de lo que puede salir mal elevará de forma automática y, con suerte, provocará la respuesta a la cuestión de la detección. La detección de los escenarios incluye dos etapas: la visibilidad y el reconocimiento. La empresa debe estar en una posición en que puede observar que algo salga mal, y se necesita la capacidad de reconocer un evento observado como algo malo.</p>

⁶ No realista significa algo estático o no fijo en el tiempo. Lo que antes era impensable, sobre todo porque nunca sucedió o porque sucedió hace mucho tiempo, se vuelve realista tan pronto ocurre o sucede de nuevo. Un ejemplo claro son los ataques terroristas del 11 de septiembre de 2001 en EE.UU. Es natural pensar que las cosas que aún no suceden, incluso cuando son teóricamente posibles, estimarlas como no posibles o extremadamente improbables. Sólo cuando ocurren, son tomados en serio en las evaluaciones de riesgos. Esto puede ser considerado como falta de visión o falta de debido cuidado, pero en realidad es la esencia de la gestión de riesgos, tratar de dar forma y contener el futuro basándose en la experiencia pasada y en predicciones futuras.

Página dejada en blanco intencionadamente

CAPÍTULO 3

ESCENARIOS GENÉRICOS DE RIESGO

Un escenario de riesgo de TI es una descripción de un evento relacionado con TI que puede conducir a un evento de pérdida que, en caso de ocurrir, tiene un impacto en el negocio. Los escenarios genéricos sirven, una vez adaptados, como entrada para las actividades de análisis de riesgos, en las que se necesita establecer, entre otros, el impacto definitivo para el negocio. Este capítulo contiene un conjunto de escenarios genéricos de riesgos de TI (**figura 38**), construido en línea con el modelo descrito en la sección previa de esta guía. El conjunto de escenarios genéricos contiene ejemplos de escenarios tanto positivos como negativos.

Advertencia: la tabla con escenarios genéricos no reemplaza la fase creativa y reflexiva que debería contener todo ejercicio de creación de escenarios. En otras palabras, no se recomienda que una empresa utilice ciegamente esta lista y asuma que no son posibles otros escenarios de riesgo, o que asuma que cada escenario contenido en la lista le es aplicable. Se necesita inteligencia y experiencia para derivar una lista relevante y personalizada, a partir de la lista genérica.

Los escenarios genéricos de riesgo de la **figura 38** incluyen la siguiente información:

- **Categoría de escenario de riesgos:** Descripción de alto nivel de la categoría del escenario (p.ej., selección de proyecto de TI). Existen 20 categorías en total;
- **Componentes del escenario de riesgos:** Ofrecen detalles sobre el tipo de amenaza, actor, evento, activos/recursos y tiempos de cada categoría de escenario;
- **Tipo de riesgos:** El tipo de escenario en el que encajarán aquellos derivados del escenario genérico, utilizando los tres tipos de riesgos explicados anteriormente:
 - **Riesgo en la habilitación de beneficio/valor para TI:** Asociado con las oportunidades perdidas de utilización de la tecnología con el fin de mejorar la eficiencia o efectividad de los procesos de negocio o como un habilitador para nuevas iniciativas para el negocio;
 - **Riesgo en la entrega de programas y proyectos de TI:** Asociado con la contribución de TI a soluciones de negocio nuevas o mejoradas, generalmente bajo la forma de programas y proyectos;
 - **Riesgo en la entrega de operaciones y servicios de TI:** Asociado con la estabilidad, disponibilidad, protección y recuperación operativa de los servicios de TI, que pueden destruir o reducir el valor para la empresa.

Una “P” indica una relación primaria (mayor grado) y una “S” representa una secundaria (menor grado). Las celdas en blanco indican que la categoría de riesgos no es relevante para el escenario bajo revisión.

- **Ejemplos de escenarios:** Para cada categoría de escenario, se brindan uno o varios ejemplos breves con un resultado negativo, indicando si es más una destrucción de valor o la eventualidad de haber dejado de ganar, y/o un resultado positivo, señalando una ganancia de valor. En total, se incluyen **111 ejemplos de escenarios de riesgos** con posibles resultados negativos y/o positivos.

Figura 38—Ejemplos de escenarios de riesgos						
Ref.	Categoría de escenario de riesgos	Tipo de riesgo			Ejemplos de escenarios	
		Habilitación de Beneficio/Valor de TI	Entrega de Programas y proyectos de TI	Entrega de operaciones y servicios de TI	Ejemplos de escenarios negativos	Ejemplos de escenarios positivos
0101	Establecimiento y mantenimiento del portafolio	P	P	S	Se seleccionan programas erróneos para implementar que no se alinean con la estrategia y las prioridades corporativas.	Se seleccionan programas que conducen a iniciativas de negocio nuevas y exitosas.
0102		P	P	S	Existen iniciativas duplicadas.	Las iniciativas alineadas tienen interfaces optimizadas.
0103		P	P	S	Un programa nuevo e importante genera incompatibilidad a largo plazo con la arquitectura empresarial.	Se evalúan los nuevos programas para verificar la compatibilidad con la arquitectura existente.
0104		P	P	S	Los recursos en competencia se asignan y gestionan en forma inefficiente y no se alinean con las prioridades del negocio.	

Figura 38—Ejemplo de escenarios de riesgos (cont.)

Ref.	Categoría de escenario de riesgos	Tipo de riesgo			Ejemplos de escenarios	
		Habilidades de Beneficio/Valor de TI	Entrega de Programas y proyectos de TI	Entrega de operaciones y servicios de TI	Ejemplos de escenarios negativos	Ejemplos de escenarios positivos
0201	Gestión del ciclo de vida de los programas/proyectos (inicio, aspectos económicos, entrega, calidad y finalización de los programas/proyectos)	P	P	S	No se completan los proyectos con fallas (debido a costos, demoras, arrastres en el alcance, prioridades cambiantes de negocios).	Los proyectos fallidos o irrelevantes se detienen en forma oportuna.
0202		S	P	S	El presupuesto para proyectos de TI se encuentra excedido.	Se completa el proyecto de TI dentro del presupuesto acordado.
0203		S	P		Ocasionalmente, se tienen entregas tardías de los proyectos de TI por un departamento interno de desarrollo.	La entrega del proyecto se realiza a tiempo.
0204		P	P	S	Rutinariamente, existen importantes retrasos en la entrega de proyectos de TI.	La ruta crítica de los proyectos se gestiona en forma acordada y la entrega es oportuna.
0205		P	P	S	Existen demoras excesivas en proyectos de desarrollo externalizado de TI.	La comunicación con terceros asegura la entrega oportuna según alcance y calidad acordados.
0206		P	P		Los programas/proyectos fallan debido a la falta de involucramiento activo de las partes interesadas (incluyendo al patrocinador) durante su ciclo de vida.	La gestión de cambios en el ciclo de vida del programa/proyecto se conduce apropiadamente para informar a las partes interesadas del avance y para el entrenamiento de usuarios futuros.
0301	Toma de decisiones sobre inversiones en TI	P		S	Los gerentes de negocios o sus representantes no se involucran en las decisiones importantes sobre inversiones de TI (p.ej. nuevas aplicaciones u oportunidades tecnológicas, priorizaciones).	Existe una toma de decisiones coordinada sobre las inversiones de TI entre las áreas de negocios y TI.
0302		P		S	Se selecciona el software equivocado para implementar en términos de costos, desempeño, características, compatibilidad, etc.	Se realiza un análisis inicial y se formula un caso de negocios para asegurar una adecuada selección del software.
0303		P		P	Se selecciona la infraestructura equivocada para implementar, en términos de costos, desempeño, características, compatibilidad, etc.	Se realiza un análisis inicial y se formula un caso de negocios para asegurar una adecuada selección de la infraestructura.
0304		P	P		Se adquiere software redundante.	
0401	Pericia y habilidades de TI	P	P	P	Faltan habilidades de TI o son incompatibles, p.ej., debido a nuevas tecnologías.	Se atrae personal adecuado para incrementar la entrega de servicios del área de TI.
0402		P	P	P	El personal de TI no comprende el negocio, lo que afecta la entrega de servicio/calidad de proyectos.	El personal correcto y la combinación de habilidades respaldan la entrega de proyectos y la entrega de valor.
0403		P	P	P	No existen suficientes habilidades para cubrir los requerimientos del negocio.	Una combinación correcta de habilidades y entrenamiento asegura profunda comprensión del negocio por parte del personal y permite la cobertura total de los requerimientos del negocio.
0404		S	P	P	No existen habilidades para contratar personal de TI.	Se atrae la cantidad correcta de personal de TI, con habilidades y competencias adecuadas para el soporte a los objetivos del negocio.
0405		S	P	P	No existe diligencia debida en el proceso de contratación del personal.	Los candidatos son evaluados para asegurar que poseen las habilidades, competencias y actitudes adecuadas.
0406		S	P	P	No existe un entrenamiento adecuado, lo que lleva a que el personal de TI abandone la empresa.	Los miembros del personal de TI pueden determinar, en colaboración con sus superiores, sus propios planes de entrenamiento en base a sus aspiraciones y áreas de interés.

Ref.	Categoría de escenario de riesgos	Tipo de riesgo			Ejemplos de escenarios	
		Habilización de Beneficio/Valor de TI	Entrega de Programas y proyectos de TI	Entrega de operaciones y servicios de TI	Ejemplos de escenarios negativos	Ejemplos de escenarios positivos
0407	Pericia y habilidades de TI (cont.)	S	P	P	Existe un retorno insuficiente de la inversión en el entrenamiento debido a la desvinculación temprana del parte del personal capacitado de TI (p.ej., MBA).	El desarrollo de la carrera profesional se realiza formalmente y se determinan planes individuales para asegurar que el personal de TI se encuentra motivado para permanecer en la empresa por un tiempo considerable.
0408		S	P	P	Existe una dependencia excesiva del personal clave de TI.	La rotación del personal asegura que más de una persona posea el conocimiento completo de la ejecución de una determinada actividad.
0409		S	P	P	Existe una incapacidad para actualizar las habilidades de TI a un nivel apropiado a través del entrenamiento.	A través del entrenamiento, la participación en seminarios y la lectura del liderazgo del pensamiento, se asegura que el personal esté actualizado en los desarrollos más recientes en su especialidad.
0501		S	S	P	Se abusa de los derechos de acceso de roles anteriores.	RRHH y Administración de TI coordinan de forma frecuente para asegurar la oportuna cancelación de los derechos de acceso, evitando cualquier posibilidad de abuso.
0502		S		P	El equipo de TI es dañado accidentalmente por el personal.	
0503		S		P	Existen errores cometidos por el personal de TI (durante las actualizaciones del sistema, las copias de respaldo, el mantenimiento,	Se aplica el principio de "4-ojos", disminuyendo la posibilidad de errores antes de la entrada a producción.
0504		S		P	La información es ingresada incorrectamente por el personal de TI o por los usuarios de los sistemas.	Se aplica el principio de "4-ojos", disminuyendo la posibilidad de ingreso de información incorrecta.
0505		S		P	El centro de datos es destruido (por sabotaje, etc.) por el personal.	Se protege adecuadamente el centro de datos, permitiendo sólo el acceso del personal autorizados de TI.
0506		S		P	Un dispositivo con datos sensibles es robado por un miembro del personal.	Los bienes de la oficina se protegen y monitorean para detectar cualquier actividad irregular.
0507		S		P	Un componente clave de la infraestructura es robado por un miembro del personal.	Los componentes clave de la infraestructura se monitorean 24x7 para supervisar el desempeño, la disponibilidad, etc. Se disparan alarmas en caso de irregularidades y se actúa en forma inmediata.
0508	Operaciones del personal (error humano e intento malicioso)	P	S	P	Se configuran erróneamente los componentes de hardware.	Se establece un sistema de gestión de la configuración, asegurando una configuración alineada en toda la organización.
0509		P	S	P	Se dañan los servidores críticos en el centro de cómputo (p.ej., por accidente, etc.)	Los componentes clave de la infraestructura se monitorean 24x7 para supervisar el desempeño, la disponibilidad, etc. Se disparan alarmas en caso de irregularidades y se actúa en forma inmediata.
0510		P	S	P	El hardware fue dañado intencionadamente (dispositivos de seguridad, etc.).	Los componentes clave de la infraestructura se monitorean 24x7 para supervisar el desempeño, la disponibilidad, etc. Se disparan alarmas en caso de irregularidades y se actúa en forma inmediata.

Figura 38—Ejemplo de escenarios de riesgos (cont.)

Ref.	Categoría de escenario de riesgos	Tipo de riesgo			Ejemplos de escenarios	
		Habilización de Beneficio/Valor de TI	Entrega de Programas y proyectos de TI	Entrega de operaciones y servicios de TI	Ejemplos de escenarios negativos	Ejemplos de escenarios positivos
0601	Información (brecha de datos: daño, fuga y acceso)	S		P	El personal interno de TI ha dañado componentes de hardware, lo que conlleva la destrucción (parcial) de los datos.	Se encuentran establecidos los procedimientos de copia de respaldo, alineados con el nivel de criticidad de los datos para la empresa, asegurando que se disponga siempre de los datos claves para el negocio en una ubicación secundaria.
0602		S	S	P	La base de datos está corrupta, lo cual hace inaccesible a los datos.	
0603		S	S	P	Se pierden/revelan medios portátiles que contienen datos sensibles (CD, USB, discos portátiles, etc.)	
0604		S	S	P	Se pierden/revelan datos sensibles mediante ataques lógicos.	
0605		S	S	P	Se pierden o no se verifica la efectividad de los medios que contienen las copias de respaldo.	
0606		P	S	P	Se revela información sensible en forma accidental debido a fallas en el seguimiento de las guías de manejo de información.	
0607		P	S	P	Se modifican intencionadamente los datos (contables, vinculados a la seguridad, información de ventas, etc.)	
0608		P	S	P	Se revela información sensible a través del correo electrónico o las redes sociales.	
0609		P	S	P	Se revela información sensible debido a procedimientos inefficientes de retención/archivo/eliminación.	
0610		P	S	P	Existen fugas de la propiedad intelectual (PI) y/o la información competitiva, debido a la desvinculación de miembros clave de la empresa.	
0611		P	S	P	La empresa tiene un flujo excesivo de datos y no puede extraer o deducir la información relevante para el negocio (p.ej., el problema del "big data").	
0701	Arquitectura (visión y diseño)	P	P	P	La arquitectura empresarial es compleja e inflexible, bloqueando una mayor evolución y expansión, lo que lleva a la pérdida de oportunidades de negocio.	Una arquitectura moderna y flexible respalda la agilidad/innovación del negocio.
0702		P	S	P	La arquitectura empresarial no se ajusta a su propósito y no respalda las prioridades del negocio.	
0703		P	S	S	Existe una falla en la adopción y explotación oportuna de la nueva infraestructura.	
0704		P	S	S	Existe una falla en la adopción y explotación oportuna de un nuevo software (funcionalidad, optimización, etc.)	

Ref.	Categoría de escenario de riesgos	Tipo de riesgo			Ejemplos de escenarios	
		Habilidades de Beneficio/Valor de TI	Entrega de Programas y proyectos de TI	Entrega de operaciones y servicios de TI	Ejemplos de escenarios negativos	Ejemplos de escenarios positivos
0801	Infraestructura (hardware, sistemas operativos y tecnología de control) (selección/ implementación, operaciones y desmantelamiento)	P	S	P	Se instala infraestructura nueva (innovadora) y como resultado los sistemas se tornan inestables, lo que lleva a incidentes operativos, p.ej., el programa BYOD.	Se lleva a cabo una prueba adecuada antes de instalar la infraestructura en el ambiente de producción para asegurar la disponibilidad y el adecuado funcionamiento de todo el sistema.
0802		P	S	P	Los sistemas no pueden manejar los volúmenes de transacciones cuando estos se incrementan.	
0803		P	S	P	Los sistemas no pueden manejar la carga que se genera cuando se despliegan nuevas aplicaciones o iniciativas.	
0804		P	S	P	Existen fallas intermitentes en los servicios (telecomunicaciones, electricidad).	Los servicios están previstos y operan 24x7 para soportar la ejecución continua de las transacciones críticas del negocio.
0805		P	S	P	TI es obsoleta y no satisface los nuevos requerimientos del negocio (redes, seguridad, base de datos, almacenamiento, etc.).	
0806				P	Fallas en el hardware por exceso de calor.	
0901	Software	P		S	No existen habilidades en el uso del software para materializar los resultados deseados (p.ej. fallas al implementar los modelos de negocio o los cambios organizacionales requeridos).	El software en uso estimula la generación de nuevas ideas.
0902		P		S	Se implementa software inmaduro (adopción temprana, fallos, etc.)	
0903		P		S	Se selecciona e implementa software equivocado según costos, desempeño, características, compatibilidad, etc.	Se realiza un análisis inicial y se formula un caso de negocio para asegurar una adecuada selección del software.
0904		P		S	Existen dificultades operativas cuando se pone un nuevo software en producción	Se realizan pruebas de aceptación de los usuarios y entrenamiento personalizado antes de decisiones de la puesta en marcha, asegurando una transición fluida del nuevo software y que continúe la generación de valor para el negocio.
0905		P		S	Los usuarios no pueden utilizar ni explotar nuevo software aplicativo.	
0906		P		S	Modificación intencional del software conduce a datos erróneos o acciones fraudulentas.	Se aplica el principio de “4-ojos”, para las entradas/modificaciones de datos específicos para crear una revisión entre pares y disminuir el estímulo a acciones fraudulentas o resultados inesperados.
0907		P		S	Modificación no intencional del software conduce a resultados inesperados.	
0908		P		S	Ocurren errores no intencionales en la gestión de configuraciones y de cambios.	La gestión de la configuración disminuye los tiempos de resolución en la gestión de incidentes y problemas.
0909		P		S	Regularmente, ocurren fallas en el funcionamiento del software o de las aplicaciones críticas.	Se realizan pruebas adecuadas antes de adoptar la decisión de puesta en marcha, para asegurar la disponibilidad y el funcionamiento adecuado del software.
0910		P		S	Intermitentemente, ocurren problemas con el software de sistemas importantes.	
0911		P		S	El software aplicativo es obsoleto (p.ej., tecnologías anticuadas, pobres documentadas, costosas de mantener, difíciles de extender, no integradas en la arquitectura vigente).	El área de TI es innovadora, asegurando una interacción de doble vía con el negocio.
0912		P		S	No existen habilidades para retornar a versiones anteriores en caso de problemas operativos con nuevas versiones.	Se establecen copias de respaldo y puntos de restauración, según la criticidad de negocio del software, para asegurar procedimientos de retorno al estado anterior.

Figura 38—Ejemplo de escenarios de riesgos (cont.)

Ref.	Categoría de escenario de riesgos	Tipo de riesgo			Ejemplos de escenarios	
		Habilización de Beneficio/Valor de TI	Entrega de Programas y proyectos de TI	Entrega de operaciones y servicios de TI	Ejemplos de escenarios negativos	Ejemplos de escenarios positivos
1001	Propiedad del negocio sobre la TI	P	P	S	El negocio no asume la responsabilidad que debería sobre las áreas de TI, p.ej., los requerimientos funcionales, las prioridades en el desarrollo, la evaluación de oportunidades a través de nuevas tecnologías.	El negocio asume una responsabilidad apropiada sobre TI y co-determina la estrategia de TI, especialmente el portafolio de aplicaciones.
1002		P	S	S	Existe una dependencia y uso excesivos de aplicaciones de usuario final y de soluciones ad-hoc para necesidades importantes de la información, lo que lleva a deficiencias en la seguridad, datos imprecisos o incrementos en los costos y el uso ineficiente de recursos.	
1003		P	S	S	Se generan costos o poca efectividad en las compras de TI que se concretan fuera de los procesos de adquisición.	Siempre se elabora un caso de negocio para asegurar la optimización de costos y la adquisición efectiva de software.
1004				P	Requerimientos inadecuados llevan a acuerdos de nivel de servicios (SLAs) poco efectivos.	
1101	Selección/desempeño del proveedor, cumplimiento contractual, discontinuidad del servicio y trasferencia.		S	P	Falta de debida diligencia respecto a la viabilidad financiera, capacidad de entrega y sustentabilidad de los servicios del proveedor.	Los proveedores actúan como socios estratégicos.
1102			S	P	Se aceptan términos de los proveedores de TI que no razonables para el negocio.	
1103			S	P	El soporte y la entrega de servicios por los proveedores son inadecuados y no alineados con los acuerdos de niveles de servicio (SLA).	Se asegura un adecuado soporte y entrega de servicios a través de adecuados indicadores clave de desempeño (KPIs), vinculados a bonificaciones y penalidades.
1104			S	P	El desempeño de los servicios externalizados es inadecuado en los acuerdos de gran escala y largo alcance.	
1105			S	P	Existen incumplimientos de las licencias de software (uso y/o distribución de software sin las correspondientes licencias, etc.)	Se acuerdan los convenios contractuales vinculados al uso de software propietario y de terceros.
1106			S	P	Incapacidad para transferir a proveedores alternativos debido a una confianza excesiva en el proveedor actual.	Los contratos con el proveedor incluyen una cláusula de cierre programado y de transferencia de conocimientos, exigiéndole que entregue lo elaborado a los nuevos proveedores. Se plantea una combinación de personal interno y externo para cada proceso, evitando que el conocimiento global esté bajo dominio exclusivo de los proveedores.
1107			S	P	Los servicios en la nube son adquiridos por el negocio sin consultar/involucrar a TI, lo que resulta en la incapacidad de integrar el servicio con los prestados en forma interna.	
1201	Cumplimiento regulatorio	P	S	S	No se cumple con regulaciones, p.ej., privacidad, contabilidad, manufactura, etc.	De cara a los clientes, se aprovecha el pleno cumplimiento de las regulaciones, para generar valor extra para el negocio.
1202		P	S	S	El desconocimiento de los cambios potenciales en la regulación tiene un impacto en el ambiente operativo de TI.	La empresa establece un departamento legal y de cumplimiento para realizar un seguimiento de los cambios regulatorios y para asegurar que se continúe generando valor para el negocio.

		Figura 38—Ejemplo de escenarios de riesgos (cont.)				
Ref.	Categoría de escenario de riesgos	Tipo de riesgo		Ejemplos de escenarios		
		Habilización de Beneficio/Valor de TI	Entrega de Programas y proyectos de TI	Entrega de operaciones y servicios de TI	Ejemplos de escenarios negativos	Ejemplos de escenarios positivos
1203		P	S	S	El regulador impide el flujo de datos a través de las fronteras debido a controles insuficientes.	
1301	Geopolítico			P	No se tiene acceso debido a incidentes disruptivos en otros ambientes de la empresa.	
1302				P	La interferencia del Estado y las políticas nacionales limitan las capacidades de	
1303				P	Las acciones dirigidas contra la empresa resultan en la destrucción de la	
1401	Robo o destrucción de la infraestructura	S	S	P	Se ha producido el robo de un dispositivo con datos sensibles.	
1402		S	S	P	Se ha producido el robo de una importante cantidad de servidores de desarrollo.	
1403		S	S	P	Se destruye el centro de datos (sabotaje, etc.).	
1404		S	S	P	Dispositivos individuales se destruyen accidentalmente.	
1501	Código malicioso	S		P	Se ha producido una intrusión de código malicioso en los servidores operativos críticos.	
1502		S		P	Las computadoras portátiles se infectan frecuentemente con código malicioso.	
1503		S		P	Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos.	
1504		S		P	Roban los datos de la compañía a través de accesos no autorizados obtenidos mediante ataques de "phishing".	
1601	Ataques lógicos	S		P	Usuarios no autorizados tratan de forzar el ingreso a los sistemas.	
1602		S		P	Existen interrupciones en los servicios debido a ataques de denegación de servicios.	
1603		S		P	El sitio web sufre un ataque que modifica su apariencia ("defacement").	
1604		S		P	Se registran casos de espionaje industrial.	
1605		S		P	Existen ataques de virus.	
1606		S		P	Se registran casos de hacktivismo ("hacktivism").	
1701	Acción industrial	S	S	P	No es posible acceder a las instalaciones y edificios debido a una huelga gremial.	
1702		S	S	P	El personal clave no se encuentra disponible debido a impedimentos de la industria (p.ej., huelga en el transporte).	
1703		S	S	P	Un tercero no puede proveer servicios por una huelga.	

Figura 38—Ejemplo de escenarios de riesgos (cont.)

Ref.	Categoría de escenario de riesgos	Tipo de riesgo			Ejemplos de escenarios	
		Habilitación de Beneficio/Valor de TI	Entrega de Programas y proyectos de TI	Entrega de operaciones y servicios de TI	Ejemplos de escenarios negativos	Ejemplos de escenarios positivos
1704		S	S	P	No hay acceso al capital debido a una huelga del sector bancario.	
1801	Ambiental	S	S	P	El equipamiento utilizado no es amigable en cuanto al medio ambiente (p.ej., consumo de energía, embalajes, etc.)	
1901	Actos de la naturaleza	S	S	P	Hay un terremoto.	
1902		S	S	P	Hay un tsunami.	
1903		S	S	P	Hay fuertes tormentas y ciclones tropicales.	
1904		S	S	P	Hay un gran incendio fuera de control.	
1905		S	S	P	Hay una inundación.	
1906		S	S	P	Hay una crecida en el nivel del agua.	
2001	Innovación	P	S	S	No se identifican tendencias nuevas e importantes de TI.	
2002		P		S	Hay una falla en la adopción y en el aprovechamiento oportuno de un nuevo software (funcionalidad, optimización, etc.).	
2003		P		S	No se identifican tendencias nuevas e importantes de software (consumismo en TI).	

El apéndice D proporciona una serie de ejemplos sobre la forma en que los catalizadores de COBIT 5 pueden ayudar a mitigar los escenarios de riesgos de la **figura 38**. También pueden utilizarse, con el mismo propósito, otros marcos de referencia para la gestión de las TI, como ITIL y la ISO/IEC 27001/2, si bien no se incluyen vínculos/mapeos detallados en este documento.

CAPÍTULO 4

AGREGACIÓN DE RIESGOS

4.1 ¿Por qué la agregación de riesgos?

La gestión de riesgos de TI sólo puede alcanzar su pleno potencial si el riesgo se gestiona a través de toda la empresa. Es menos valiosa cuando solo se obtiene una visión parcial del riesgo. El término “parcial” tiene dos aspectos en este contexto:

- Sólo una parte de los elementos de riesgo potenciales son considerados durante el análisis y la gestión de riesgos.
- Sólo una parte de la empresa se encuentra dentro del alcance de la gestión de riesgos, es decir, no se considera a toda la empresa.

Cada empresa necesita una visión agregada del riesgo de extremo a extremo (actividad de negocio), más allá de las cuestiones técnicas, para evitar una falsa sensación de seguridad o un falso sentido de urgencia. Una visión agregada del riesgo permite la revisión adecuada del apetito y la tolerancia por el riesgo, en lugar de tener solamente vistas focalizadas en elementos de riesgo individuales o parciales, p.ej., un problema de gestión del cambio en un sistema ERP podría tener consecuencias de largo alcance a través de múltiples líneas de negocios, socios, clientes y países. La gerencia ejecutiva necesita ver el impacto agregado de este riesgo para toda la empresa, en lugar de sólo percibir que es un riesgo en un servidor en un centro de datos en un solo lugar.

En la práctica, algunos obstáculos interfieren efectivamente en obtener una visión agregada, consistente y realista de la exposición actual, al nivel de empresa:

- Ausencia de una terminología clara y consistente a través de toda la empresa.
- Empresas complejas con diferentes (sub)culturas existentes, generan dificultades para contener y definir las diferentes entidades donde los riesgos necesitan ser descritos, así como para obtener datos coherentes, confiables y consistentes sobre los riesgos, incluso el requisito mínimo absoluto de una evaluación de riesgos de alto nivel.
- Presencia de datos cualitativos (y ausencia de datos cuantitativos) en la mayoría de los casos, con una limitada confianza sobre la fiabilidad de los niveles de riesgos reportados, o utilizando escalas diferentes y/o incompatibles para evaluar el impacto y la frecuencia.
- Las dependencias desconocidas entre los riesgos reportados pueden ocultar riesgos mayores, p.ej., diferentes áreas de negocio que reportan el mismo riesgo de nivel medio, que de ocurrir, podría convertirse en un riesgo mayor para toda la empresa.
- El uso de escalas ordinales para expresar riesgos en distintas categorías, lo que podría significar dificultades matemáticas o riesgos por la utilización de estos números en cualquier tipo de cálculos.
- En empresas complejas, un riesgo particular a nivel de área de negocio, puede ser importante para ella, pero por varias razones (p.ej., tamaño o estrategia de la empresa), puede ser menos importante al nivel de la empresa. Esta escala de los riesgos debe ser bien comprendida al agregar la información de los riesgos.
- Diferentes partes interesadas (grupos de riesgos operacionales, auditoría interna, gestión de los riesgos tecnológicos, gobierno, mejora de procesos de negocio, la oficina de gestión de proyectos, arquitectura empresarial, control de calidad) de empresas grandes y complejas, utilizan diferentes metodologías o marcos de referencia para entender, medir y responder a los riesgos, lo que interfiere con una efectiva agregación de los riesgos.
- Falta de madurez de la empresa en términos de gestión de procesos, derivando en fallas para medir el desempeño de los procesos y sus resultados, por tanto, impidiendo tener una visión precisa sobre los factores de riesgos.
- Fallas de comprensión de las brechas, tanto para la capacidad de detectar la ocurrencia de un evento como para su respuesta.

4.2 Enfoque hacia la agregación de riesgos

Existen diferentes formas para realizar la agregación de riesgos. A continuación, se brinda alguna orientación al respecto:

- Asegurar que exista un método uniforme, consistente, acordado y comunicado para evaluar la frecuencia y el impacto de los escenarios de riesgos. El mismo método debe ser utilizado para representar los riesgos agregados. Utilizar una taxonomía consistente para describir los riesgos permite la agregación y reporte de distintos tipos de riesgos, p.ej., los riesgos relacionados con la creación de valor, el riesgo de ejecución de proyectos y el riesgo operacional, ya que están expresados en términos de impacto para el negocio, utilizando las mismas métricas.

- Prudencia con las matemáticas, y solo agregar datos y números significativos. No agregar datos de diferente naturaleza, p.ej., sobre el estado de controles o métricas operativas de TI. Más allá de que en forma separada sean buenos indicadores de riesgos, no tienen sentido cuando no están asociados al impacto final para el negocio. Por ejemplo, si ciertos controles no son plenamente efectivos o están mal diseñados, no constituyen un riesgo por sí mismos. Sólo existe un problema cuando los escenarios de riesgos que se basan en esos controles son inaceptables debido a fallas de dichos controles. Por lo tanto, la información de controles que fallan no es una métrica confiable por sí misma.
- Enfoque en riesgos reales para las actividades de negocio y en sus indicadores más importantes, evitando centrarse en agregar cosas que son fácilmente medibles pero de escasa relevancia. Reportar ataques al firewall puede ser fácil de medir, pero si las medidas de seguridad están implementadas y actualizadas, más allá de que posiblemente dichos ataques sean muy frecuentes, pueden acarrear un impacto menor para el negocio.
- No agregar información de riesgos de forma que oculte detalles accionables. Esto puede ocurrir debido a reportes organizacionales por “niveles de responsabilidad” que deben ser gestionados por una cierta capa de la organización y que deben ser visibles para dicha capa, pero que pueden ser agregados y ocultos para el siguiente nivel más alto de autoridad debido a que no se requieren acciones inmediatas desde dicho nivel. La causa raíz del riesgo debe estar visible para los responsables de su gestión. Debe brindarse atención a los algoritmos de agregación a utilizarse.
- La agregación es posible en múltiples dimensiones, p.ej., unidades organizacionales, tipos de elementos de riesgos, procesos de negocio. El beneficio de la agregación en procesos de negocio es que revela vínculos débiles para alcanzar resultados de negocio exitosos. Pueden ser necesarias múltiples vistas (utilizando una combinación de varias dimensiones) para satisfacer la gestión de los riesgos y las necesidades del negocio.
- Agregar riesgos a nivel de la empresa, donde los riesgos pueden ser considerados en combinación con todos los otros riesgos que la empresa necesita gestionar (integración con ERM). Considerar la estructura organizativa (divisiones geográficas, unidades de negocio, etc.) para establecer una agregación significativa de riesgos en cascada, sin perder de vista la importancia de elementos de riesgos específicos.
- Considerar las dependencias a distintos niveles:
 - Se debe comprender la dependencia entre un evento y el impacto final para el negocio. Por ejemplo, si un servidor queda fuera de servicio, ¿qué procesos de negocio podrían verse impactados y cómo esto se traduce en un impacto financiero, impacto para el cliente, etc.? Esto es parte del proceso inicial de análisis de riesgos.
 - Las dependencias entre eventos hacen la agregación más que una sumatoria matemática, pues existen eventos que pueden amplificarse entre sí. Por ejemplo:
 - Un centro de datos fuera de servicio podría ser aceptable, pero un segundo centro de datos fuera de servicio y en forma simultánea podría significar una catástrofe.
 - Un incidente de seguridad, seguido de un error durante una actualización de emergencia al software de seguridad (debido a inadecuados procedimientos de gestión de cambios y gestión de la configuración), podría resultar en una extensión de los tiempos de recuperación para los servicios críticos afectados.
 - Un proyecto que desarrolla una nueva arquitectura de TI, incluyendo modelos de datos, infraestructura, etc., sufre una demora significativa, retrasando varios proyectos de desarrollo de nuevas aplicaciones, las cuales normalmente se basan en la finalización oportuna del proyecto de arquitectura de TI.

La **figura 39** muestra un enfoque simple y posible para la agregación de riesgos. Este enfoque es solo válido cuando los elementos de riesgos son independientes entre entidades. Cuando los elementos de riesgos son compartidos o conectados, este enfoque no es válido y puede derivar en una subestimación del riesgo real. En el ejemplo de la **figura 40**:

- Dos entidades crean, después del debido análisis de riesgos, sus propios mapas de riesgos. Es notorio que la entidad de la derecha tiene riesgos más severos comparados con la entidad de la izquierda.
- Los escenarios de riesgos en los mapas son consolidados en un mapa agregado. Este enfoque es válido cuando todas las entidades usan las mismas métricas y escalas en sus mapas de riesgos.
- La figura agregada muestra un reparto equilibrado de los riesgos a través de toda la empresa, permitiendo que se definan respuestas apropiadas de gestión.

La **figura 39** muestra un método para la agregación de riesgos mediante simple adición; otros métodos pueden existir, p.ej., que cada entidad solo muestre los diez principales elementos de riesgos. Como se mencionó previamente, el método de agregación mostrado debe permitir la suficiente sensitividad, es decir, no deberían permanecer ocultos los riesgos más significativos ni las causas que los originan, frente a los encargados de tomar decisiones apropiadas.

El enfoque de agregación descrito anteriormente es solo válido cuando los elementos de riesgos en diferentes entidades son independientes, es decir, cuando no están compartidos ni se influencian mutuamente. Por lo tanto, una actividad

clave en la agregación de riesgos es evaluar los resultados del análisis de riesgos desde diferentes entidades, y verificar si existen tales dependencias, en cuyo caso, se deben adaptar los mapas agregados de riesgos en forma acorde.

Si por ejemplo, todas las unidades estuvieran utilizando el mismo centro de datos o red de energía, y cuando este centro de datos o red de energía no estuvieron disponibles, la empresa entera se ve afectada al mismo tiempo. Esto puede ser evaluado en forma diferente, es decir, más seriamente, comparado con un área de negocio que se queda sin disponibilidad por un lapso breve.

Cuando se discuten los riesgos en cascada, la magnitud de una falla conjunta podría ser incrementada, pero generalmente, la frecuencia de las fallas conjuntas son menores. En otras palabras, la probabilidad de que dos o más elementos fallen en forma simultánea es invariablemente menor que la probabilidad de sus fallas individuales.

El mapa agregado de riesgos podría ser similar al mostrado en la **figura 40**.

Figura 39—Agregación de mapas de riesgos — Riesgos independientes

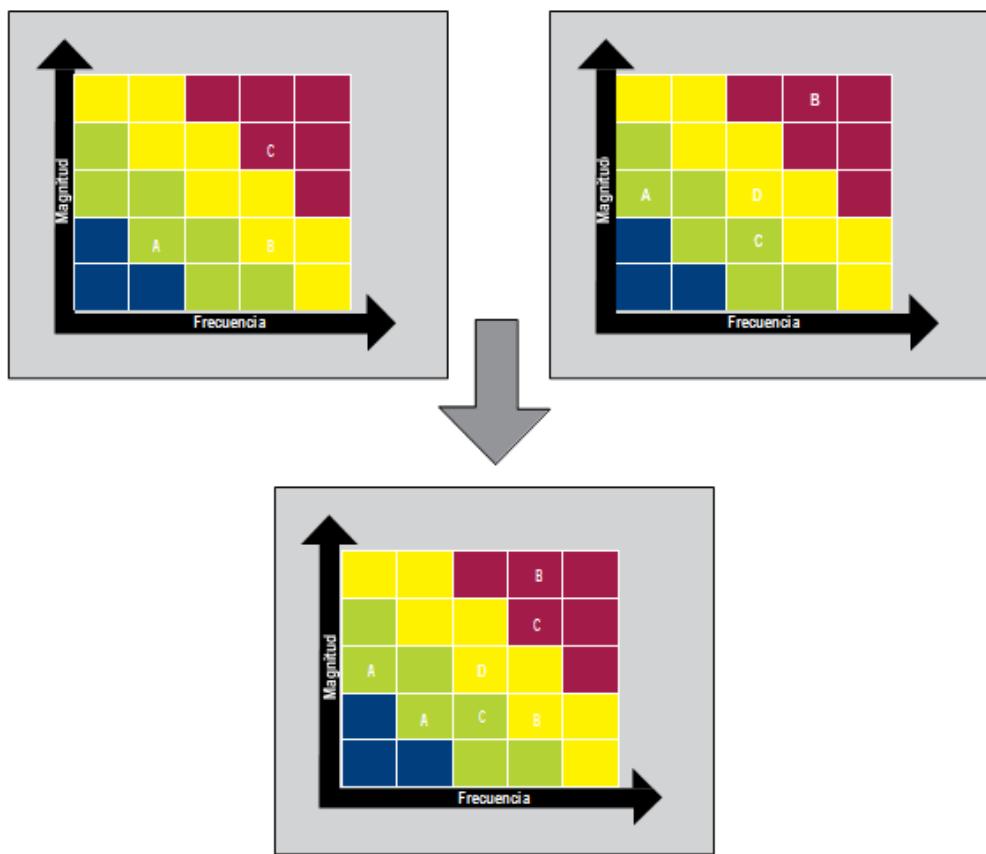
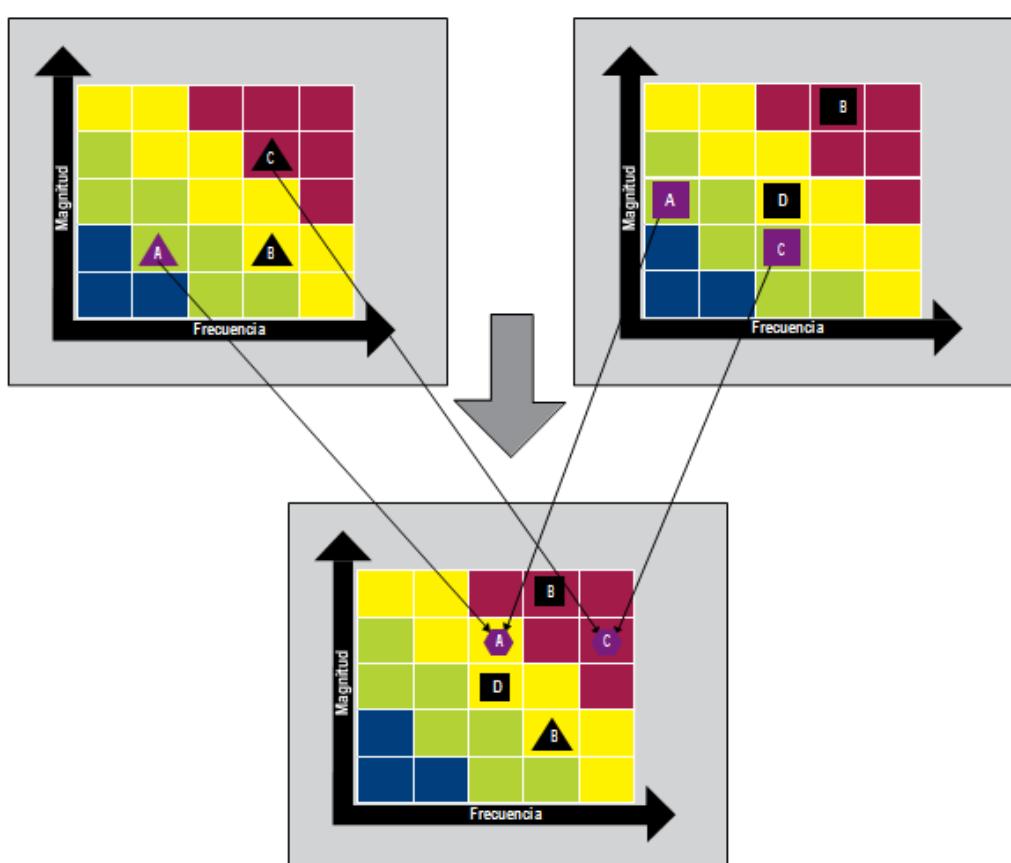


Figura 40—Agregación de mapas de riesgos — Riesgos compartidos



Uno de los beneficios de la agregación, y desde luego en el caso de las dependencias, es que el riesgo a nivel empresa se hace muy visible, favoreciendo el financiamiento para definir una respuesta al riesgo en toda la empresa. Mientras que a nivel entidad (gerencia o área), tal respuesta no habría sido factible o justificable. La agregación permite definir e implementar una respuesta eficiente en costos al riesgo vigente, y la reducción del riesgo residual dentro de los niveles definidos de apetito de riesgo.

Los mapas agregados de riesgos pueden ser parte del perfil de riesgos de la empresa, el cual a su vez es parte de los reportes de riesgos.

Página dejada en blanco intencionadamente

CAPÍTULO 5

RESPUESTA AL RIESGO

5.1 Definiciones

Los conceptos en la **figura 41** son frecuentemente utilizados en la gestión de riesgos y en este documento.

Figura 41—Definición de términos de riesgos	
Término	Definición
Apetito de riesgo	El nivel de riesgo, a un nivel amplio, que una entidad está dispuesta a aceptar en pos del logro de su misión.
Tolerancia al riesgo	El nivel aceptable de variación que la gerencia está dispuesta a permitir para cualquier riesgo en particular, con la finalidad de lograr sus objetivos.
Capacidad de riesgo	El nivel objetivo de pérdida que una empresa puede tolerar sin arriesgar su viabilidad. Difiere del apetito del riesgo, el cual es una decisión de la gerencia o del directorio, sobre cuánto riesgo es deseable aceptar.

Estos conceptos son mejor ilustrados en el apéndice B.5.6.

5.2 Flujo y opciones de respuesta al riesgo

El propósito de definir una respuesta al riesgo es alinearla con el apetito de riesgo definido por la empresa. En otras palabras, una respuesta necesita ser definida de tal manera que todo el futuro riesgo residual posible (riesgo actual con su respuesta al riesgo definida e implementada) resulte dentro de los límites de tolerancia definidos (usualmente esto depende del presupuesto disponible). El flujo completo de respuesta al riesgo es mostrado en la **figura 42**. Los procesos EDM03 y APO12 de COBIT 5 incluyen una guía en relación a estas actividades, específicamente, en las prácticas EDM03.02 y APO12.02.

Esta evaluación de respuesta al riesgo no es un esfuerzo de una sola vez, sino que es parte del ciclo del proceso de gestión de riesgos. Cuando el análisis de riesgos de todos los escenarios de riesgo identificados, después de comparar el riesgo contra el retorno potencial, muestra que el riesgo no está alineado con el apetito de riesgo o los niveles de tolerancia definidos, se requiere una respuesta. Esta puede ser cualquiera de las cuatro posibles respuestas explicadas en las secciones subsiguientes.

Evitar el riesgo

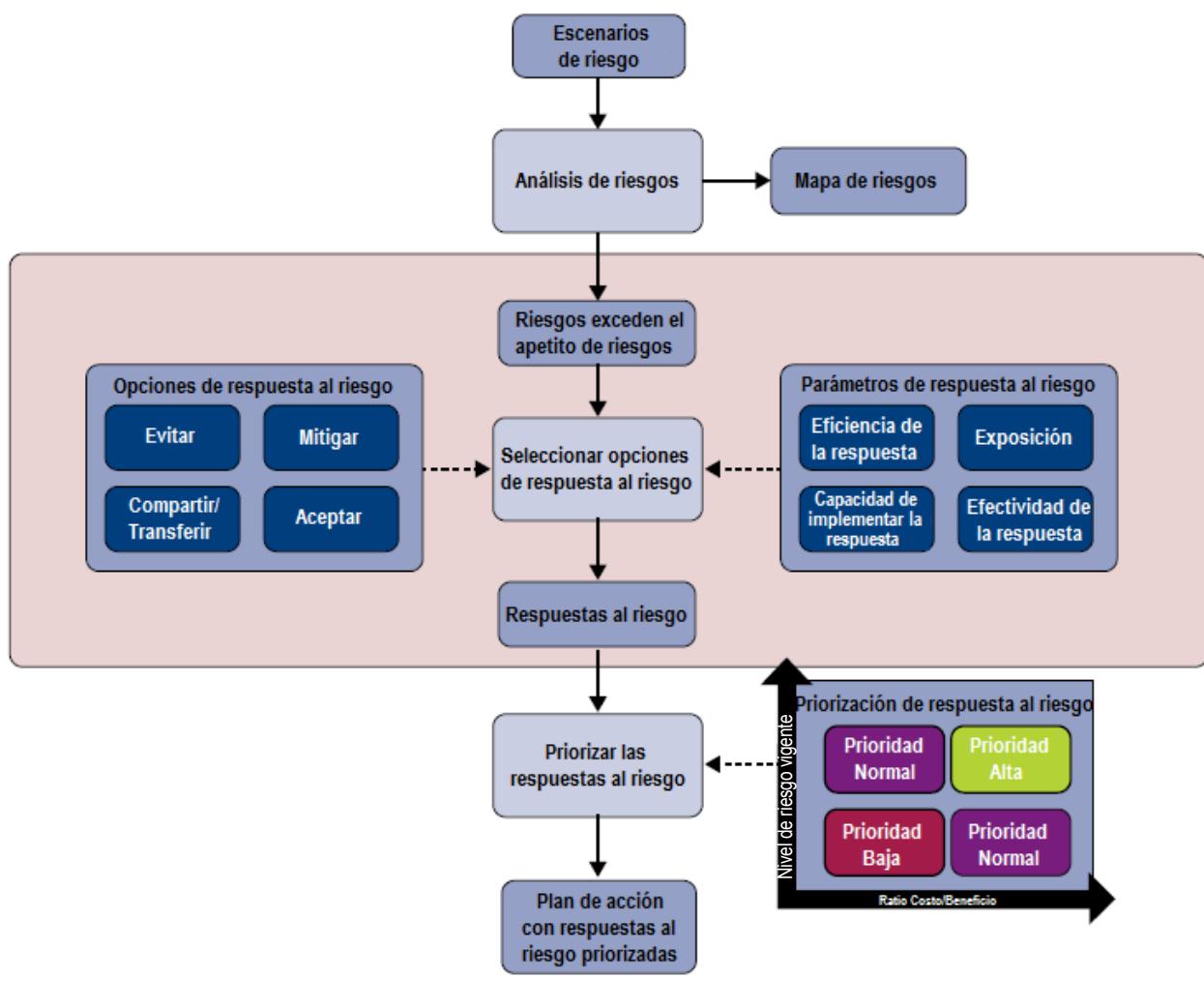
Significa dejar de hacer las actividades o salir de las condiciones que permiten que el riesgo se presente. Evitar el riesgo sólo aplica cuando ninguna otra respuesta al riesgo es adecuada. Este es el caso cuando:

- No existe ninguna otra respuesta efectiva en costo que pueda ser exitosa para disminuir la frecuencia o el impacto debajo de los umbrales definidos para el apetito de riesgo.
- El riesgo no puede ser compartido o transferido.
- El nivel de exposición ha sido considerado inaceptable por la gerencia.

Algunos ejemplos relacionados a TI sobre evitar el riesgo son:

- Reubicar un centro de datos lejos de una región con amenazas naturales significativas.
- Declinar involucrarse en un proyecto grande cuando el caso de negocio muestra un notable riesgo de falla.
- Declinar involucrarse en un proyecto que se construirá sobre sistemas obsoletos y complejos porque no existe un grado aceptable de confianza sobre el éxito del proyecto.
- Decidir no usar una determinada tecnología o paquete de software porque impedirán el crecimiento futuro del negocio.

Figura 42 —Flujo de respuesta al riesgo



Aceptar el riesgo

Aceptar significa que se reconoce la exposición a la pérdida pero no se toman acciones relativas a un riesgo en particular y la pérdida es aceptada, en caso ocurra. Esto es diferente a no estar consciente de un riesgo. Aceptar un riesgo supone que se conoce el riesgo y que la gerencia ha tomado una decisión informada para aceptarlo como tal (p.ej., cuando un costo de remediación excede el riesgo).

Si una empresa adopta una postura de aceptación del riesgo, debe considerar cuidadosamente quién puede aceptar el riesgo, incluso más con los riesgos relacionados con TI. El riesgo de TI debe ser aceptado solo por la gerencia del negocio (y los propietarios de los procesos de negocios), con la colaboración y el soporte de TI. La aceptación debe ser comunicada y documentada a la alta gerencia y al directorio (ver EDM3.02, actividades 5.3 y 5.4). Las empresas deberían también considerar niveles autorizados de aceptación del riesgo, estableciendo responsables de la empresa que están autorizados para aceptar diferentes niveles de riesgo, lo que ayudará a asegurar que el riesgo sea aceptado en un nivel adecuado dentro de la empresa.

Algunos ejemplos de aceptación de riesgos son:

- Pueden haber riesgos que un proyecto de desarrollo no entregue las funcionalidades de negocio requeridas en la fecha planificada. La gerencia puede decidir aceptar el riesgo y proseguir con el proyecto.
- Si un riesgo en particular es evaluado como extremadamente raro, pero con un impacto muy alto (catastrófico) y cualquier costo de mitigarlo es prohibitivo, la gerencia puede decidir aceptarlo.

Contratar seguros también es una manera de aceptar el riesgo, aunque esto sólo mitigue la magnitud de la pérdida y no disminuya la frecuencia esperada.

Compartir/Transferir el riesgo

Compartir significa reducir la frecuencia o el impacto del riesgo transfiriendo o compartiendo una porción del riesgo. Las técnicas comunes incluyen la contratación de seguros y la externalización.

Algunos ejemplos incluyen adquirir cobertura de seguros para incidentes relacionados con TI, externalizar algunas actividades de TI, compartir riesgos de proyectos de TI con el proveedor a través de acuerdos de precios fijos o acuerdos de inversión compartida. Tanto a nivel físico como a nivel legal, estas técnicas no liberan a la empresa de la propiedad del riesgo, pero pueden involucrar las habilidades y competencias de terceros en la gestión de riesgos para reducir las consecuencias financieras si ocurrieran eventos adversos. Así mismo, desde el punto de vista de la reputación, compartir o transferir riesgos no traslada la propiedad ni la responsabilidad sobre los mismos.

Algunos ejemplos de compartir o transferir riesgos relacionados con TI son:

- Una empresa de gran tamaño identificó y evaluó el riesgo de incendio en su infraestructura a través de diversas regiones geográficas, evaluando el costo de compartir el impacto del riesgo a través de una cobertura de seguros. Se concluyó que debido a la ubicación de los sitios, el costo del seguro y de los deducibles relacionados no era prohibitivo, de tal forma que se optó por contratar la cobertura del seguro.
- En una gran inversión relacionada con TI, el riesgo del proyecto puede ser compartido externalizando el desarrollo de la solución a un proveedor por un precio fijo, basado en un esquema de bonificaciones.
- Algunas empresas externalizan todas o algunas de las funciones de TI, compartiendo una fracción del riesgo de manera contractual.
- Cuando se externaliza el servicio de hosting de aplicaciones, la empresa siempre conserva la responsabilidad de proteger la privacidad de los datos del cliente, pero si el proveedor es negligente y ocurre una brecha de seguridad, el riesgo (impacto financiero) puede por lo menos ser compartido con la empresa que brinda el hosting.

Otras técnicas que contribuyen a compartir el riesgo incluyen:

- Empresas grandes con muchas entidades legales, donde los riesgos de TI pueden ser transferidos a otras divisiones dentro de la empresa (los reaseguros son un ejemplo común).
- La certificación SSAE16, que permite a una organización que brinda servicios, transfiera una fracción del riesgo al cliente, a través de la sección “Consideraciones del Cliente” del reporte SSAE16.

Mitigar el riesgo

Significa tomar acciones de mitigación para reducir la frecuencia y/o el impacto de un riesgo. Las maneras más comunes de mitigar un riesgo incluyen:

- Reforzar las prácticas de gestión de riesgos de TI, p.ej., implementar procesos de gestión de riesgos de TI lo suficientemente maduros, como se define en el marco COBIT 5.
- Introducir medidas de control orientadas a reducir la frecuencia de ocurrencia de un evento adverso y/o el impacto de un evento en el negocio. Los controles son, en el contexto de la gestión de riesgos, empleados para mitigar un riesgo, p.ej., las políticas, procedimientos y prácticas, estructuras, flujos de información, etc. El conjunto de catalizadores interconectados de COBIT 5 ofrece un conjunto comprehensivo de controles que pueden ser implementados. Es posible identificar, para cualquier escenario de riesgo que excediera el apetito de riesgo, un conjunto de catalizadores de COBIT 5 (procesos, estructuras organizativas, comportamientos, etc.) que puedan mitigar dicho escenario de riesgo. El apéndice D incluye una lista detallada de controles (expresados como catalizadores COBIT 5) que puedan mitigar riesgos (ver la lista de ejemplos de escenarios genéricos de riesgos definidos en el capítulo 3).
- La mitigación de riesgos también es posible por otros medios o métodos, es decir, existen estándares y marcos de referencia de TI bastante conocidos que pueden ser de ayuda.

5.3 Selección y priorización de la respuesta al riesgo

La sección previa discute sobre las opciones disponibles de respuesta al riesgo. En esta sección, se trata la selección de una respuesta apropiada, es decir, dado un riesgo en particular, se discute cómo responder y cómo escoger entre las opciones disponibles de respuesta. Como se ilustra en la **figura 43**, en este proceso se deben considerar los siguientes parámetros:

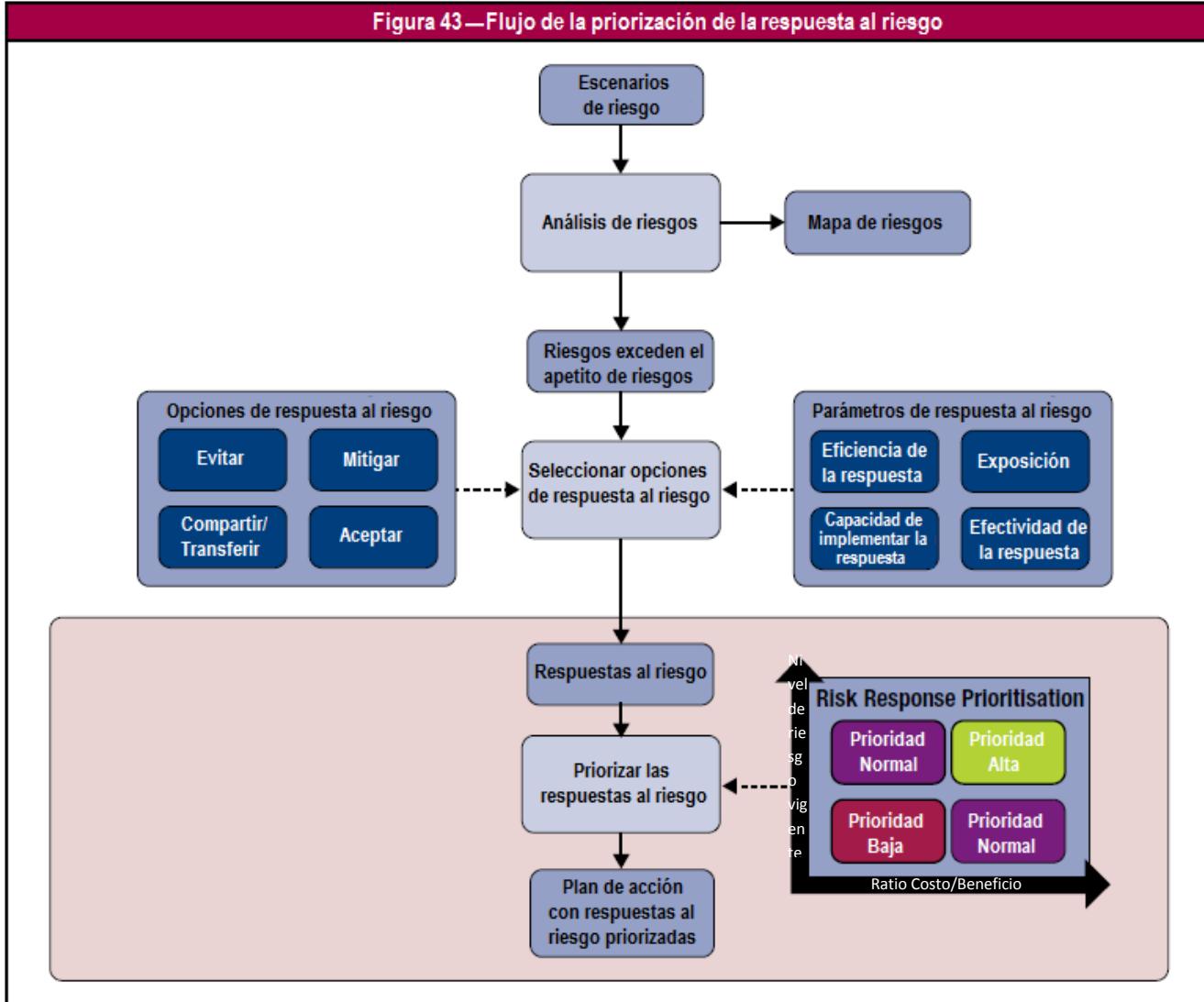
- Eficiencia de la respuesta, es decir, los beneficios relativos esperados de la respuesta en comparación con:
 - Otras inversiones (invertir en medidas de respuesta al riesgo siempre compite con otras inversiones).
 - Otras respuestas (una respuesta puede resolver varios riesgos mientras que otra no).

Esto también considera el costo de una respuesta, p.ej., en el caso de una transferencia de riesgos, el costo de una

cobertura de seguros premium; en el caso de una mitigación de riesgos, el costo de implementar medidas de control (gastos de capital, salarios, consultorías, etc.)

- Exposición, es decir, la importancia del riesgo que aborda la respuesta, representado por su posición en el mapa de riesgos (que refleja los niveles combinados de frecuencia e impacto).
 - La capacidad de la empresa para implementar la respuesta. Cuando la empresa es madura en sus procesos de gestión de riesgos, se pueden implementar respuestas al riesgo más sofisticadas; si no es tan madura, es mejor empezar con respuestas básicas al riesgo.
 - Efectividad de la respuesta, es decir, la medida en que la respuesta reducirá el impacto y la magnitud del riesgo.

Figura 43—Flujo de la priorización de la respuesta al riesgo



El esfuerzo agregado requerido para las respuestas de mitigación, es decir, el grupo de controles que se necesitan implementar o reforzar, pueden exceder los recursos disponibles. Siempre que no haya una urgencia requerida, se necesita preparar un caso de negocios priorizado para las inversiones. Utilizando el mismo criterio de la selección de la respuesta al riesgo, las respuestas al riesgo pueden ser establecidas en un cuadrante que ofrece **tres posibles prioridades**, como se muestra en la **figura 43**.

- **Prioridad alta:** Respuestas muy efectivas y eficientes en costos para los riesgos altos.
 - **Prioridad normal:** Tanto las respuestas más costosas o difíciles para los riesgos altos, como las respuestas efectivas y eficientes para los riesgos menores, requieren un análisis cuidadoso y decisión de la gerencia sobre las inversiones.
 - **Prioridad baja:** Las respuestas para los riesgos bajos pueden resultar costosas y pueden no demostrar un buen ratio de costo/beneficio.

Algunos ejemplos de priorización incluyen:

- Se identificó un riesgo en la arquitectura de TI de una empresa, que, debido a su complejidad, dentro de unos pocos años se tornará difícil y el mantenimiento del software será muy costoso. La respuesta identificada fue el

fortalecimiento del proceso APO03 *Gestionar la arquitectura de la empresa* de COBIT, así como empezar un proyecto grande para optimizar la arquitectura completa. Dados los costos del proyecto, esta respuesta está categorizada como “normal”.

- Se identificó un riesgo de incumplimiento con regulaciones dado que no se cuenta con algunos procedimientos relativamente simples de TI. La respuesta consistió en crear e implementar los procedimientos de TI faltantes. Esto fue clasificado como “alto”.

5.4 Guía en la selección y priorización de respuesta al riesgo

Las estructuras organizativas en *COBIT 5 para Riesgos* incluyen cuadros de roles y responsabilidades (RACI por sus siglas en inglés) para todas las actividades del proceso de gestión de riesgos de TI, incluyendo la definición y priorización de la respuesta al riesgo. Las principales partes interesadas deben involucrarse en estas decisiones: la alta gerencia, la gerencia del negocio, la gerencia de riesgos y la gerencia de TI.

Basado en los resultados del análisis de riesgos y en la experiencia ganada durante la definición y priorización de la respuesta al riesgo, la empresa también puede decidir sobre cambios más fundamentales en su posición contra el riesgo, por ejemplo:

- Revisar los umbrales de apetito de riesgo o, temporalmente, incrementar o disminuir los niveles de apetito de riesgo.
- Incrementar (o disminuir) los recursos disponibles para ejecutar la respuesta al riesgo.
- Aceptar riesgos que normalmente excederían los umbrales de apetito de riesgo.

En la evaluación y diseño de la respuesta al riesgo, las empresas siempre deberían procurar un conjunto balanceado de respuestas, es decir, una combinación de concientización/capacitación, proceso/gobierno y automatización.

Página dejada en blanco intencionadamente

SECCIÓN 3: ¿CÓMO SE ALINEA ESTA PUBLICACIÓN CON OTROS ESTÁNDARES?

COBIT 5 para Riesgos, al igual que COBIT 5, es un marco de referencia paraguas para el gobierno y la gestión del riesgo. Para entender mejor esta posición paraguas, esta sección contiene el posicionamiento de *COBIT 5 para Riesgos* respecto de los siguientes estándares relacionados con riesgos de TI.

- ISO 31000
- ISO/IEC 27005
- COSO ERM

CAPÍTULO 1 ISO 31000 Y COBIT 5 PARA RIESGOS

1.1 ISO 31000:2009 Principios y directrices para la gestión de riesgos

Este estándar contiene tres cláusulas principales:

- Capítulo 4: Principio para la gestión de riesgos.
- Capítulo 5: Marco de referencia para la gestión de riesgos.
- Capítulo 6: Procesos para la gestión de riesgos.

En general, se puede notar que los procesos definidos en la ISO 31000 están cubiertos totalmente por los diferentes procesos y prácticas del modelo de procesos de *COBIT 5 para Riesgos*; sin embargo, *COBIT 5 para Riesgos*, provee una guía más extensa e incluye áreas no cubiertas por ISO 31000, tales como el gobierno del riesgo.

Principios para la gestión de riesgos

La figura 44 contiene los 11 principios de la gestión de riesgos que ISO 31000 ha definido y en qué medida son cubiertas por *COBIT 5 para Riesgos*.

Figura 44—ISO 31000 Principios de la gestión de riesgos cubiertos por <i>COBIT 5 para Riesgos</i>	
Principios ISO 31000	Cobertura de <i>COBIT 5 para Riesgos</i>
La gestión de riesgos crea y protege el valor.	<ul style="list-style-type: none"> • Principio 1: Gestionar las necesidades de las partes interesadas. • Cada habilitador proporciona valor a través del cumplimiento de sus metas.
La gestión de riesgos es una parte integral de los procesos organizacionales.	<ul style="list-style-type: none"> • Principio 2: Cobertura de la empresa de extremo a extremo. • Cuenta con un modelo de proceso que promueve la integración en los procesos de gestión del riesgo empresarial (ERM) y los procesos operativos (APO12 Gestionar el riesgo).
La gestión de riesgos es parte de la toma de decisiones.	<ul style="list-style-type: none"> • Dedica un proceso entero (EDM03 Asegurar la optimización del riesgo) a las decisiones de negocio conscientes de los riesgos. • Los modelos de capacidad ilustran cómo las decisiones empresariales mejoran, basadas en la adecuada y mayor participación de las partes interesadas y la mejora de la calidad y disponibilidad de los resultados del análisis de riesgos. • El modelo de procesos proporciona un conjunto completo de tablas RACI que indican cómo pueden asignarse las responsabilidades y la rendición de cuentas de la gestión de riesgos.
La gestión de riesgos aborda explícitamente la incertidumbre.	<ul style="list-style-type: none"> • Recomienda prácticas de gestión que estiman los riesgos de TI basados en escenarios de frecuencia e impacto variables. Los escenarios permiten considerar diferentes factores que generan o crean incertidumbre.
La gestión de riesgos es sistemática, estructurada y oportuna.	<ul style="list-style-type: none"> • Catalizador: Procesos. • Catalizador: Principios, políticas y marcos de referencia. • La dimensión de ciclo de vida de los catalizadores es una forma sistemática y estructurada de gestionar los riesgos. • La dimensión de buenas prácticas de los catalizadores proporciona prácticas de gestión que consisten de prácticas y actividades de proceso y actividades detalladas.
La gestión de riesgos se basa en la mejor información disponible.	<ul style="list-style-type: none"> • Catalizador: Información.
La gestión de riesgos está hecha a medida.	<ul style="list-style-type: none"> • Principio 1: Gestionar las necesidades de las partes interesadas. • Describe procesos (EDM03, MEA01, MEA02 y MEA03) que se adaptan a las necesidades específicas de desempeño y requisitos externos de la organización.

Figura 44—ISO 31000 Principios de la gestión de riesgos cubiertos por COBIT 5 para Riesgos (cont.)

Principios ISO 31000	Cobertura de COBIT 5 para Riesgos
La gestión de riesgos considera factores personales y culturales.	<ul style="list-style-type: none"> • Catalizador: Cultura, ética y comportamiento. • Ofrece escenarios de ejemplo que cubren factores personales.
La gestión de riesgos es transparente e inclusiva.	<ul style="list-style-type: none"> • Principio 4: Promueve comunicaciones abiertas y transparentes sobre riesgos de TI. • Proceso de soporte EDM05 asegura transparencia hacia las partes interesadas. • El proceso APO12 promueve la transparencia e inclusión en la gestión de riesgos. • Recomienda la transparencia como un comportamiento en toda la empresa
La gestión de riesgos es dinámica, iterativa y sensible al cambio.	<ul style="list-style-type: none"> • Principio 1: Gestionar las necesidades de las partes interesadas. • Dedica un proceso entero (APO12) para el mantenimiento del perfil de riesgo de TI para ayudar a que las actividades de la gestión de riesgos de TI sintonicen con los cambios organizacionales. • Describe la forma de utilizar los siete catalizadores para responder al riesgo. • Cada habilitador tiene un ciclo de vida. Las fases Evaluar/Supervisar y Actualizar/Eliminar aseguran un carácter dinámico, iterativo y sensible.
La gestión de riesgos facilita la mejora continua en la organización.	<ul style="list-style-type: none"> • Incluye prácticas de gestión y flujos de información que soporta la mejora de procesos sobre la base de lecciones aprendidas de los eventos de riesgo, excepciones a las políticas y los datos en el cambio cultural consciente de los riesgos. • El modelo de procesos incluye metas y métricas (MEA02) que pueden ser utilizadas para medir el desempeño.

Marco de referencia para la gestión de riesgos

ISO 31000 define un marco de referencia de cinco bloques para la gestión de riesgos. La **figura 45** contiene los cinco bloques (de la A a la E) y explica la forma en que *COBIT 5 para Riesgos* cubre cada uno de esos componentes.

Figura 45—ISO 31000 Marco de referencia para la gestión de riesgos cubierto por COBIT 5 para Riesgos

Componentes del marco ISO 31000	Cobertura de COBIT 5 para Riesgos
A. Mandato y compromiso	<ul style="list-style-type: none"> • Incluye prácticas para alinear los objetivos e indicadores de desempeño de la gestión de riesgos de TI con los de ERM. • Define los roles de la gestión de riesgos de TI y sugiere la asignación de responsabilidades y rendición de cuentas para las actividades clave. • El modelo de catalizadores incluye contenido específico para las partes interesadas, tales como información específica a ser comunicada, roles y responsabilidades. • Catalizador: Principios, políticas y marcos de referencia; detalles principales y otras políticas de riesgo. • Incluye el proceso MEA03 dedicado a la evaluación, supervisión y valoración del cumplimiento de requerimientos
B. Diseño de marco de referencia para la gestión de riesgos	
1. Comprendiendo la organización y su contexto.	<ul style="list-style-type: none"> • Catalizador: Estructuras organizativas. • Incluye prácticas para recolectar datos sobre el ambiente de operaciones. • Incluye prácticas de gestión para entender el contexto interno y determinar dónde y cómo los procesos de la empresa dependen de TI para el éxito.
2. Política de gestión de riesgos.	<ul style="list-style-type: none"> • Catalizador: Principios, políticas y marcos de referencia. • Incluye prácticas de gestión para traducir el apetito y la tolerancia al riesgo en políticas y alinear las políticas existentes relacionadas con TI con la tolerancia al riesgo aprobada. • Incluye las rutas de escalamiento para lidiar con situaciones conflictivas relacionadas con la aplicación de políticas.
3. Rendición de cuentas.	<ul style="list-style-type: none"> • Catalizador: Personas, habilidades y competencias. • Define los roles de la gestión de riesgos de TI y sugiere la asignación de responsabilidades y rendición de cuentas para las actividades clave de esos roles. • Incluye prácticas de gestión para establecer y mantener la rendición de cuentas para la gestión de riesgos de TI.
4. Integración en los procesos organizacionales.	<ul style="list-style-type: none"> • Catalizador: Procesos. • Principio 2: Cobertura de la empresa de extremo a extremo. • Dedica un proceso entero para la integración con ERM. • Incluye vínculos detallados con COBIT 5 que modelan un amplio rango de proceso de negocios y de TI.
5. Recursos.	<ul style="list-style-type: none"> • Incluye prácticas de gestión para proporcionar recursos adecuados para la gestión de riesgos de TI (APO07).

Figura 45—ISO 31000 Marco de referencia para la gestión de riesgos cubierto por COBIT 5 para Riesgos (cont.)

Componentes del marco ISO 31000	Cobertura de COBIT 5 para Riesgos
6. Establecer mecanismos de comunicación interna y de reporte.	<ul style="list-style-type: none"> • Catalizador: Información. • Catalizador: Servicios, infraestructura y aplicaciones. • Incluye prácticas de gestión para fomentar la comunicación efectiva de riesgos de TI (EDM03). • El modelo de procesos incluye información específica a ser comunicada entre las prácticas clave de gestión. • La introducción del marco de referencia cuenta con una sección sobre la comunicación de riesgos con los flujos de información sugerida entre las diferentes partes interesadas
7. Establecer mecanismos de comunicación externa y de reporte.	<ul style="list-style-type: none"> • Catalizador: Información. • Catalizador: Servicios, infraestructura y aplicaciones. • Incluye prácticas de gestión para comunicar y reportar actividades en curso de la gestión de riesgos, así como la comunicación con las partes interesadas en el evento de una crisis o contingencia. (Catalizador: Cultura, ética y comportamiento). • Incluye prácticas para proporcionar aseguramiento independiente sobre la gestión de riesgos de TI (MEA02).
C. Implementar la gestión de riesgos	
1. Implementar el marco de referencia para la gestión de riesgos.	<ul style="list-style-type: none"> • El apéndice B describe la forma de implementar los siete catalizadores.
2. Implementar el proceso de la gestión de riesgos.	<ul style="list-style-type: none"> • Incluye prácticas de gestión para desarrollar métodos integrados de gestión de riesgos, basados en una estrategia integrada de gestión de riesgos. • Puede ayudar a las empresas a desarrollar prácticas líderes en técnicas de gestión de riesgos de TI, en línea con los catalizadores.
D. Supervisar y revisar el marco de referencia	
E. Mejora continua del marco de referencia	
	<ul style="list-style-type: none"> • Contiene métricas para el logro de metas y métricas para la aplicación de prácticas.
	<ul style="list-style-type: none"> • Incluye prácticas de gestión y flujos de información que soportan la mejora de procesos basado en datos de eventos o incidentes post mortem, adherencia a las políticas y estándares, así como datos sobre el cambio cultural consciente de los riesgos.

Proceso para la gestión de riesgos

ISO 31000 describe los seis mayores componentes de los procesos de gestión de riesgos. La **figura 46** enumera cada uno de esos componentes (de la A a la F) y describe cómo y dónde *COBIT 5 para Riesgos* cubre estos componentes.

Figura 46—ISO 31000 Procesos de gestión de riesgos cubiertos por COBIT 5 para Riesgos

ISO 31000 Procesos de gestión de riesgos	Cobertura de COBIT 5 para Riesgos
A. Comunicación y consulta	<ul style="list-style-type: none"> • El habilitador “Información” incluye información específica a ser comunicada entre las partes interesadas.
B. Establecer el contexto	
1. Establecer el contexto externo.	<ul style="list-style-type: none"> • Incluye prácticas de gestión para trabajar con las funciones de riesgo al más amplio nivel de la empresa para comprender el contexto externo.
2. Establecer el contexto interno.	<ul style="list-style-type: none"> • Incluye prácticas de gestión para comprender el contexto interno, lo que incluye determinar dónde y cómo los procesos organizacionales dependen de TI para el éxito, y compararlo con las capacidades de TI existentes.
3. Establecer el contexto del proceso de gestión de riesgos.	<ul style="list-style-type: none"> • Cuenta con un dominio llamado gobierno del riesgo para ayudar a asegurar que el enfoque adoptado de gestión de riesgos es adecuado para la situación de la empresa y para los riesgos que afectan al logro de sus objetivos.
4. Desarrollar los criterios del riesgo.	<ul style="list-style-type: none"> • Ofrece una guía a las empresas para desarrollar sus criterios específicos de riesgos, tal como la medición de consecuencias, la definición del impacto al negocio, el establecimiento de los umbrales del apetito y la tolerancia al riesgo así como la agregación del riesgo. • El modelo de catalizadores incluye prácticas de gestión para establecer los criterios del riesgo.
C. Evaluación del riesgo	
1. Identificar el riesgo.	<ul style="list-style-type: none"> • Incluye prácticas de gestión para identificar los riesgos asociados con los productos y servicios clave de la organización que dependen de TI, y para identificar factores de riesgo que contribuyen a los incidentes y eventos históricos. • Incluye técnicas específicas para identificar escenarios basados en un actor, tipo de amenaza, evento, recursos/activos y una dimensión de tiempo.
2. Analizar el riesgo.	<ul style="list-style-type: none"> • El análisis del riesgo es el proceso que estima la frecuencia y el impacto de los escenarios de riesgo.
3. Valorar el riesgo.	<ul style="list-style-type: none"> • Aborda esta fase del proceso en forma intrínseca.

Figura 46—ISO 31000 Procesos de gestión de riesgos cubiertos por COBIT 5 para Riesgos (cont.)

ISO 31000 Procesos de gestión de riesgos	Cobertura de COBIT 5 para Riesgos
D. Tratamiento del riesgo	
1. Seleccionar opciones.	<ul style="list-style-type: none"> Incluye una guía sobre las opciones comunes de respuesta y cómo se aplican en un contexto de TI.
2. Preparar e implementar planes de tratamiento del riesgo.	<ul style="list-style-type: none"> Define respuestas específicas al riesgo para abordar diferentes tratamientos del riesgo (sección 2B). Utiliza desarrollo de escenarios para la identificación de riesgos.
E. Supervisión y revisión	<ul style="list-style-type: none"> Incluye metas y métricas que pueden ser utilizadas para medir el desempeño, y un modelo de madurez para establecer una hoja de ruta para mejorar el proceso de gestión de riesgos.
F. Registrar el proceso de gestión de riesgos	<ul style="list-style-type: none"> Incluye prácticas de gestión para rastrear las decisiones clave de riesgos, y especifica las entradas y salidas entre sus prácticas de gestión.

Conclusión

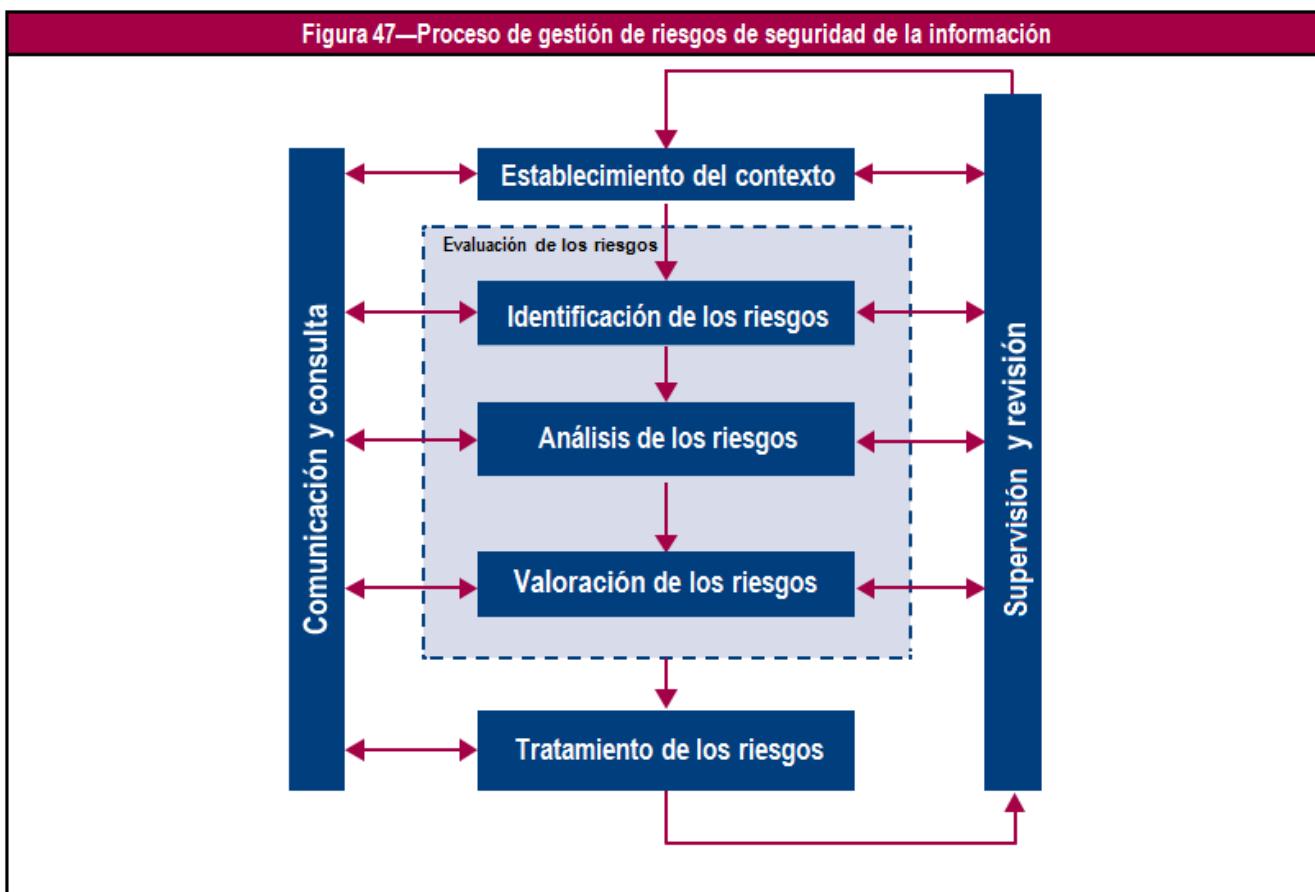
COBIT 5 para Riesgos abarca todos los principios de ISO 31000, por intermedio de los principios y catalizadores, su diseño conceptual o a través del modelo de catalizadores. Además, los aspectos del marco de referencia y del modelo de procesos están cubiertos con mayor detalle por el modelo de procesos de *COBIT 5 para Riesgos*. Todos los elementos están incluidos en *COBIT 5 para Riesgos*, y a menudo, se amplían y detallan, específicamente para el gobierno y la gestión de riesgos de TI.

CAPÍTULO 2

ISO/IEC 27005 Y *COBIT 5 PARA RIESGOS*

2.1 ISO/IEC 27005:2011–Tecnología de información–Técnicas de seguridad–Gestión de riesgos de seguridad de información

ISO/IEC 27005:2011–Tecnología de información–Técnicas de seguridad–Gestión de riesgos de seguridad de información (en adelante, ISO/IEC 27005) define un proceso de gestión de riesgos de seguridad de información que incluye las etapas de proceso mostradas en la **figura 47**.



Comparación entre ISO/IEC 27005 y COBIT 5 para Riesgos

La **figura 48** resalta las distintas etapas de proceso de ISO/IEC 27005, un resumen de los conceptos importantes de estas etapas y discute sobre cómo y en qué medida están cubiertas por *COBIT 5 para Riesgos*.

En general, se puede notar que el proceso como se define en ISO/IEC 27005 está totalmente cubierto por los distintos procesos y prácticas del modelo de proceso de *COBIT 5 para Riesgos*, modelo que proporciona una guía más amplia e incluye áreas que no están cubiertas por ISO/IEC 27005, tales como el gobierno de los riesgos y las reacciones a eventos.

La diferencia fundamental entre los dos marcos de referencia es que *COBIT 5 para Riesgos* considera una amplia variedad de categorías de riesgos de TI, mientras que ISO/IEC 27005 se enfoca de manera específica en los riesgos de seguridad de información. ISO/IEC 27005 define al riesgo de seguridad de información como “el potencial de que una amenaza explote las vulnerabilidades de los activos o grupos de activos de información, y por lo tanto, causar daño a la organización”, mientras que en *COBIT 5 para Riesgos* se define al riesgo de TI como el riesgo de negocio asociado al uso, propiedad, operación, involucramiento, influencia y adopción de TI en la organización.

Figura 48—ISO/IEC 27005 Etapas de proceso cubiertas por COBIT 5 para Riesgos

Etapa de proceso ISO/IEC 27005	Conceptos importantes del componente	Cobertura de COBIT 5 para Riesgos
Establecimiento del contexto.	<p>Esta etapa incluye:</p> <ul style="list-style-type: none"> • Establecer los criterios básicos necesarios para la gestión de riesgos de seguridad de la información (GRSI). • Definir el alcance y los límites. • Establecer una organización apropiada que opere la GRSI. 	<p>Esta etapa está incluida en la meta de la dimensión de habilitador. Más específicamente, calidad contextual: la medida en que los resultados del habilitador cumplen con el propósito, dado el contexto en el cual operan.</p>
Evaluación de los riesgos.	<p>La evaluación de los riesgos determina el valor de los activos de información, identifica las amenazas y vulnerabilidades aplicables existentes (o que podrían existir), identifica los controles existentes y su efecto en los riesgos identificados, determina las consecuencias potenciales y, por último, prioriza los riesgos derivados y los clasifica de acuerdo a los criterios de evaluación de riesgos definidos al establecer el contexto. Esta etapa de proceso consta de las siguientes actividades: identificación de los riesgos, análisis de los riesgos y valoración de los riesgos.</p>	<p>El apéndice B.3 describe la evaluación de los riesgos como un elemento del habilitador Información.</p>
Identificación de los riesgos.	<p>La identificación de los riesgos incluye la identificación de:</p> <ul style="list-style-type: none"> • Activos. • Amenazas. • Vulnerabilidades. • Controles existentes. • Consecuencias. <p>El resultado de este proceso es una lista de escenarios de incidentes y sus consecuencias en relación a los activos y procesos de negocio.</p>	<p>La secuencia utilizada en ISO/IEC 27005 para la identificación de los riesgos está alineada parcialmente con el enfoque de COBIT 5 para Riesgos. La identificación de riesgos en COBIT 5 para Riesgos consta de los siguientes elementos:</p> <ul style="list-style-type: none"> • Control. • Valor. • Condición de amenaza que impone un nivel notable de riesgo de TI. <p>COBIT 5 para Riesgos también utiliza el desarrollo de escenarios para identificar riesgos.</p> <p>Los atributos clave de eventos de riesgo conocidos y potenciales son almacenados en un repositorio. Los atributos pueden incluir nombre, descripción, dueño, frecuencia actual/esperada, magnitud actual/potencial, impacto de negocio actual/potencial, eliminación, etc.</p>
Análisis de los riesgos.	<p>La etapa de estimación de riesgos incluye los siguientes conceptos importantes:</p> <ul style="list-style-type: none"> • Evaluación de las consecuencias. • Evaluación de la probabilidad de incidentes. • Determinación del nivel de riesgo. 	<p>El análisis de los riesgos es el proceso en donde se estiman la frecuencia y el impacto de los escenarios de riesgo de TI.</p>
Valoración de los riesgos.	<p>En esta etapa, los niveles de riesgo se comparan de acuerdo a los criterios de valoración y aceptación de los riesgos. El resultado es una lista priorizada de los elementos de riesgo y de los escenarios de incidentes que conducen a los elementos identificados de riesgo.</p>	<p>De forma intrínseca, considera a esta etapa como parte de la “agregación de riesgos”. Evalúa los riesgos de acuerdo a “la tolerancia al riesgo de la gerencia con respecto al apetito de riesgo del consejo directivo”.</p> <p>Utiliza un mapa de riesgos para priorizar y mostrar gráficamente los riesgos por rangos definidos de frecuencia e impacto.</p>
Tratamiento de los riesgos.	<p>Las opciones para el tratamiento de los riesgos incluyen:</p> <ul style="list-style-type: none"> • Modificar los riesgos. • Retener los riesgos. • Evitar los riesgos. • Compartir los riesgos. 	<p>La sección 2B describe los tratamientos de los riesgos identificados. Estos son:</p> <ul style="list-style-type: none"> • Evitar los riesgos. • Reducir/mitigar los riesgos. • Compartir/transferir los riesgos. • Aceptar los riesgos.
Aceptación de los riesgos de seguridad de información.	<p>La entrada es un plan de tratamiento de riesgos y la evaluación del riesgo residual sujeto a los criterios de aceptación del riesgo. Esta etapa consta de la aceptación formal y el registro de los planes sugeridos para el tratamiento de los riesgos, la evaluación del riesgo residual por la gerencia, con la justificación para aquellos que no cumplen con los criterios de la empresa.</p>	<p>La sección 2B, sub-sección 5.2 Respuesta al riesgo, cubre la etapa de aceptación de los riesgos.</p> <p>Si una organización adopta una postura de aceptación de los riesgos, debería considerar cuidadosamente quién puede aceptar el riesgo, especialmente si se trata de riesgo de TI. El riesgo de TI debería ser aceptado solo por la gerencia (y los propietarios de los procesos de negocio), apoyados por TI. La aceptación debería ser comunicada a la alta gerencia y al consejo directivo.</p>

Figura 48—ISO/IEC 27005 Pasos de proceso cubiertos por <i>COBIT 5 para Riesgos</i> (cont.)		
ISO/IEC 27005 Etapa de proceso	Conceptos importantes del componente	Cobertura de <i>COBIT 5 para Riesgos</i>
Comunicación y consulta de los riesgos de seguridad de información	Este es un proceso transversal. La información sobre los riesgos debería ser intercambiada y compartida entre quienes toman las decisiones y otras partes interesadas a través de todas las etapas del proceso de gestión de riesgos.	<ul style="list-style-type: none"> • Principio 1: Satisfacer las necesidades de las partes interesadas. • El habilitador “Información” incluye información específica para ser comunicada entre las partes interesadas.
Supervisión y revisión de los riesgos de seguridad de información.	Los riesgos y los factores que influyen en ellos deberían ser supervisados y revisados para identificar cualquier cambio en el contexto de la organización en etapa temprana, y para mantener una visión general del panorama total de riesgo.	Incluye metas y métricas que pueden ser utilizadas para medir el desempeño y un modelo de madurez para establecer una hoja de ruta para el mejoramiento de los procesos de gestión de riesgos.

Conclusión

COBIT 5 para Riesgos considera todos los componentes descritos en ISO/IEC 27005. Algunos de estos elementos aparecen estructurados o mencionados de forma distinta. *COBIT 5 para Riesgos* asume una perspectiva más amplia de la gestión de riesgos de TI en comparación con ISO/IEC 27005, que está enfocada en la gestión de riesgos relacionados a la seguridad de información. Por tanto, *COBIT 5 para Riesgos* enfatiza fuertemente en procesos y prácticas para asegurar el alineamiento con los objetivos del negocio, la aceptación en toda la empresa y un alcance completo, entre otros factores.

Página dejada en blanco intencionadamente

CAPÍTULO 3

COSO ERM Y *COBIT 5 PARA RIESGOS*

3.1 COSO ERM – Marco de Referencia Integrado

La Gestión del Riesgo Empresarial (ERM) – Marco de Referencia Integrado del *Committee of Sponsoring Organisations of the Treadway Commission (COSO)*, también conocida como COSO ERM, define ocho componentes con relación con la gestión de riesgos de negocio. Estos componentes interrelacionados son derivados de la manera en que la gerencia administra una empresa y están integrados con el proceso de gestión. Los componentes son:

- Ambiente interno.
- Establecimiento de objetivos.
- Identificación de eventos.
- Evaluación del riesgo.
- Respuesta al riesgo.
- Actividades de control.
- Información y comunicación
- Supervisión.

Componentes de COSO ERM

La **figura 49** contiene los ocho componentes que COSO ERM define, un resumen de los conceptos importantes relacionados con estos componentes así como también la forma en que *COBIT 5 para Riesgos* los cubre.

Figura 49—Componentes COSO ERM cubiertos por COBIT 5 para Riesgos		
Componente COSO ERM	Conceptos importantes del componente	Cobertura de COBIT 5 para Riesgos
Ambiente interno.	<p>Este componente abarca el enfoque o matiz de una organización, influyendo en la conciencia del riesgo de su personal, y es la base para los demás componentes de la gestión corporativa del riesgo, proporcionando disciplina y estructura. Los factores del ambiente interno incluyen la filosofía de la gestión de riesgos de la entidad, su apetito de riesgo, la supervisión por parte del consejo directivo, la integridad, los valores éticos, las competencias del personal, así como la forma en que la gerencia asigna autoridad y responsabilidad, organiza y desarrolla a su personal.</p> <p>Por lo tanto, este componente del ERM se enfoca en brindar una guía a los profesionales con relación a la gestión de riesgos y asegurar que ERM es una forma de pensar totalmente integrada en la organización.</p>	<p>Los conceptos descritos en el capítulo sobre Ambiente Interno son inherentes en todo el marco de referencia:</p> <ul style="list-style-type: none"> • Principio 2: Cobertura de la empresa de extremo a extremo. • El principio 4: Aplicar un enfoque holístico, define un conjunto de catalizadores para apoyar la implementación de un sistema integral de gobierno y gestión de TI. • Tanto el habilitador “Personas, habilidades y competencias” en su capítulo 8 y sección 2A, como el habilitador “Estructuras organizativas”, en el capítulo 4 del marco de referencia, describen una distribución elaborada de roles y responsabilidades. • El habilitador “Información” en su capítulo 6 y sección 2A, describe conceptos tales como el universo de riesgos, apetito de riesgo y tolerancia al riesgo. • El habilitador “Cultura, ética y comportamiento” en su capítulo 5 y sección 2A, describe el vínculo entre la concientización y comunicación del riesgo en la creación de una cultura consciente del riesgo. • El habilitador “Principios, políticas y marcos de referencia”, en su capítulo 2 y sección 2A, describe la filosofía de la gestión de riesgos de la entidad.

Figura 49—Componentes COSO ERM cubiertos por COBIT 5 para Riesgos (cont)

Componente COSO ERM	Conceptos importantes del componente	Cobertura de COBIT 5 para Riesgos
Establecimiento de objetivos.	<p>COSO ERM establece que los objetivos se determinan a nivel estratégico, estableciendo una base para los objetivos de operaciones, reportes, y de cumplimiento. Cada entidad enfrenta una variedad de riesgos de fuentes externas e internas. El establecimiento de objetivos es una precondition para la identificación de eventos, evaluación de riesgo y respuesta al riesgo efectivas. Los objetivos se alinean con el apetito de riesgo de la entidad, lo que define los niveles de tolerancia al riesgo de la entidad.</p>	<p>Este componente está relacionado estrechamente con el gobierno del riesgo. Las siguientes partes de esta guía son relevantes al establecimiento de objetivos:</p> <ul style="list-style-type: none"> • El principio 1: Satisfacer las necesidades de las partes interesadas, ayuda a asegurar que los objetivos de la empresa se cumplan a través de metas en cascada. • Dos de los siete principios de riesgo explicados en el apéndice B.1.1: Principios del riesgo, están relacionados con establecer los objetivos: "Enfocarse en los objetivos del negocio" y "Promover una comunicación abierta y transparente". • El principio 2: Cobertura de la empresa de extremo a extremo, se enfoca en integrar el gobierno de TI de la empresa (GEIT) en el gobierno corporativo. • La sección 2A del capítulo 5 cubre la concientización y comunicación del riesgo. La figura 63 del apéndice B: Plan de comunicación del riesgo, señala la provisión de información a las partes interesadas. • El habilitador "Información" en su capítulo 6 y sección 2A, discute el apetito y la tolerancia al riesgo. <p>Es importante, sin embargo, reconocer que en COBIT 5 para Riesgos, los objetivos de la empresa son tratados como entradas externas, dado que son definidos al nivel de gobierno corporativo y se derivan de las necesidades de las partes interesadas.</p>
Identificación de eventos.	<p>Este componente se ocupa de la gestión de la identificación de potenciales eventos que, de ocurrir, afectarán a la entidad, y determina si estos representan oportunidades o si pueden afectar adversamente a la habilidad de la entidad de implementar una estrategia y alcanzar los objetivos de forma exitosa. Los eventos con un impacto negativo representan riesgos que requieren la evaluación y respuesta de parte de la gerencia. Los eventos con impacto positivo representan oportunidades que la gerencia retroalimenta en la estrategia y el proceso de establecimiento de objetivos. La gerencia considera una variedad de factores internos y externos al identificar eventos, que pueden potenciar las oportunidades y el riesgo, en el contexto del alcance total de la organización.</p>	<p>La identificación de eventos ha sido más desarrollada y ampliada. Los eventos se discuten en los capítulos que describen los escenarios de riesgo. Desarrollar escenarios de riesgo es una técnica de identificación de eventos. Esta guía proporciona estructuras, componentes y directrices en la construcción de escenarios de riesgo. Las siguientes partes discuten el componente de la identificación de eventos:</p> <ul style="list-style-type: none"> • La sección 2B: <i>La perspectiva de la gestión de riesgos y el uso de los catalizadores de COBIT 5</i>, cubren lo básico sobre el desarrollo de escenarios de riesgo, incluyendo la identificación de eventos. • El apéndice D: <i>Uso de los catalizadores de COBIT 5 para mitigar escenarios de riesgo de TI</i>, provee una guía sobre el desarrollo de escenarios basados en específicos actores, tipos de amenazas, eventos, activos/recursos y una dimensión de tiempo.
Evaluación del riesgo.	<p>COSO ERM define evaluación del riesgo como lo que permite que una entidad considere la medida en que un potencial evento tiene un impacto en el logro de los objetivos. La gerencia evalúa los eventos desde dos perspectivas (probabilidad e impacto), y normalmente usa una combinación de métodos cualitativos y cuantitativos. El impacto positivo y negativo de potenciales eventos deberían ser categorizados en toda la entidad. El riesgo se evalúa tanto en base inherente como residual.</p>	<p>Define la evaluación de riesgo como la determinación de la exposición cuantitativa o cualitativa en relación con un evento.</p> <p>El apéndice B.5 describe la forma en que cada habilitador contribuye a la evaluación del riesgo.</p>
Respuesta al riesgo.	<p>Una vez evaluado el riesgo relevante, la gerencia determina la forma de respuesta. Las respuestas incluyen evitar, reducir, compartir y aceptar el riesgo. Al considerar su respuesta, la gerencia evalúa los efectos en la probabilidad e impacto del riesgo, así como los costos y beneficios, seleccionando una respuesta que acerque el riesgo residual dentro de los márgenes de la tolerancia al riesgo. La gerencia identifica cualquier oportunidad que pueda estar disponible y toma una visión del riesgo a nivel de entidad o de portafolio, para determinar si el riesgo residual global está dentro del apetito de riesgo de la entidad.</p>	<p>La sección 2B: <i>La perspectiva de la gestión de riesgos y el uso de los catalizadores de COBIT 5</i>, está dedicada a la respuesta al riesgo, proporcionando procesos completamente desarrollados para estas actividades. Están totalmente alineados con este componente de COSO ERM. Este dominio de procesos tiene la meta de asegurarse que los temas de riesgo, oportunidades y eventos se gestionen racionalizando los costos y en forma consistente con las prioridades del negocio.</p> <p>El apéndice B: <i>Catalizadores detallados de gobierno y gestión de riesgos</i>, proporciona una guía práctica para la respuesta al riesgo y su priorización.</p>

Figura 49—Componentes COSO ERM cubiertos por *COBIT 5 para Riesgos* (cont)

Componente COSO ERM	Conceptos importantes del componente	Cobertura de <i>COBIT 5 para Riesgos</i>
Actividades de control.	Las actividades de control son las políticas y procedimientos que ayudan a asegurar que se cumplan las respuestas al riesgo de la gerencia. Las actividades de control se presentan a través de toda la organización, en todos los niveles y en todas las funciones. Incluyen un rango de actividades tan diverso como son aprobaciones, autorizaciones, verificaciones, reconciliaciones, revisiones de desempeños operativos, seguridad de activos, y segregación de funciones. Los conceptos importantes en este contexto son los tipos de actividades, políticas y procedimientos y controles sobre los sistemas de información.	El apéndice B detalla como los catalizadores pueden ser utilizados para elaborar matrices de actividades de control y riesgo. El apéndice D: <i>Uso de los catalizadores de COBIT 5 para mitigar escenarios de riesgo de TI</i> , vincula los controles y las prácticas de gestión especificadas en COBIT 5 para una serie de escenarios de riesgo de TI.
Información y comunicación.	La información pertinente es identificada, capturada y comunicada en una forma y oportunidad que les facilite a las personas cumplir sus responsabilidades. Los sistemas de información utilizan datos internamente generados e información de fuentes externas, suministrando información para gestionar el riesgo y para tomar decisiones informadas con respecto a los objetivos. La comunicación efectiva también ocurre, fluyendo hacia abajo, arriba y en forma transversal a la organización. También existe comunicación efectiva con externos tales como los clientes, proveedores, reguladores y accionistas.	El principio 1: Satisfacer las necesidades de las partes interesadas, proporciona una guía sobre la concientización y comunicación, incluyendo la figura 2 con diferentes partes interesadas, tanto internos como externos a la empresa. El habilitador “Estructuras organizativas”, en su sección 2A, capítulo 4, discute la responsabilidad y la rendición de cuentas asociadas al riesgo. El habilitador “Cultura, ética y comportamiento”, en su sección 2A, capítulo 5, discute la promoción de una cultura consciente de los riesgos de TI y fomenta la comunicación efectiva del riesgo de TI.
Supervisión.	En esta sección, COSO ERM se ocupa de la gestión de riesgos que es supervisada, evaluando la presencia y el funcionamiento de sus componentes a través del tiempo. Esto se cumple a través de actividades de supervisión continua, evaluaciones separadas o una combinación de ambas. La supervisión continua ocurre en el curso normal de las actividades de gestión. El alcance y la frecuencia de las evaluaciones separadas dependerán principalmente de una evaluación del riesgo y de la efectividad de los procedimientos de monitoreo continuo.	Incluye metas y métricas que pueden ser utilizadas para medir el desempeño e incluye un modelo de madurez para establecer una hoja de ruta para mejorar los procesos de gestión de riesgos.

Conclusión

COBIT 5 para Riesgos incluye todos los componentes definidos en COSO ERM, y para algunos componentes extiende la cobertura de COSO ERM a los temas específicos del uso de TI en la organización. Aunque *COBIT 5 para Riesgos* se enfoca menos en el control, ofrece vínculos con las prácticas de gestión en COBIT 5. Los fundamentos del control y de la gestión general de los riesgos, definidos en COSO ERM, están presentes en *COBIT 5 para Riesgos*, ya sea a través de los principios, el diseño conceptual del marco de referencia, el modelo de proceso o de las guías adicionales proporcionadas en el marco de referencia.

Página dejada en blanco intencionadamente

CAPÍTULO 4**COMPARACIÓN CON FUENTES DE REFERENCIA DE RIESGO DEL MERCADO****4.1 Comparaciones de vocabulario—COBIT 5 para Riesgos vs. ISO Guide 73 y COSO ERM****COBIT 5 para Riesgos e ISO Guide 73: Vocabulario – Gestión de Riesgos**

ISO/IEC 27005 e ISO 31000 utilizan el estándar ISO Guide 73 “Vocabulario – Gestión de Riesgos” (glosario general de las publicaciones de gestión de riesgos en ISO/IEC), con respecto a la definición de conceptos importantes. En la **figura 50** se brinda una comparación de las definiciones de la ISO Guide 73 y de *COBIT 5 para Riesgos*, que comprende:

- Columna 1: Término de ISO Guide 73.
- Columna 2: Definición de ISO Guide 73.
- Columna 3: Disposición de la definición del mismo término en *COBIT 5 para Riesgos* (indicado como Idéntico, Implícito, Ausente o Equivalente).
- Columna 4: La definición del término en *COBIT 5 para Riesgos*.
- Columna 5: Comentario si fuera necesario o relevante.

Figura 50—Comparación de las definiciones de ISO Guide 73 con las de COBIT 5 para Riesgos

Término en ISO Guide 73	Definición en ISO Guide 73	Disposición en COBIT 5 para Riesgos	Definición en COBIT 5 para Riesgos	Comentario
Riesgo absoluto	Nivel de riesgo sin tener en cuenta los controles existentes de riesgos.	Ausente	N/A	Esta noción corresponde al concepto “Riesgo inherente”. En general, <i>COBIT 5 para Riesgos</i> no utiliza este concepto.
Consecuencia	Resultado de un evento que afecta a los objetivos.	Implícito	N/A	<i>COBIT 5 para Riesgos</i> utiliza el concepto “Impacto en el negocio”.
Evento	Ocurrencia o cambio de un conjunto particular de circunstancias.	Equivalente	N/A	Se utiliza el término “escenario” para describir “cosas que suceden”, y “evento” es un componente de un escenario.
Exposición	Susceptibilidad a la ganancia o pérdida; generalmente se cuantifica en términos de impacto potencial.	Equivalente	N/A	<i>COBIT 5 para Riesgos</i> utiliza los términos “exposición” e “impacto en el negocio”.
Contexto externo	Ambiente externo en el que las organizaciones buscan lograr sus objetivos.	Idéntico	N/A	Como parte de los “factores de riesgo” en el “perfil de riesgo” del elemento Información.
Frecuencia	Número de ocurrencias de un evento o resultado para un periodo de tiempo definido.	Idéntico	N/A	N/A
Mapa de calor	Visión general de los principales riesgos de la organización representados en su matriz de riesgos.	Equivalente	N/A	<i>COBIT 5 para Riesgos</i> utiliza el término “mapa de riesgos”.
Incidente	Evento en el que se produce una pérdida o se podría haber producido, independientemente de la severidad.	Implícito	N/A	En su lugar se utiliza el término “pérdida”.

Figura 50—Comparación de las definiciones de ISO Guide 73 con las de COBIT 5 para Riesgos (cont.)

Término en ISO Guide 73	Definición en ISO Guide 73	Disposición en COBIT 5 para Riesgos	Definición en COBIT 5 para Riesgos	Comentario
Contexto interno	Ambiente interno en el que la organización busca lograr sus objetivos	Equivalente	N/A	El contexto interno se incluye como parte de los “factores de riesgo” en el “perfil de riesgo” del ítem Información.
Nivel de riesgo	Magnitud de un riesgo expresada en términos de la combinación de las consecuencias y su probabilidad	Implícito	N/A	La magnitud del riesgo se discute en el marco de referencia, que también discute el apetito al riesgo, la reacción ante el riesgo, etc.
Posibilidad	Oportunidad de que algo suceda o no.	Ausente	N/A	COBIT 5 para Riesgos utiliza el término “frecuencia”, lo que permite una evaluación más precisa de los eventos que ocurren más de una vez en un período determinado.
Probabilidad	Medida de la posibilidad de ocurrencia expresada entre 0 y 1, donde 0 es imposibilidad y 1 es la certeza absoluta.	Equivalente	N/A	En su lugar, se utiliza el término “frecuencia”.
Riesgo residual	Riesgo remanente después del tratamiento del riesgo.	Equivalente	N/A	El marco no utiliza “inherente” o “riesgo absoluto”. En su lugar usa el término “riesgo vigente” y “riesgo residual”, ambos tienen en cuenta los controles vigentes y los planificados.
Riesgo	Efecto de la incertidumbre sobre los objetivos.	Equivalente	Potencial de que una amenaza dada aproveche una vulnerabilidad de un activo o grupo de activos que puede causar su pérdida o daño. O el potencial de que no se alcancen los objetivos del negocio.	Las definiciones son diferentes pero equivalentes. Ambas contienen el concepto de incertidumbre.
Agregación del riesgo	Proceso para identificar e ilustrar la interacción de varios elementos de riesgos individuales de una organización, correlacionados de manera diferente, con el fin de obtener el riesgo global.	Idéntico	N/A	N/A
Análisis de riesgos	Proceso de comprender la naturaleza del riesgo y determinar el nivel de riesgo.	Idéntico	N/A	N/A
Evaluación de riesgos	Proceso general de identificación de riesgos, análisis de riesgo y valoración del riesgo.	Idéntico	N/A	N/A
Evitar los riesgos	Decisión de no participar, o de retirarse de una situación de riesgo.	Idéntico	N/A	N/A
Comunicación del riesgo	Procesos continuos e iterativos que una organización realiza para proporcionar, compartir u obtener información, y entablar un diálogo con las partes interesadas en relación con la gestión de riesgos.	Implícito	N/A	La comunicación sobre el riesgo es una parte importante de COBIT 5 para Riesgos.

Figura 50—Comparación de las definiciones de ISO Guide 73 con las de COBIT 5 para Riesgos (cont.)

Término en ISO Guide 73	Definición en ISO Guide 73	Disposición en COBIT 5 para Riesgos	Definición en COBIT 5 para Riesgos	Comentario
Control de riesgo	Medida que modifica el riesgo.	Equivalente	N/A	COBIT 5 para Riesgos principalmente vincula el riesgo de TI de una empresa a los catalizadores de COBIT 5, metas, métricas y actividades (detalladas) relacionadas (ver sección 2B). COBIT 5 prefiere no utilizar la palabra "control" sino más bien "habilitador" y "prácticas de gobierno y gestión".
Criterios de riesgo	Términos de referencia contra el cual se evalúa la significancia de un riesgo.	Equivalente	N/A	Los procesos principales de COBIT 5 para Riesgos incluyen prácticas y actividades para desarrollar y mantener criterios de riesgo.
Valoración del riesgo	Proceso de comparar los resultados del análisis de riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables.	Equivalente	N/A	Existe un proceso equivalente en COBIT 5 para Riesgos para describir la estimación del impacto y la frecuencia como se mencionó anteriormente.
Identificación del riesgo	Proceso de encontrar, reconocer y describir el riesgo.	Implícito	N/A	Como se mencionó en la comparación previa COBIT 5 para Riesgos utiliza la técnica de escenarios como un enfoque práctico para la identificación del riesgo.
Gestión de riesgos	Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.	Implícito	N/A	El término "gestión de riesgos" se usa de manera holística con el fin de cubrir todos los conceptos (de gobierno y gestión) y procesos asociados con la gestión de los riesgos.
Proceso de gestión de riesgos	La aplicación sistemática de políticas, procedimientos y prácticas de gestión a las tareas de comunicación, consultoría, establecer el contexto, identificar, analizar, valorar, tratar, supervisar y revisar los riesgos.	Implícito	N/A	Ver "gestión de riesgos".
Matriz de riesgos	Herramienta para clasificar y visualizar el riesgo mediante la definición de categorías de riesgo (por ej., riesgo financiero, de seguridad y contextual, etc.); definiendo rangos para las consecuencias y los niveles de posibilidad de cada categoría.	Idéntico	N/A	COBIT 5 para Riesgos utiliza el término "mapa del riesgo". Ver "Mapa de calor".
Propietario del riesgo	Persona con la autoridad y responsabilidad para tomar las decisiones de tratar o no un riesgo	Equivalente	N/A	Los diagramas RACI en COBIT 5 para Riesgos del habilitador "Estructuras organizativas", asignan los propietarios de riesgos.
Perfil de riesgo	Descripción del riesgo de una organización.	Idéntico	N/A	N/A
Registro de riesgos	Registro de información sobre los riesgos identificados.	Idéntico	N/A	N/A
Compartir el riesgo	Forma de tratamiento del riesgo que involucra la distribución acordada del riesgo con otras partes.	Idéntico	N/A	COBIT 5 para Riesgos utiliza el término "transferencia del riesgo" en combinación con "Compartir el riesgo". Compartir el riesgo es una consecuencia de la transferencia del riesgo a otras partes.
Tolerancia al riesgo	Disposición de la organización para aceptar el riesgo residual después del tratamiento del riesgo con el fin de alcanzar los objetivos de la organización.	Equivalente	El nivel de variación aceptable que la gerencia está dispuesta a permitir para un riesgo en particular en pos del cumplimiento de sus objetivos.	COBIT 5 para Riesgos distingue entre "apetito al riesgo" y "tolerancia al riesgo" (Ver glosario).

Figura 50—Comparación de las definiciones de ISO Guide 73 con las de COBIT 5 para Riesgos (cont.)

Término en ISO Guide 73	Definición en ISO Guide 73	Disposición en COBIT 5 para Riesgos	Definición en COBIT 5 para Riesgos	Comentario
Tratamiento de riesgos	Proceso para modificar el riesgo.	Idéntico	N/A	COBIT 5 para Riesgos utiliza el término “reducción del riesgo” en combinación con “mitigación del riesgo”. Pueden utilizarse ambos de forma indistinta.
Incertidumbre	Estado total o parcial de la falta de información relacionada a la comprensión o el conocimiento de un evento, su consecuencia o probabilidad de ocurrencia.	Ausente	N/A	COBIT 5 para Riesgos describe los diferentes factores de riesgos que habilitan o generan incertidumbre.
Vulnerabilidad	Una debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.	Equivalente	N/A	Además de utilizar el mismo término, cuando se analizan los escenarios de riesgo, COBIT 5 considera “factores de riesgo” que conlleva el mismo significado.

COBIT 5 para Riesgos y COSO ERM: Vocabulario – Gestión de riesgos

COSO ERM y COBIT 5 para Riesgos han definido una cantidad de términos, cuya definición exacta o algunas veces, el significado de estos términos pueden ser diferentes en ambos marcos de referencia. Para comprender estas diferencias, la **figura 51** enumera lo siguiente:

- Columna 1: Término COSO ERM.
- Columna 2: Definición COSO ERM.
- Columna 3: Disposición de la definición en COBIT 5 para Riesgos del mismo término (indicado como Idéntico, Implícito, Ausente, Equivalente).
- Columna 4: La definición del término en COBIT 5 para Riesgos.
- Columna 5: Comentario si fuera necesario o relevante.

El propósito es brindar información sobre COSO ERM en comparación con COBIT 5 para Riesgos a partir de una base conocida. Además, esta figura ayuda a prevenir discusiones puramente semánticas. Debido al carácter del enfoque de control de COSO ERM, solo se comparan los conceptos relevantes relativos al riesgo. Los conceptos relacionados con el control están más ligados a otros marcos de ISACA y por lo tanto no se encuentran en esta lista.

Figura 51—Comparación de definiciones en COSO ERM y COBIT 5 para Riesgos

Término en COSO ERM	Definición en COSO ERM	Disposición en COBIT 5 para Riesgos	Definición en COBIT 5 para Riesgos	Comentario
Criterio	Conjunto de estándares contra los que la gestión de riesgos de la empresa puede medirse para determinar la efectividad. Los ocho componentes, tomados en el contexto de las limitaciones inherentes a la gestión corporativa de riesgos, representan los criterios de efectividad para cada una de las cuatro categorías de objetivos.	Implícito	N/A	Se puede encontrar un enfoque más práctico para la medición de la efectividad de la gestión de riesgos en las métricas y el modelo de capacidad de COBIT 5.
Deficiencia	Una condición en la gestión corporativa de riesgos digna de atención que puede representar una deficiencia real, potencial o percibida, o una oportunidad para fortalecer la gestión corporativa de riesgos para proporcionar una mayor probabilidad de alcanzar los objetivos de la entidad.	Implícito	N/A	COBIT 5 para Riesgos utiliza más frecuentemente el término “factor de riesgo”.

Figura 51—Comparación de definiciones en COSO ERM y COBIT 5 para Riesgos (cont.)

Término en COSO ERM	Definición en COSO ERM	Disposición en COBIT 5 para Riesgos	Definición en COBIT 5 para Riesgos	Comentario
Diseño	1. Intención: Como se plantea en la definición, la gestión corporativa de riesgos se diseña para identificar los eventos potenciales que pueden afectar a la entidad y gestionar el riesgo para estar dentro de los márgenes del apetito de riesgo, para brindar aseguramiento razonable en cuanto al logro de los objetivos. 2. Plan: La forma en que un proceso se supone que funciona, en contraste con la forma en que realmente funciona.	Implícito	N/A	N/A
Efectuado	Se usa con la gestión corporativa de riesgos: ideado y mantenido.	Ausente	N/A	N/A
Proceso de gestión corporativa de riesgos	Un sinónimo de gestión de riesgos de la empresa aplicado a una entidad.	Implícito	N/A	El término “gestión de riesgos” se usa de manera integral con el fin de cubrir todos los conceptos asociados a la gestión de riesgos.
Evento	Un incidente u ocurrencia de fuente interna o externa a la entidad que afecta al logro de los objetivos	Implícito	Escenario de riesgo de TI: La descripción de un evento relacionado con TI que puede tener impacto en el negocio	El término escenario se utiliza para describir “cosas que suceden”.
Impacto	Resultado o efecto de un evento. Puede haber un rango de posibles impactos asociados a un evento. El impacto de un evento puede ser positivo o negativo en relación a los objetivo de la entidad.	Idéntico	N/A	N/A
Limitaciones inherentes	Aquellas limitaciones de la gestión corporativa de riesgos. Limitaciones relacionadas al juicio humano, a las restricciones de recursos, la necesidad de considerar el costo de los controles en relación a los beneficios esperados, la realidad de que pueden ocurrir caídas y la posibilidad de ignorar a la gerencia y la colusión.	Implícito	N/A	N/A
Riesgo inherente	El riesgo de una entidad en ausencia de acciones que la gerencia puede tomar para alterar la probabilidad o el impacto del riesgo.	Ausente	N/A	COBIT 5 para Riesgos no utiliza “inherente” o ‘riesgo absoluto’, en vez de los cuales utiliza “riesgo residual”.
Posibilidad	Es la posibilidad que un evento dado ocurra. El término a veces toma connotaciones más específicas, con “posibilidad” se indica la posibilidad que un evento dado ocurrirá en términos cualitativos tales como alta, media o baja, u otros criterios; y la “probabilidad” indica una medida cuantitativa, como un porcentaje, frecuencia de ocurrencia, u otra métrica numérica.	Ausente	N/A	COBIT 5 para Riesgos usa el término “frecuencia”, que permite una evaluación más precisa de los eventos ocurridos más de una vez en un periodo determinado.
Intervención de la gerencia	Acciones de la gerencia para suspender las políticas o procedimientos prescritos con propósitos legítimos; usualmente es necesaria para hacer frente a eventos o transacciones no recurrentes o no estándares, que de otro modo podrían ser manejados de manera inapropiada por los sistemas (contrastar este término con “Ignorar a la gerencia”).	Ausente/Implícito	N/A	No forma parte del marco COBIT 5 para Riesgos en sí mismo, sino que COBIT 5 brinda un marco de gobierno y gestión conformada por principios, políticas, responsabilidades y controles del negocio.

Figura 51—Comparación de definiciones en COSO ERM y COBIT 5 para Riesgos (cont.)

Término en COSO ERM	Definición en COSO ERM	Disposición en COBIT 5 para Riesgos	Definición en COBIT 5 para Riesgos	Comentario
Ignorar a la gerencia	La capacidad de eludir los controles, las políticas y procedimientos con fines ilegítimos, con la intención de beneficio	Ausente	N/A	No forma parte del marco COBIT 5 para Riesgos en sí mismo, sino que COBIT 5 brinda un marco de gobierno y gestión
Proceso de gestión	Serie de acciones realizadas por la gerencia para gestionar una entidad. La gestión corporativa de riesgos es parte de	Implícito	N/A	COBIT 5 para Riesgos define un proceso con el enfoque para integrarlo con el proceso de gestión ERM.
Oportunidad	La posibilidad de que un evento ocurra y afecte positivamente al logro de los objetivos.	Idéntico	N/A	El aspecto positivo del riesgo también se reconoce en COBIT 5 para Riesgos.
Política	Declaración de la gerencia de lo que debe hacerse para efectuar el control. Una política sirve como base para la implementación de sus procedimientos.	Idéntico	N/A	El término se describe en el habilitador "Principios, políticas y marcos de referencia".
Procedimiento	Una acción que implementa una política.	Idéntico	N/A	El término se describe en el habilitador "Principios, políticas y marcos de referencia".
Reportes	Utilizado con "objetivos": tiene que ver con la confiabilidad de los informes de la entidad, incluyendo tanto informes internos como externos sobre información financiera y no financiera.	Implícito	N/A	COBIT 5 para Riesgos se centra en gran medida en los elementos de información que se utilizan para elaborar reportes en el habilitador "Información".
Riesgo residual	El riesgo remanente después de que la gestión de riesgos ha tomado acciones para modificar la probabilidad o el impacto del riesgo.	Ausente	N/A	COBIT 5 para Riesgos no utiliza "inherente" o "riesgo absoluto", en vez de los cuales utiliza "riesgo residual".
Riesgo	La posibilidad de que un evento ocurra y afecte de manera adversa al logro de los objetivos.	Equivalente	1. El potencial de que una amenaza dada aprobéche la vulnerabilidad de un activo o de un grupo de activos para causar su pérdida o daño. 2. El potencial de no alcanzar los objetivos del negocio. 3. La combinación de la probabilidad de ocurrencia de un evento y sus consecuencias.	Las definiciones son diferentes pero equivalentes. COBIT 5 también habla del aspecto positivo del riesgo.
Apetito de riesgo	El nivel más amplio de riesgo que una organización está dispuesta a aceptar en el cumplimiento de su misión (o visión).	Equivalente	El nivel más amplio de riesgo que una entidad está dispuesta a aceptar en el cumplimiento de su misión. El apetito de riesgo se define en el contexto de declaración de la misión o de la formulación de la estrategia, por lo tanto será más cualitativa que la tolerancia al riesgo.	N/A
Tolerancia al riesgo	La variación aceptable en relación al logro de los objetivos.	Equivalente	El nivel de variación aceptable que la gerencia está dispuesta a permitir para un riesgo en particular en el cumplimiento de sus objetivos.	N/A

Figura 51—Comparación de definiciones en COSO ERM y *COBIT 5 para Riesgos* (cont.)

Término en COSO ERM	Definición en COSO ERM	Disposición en <i>COBIT 5 para Riesgos</i>	Definición en <i>COBIT 5 para Riesgos</i>	Comentario
Partes interesadas	Son las partes que se ven afectadas por la entidad, tales como accionistas, la comunidad en la que opera la entidad, empleados, clientes y proveedores.	Implícito	N/A	El término está cubierto en el Principio 1: Satisfacer las necesidades de las partes interesadas y en el habilitador “Estructuras organizativas”.
Incertidumbre	Incapacidad para saber de antemano la probabilidad o el impacto exactos de eventos futuros.	Ausente	N/A	En su lugar, <i>COBIT 5 para Riesgos</i> describe los diferentes factores capaces de generar o facilitar la incertidumbre.

Página dejada en blanco intencionadamente

APÉNDICE A GLOSARIO

Término	Explicación
Activo	Algo de valor, ya sea tangible o intangible, que vale la pena proteger, incluyendo personas, sistemas, infraestructura, finanzas y reputación
Finalidad del negocio	La traducción de la misión de la empresa en los objetivos de rendimiento y resultados desde una declaración de intenciones
Impacto en el negocio	El efecto neto, positivo o negativo, sobre la consecución de los objetivos de negocio
Análisis de impacto en el negocio (BIA)	La evaluación de la criticidad y sensibilidad de los activos de información. Un ejercicio que determina el impacto de perder el apoyo de cualquier recurso a una empresa, establece el incremento de esa pérdida con el tiempo, identifica los recursos mínimos necesarios para recuperarse, y prioriza la recuperación de los procesos y el sistema de soporte
Objetivo de negocio	Un desarrollo más a fondo de la finalidad del negocio en objetivos tácticos y resultados deseados
Gestión del riesgo corporativo (ERM)	La disciplina por la cual una empresa de cualquier industria evalúa, controla, explota, financia, y monitorea el riesgo de todas las fuentes con el fin de incrementar el valor de la empresa a corto y largo plazo para sus inversores
Evento	Algo que sucede en un lugar y/o tiempo específico.
Tipo de evento	A los efectos de la gestión de riesgos de TI, uno de los tres posibles tipos de eventos: eventos de amenazas, eventos de pérdida y eventos de vulnerabilidades
Frecuencia	Medida del ratio de ocurrencia de eventos durante un cierto período de tiempo
Riesgo de TI	El riesgo del negocio asociado con el uso, propiedad, operación, participación, influencia y adopción de las TI dentro de una empresa
Perfil de riesgo de TI	Una descripción del riesgo de TI general (identificado) al que la empresa está expuesta
Registro de riesgos de TI	Un repositorio de los atributos clave de los problemas de riesgo de TI potenciales y conocidos. Los atributos pueden incluir el nombre, descripción, propietario, frecuencia esperada/actual, magnitud potencial/actual, impacto potencial/real en el negocio y propensión
Escenario de riesgo de TI	La descripción de un evento relacionado con TI que puede conducir a un impacto en el negocio
Incidente relacionado con TI	Un evento relacionado con TI que causa un impacto operacional, de desarrollo y/o estratégico en el negocio
Indicador de riesgo clave (KRI)	Un subconjunto de los indicadores de riesgo que son altamente relevantes y poseen una alta probabilidad de predecir o señalar un riesgo importante
Indicador de retraso	Métrica para la consecución de objetivos-Un indicador relativo a un resultado o al resultado de un facilitador, es decir, el indicador sólo está disponible después de que los hechos o eventos ocurran
Indicador principal	Métrica para la aplicación de buenas prácticas-Un indicador relativo al funcionamiento de un facilitador, es decir, el indicador proporcionará una indicación sobre el posible resultado del facilitador
Evento de pérdida	Cualquier evento durante el cual una amenaza ocasiona una pérdida
Magnitud	Una medida de la posible gravedad de la pérdida o la potencial ganancia de eventos/escenarios conocidos
Riesgo residual	El riesgo que queda después de que la dirección haya implementado una respuesta al riesgo
Riesgo (negocio)	Una situación probable con frecuencia y magnitud de pérdida (o ganancia) inciertas
Agrupación de riesgos	El proceso de integración de las evaluaciones de riesgo a nivel corporativo para obtener una visión completa sobre el riesgo global de la empresa
Análisis de riesgo	<ol style="list-style-type: none"> 1. Un proceso por el cual se estima la frecuencia y magnitud de los escenarios de riesgo de TI 2. Los pasos iniciales de la gestión de riesgos: análisis del valor de los activos para la empresa, identificación de las amenazas para esos activos y la evaluación de lo vulnerable que cada activo es a esas amenazas
Aceptación de riesgo	La cantidad de riesgo, a nivel global, que la entidad está dispuesta a aceptar en el cumplimiento de su misión
Evaluación de riesgos	Proceso usado para identificar y evaluar los riesgos y sus posibles efectos
Cultura del riesgo	El conjunto de valores y creencias compartidas que rigen la actitud hacia la asunción de riesgos, la atención y la integridad, y determina cuán abiertamente riesgo y pérdidas se presentan y discuten

Término	Explicación
Factor de riesgo	Una condición que puede influir en la frecuencia y/o magnitud y, en última instancia, en el impacto en el negocio de los eventos/escenarios relacionados con las TI
Indicador de riesgo	Una métrica capaz de demostrar que la empresa está sujeta, o tiene una alta probabilidad de ser sometida, a un riesgo que excede la aceptación de riesgo definida
(TI) Problema de riesgo	1. Un ejemplo de riesgo de TI 2. Una combinación de condiciones de control, valor y amenaza que impone un nivel notable de riesgo de TI
Mapa de riesgo	Una herramienta (gráfica) para clasificar y visualizar riesgos mediante rangos definidos para su frecuencia y magnitud
Respuesta al riesgo	Eliminación de riesgos, aceptación de riesgos, compartición/transferencia de riesgos, mitigación de riesgos, que lleva a una situación en que el futuro riesgo residual (riesgo actual con la respuesta al riesgo definida e implementada) cae tanto como sea posible (por lo general en función de los presupuestos disponibles) dentro de los límites de aceptación de riesgo
Declaración de riesgo	Una descripción de las condiciones actuales que pueden conducir a la pérdida; y una descripción de la pérdida. Fuente: Software Engineering Institute (SEI). Para que un riesgo sea comprensible, debe expresarse con claridad. Tal declaración debe incluir una descripción de las condiciones actuales que pueden conducir a la pérdida; y una descripción de la pérdida
Tolerancia al riesgo	El nivel de variación aceptable que la gerencia está dispuesta a permitir en algún riesgo en particular, en el seguimiento de los objetivos por parte de la empresa
Amenaza	Cualquier cosa (p. ej., objeto, sustancia, ser humano) que es capaz de actuar contra un activo de manera que pueda ocasionar un perjuicio
Evento de amenaza	Cualquier evento durante el cual un elemento/actor de una amenaza actúa en contra de un activo de forma que tiene la posibilidad de causar directamente un perjuicio
Vulnerabilidad	Una debilidad en el diseño, implementación, operación o control interno de un proceso que podría exponer al sistema a las adversidades de eventos de amenaza
Evento de vulnerabilidad	Cualquier evento durante el cual se da como resultado un aumento sustancial de la vulnerabilidad. Téngase en cuenta que este aumento de la vulnerabilidad puede ser el resultado de cambios en las condiciones de control o de los cambios en la capacidad/fuerza de la amenaza

APÉNDICE B**DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS**

El Apéndice B proporciona una guía más detallada de los catalizadores para el gobierno y la gestión de los riesgos, tal y como se mostraron en la sección 2A de esta guía. Este apéndice puede ser utilizado para obtener un mayor entendimiento del contenido y significado de cada uno de los elementos de los catalizadores.

B.1 Catalizador: Principios, Políticas y Marcos de referencia

La **figura 52** proporciona los principios del riesgo.

Figura 52 – Principios del riesgo		
Ref.	Principio	Explicación
1	Conectar con los objetivos de la empresa	Los objetivos de la empresa y la cantidad de riesgo que la empresa está preparada para tomar están claramente definidos y conducen la gestión de riesgos de TI.
2	Alinear con el ERM	Los riesgos de TI son tratados como un riesgo de negocio, y no como un tipo de riesgo separado, y el enfoque es completo y multidisciplinar.
3	Balancear el coste / beneficio de los riesgos de TI	El riesgo es priorizado y tratado de acuerdo con la propensión y tolerancia al riesgo.
4	Promover la comunicación justa y abierta	La información abierta, precisa, oportuna y transparente sobre los riesgos de TI es intercambiada y sirve de base para todas las decisiones relacionadas con el riesgo.
5	Establecer la actitud de la cúpula empresarial y las responsabilidades	La gente clave, por ejemplo, personas influyentes, propietarios de negocio y la junta directiva, están comprometidos con la gestión de riesgos de TI y tienen en cuenta la cultura y el comportamiento. Toman decisiones informadas asumiendo las responsabilidades apropiadas basándose en la mejor información disponible. Tratan explícitamente la incertidumbre.
6	Funcionar como parte de las actividades diarias	Las prácticas de gestión de riesgos son adecuadamente priorizadas e incluidas en los procesos de toma de decisiones de la empresa.
7	Enfoque coherente	Las prácticas de gestión de riesgos se aplican continuamente y son mejoradas, destacadas y alineadas.

B.1.2 Política de riesgos

La **figura 53** es una posible tabla de contenidos para una política de riesgos. Se proporcionan los detalles para cada una de las entradas, a menudo refiriéndose a otras secciones de esta publicación.

Figura 53 – Ejemplo de tabla de contenidos de una política de riesgos	
Tabla de contenidos	
1. Alcance	
2. Vigencia	
3. Compromiso de Gestión y Responsabilidad	
4. Gobierno de Riesgos	
4.1 Principios	
4.2 Evaluar	
4.2.1 Necesidades de las partes interesadas	
4.2.2 Motivadores y Metas	
4.3 Dirigir	
4.3.1 Empresa	
4.3.2 Roles y Responsabilidades	
4.3.3 Objetivos	
4.4 Monitorear	
4.4.1 Métricas	
4.4.2 Comunicación	
5. Marco de referencia para la Gestión de Riesgos	

Orientaciones adicionales sobre algunos capítulos

1. ALCANCE

El siguiente texto es un ejemplo de una declaración del alcance de una política de riesgos.

Una política de riesgos comprende gobernar y gestionar todos los factores externos e internos además de los riesgos estratégicos, de entrega y operacionales. Esta política de riesgos ayuda a demostrar una buena práctica del gobierno y la gestión de riesgos, a ganar ventaja competitiva y a apoyar a los objetivos de negocio. Además, el gobierno y la gestión de riesgos también son vistos como un componente esencial del gobierno corporativo, fuertemente apoyados por el sistema de control interno y por el valor estatutario de la organización

Para ser eficaz, la gestión de riesgos debe estar integrada en los procesos normales y formar parte de las prácticas de gestión diaria. Esto conducirá a una toma de decisiones sólida y basada en el riesgo, a establecer una cultura de concienciación de riesgos entre todos los empleados y a todos los niveles y a proporcionar la seguridad necesaria a las partes interesadas.

El propósito de esta política es desplegar un proceso de gestión de riesgos dentro de las unidades corporativas de acuerdo con el plan estratégico de TI, que proporciona la visión, los objetivos y los principios de TI que deben aplicarse en toda la empresa y las directrices básicas sobre cómo aplicarlas en la práctica. El objetivo de esta política es la construcción de un marco de referencia de riesgos de TI sostenible que apoye la gestión de riesgos de TI de una manera rentable y pragmática, al mismo tiempo que cumple con los requisitos.

2. VIGENCIA

La **figura 54** describe los tres aspectos acerca de la vigencia que deben ser claramente identificados en una política de riesgos.

Figura 54 – Aspectos acerca de la vigencia que deben ser identificados en una política de riesgos

Aspecto	Descripción
Relevancia	Define a quién en la empresa la política es relevante.
Actualización y revalidación	Define la frecuencia de actualización de la política y las personas de la empresa que revalidarán la política actualizada.
Distribución	Define la lista de distribución de la política de riesgos. Hay que diferenciar entre las personas a las que la política se les comunica directamente y las personas para las que la política está disponible. Es responsabilidad de la alta dirección asegurar que la distribución se hace adecuadamente, con una distribución mínima a quien la política es aplicable.

3. COMPROMISO DE GESTIÓN Y RESPONSABILIDAD

Probablemente el factor que más influya en la gestión eficaz de los riesgos es la muestra de apoyo de la dirección ejecutiva al programa de gestión de riesgos. Esto significa que se le debe dar una consideración razonable y que se deben tomar las medidas adecuadas sobre las propuestas viables o sobre las recomendaciones.

Por esa razón, hacer responsable a la gerencia a todos los niveles de la jerarquía de la justa y consistente aplicación de las prácticas de gestión de riesgos es un factor influenciador clave. Este compromiso y la responsabilidad deben ser claramente comunicados y detallados en la política de riesgos.

4. GOBIERNO DE RIESGOS

- 4.1. **Principios** - Los principios para el gobierno de riesgos se enumeran en la sección sobre los principios de riesgos (B.1.1).
- 4.2. **Evaluar** - Determinar los objetivos corporativos equilibrados y consensuados a alcanzar.
 - 4.2.1. **Necesidades de las partes interesadas** - Es necesario definir las partes interesadas en la gestión de riesgos. La **Figura 2** identifica todas las posibles partes interesadas y su interés. En base a esa información, esta sección de la política podrá ser completada. Las necesidades de las partes interesadas pueden abordarse también en términos de metas corporativas y de metas relacionados con TI de COBIT 5, según se define en el marco de referencia de COBIT 5.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

- 4.2.2. **Motivos y metas** - Las metas de la gestión de riesgos se deben definir en base a las necesidades de las partes interesadas antes mencionadas y en base a las metas corporativas y las metas relacionadas con TI.
- 4.3. **Dirigir** - La dirección de la gestión de riesgos se expresa por objetivos en las actividades, funciones y responsabilidades:
- 4.3.1. **Empresa** – La(s) estructura(s) organizativa(s) puesta(s) en marcha para gestionar los riesgos debe(n) describirse; las Estructuras Organizativas (sección 2A, capítulo 4) se pueden utilizar para ese fin. El Apéndice B.3 contiene una descripción mucho más detallada de estas estructuras organizativas, sus prácticas clave y la forma en que se pueden implementar. Esta sección se puede utilizar para definir esta parte de la política de riesgos.
 - 4.3.2. **Roles y Responsabilidades** - Se deben establecer donde se definen responsabilidades clave. La responsabilidad general debe estar claramente asignada a la junta de dirección. Una guía práctica a este respecto se puede encontrar en la sección 2A, capítulo 4, anexos B.2 y B.3, donde se discuten las matrices RACI de responsabilidades. Las tres líneas del principio de defensa también se aplican aquí.
 - 4.3.3. **Objetivos** - Los objetivos clave de la gestión de riesgos deben ser definidos y alineados con las metas de la sección 2.3. Los objetivos deben ser SMART (específicos, medibles, realizables, realistas y limitados en el tiempo) y tener en cuenta la eficiencia y la eficacia de la gestión de riesgos y sus procesos relacionados.
- 4.4. **Monitorear** – Las actividades asociadas a la gestión de riesgos deben monitorearse en base a informes estándares sobre riesgos que permitan la toma de decisiones.
- 4.4.1. **Métricas** – Deben definirse las métricas apropiadas para la medición de la gestión de riesgos y sus procesos relacionados. COBIT 5 contiene un modelo de rendimiento de los catalizadores genéricos, y todas las métricas pueden basarse en este modelo. Por ejemplo:
 - Todas las métricas relacionadas con la consecución de los objetivos de los catalizadores, por ejemplo, las metas de los procesos o las metas de la estructura organizativa.
 - Todas las métricas relacionadas con la aplicación de buenas prácticas para los catalizadores, por ejemplo, la aplicación de prácticas de proceso.
 - Todas las métricas relacionadas con la gestión del ciclo de vida de los catalizadores.
 - Métricas combinadas, por ejemplo, los niveles de capacidad de proceso (de acuerdo con los procesos de evaluación basados en la norma ISO/IEC 15504).
 - KRIIs (Indicadores clave de riesgo).
 - 4.4.2. **Comunicación** - Las capacidades, situación y perfil de los riesgos deben ser mantenidas y comunicadas a todas las partes interesadas. Varios mecanismos de comunicación se identifican en esta guía, por ejemplo:
 - Procesos relevantes de gestión de riesgos.
 - Elementos de información apropiados - el más importante aquí es el perfil de riesgo; la política de riesgo podría, por ejemplo, identificar los componentes clave que el perfil de riesgo debe contener y la frecuencia con que éstos deben ser puestos a disposición.

5. MARCO DE REFERENCIA PARA LA GESTIÓN DE RIESGOS

El marco de referencia para la gestión de riesgos define - a un alto nivel - todos los catalizadores que la empresa va a implementar para su gestión de riesgos. A este respecto, esta descripción se puede basar en la sección 2A en su totalidad.

Página dejada en blanco intencionadamente

B.2. Catalizador: Procesos

Esta sección contiene una guía más detallada sobre el facilitador de procesos para el gobierno y la gestión de riesgos, es decir, más detalles sobre los procesos que son importantes para construir y mantener una función de riesgos eficaz y eficiente en una empresa.

Para cada proceso de apoyo clave, se proporciona la siguiente información:

- Descripción y declaración del propósito del proceso;
- Metas y métricas específicas de riesgos del proceso;
- Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso.

B.2.1 Procesos de Soporte Clave

Los procesos indicados en la **figura 55** son procesos de soporte clave para la construcción de una función de riesgos eficaz y eficiente en la empresa, según se identifica en la sección 2A, epígrafe 3.2.

Figura 55-Procesos de Soporte a las Funciones Clave de Riesgo

Identificación del Proceso	Justificación	Salida
EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	El gobierno y la gestión de riesgos requieren la configuración de un marco de gobierno adecuado, para implantar estructuras, principios, procesos y prácticas.	Principios de orientación al gobierno de riesgos.
EDM02 Asegurar la Entrega de Beneficios	Este proceso se enfoca en gestionar el valor que la función de riesgo genera.	Acciones para mejorar el flujo de valor de riesgo.
EDM05 Asegurar la Transparencia hacia las Partes Interesadas	La función del riesgo empresarial requiere de un desempeño transparente y de una medición de la conformidad, con metas y métricas aprobadas por las partes interesadas.	Evaluación de requisitos de generación de informes de riesgo.
APO02 Gestionar la Estrategia	La estrategia de gestión de riesgos de TI debe estar bien definida y alineada al enfoque de ERP.	Estrategia de gestión de riesgos.
APO06 Gestionar el Presupuesto y los Costes	La función del riesgo tiene que ser presupuestada.	Requisitos presupuestarios y financieros.
APO07 Gestionar los Recursos Humanos	La gestión de riesgos requiere la cantidad adecuada de personas, habilidades y experiencia.	Marco de trabajo de competencias de recursos humanos.
APO08 Gestionar las Relaciones	Mantener las relaciones entre las funciones de riesgo y el negocio.	Plan de comunicación.
APO11 Gestionar la Calidad	La calidad es un componente esencial de una gestión de riesgos efectiva.	Revisión de calidad de los entregables de riesgo.
BAI08 Gestionar el Conocimiento	La función de riesgo necesita ser proporcionada con el conocimiento necesario para dar soporte al personal en sus actividades laborales.	Clasificación de la información de la función de riesgo, control de acceso sobre la información, normas para la disposición de la información.
MEA01 Supervisar, Evaluar y Valorar Rendimiento y Conformidad	El riesgo es un aspecto clave en el monitoreo, evaluación y valoración de la organización y de TI.	Métricas y objetivos del monitoreo del riesgo
MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno	Los controles internos son clave en el monitoreo y la contención del riesgo, para evitar que el riesgo se convierta en un problema.	Resultados del monitoreo de control interno y de sus revisiones.
MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requisitos Externos	El cumplimiento con leyes, regulaciones y requisitos contractuales representa un riesgo y tiene que ser monitoreado, analizado y valorado de forma alineada con la estrategia de la organización.	Informes de problemas de no cumplimiento y de causas raíz.

Página dejada en blanco intencionadamente

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	Área: Gobierno Dominio: Evaluar, Dirigir y Monitorear
COBIT 5 Descripción del Proceso	
Analiza y articula los requisitos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadoras, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.	
COBIT 5 Declaración del Propósito del Proceso	
Proporcionar un enfoque consistente, integrado y alineado con el alcance del gobierno de la empresa. Para garantizar que las decisiones relativas a TI se han adoptado en línea con las estrategias y objetivos de la empresa, garantizando la supervisión de los procesos de manera efectiva y transparentemente, el cumplimiento con los requisitos regulatorios y legales y que se han alcanzado los requisitos de gobierno de los miembros del Consejo de Administración.	
EDM01 Metas y Métricas del Proceso específicas de Riesgos	
Metas del Proceso específicas de Riesgos	Métricas Relacionadas
1. El Sistema de gobierno de riesgos está integrado en la empresa.	<ul style="list-style-type: none"> Número de procesos de TI y de la empresa en los que las actividades de riesgo están integradas; Grado en el que los principios de gobierno TI acordados son evidenciados en procesos y prácticas (porcentaje de los procesos y prácticas con trazabilidad clara de los principios).
2. Aseguramiento obtenido por el sistema de gobierno de riesgos.	<ul style="list-style-type: none"> Frecuencia de revisiones independientes de la documentación del gobierno de riesgos de TI; Número de problemas de gobierno de riesgo TI informados; Frecuencia de reporte de gobierno de riesgos de TI al Comité Ejecutivo y el Consejo. Número de auditorías internas/externas y de revisiones.

EDM01 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso				
Prácticas de Gobierno	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
EDM01.01 Evaluar el sistema de gobierno. Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar la comprensión de los requisitos y realizar una estimación del actual y futuro diseño del gobierno de TI de la empresa.	Externo a COBIT 5 para Riesgos	Factores del entorno interno y externo (legales, regulatorios y obligaciones contractuales) y tendencias.	Modelo de toma de decisión para Riesgoss de TI Requisitos de las partes interesadas respecto a prioridades de riesgo y objetivos.	EDM01.02 EDM01.03 EDM02.03 EDM01.03 EDM02.01 EDM05.02 MEA01.01
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Analizar y determinar los factores internos y externos de riesgo del contexto (obligaciones legales, reglamentarias y contractuales) y las tendencias en el entorno empresarial y de las TI que pueden influir en el diseño del gobierno de riesgos. 2. Determinar la importancia del riesgo de las TI y su papel en relación con el negocio. 3. Determinar las implicaciones del riesgo de las TI como resultado del entorno general de control de la empresa. 4. Identificar las partes interesadas relevantes en lo que respecta al gobierno de riesgos (propietarios de los procesos de negocio, la Dirección, Director del Área de Riesgos - CRO, etc.). 5. Reunir requisitos de las partes interesadas con respecto a las prioridades y objetivos de riesgo. 6. Articular la toma de decisiones de riesgos de las TI en consonancia con los principios corporativos de diseño del gobierno de riesgos. 7. Comprender la cultura de toma de decisiones de la empresa y determinar el modelo de toma de decisiones óptimo para los riesgos de TI. 8. Determinar los niveles apropiados de delegación de autoridad, incluyendo las normas de mínimos, para decisiones de riesgos de TI. 9. Gestión del entrenamiento de los tomadores de decisiones en el enfoque de análisis de riesgo de TI propuesto. Ilustrar cómo los resultados de los análisis de riesgo pueden beneficiar las decisiones importantes. Describir el nivel de calidad que deberían esperar los tomadores de decisiones, cómo interpretar los informes de análisis de riesgos, las definiciones de términos clave y las limitaciones de medidas y estimaciones basadas en datos incompletos. Identificar las lagunas en las expectativas de riesgos de la empresa.				

EDM01 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso (cont.)

Prácticas de Gobierno	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
EDM01.02 Orientar el sistema de gobierno. Informar a los líderes y obtener su apoyo, su aceptación y su compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de TI en línea con los principios, modelos para la toma de decisiones y niveles de autoridad diseñados para el gobierno. Definir la información necesaria para una toma de decisiones informadas.	EDM01.01	Modelo de toma de decisiones para Riesgoss de TI	<ul style="list-style-type: none"> • Mandato de función de riesgo • Principios de gobierno de riesgos de TI 	Interna

Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)

1. Comunicar los principios de gobierno de riesgos de TI y acordar con la dirección ejecutiva el camino a seguir para establecer un liderazgo informado y comprometido.
2. Establecer o delegar el establecimiento de estructuras de gestión de riesgos de TI, procesos y prácticas de acuerdo con los principios de diseño acordados.
3. Asignar responsabilidades, autoridad y rendición de cuentas en línea con los acordados principios de diseño de gobierno de riesgos de TI, modelos de toma de decisiones y delegación. Exigir una función de riesgo corporativa.
4. Asegurar que los mecanismos de comunicación y generación de informes de riesgos de TI proporciona a los responsables de la supervisión y toma de decisiones la información adecuada y en el momento oportuno.

Prácticas de Gobierno	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
EDM01.03 Supervisar el sistema de gobierno. Supervisar la ejecución y la efectividad del gobierno de TI de la empresa. Analizar si el sistema de gobierno y los mecanismos implementados (incluyendo estructuras, principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada de TI.	EDM01.01	<ul style="list-style-type: none"> • Modelo de toma de decisiones para Riesgoss de TI • Requisitos de las partes interesadas respecto a prioridades de riesgo y objetivos 	<ul style="list-style-type: none"> • Evaluación de los mecanismos de gobierno de riesgos TI • Actas formales de las reuniones y comunicación de los planes de acción 	Interna

Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)

1. Evaluar periódicamente si los mecanismos de gobierno de riesgos de TI acordados (estructuras, principios, procesos, etc.) se han establecido y funcionan eficazmente.
2. Identificar acciones para rectificar cualquier desviación encontrada.
3. Monitorear los procesos de TI y del negocio para asegurar que estos cumplen con las actividades de riesgo de TI.
4. Documentar la toma de decisiones en el gobierno de riesgos a través de actas de reuniones formales y comunicación de planes de acción.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

EDM02 Asegurar la Entrega de Beneficios	Área: Gobierno Dominio: Evaluar, Orientar y Supervisar
COBIT 5 Descripción del Proceso Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables.	
COBIT 5 Declaración del Propósito del Proceso Asegurar un valor óptimo de las iniciativas de TI, servicios y activos disponibles; una entrega coste eficiente de los servicios y soluciones y una visión confiable y precisa de los costes y de los beneficios probables de manera que las necesidades del negocio sean soportadas efectiva y eficientemente.	
MEA02 Metas y Métricas del Proceso específicas de Riesgos	
Metas del Proceso específicas de Riesgos	Métricas Relacionadas
1. Los beneficios y costes de la función de riesgo están balanceados y gestionados y contribuyen al valor óptimo.	<ul style="list-style-type: none"> • Porcentaje de reducción del riesgo frente a la desviación de presupuesto (presupuestado vs proyección); • Nivel de satisfacción de las partes interesadas con las medidas de gestión de riesgos que se aplican, en base a las encuestas.

EDM02 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso				
Prácticas de Gobierno		Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)
De	Descripción	Descripción	A	
EDM02.01 Evaluar la optimización de valor. Evaluar continuamente las inversiones, Servicios y activos del portafolio de TI para determinar la probabilidad de alcanzar los objetivos de la empresa y aportar valor a un coste razonable. Identificar y juzgar cualquier cambio en la dirección que necesita ser dada a la gestión para optimizar la creación de valor.	EDM01.01	Requisitos de las partes interesadas con respecto a las prioridades de riesgo y objetivos	Documentación formal de los requisitos de las partes interesadas y de dirección con respecto a los niveles de tolerancia al riesgo en la política de inversiones de TI	EDM02.02 EDM02.03
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Establecer la dirección de conformidad con los requisitos de las partes interesadas (tales como accionistas, reguladores, auditores y clientes) para la protección de sus intereses y de la entrega de valor.				
Prácticas de Gobierno		Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)
De	Descripción	Descripción	A	
EDM02.02 Orientar la optimización del valor. Orientar los principios y las prácticas de gestión de valor para posibilitar la realización del valor óptimo de las inversiones TI a lo largo de todo su ciclo de vida económico.	EDM02.01	Documentación formal de los requisitos de las partes interesadas y de dirección con respecto a los niveles de tolerancia al riesgo en la política de inversiones de TI	Requisitos de las partes interesadas con respecto a las prioridades de riesgo y objetivos	Interna
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Establecer un método de demostración del valor de la gestión de riesgos (incluyendo la definición y recopilación de datos pertinentes) para asegurar el eficiente uso de los activos. 2. Demostrar el valor de la función del riesgo, poniendo de relieve la contribución de la función de riesgo a los objetivos del negocio.				

EDM02 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso (cont.)

Prácticas de Gobierno	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)			
	De	Descripción	Descripción	A		
EDM02.03 Supervisar la optimización de valor. Supervisar los indicadores clave y sus métricas para determinar el grado en que el negocio está generando el valor y los beneficios previstos de los servicios e inversiones TI. Identificar los problemas significativos y considerar las acciones correctivas.	EDM01.01	Modelo de toma de decisiones para los riesgos de TI	Retroalimentación en la entrega de iniciativas de riesgo	Interna		
	EDM02.01	Documentación formal de los requisitos de las partes interesadas y de dirección con respecto a los niveles de tolerancia al riesgo en la política de inversiones de TI				
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)						
<ol style="list-style-type: none"> Monitorear el valor de las iniciativas de riesgo y compararlo con los requisitos de las partes interesadas que fueron establecidos para asegurar la entrega de valor. Utilizar métodos enfocados a negocio para reportar acerca del valor añadido de las iniciativas de gestión de riesgos. 						

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Área: Gobierno Dominio: Evaluar, Orientar y Supervisar				
EDM05 Asegurar la Transparencia hacia las Partes Interesadas				
COBIT 5 Descripción del Proceso Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa son transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.				
COBIT 5 Declaración del Propósito del Proceso Asegurar que la comunicación con las partes interesadas sea efectiva y oportuna y que se ha establecido una base para la elaboración de informes con el fin de aumentar el desempeño, identificar áreas susceptibles de mejora y confirmar que las estrategias y los objetivos relacionados con TI concuerdan con la estrategia corporativa.				
EDM05 Metas y Métricas del Proceso específicas de Riesgos				
Metas del Proceso específicas de Riesgos	Métricas Relacionadas			
1. La presentación de informes de riesgos está establecida y es completa, oportuna en el tiempo y precisa.	<ul style="list-style-type: none"> • Porcentaje de informes que son entregados a tiempo. • Porcentaje de informes con datos de reporte validados. 			
2. Las partes interesadas son informadas de la situación actual de los riesgos y de la gestión de riesgos en toda la empresa.	<ul style="list-style-type: none"> • Satisfacción de las partes interesadas con el proceso de generación de informes de gestión de riesgos (oportunos en el tiempo, completos, relevantes, fiables, precisos, etc.) y su frecuencia, en base a las encuestas • Número de partes interesadas que reciben percepciones de riesgo 			
EDM05 Metas y Métricas específicas de Riesgos del Proceso				
Prácticas de Gobierno	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas. Examinar y juzgar continuamente los requisitos actuales y futuros de comunicación con las partes interesadas y de la elaboración de informes, incluyendo tanto los requisitos obligatorios (p. ej. de regulación) de elaboración de informes como la comunicación a otros interesados. Establecer los principios de la comunicación.	Externo a COBIT 5 para Riesgos	Evaluación de los requisitos de presentación de informes de la empresa	Evaluación de los requisitos de presentación de informes y de canales de comunicación	EDM05.03
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Determinar los destinatarios, incluyendo personas o grupos internos y externos, de las comunicaciones e informes. 2. Analizar y valorar los requisitos de generación de informes relativos a riesgos TI tanto presentes como futuros en la empresa (regulación, legislación, derecho común, contractual) incluyendo alcance y frecuencia. 3. Identificar los medios y canales para comunicar los problemas de riesgos.				
Prácticas de Gobierno	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes. Garantizar el establecimiento de una comunicación y una elaboración de informes eficaces, incluyendo mecanismos para asegurar la calidad y la completitud de la información, vigilar la elaboración obligatoria de informes y crear una estrategia de comunicación con las partes interesadas.	4. EDM01.01	5. Requisitos de las partes interesadas con respecto a las prioridades de riesgo y objetivos	6. Resumen de las actividades al comité de riesgos de la empresa	7. Interna

EDM05 Metas y Métricas específicas de Riesgos del Proceso (cont.)

Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)

1. Priorizar la generación de informes de problemas de riesgos a las partes interesadas.
2. Generar para las partes interesadas informes regulares sobre riesgos y gestión de riesgos que incluyan las actividades de gestión de riesgos, el tratamiento de riesgos respecto a las fechas objetivo, el rendimiento, los logros, los perfiles de riesgo, los beneficios empresariales, los "temas candentes" (por ejemplo, la nube, productos de consumo), los riesgos excepcionales y las carencias de capacidad

Prácticas de Gobierno	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
EDM05.03 Supervisar la comunicación con las partes interesadas. Supervisar la eficacia de la comunicación con las partes interesadas. Evaluar los mecanismos para asegurar la precisión, la fiabilidad y la eficacia y determinar si se están cumpliendo los requisitos de los diferentes interesados.	EDM05.01	Evaluación de requisitos de presentación de informes de riesgo y canales de comunicación	Monitoreo y reporte de riesgo	Interna
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Establecer el monitoreo y presentación de informes de riesgos (por ejemplo utilizando KPIs para Riesgoss y gestión de riesgos basados en métricas y medidas en el dominio MEA).				

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

APO02 Gestionar la Estrategia	Área: Gestión Dominio: Alinear, Planificar y Organizar			
Descripción del Proceso Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.				
Declaración del Propósito del Proceso Alinear los planes estratégicos de TI con los objetivos del negocio. Comunicar claramente los objetivos y las cuentas asociadas para que sean comprendidos por todos, con la identificación de las opciones estratégicas de TI, estructurados e integrados con los planes de negocio.				
APO02 Metas y Métricas del Proceso específicas de Riesgos				
Metas del Proceso específicas de Riesgos	Métricas Relacionadas			
1. El capítulo de la función de riesgo está definido y mantenido.	<ul style="list-style-type: none"> • Aprobación de las partes interesadas del capítulo de la función de riesgo 			
2. La estrategia de la función de riesgo es rentable, apropiada, realista, alcanzable, enfocada a la empresa y equilibrada	<ul style="list-style-type: none"> • Porcentaje y número de iniciativas para las que ha sido calculado un valor métrico (por ejemplo retorno de la inversión [ROI]). • Retroalimentación de las encuestas de satisfacción entre las partes interesadas de la empresa respecto a la eficacia de la estrategia de gestión de riesgos. 			
3. La estrategia de la función de riesgo está alineada con las metas y objetivos de la empresa a corto y largo plazo.	<ul style="list-style-type: none"> • Porcentaje de proyectos en los portafolios de proyectos de TI y de la empresa que involucran a la gestión de riesgos. • Porcentaje de proyectos de TI que tienen requisitos de riesgos promovidos por los propietarios de negocio. 			
APO02 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO02.01 Comprender la dirección de la empresa. Considerar el entorno actual y los procesos de negocio de la empresa, así como la estrategia y los objetivos futuros de la compañía. Tomar también en cuenta el entorno externo a ella (motivadores de la industria, reglamentos relevantes, bases para la competencia).			Listado de potenciales brechas de cobertura de la función de riesgos	APO02.02
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Comprender cómo la función de riesgo debería apoyar los objetivos generales de la empresa y proteger los intereses de las partes interesadas, teniendo en cuenta la necesidad de gestionar el riesgo al mismo tiempo que se cumplen los requisitos regulatorios y que se ofrece valor a la empresa. 2. Entender la arquitectura actual de la empresa e identificar posibles brechas de cobertura de la función de riesgo.				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO02.02 Evaluar el entorno, capacidades y rendimiento actuales. Evaluar el rendimiento del negocio interno actual y las capacidades de TI y los servicios externos de TI para desarrollar un entendimiento de la arquitectura empresarial en relación con TI. Identificar los problemas que se están experimentando y generar recomendaciones en las áreas que pueden beneficiarse de estas mejoras. Considerar los aspectos diferenciadores y las opciones de proveedores de servicios y el impacto financiero, los costes y los beneficios potenciales de utilizar servicios externos.	APO02.01	Listado de posibles brechas de cobertura de la función de riesgos	Capacidades de la función de riesgo	APO02.03
			Línea base del entorno actual del negocio y de las TI	APO02.04

APO02 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso (cont.)

Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)

1. Desarrollar una línea base para el entorno actual de TI y del negocio, capacidades y servicios contra la que se puedan comparar requisitos futuros. Se debe incluir a alto nivel de detalle los aspectos relevantes correspondientes a la arquitectura actual de la empresa (negocio, información, datos, aplicaciones y dominios tecnológicos), al riesgo, a los procesos de negocio, a los procesos y procedimientos de TI, a la estructura de la organización de TI, a la provisión de servicios externos, al gobierno de las TI, y a las capacidades y competencias relacionadas con las TI de toda la organización.
2. Identificar los riesgos de las tecnologías actuales, potenciales y en declive.
3. Identificar las brechas entre las capacidades y servicios actuales de negocio y de TI respecto a normas de referencia y mejores prácticas, negocios y capacidades de TI de los competidores y los puntos de referencia comparativos de las mejores prácticas y de prestación de servicios TI emergentes.
4. Identificar los problemas, fortalezas, oportunidades y amenazas en el entorno actual, las capacidades y los servicios para entender el desempeño actual, e identificar áreas de mejora en términos de la contribución de TI a los objetivos empresariales.

Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO02.03 Definir el objetivo de las capacidades de TI. Definir el objetivo del negocio, las capacidades de TI y los servicios de TI necesarios. Esto debería estar basado en el entendimiento del entorno empresarial y sus necesidades; la evaluación de los actuales procesos de negocio, el entorno de TI y los problemas presentados; considerando los estándares de referencia, las mejores prácticas y las tecnologías emergentes o propuestas de innovación.	APO02.02	Capacidades de la función de riesgo	Requisitos de gestión de riesgos en el objetivo de las capacidades de TI	APO02.04 APO02.05

Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)

1. Asegurar la realización de un análisis de riesgos apropiado al definir el objetivo de las capacidades de TI. Identificar las amenazas desde la tecnología en proceso de obsolescencia, actual y recién adquirida.
2. Acordar el impacto de los riesgos en los cambios en la arquitectura empresarial (negocio, información, datos, aplicaciones y dominios de tecnología), en el negocio y en los procesos y procedimientos de TI, en la estructura de la organización de TI, en los proveedores de servicio de TI, en el gobierno de TI y en las competencias y habilidades de TI.

Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO02.04 Realizar un análisis de diferencias. Identificar las diferencias entre el entorno actual y el deseado y considerar la alineación de activos (las capacidades que soportan los servicios) con los resultados de negocio para optimizar la inversión y la utilización de la base de activos internos y externos. Considerar los factores críticos de éxito que apoyan la ejecución de la estrategia.	APO02.02	Línea de base del entorno actual de TI y del negocio	BRECHAS EN LA COBERTURA DE GESTIÓN DE RIESGOS POR RESOLVER	APO02.05
	APO02.03	Requisitos de gestión de riesgos en el objetivo de las capacidades de TI		
	Externo a COBIT 5 para Riesgos	Requisitos de regulación y de cumplimiento para las TI corporativas		

Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)

1. Identificar todas las brechas para cerrar y los cambios necesarios para lograr el entorno objetivo, a la luz de los procesos de gestión de riesgos, los requisitos y el apetito de riesgo de la empresa.
2. Examinar el entorno actual con respecto a las regulaciones y requisitos de cumplimiento.
3. Donde se identifique el riesgo y la decisión sea aceptarlo, el proceso de aceptación del riesgo debe ser realizado.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

APO02 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso (cont.)				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO02.05 Definir el plan estratégico y la hoja de ruta. Crear un plan estratégico que defina, en cooperación con las partes interesadas más relevantes, cómo los objetivos de TI contribuirán a los objetivos estratégicos de la empresa. Incluyendo cómo TI apoyará el programa aprobado de inversiones, los procesos de negocio, servicios y activos de TI. Orientar las tecnologías para definir las iniciativas que se requieren para cerrar las diferencias, la estrategia de abastecimiento y las medidas que se utilizarán para supervisar el logro de los objetivos, para dar prioridad a las iniciativas y combinarlas en una hoja de ruta a alto nivel.	APO02.03	Requisitos de gestión de riesgos en el objetivo de las capacidades de TI	Estrategia de gestión de riesgos	APO02.06
	APO02.04	Brechas en la cobertura de gestión de riesgos por resolver	Plan estratégico y hoja de ruta de TI actualizados teniendo en cuenta los requisitos de gestión de riesgos.	Interna
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Definir la estrategia de la función de riesgo y alinearla con las estrategias del negocio y con los objetivos globales y el apetito de riesgo corporativos. 2. Garantizar que el actual plan estratégico y hoja de ruta de TI tienen en cuenta los requisitos de riesgo.				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO02.06 Comunicar la estrategia y la dirección de TI. Crear conciencia y comprensión del negocio y de los objetivos y dirección de TI, como se encuentra reflejada en la estrategia de TI, a través de comunicaciones a las partes interesadas adecuadas y a los usuarios de toda la empresa.	APO02.05	Estrategia de gestión de riesgos	Plan de gestión de riesgos	APO07.01 APO11.01
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Desarrollar un plan de gestión de riesgos basado en una estrategia de gestión de riesgos. 2. Obtener la aprobación de las partes interesadas autorizadas (por ejemplo, CIO, la dirección ejecutiva, la junta directiva) y comunicar la estrategia de gestión de riesgos y el plan a todas las partes interesadas relevantes.				

Página dejada en blanco intencionadamente

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

APO06 Gestionar el Presupuesto y los Costes	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso	
Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, coste y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costes a la empresa. Consultar a las partes interesadas para identificar y controlar los costes totales y los beneficios en el contexto de los planes estratégicos y tácticos de TI, e iniciar acciones correctivas cuando sea necesario.	
Declaración del Propósito del Proceso	
Fomentar la colaboración entre TI y las partes interesadas de la empresa para catalizar el uso eficaz y eficiente de los recursos relacionados con las TI y brindar transparencia y responsabilidad sobre el coste y valor de negocio de soluciones y servicios. Permitir a la empresa tomar decisiones informadas con respecto a la utilización de soluciones y servicios de TI.	
APO06 Metas y Métricas del Proceso específicas de Riesgos	
Metas del Proceso específicas de Riesgos	Métricas Relacionadas
1. La asignación del presupuesto y de los costes para la gestión de riesgos es priorizada de manera efectiva.	<ul style="list-style-type: none"> • Porcentaje de alineación entre los recursos de riesgo y las actividades de riesgos y de control con prioridad alta.

APO06 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO06.01 Gestionar las finanzas y la contabilidad Establecer y mantener un método de contabilización para todos los costes, inversiones y depreciaciones relacionadas con las TI, como parte integral de los sistemas financieros empresariales y el plan de cuentas para administrar las inversiones y los costes de TI. Capturar y asignar los costes reales, analizar las desviaciones entre las previsiones y los costes reales, e informar usando los sistemas empresariales de medición financiera.				
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
No es relevante para esta práctica una guía de riesgo específica. Las actividades genéricas de COBIT 5 se pueden utilizar como orientación adicional.				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO06.02 Priorizar la asignación de recursos. Implementar un proceso de toma de decisiones para priorizar la asignación de recursos y definir las reglas para las inversiones discrecionales por parte de unidades de negocio individuales. Incluir el uso potencial de proveedores de servicio externos y considerar las opciones de compra, desarrollo y alquiler.				
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Establecer un órgano de toma de decisiones para la priorización de los recursos empresariales y de TI, incluyendo el uso de mapas de riesgo y el uso de proveedores de servicios externos dentro de las asignaciones presupuestarias de alto nivel para los programas de TI, servicios de TI y activos de TI según lo establecido por los planes estratégicos y tácticos. Tener en cuenta las opciones para la compra o el desarrollo de bienes y servicios capitalizados frente a los activos y servicios utilizados externamente sobre una base de pago por uso.				

APO06 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso (cont.)

Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO06.03 Crear y mantener presupuestos. Preparar un presupuesto que refleje las prioridades de inversión que apoyen los objetivos estratégicos basado en la cartera de programas habilitados por TI y servicios de TI.			Presupuesto de la función de riesgo	Interna
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Desarrollar un presupuesto de la función de riesgo.				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO06.04 Modelar y asignar costes. Establecer y utilizar un modelo de costes de TI basado en la definición del servicio, asegurando que la asignación de costes de los servicios es identificable, medible y predecible, para fomentar el uso responsable de los recursos, incluyendo aquellos proporcionados por proveedores de servicio. Revisar regularmente y comparar la idoneidad del modelo de costes/prorrateo de costes para mantener su pertinencia y adecuación al negocio en evolución y las actividades de TI que le dan soporte.				
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
No es relevante para esta práctica una guía de riesgo específica. Las actividades genéricas de COBIT 5 se pueden utilizar como orientación adicional.				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO06.05 Gestionar costes. Implementar un proceso de gestión de costes comparando los costes reales con los presupuestos. Los costes deben ser supervisados y comunicados y, en el caso de desviaciones, identificados oportunamente, así como evaluado su impacto en los procesos y servicios empresariales.				
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
No es relevante para esta práctica una guía de riesgo específica. Las actividades genéricas de COBIT 5 se pueden utilizar como orientación adicional.				

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

APO07 Gestionar los Recursos Humanos	Área: Gestión Dominio: Alinear, Planificar y Organizar
COBIT 5 Descripción del Proceso	
Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.	
COBIT 5 Declaración del Propósito del Proceso	
Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.	
APO07 Metas y Métricas del Proceso específicas de Riesgos	
Metas del Proceso específicas de Riesgos	Métricas relacionadas
1. Las capacidades y los procesos de recursos humanos están alineados con los requisitos de la función de riesgo.	<ul style="list-style-type: none"> • Tasa de rotación en la función de riesgo • Cualificaciones del personal en términos de certificación, formación y años de experiencia

APO07 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso				
Prácticas de gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO07.01 Mantener la dotación de personal suficiente y adecuada. Evaluar las necesidades de personal en forma regular o en cambios importantes en la empresa, operativas o en los entornos para asegurar que la empresa tiene suficientes recursos humanos para apoyar las metas y objetivos empresariales. El personal incluye recursos tanto internos como externos.	APO02.06	Plan de gestión de riesgos	Requisitos de la función de riesgo para el proceso de dotación de personal	Interna
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Identificar los requisitos de recursos para la gestión de riesgos de las TI, tanto a nivel de negocio como de las TI y en el contexto de los problemas de riesgos que competen al negocio, las limitaciones de recursos y los objetivos. 2. Asignar fondos apropiados para llenar los vacíos y posicionar la empresa para aprovechar las oportunidades. 3. Crear compensaciones de riesgo / recompensa en relación con los objetivos organizacionales. 4. Considerar las habilidades requeridas (especificar cómo las capacidades de gestión de riesgos de los directivos y del personal se desarrollarán y mantendrán), procesos y procedimientos documentados para la gestión de riesgos de TI, sistemas de la información y bases de datos para la gestión de problemas de riesgos de TI, el presupuesto y otros recursos para las actividades de respuesta específicas de riesgos, las expectativas de los reguladores y los auditores externos, etc.				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO07.02 Identificar personal clave de TI. Identificar el personal clave de TI a la vez que se reduce al mínimo la dependencia de una sola persona en la realización de una función crítica de trabajo mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión y el respaldo (backup) del personal.				
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
No es relevante para esta práctica una guía de riesgo específica. Las actividades genéricas de COBIT 5 se pueden utilizar como orientación adicional.				

APO07 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso (cont.)

Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO07.03 Mantener las habilidades y competencias del personal. Definir y gestionar las habilidades y competencias necesarias del personal. Verificar regularmente que el personal tenga las competencias necesarias para cumplir con sus funciones sobre la base de su educación, formación y/o experiencia y verificar que estas competencias se mantienen, con programas de capacitación y certificación en su caso. Proporcionar a los empleados aprendizaje permanente y oportunidades para mantener sus conocimientos, habilidades y competencias al nivel requerido para conseguir las metas empresariales.			Plan de Entrenamiento de la función de riesgo	APO07.04

Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)

1. Proporcionar formación de desarrollo profesional y programas sobre gestión de riesgos;
2. Usar la certificación para asegurar la calidad de las habilidades profesionales de gestión del riesgo establecidas;
3. Establecer de forma apropiada a lo largo de toda la empresa educación, entrenamiento y programas de concienciación en materia de riesgos.

Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO07.04 Evaluar el desempeño laboral de los empleados. Lleve a cabo oportunamente evaluaciones de rendimiento de manera regular respecto a los objetivos individuales derivados de los objetivos de la empresa, las normas establecidas, las responsabilidades específicas del trabajo y el marco de habilidades y competencias. Los empleados deberían recibir preparación sobre el desempeño y conducta siempre que sea apropiado.	APO07.03	Plan de entrenamiento de la función de riesgo	Evaluaciones del personal de la función de riesgo	Internia
	Externo a COBIT 5 para Riesgos	Política de recursos humanos		

Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)

1. Incorporar criterios de gestión de riesgos en el proceso de evaluación del personal.

Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio. Comprender y realizar un seguimiento de la demanda actual y futura de recursos humanos para el negocio y TI con responsabilidades en TI corporativa. Identificar las carencias y proporcionar datos de entrada a los planes de aprovisionamiento, planes de abastecimiento de procesos de contratación del negocio y de TI y procesos de contratación del negocio y de TI.	Externo a COBIT 5 para Riesgos	Requisitos, asignaciones de presupuesto, listas de personal, y habilidades de personal en el proceso de recursos	Plan de seguimiento e indicadores del rendimiento de los recursos, plan de asignación de recursos.	Internia

Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)

1. Gestionar la asignación de personal de gestión de riesgos de acuerdo con el plan de gestión de riesgos.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

APO07 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso (cont.)				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO07.06 Gestionar el personal contratado. Asegúrese de que los consultores y el personal contratado que apoyan a la empresa con capacidades de TI conocen y cumplen las políticas de la organización así como los requisitos contractuales previamente acordados.				
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
No es relevante para esta práctica una guía de riesgo específica. Las actividades genéricas de COBIT 5 se pueden utilizar como orientación adicional.				

Página dejada en blanco intencionadamente

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

APO08 Gestionar las Relaciones		Área: Gestión Dominio: Alinear, Planificar y Organizar		
COBIT 5 Descripción del Proceso				
Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves.				
COBIT 5 Declaración del Propósito del Proceso				
Crear mejores resultados, mayor confianza en la tecnología y conseguir un uso efectivo de los recursos.				
APO08 Metas y Métricas del Proceso específicas de Riesgos				
Metas del Proceso específicas de Riesgos		Métricas Relacionadas		
1. Establecer coordinación, comunicación y consulta entre la función de riesgo y otras partes interesadas		<ul style="list-style-type: none"> • Porcentaje de representantes de la función de riesgo en los comités de negocio; • Número de comunicaciones directas de la función de riesgo a las diversas partes interesadas. 		
2. Las partes interesadas perciben el valor añadido que ofrece la gestión de riesgos y reconocen la función del riesgo como un habilitador para el negocio.		<ul style="list-style-type: none"> • Ratio de incorporación de iniciativas de gestión de riesgos en las propuestas de inversión; • Satisfacción de las partes interesadas con las actividades de gestión de riesgos y con sus resultados, medida a través de encuestas de satisfacción. 		
APO08 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO08.01 Entender las expectativas del negocio. Entender el enfoque y expectativas actuales del negocio para TI. Asegurar que los requisitos son entendidos, gestionados y comunicados y su estado acordado y aprobado.	Externo a COBIT5 para Riesgos	Metas y objetivos de negocio	Comprensión de los procesos de negocio y de las expectativas de la empresa	APO08.02 APO08.03
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Comprender el negocio y cómo los riesgos de TI le ayudan o afectan.				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO08.02 Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio. Identificar oportunidades potenciales para que la TI sea catalizadora de la mejora del rendimiento empresarial.	APO08.01	Comprensión de los procesos de negocio y de las expectativas de la empresa		
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Comprender las tendencias de gestión de riesgos y las nuevas tecnologías, y cómo se pueden aplicar de forma innovadora para mejorar el desempeño de los procesos de negocio				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO08.03. Gestionar las relaciones con el negocio. Gestionar la relación con los clientes (representantes del negocio). Asegurar que los roles y responsabilidades de la relación están definidos, asignados y se facilita la comunicación.	APO08.01	Comprensión de los procesos de negocio y de las expectativas de la empresa	Estrategia para obtener el compromiso de las partes interesadas	Interna
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Establecer un enfoque adecuado para interactuar con las partes interesadas clave del negocio				

APO08 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso (cont.)

Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO08.04 Coordinar y comunicar. Trabajar con las partes interesadas y coordinar de extremo a extremo la entrega de los servicios TI y las soluciones proporcionadas al negocio.	Externo a COBIT 5 para Riesgos	Plan de comunicación corporativo	Estrategia de comunicación definida en la gestión de riesgos	Interna
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Establecer canales de comunicación adecuados entre la función de riesgo y el negocio; 2. Establecer la presentación de informes y de las métricas apropiadas en materia de gestión de riesgos.				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO08.05. Proveer datos de entrada para la mejora continua de los servicios. Mejorar y evolucionar continuamente los servicios basados en TI y la entrega del servicio a la empresa para alinearlos con unos cambiantes requisitos de empresa y tecnológicos.			Integración de la gestión de riesgos en el proceso de mejora continua	Interna
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Utilizar los resultados del análisis de riesgos para alimentar la definición de planes de acción y la mejora continua de la empresa.				

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

APO11 Gestionar la Calidad	Área: Gestión Dominio: Alinear, Planificar y Organizar
COBIT 5 Descripción del Proceso Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.	
COBIT 5 Declaración del Propósito del Proceso Asegurar la entrega consistente de soluciones y servicios que cumplan con los requisitos de la organización y que satisfagan las necesidades de las partes interesadas.	
APO11 Metas y Métricas del Proceso específicas de Riesgos	
Metas del Proceso específicas de Riesgos	Métricas Relacionadas
1. Los requisitos de calidad para los servicios de la función de riesgos son definidos e implementados.	<ul style="list-style-type: none"> Satisfacción de las partes interesadas con las actividades de gestión de riesgos y sus resultados, medida mediante encuestas de satisfacción; Frecuencia de presentación de informes (semanal, mensual, trimestral, anual); Porcentaje de personal de riesgo con certificaciones profesionales; Número de horas de educación profesional continua (CPE) u horas de asistencia a actividades de formación o a eventos del sector.

APO11 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO11.01 Establecer un sistema de gestión de la calidad (SGC). Establecer y mantener un SGC que proporcione una aproximación a la gestión de la calidad para la información, la tecnología y los procesos de negocio que sea continua, estandarizada, formal y que esté alineada con los requerimientos del negocio y con la gestión de la calidad a nivel corporativo.	APO02.06	Plan de gestión de riesgos	Mejores prácticas y estándares relevantes de la función de riesgos.	APO11.02 MEA01.01
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Identificar las mejores prácticas en la función de riesgos.				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO11.02 Definir y gestionar estándares, procesos y prácticas de calidad. Identificar y mantener los requisitos, normas, procedimientos y prácticas de los procesos clave para orientar a la organización en el cumplimiento del SGC. Este debería estar en consonancia con los requisitos del marco de control TI. Considerar la posibilidad de certificar los procesos, las unidades de la organización, los productos o los servicios clave.	APO11.01	Mejores prácticas y estándares relevantes de la función de riesgos	Estándares de calidad de la función de riesgos.	APO11.03 APO11.04
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Alinear las prácticas de gestión de riesgos con el SGC; 2. Valorar los beneficios y costes asociados de realizar revisiones externas de calidad.				

APO11 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso (cont.)

Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO11.03 Enfocar la gestión de la calidad en los clientes. Enfocar la gestión de la calidad en los clientes, mediante la determinación de sus necesidades y asegurar el alineamiento con las prácticas de gestión de calidad.	APO11.02	Estándares de calidad de la función de riesgos.		

Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)

No es relevante para esta práctica una guía de riesgo específica. Las actividades genéricas de COBIT 5 se pueden utilizar como orientación adicional.

Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO11.04 Supervisar y hacer controles y revisiones de la calidad. Supervisar la calidad de los procesos y servicios de forma permanente como se defina en el SGC. Definir, planificar y aplicar medidas para supervisar la satisfacción del cliente con la calidad, así como el valor que proporciona el SGC. La información recogida debería ser utilizada por los propietarios de los procesos para mejorar la calidad.	APO11.02	Estándares de calidad de la función de riesgos	Indicadores de calidad de la función de riesgos alineados con las mejores prácticas	APO11.05 MEA01.01

Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)

1. Definir indicadores de calidad de la gestión de riesgos para medir el cumplimiento de los requisitos de gestión de riesgos y la eficacia de los controles de riesgo;
2. Monitorear los indicadores de calidad de la gestión de riesgos;
3. Adoptar medidas correctivas para resolver los problemas de calidad en la función de riesgos.

Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO11.05 Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios. Incorporar las prácticas pertinentes de gestión de la calidad en la definición, supervisión, notificación y gestión continua de los desarrollos de soluciones y en los servicios ofrecidos.	APO11.04	Indicadores de calidad de la función de riesgos implementados siguiendo las mejores prácticas	Causas raíz documentadas en los problemas de la gestión de riesgos incorporando métricas de calidad	Interna

Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)

1. Identificar, documentar y comunicar las causas raíz de los problemas abordados en la gestión de riesgos incorporando métricas de calidad;
2. Aplicar prácticas correctivas para remediar los problemas de calidad.

Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO11.06 Mantener una mejora continua. Mantener y comunicar regularmente un plan de la calidad global que promueva la mejora continua. Esto debería incluir la necesidad y los beneficios de una mejora continua. Recoger y analizar datos sobre el SGC y mejorar su eficacia. Corregir las no conformidades para prevenir la recurrencia. Promover una cultura de mejora continua de la calidad.				

Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)

No es relevante para esta práctica una guía de riesgo específica. Las actividades genéricas de COBIT 5 se pueden utilizar como orientación adicional.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

BAI08 Gestionar el Conocimiento	Area: Gestión Dominio: Construir, Adquirir e Implementar
COBIT 5 Descripción del Proceso	
Mantener la disponibilidad de conocimiento relevante, actual, validado y fiable para dar soporte a todas las actividades de los procesos y facilitar la toma de decisiones. Planificar la identificación, recopilación, organización, mantenimiento, uso y retirada de conocimiento.	
COBIT 5 Declaración del Propósito del Proceso	
Proporcionar el conocimiento necesario para dar soporte a todo el personal en sus actividades laborales, para la toma de decisiones bien fundadas y para aumentar la productividad.	
BAI08 Metas y Métricas del Proceso específicas de Riesgos	
Metas del Proceso específicas de Riesgos	Métricas Relacionadas
1. El intercambio de conocimiento es facilitado con las garantías apropiadas.	<ul style="list-style-type: none"> • Número de eventos de fugas de información

BAI08 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso				
Prácticas de Gestión		Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)	Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
De	Descripción	Descripción	A	
BAI08.01 Cultivar y facilitar una cultura de intercambio de conocimientos.	Externo a COBIT 5 para Riesgos	Plan de formación y concienciación en seguridad de la información		
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Formar y concienciar a la función de riesgo en el intercambio de conocimiento.				
Prácticas de Gestión		Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)	Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
De	Descripción	Descripción	A	
BAI08.02 Identificar y clasificar las fuentes de información.			Clasificación de la información de la función de riesgos	BAI08.04
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Dar soporte al uso e intercambio de información dentro de la función de riesgos en relación con su clasificación y sensibilidad;				
2. Desarrollar una estructura de clasificación de la información de gestión de riesgos.				
Prácticas de Gestión		Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)	Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
De	Descripción	Descripción	A	
BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento.			Repositorios de conocimiento publicados	BAI08.04
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Vincular roles de gestión de riesgos a áreas de conocimiento y garantizar un adecuado control de acceso a la información relevante.				

BAI08 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso (cont.)

Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)			
	De	Descripción	Descripción	A		
BAI08.04 Utilizar y compartir el conocimiento. Difundir las fuentes de conocimiento disponibles entre las partes interesadas relevantes y comunicar cómo estos recursos pueden ser utilizados para tratar diferentes necesidades (ej. resolución de problemas, aprendizaje, planificación estratégica y toma de decisiones).	BAI08.02	Clasificación de la información de la función de riesgos	Control de acceso sobre la información de gestión de riesgos	Interna		
	BAI08.03	Repositorios de conocimiento publicados				
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)						
1. Garantizar que se han implementado las medidas apropiadas para proteger los datos (por ejemplo, de pérdida, de robo, de corrupción). 2. Implementar controles de acceso mediante políticas y procesos para restringir el uso no autorizado y el intercambio de información sobre la gestión de riesgos.						
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)			
	De	Descripción	Descripción	A		
BAI08.05 Evaluar y retirar la información. Medir el uso y evaluar la actualización y relevancia de la información. Retirar la información obsoleta.			Normas actualizadas para el retiro del conocimiento y la puesta a disposición de la información	Interna		
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)						
1. Poner a disposición de forma segura la información de la gestión de riesgos; 2. Enviar confirmación al propietario o custodio de la información sobre la puesta a disposición de la información.						

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

MEA01 Monitorear, Analizar y Valorar el Rendimiento y la Conformidad	Área: Gestión Dominio: Monitorear, Analizar y Valorar
COBIT 5 Descripción del Proceso Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.	
COBIT 5 Declaración del Propósito del Proceso Proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.	
MEA01 Metas y Métricas del Proceso específicas de Riesgos	
Metas del Proceso específicas de Riesgos	Métricas Relacionadas
1. El rendimiento de la función de riesgos es monitoreado de forma permanente;	• Porcentaje de los procesos de negocios que cumplen con los requisitos de gestión de riesgo definidos • Porcentaje de resultados de encuestas que reflejan la satisfacción con la prestación de servicios de la función de riesgos
2. La gestión de riesgos y sus prácticas se ajustan a los requisitos internos.	• Porcentaje de las prácticas de gestión de riesgo que satisfacen los requisitos de cumplimiento internos

MEA01 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso				
Prácticas de Gestión		Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)
	De	Descripción	Descripción	A
MEA01.01 Establecer un enfoque de la supervisión. Involucrar a las partes interesadas en el establecimiento y mantenimiento de un enfoque de supervisión que defina los objetivos, alcance y método de medición de las soluciones de negocio, la entrega del servicio y la contribución a los objetivos de negocio. Integrar este enfoque con el sistema de gestión del rendimiento de la compañía.	APO11.01	Mejores prácticas y estándares de la función de riesgos relevantes	Proceso y procedimiento de seguimiento de la gestión de riesgos	MEA01.02
	APO11.04	Indicadores de calidad de la función de riesgos implementados conforme a las mejores prácticas		
	EDM01.01	Requisitos de las partes interesadas en relación con las prioridades y objetivos de riesgo		
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Identificar y confirmar las partes interesadas en el ámbito de gestión de riesgos; 2. Involucrar a las partes interesadas, comunicar los requisitos de gestión de riesgos y los objetivos del monitoreo y presentación de informes; 3. Establecer el proceso y el procedimiento de seguimiento de la gestión de riesgos; 4. Alinear y mantener alineado de forma constante el seguimiento de la gestión de riesgos y el modelo de evaluación con el enfoque de TI y con el corporativo; 5. Acordar la gestión del ciclo de vida y el proceso de control de cambios para el monitoreo y presentación de informes de la gestión de riesgos; 6. Solicitar, priorizar y asignar recursos para el seguimiento de la gestión de riesgos.				
Prácticas de Gestión		Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)
	De	Descripción	Descripción	A
MEA01.02 Establecer los objetivos de cumplimiento y rendimiento. Colaborar con las partes interesadas en la definición, revisión periódica, actualización y aprobación de los objetivos de rendimiento y cumplimiento enmarcados dentro del sistema de medida del rendimiento.	MEA01.01	Proceso y procedimiento de seguimiento de la gestión de riesgos	Métricas y objetivos acordados en la gestión de riesgos	MEA01.04
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Definir los objetivos de rendimiento de la gestión de riesgos de acuerdo con los estándares de rendimiento generales de las TI; 2. Comunicar los objetivos de desempeño y conformidad de la gestión de riesgos a las partes interesadas clave en el ámbito de la debida diligencia; 3. Evaluar si las metas y métricas de la gestión de riesgos son las adecuadas (es decir, específicas, medibles, realizable, pertinentes y de duración determinada).				

MEA01 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso (cont.)

Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento. Recopilar y procesar datos oportunos y precisos de acuerdo con los enfoques del negocio.	Externo a COBIT 5 para Riesgos	Regulaciones aplicables	Datos de monitoreo procesados	Interna

Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)

1. Recopilar y analizar los datos de rendimiento y de conformidad relativos a la gestión de riesgos.
2. Evaluar la eficacia, la idoneidad y la integridad de los datos recogidos.

Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA01.04 Analizar e informar sobre el rendimiento. Revisar e informar de forma periódica sobre el desempeño respecto de los objetivos, utilizando métodos que proporcionen una visión completa y sucinta del rendimiento de las TI y encaje con el sistema corporativo de supervisión.	MEA01.02	Métricas y objetivos de gestión de riesgos acordados	Informes de desempeño de la gestión de riesgos y actualizaciones de los planes de acciones correctivas	MEA01.05

Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)

1. Diseñar, implementar y acordar una serie de informes de desempeño de gestión de riesgos;
2. Comparar los valores de rendimiento con los objetivos y criterios de referencia internos.

Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA01.05 Asegurar la implantación de medidas correctivas. Apoyar a las partes interesadas en la identificación, inicio y seguimiento de las acciones correctivas para solventar anomalías.	MEA01.04	Informes de desempeño de la gestión de riesgos y actualizaciones de los planes de acciones correctivas.	Proceso de seguimiento de las acciones correctivas en materia de gestión de riesgos	Interna
	Externo a Cobit5 para Riesgos	Directrices de escalado.		

Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)

1. Desarrollar un proceso de seguimiento de las acciones correctivas en materia de gestión de riesgos.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

MEA02 Monitorear, Analizar y Valorar el Sistema de Control Interno		Área: Gestión Dominio: Monitorear, Analizar y Valorar		
Descripción del Proceso Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.				
Declaración del Propósito del Proceso Ofrecer transparencia a las partes interesadas claves respecto de la adecuación del sistema de control interno para generar confianza en las operaciones, en el logro de los objetivos de la compañía y un entendimiento adecuado del riesgo residual.				
MEA02 Metas y Métricas del Proceso específicas de Riesgos				
Metas del Proceso específicas de Riesgos		Métricas relacionadas		
1. Los controles de gestión de riesgos se despliegan y funcionan con eficacia.		<ul style="list-style-type: none"> Porcentaje de los procesos que satisfagan los requisitos de control de gestión de riesgos Porcentaje de controles en los que se cumplen los requisitos de control de gestión de riesgos 		
MEA02 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)	Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)		
	De	Descripción	Descripción	A
MEA02.01 Supervisar el control interno. Realizar, de forma continua, la supervisión, los estudios comparativos y la mejora del entorno de control de TI y el marco de control para alcanzar los objetivos organizativos.	Externo a COBIT 5 para Riesgos	Auditorías externas independientes	Alcance de aseguramiento de gestión de riesgos definido y enfoque para evaluar los controles internos	MEA02.03
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Proporcionar una garantía independiente sobre la gestión de riesgos de TI. Supervisar los planes de acción de riesgos de TI, obtener garantías sobre el desempeño de las prácticas clave de gestión de riesgos de TI y validar si los riesgos de TI están siendo gestionados de acuerdo con el apetito de riesgo y la tolerancia definidos; 2. Garantizar que las actividades de control se ejecutan oportunamente y que las excepciones son rápidamente notificadas, observadas y analizadas; y que las acciones correctivas apropiadas son priorizadas e implementadas de acuerdo con su perfil en la gestión de riesgos (por ejemplo, clasificar ciertas excepciones como riesgo clave y otras como riesgo no-clave); 3. Mantener el sistema de control interno de TI, teniendo en cuenta los cambios en curso en el negocio y en los riesgos de TI, el entorno de control corporativo, los procesos relevantes de negocio y de TI, y los riesgos de TI. Si existen carencias, evaluarlas y recomendar cambios.				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)	Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)		
	De	Descripción	Descripción	A
MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio. Revisar la operación de controles, incluyendo la revisión de las evidencias de supervisión y pruebas, para asegurar que los controles incorporados en los procesos de negocio operan de manera efectiva. Incluir actividades de mantenimiento de evidencias de la operación efectiva de controles a través de mecanismos como la comprobación periódica de controles, supervisión continua de controles, evaluaciones independientes, centros de mando y control y centros de operación de red. Esto proporciona al negocio de la seguridad de la efectividad del control para satisfacer los requisitos relativos al negocio y a las responsabilidades sociales y regulatorias.			La evidencia de la efectividad de los controles de gestión de riesgos	Interna
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Medir la eficacia de los controles de gestión de riesgos.				

MEA02 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso (cont.)

Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA02.03 Realizar autoevaluaciones de control. Estimular a la Dirección y a los propietarios de los procesos a tomar posesión de manera firme del procedimiento de mejora del control, a través de programas continuos de autoevaluación que valoren la completitud y efectividad del control de la Dirección sobre los procesos, políticas y contratos.	MEA02.01	Alcance de aseguramiento de gestión de riesgos definido y enfoque para evaluar los controles internos	Evaluaciones de aseguramiento de la gestión de riesgos	MEA02.04
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Realizar evaluaciones de aseguramiento de la gestión de riesgos (independientes y auto-evaluaciones) para identificar debilidades de control.				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA02.04 Identificar y comunicar las deficiencias de control. Identificar deficiencias de control y analizar e identificar las causas raíz subyacentes. Escalar las deficiencias de control y comunicarlas a las partes interesadas.	MEA02.03	Evaluaciones de aseguramiento de la gestión de riesgos	Resultados de la evaluación y medidas correctivas	MEA02.08
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Revisar los informes de gestión de riesgos en busca de deficiencias de control. Informar y reconducir las deficiencias detectadas.				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA02.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados. Asegurar que las entidades que realizan el aseguramiento son independientes de la función, grupo u organización en el alcance. Las entidades que realizan el aseguramiento deberían demostrar una actitud y apariencia apropiadas y adecuada competencia en las habilidades y conocimientos que son necesarios para realizar el aseguramiento y la adherencia a los códigos de ética y los estándares profesionales.			Competencia en habilidades y conocimiento	Interna
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Establecer las competencias y cualificaciones del proveedor de aseguramiento.				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA02.06 Planificar iniciativas de aseguramiento. Planificar las iniciativas de aseguramiento basándose en los objetivos empresariales y las prioridades estratégicas, riesgo inherente, restricciones de recursos y suficiente conocimiento de la compañía.	Externo a COBIT 5 para Riesgos	Plan de compromiso	Plan de compromiso actualizado	MEA02.07

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

MEA02 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso (cont.)						
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)						
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)			
	De	Descripción	Descripción	A		
MEA02.07 Estudiar las iniciativas de aseguramiento. Definir y acordar con la dirección el ámbito de la iniciativa de aseguramiento, basándose en los objetivos de aseguramiento.	MEA02.06	Plan de compromiso actualizado	Plan de compromiso actualizado	MEA02.08		
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)						
1. Definir prácticas para validar el diseño de controles y sus resultados, y determinar si el nivel de efectividad es compatible con el riesgo aceptable (el requerido por la evaluación de riesgos corporativa o del proceso); 2. Donde la efectividad del control no es aceptable, definir prácticas para identificar el riesgo residual (preparando la generación de informes).						
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)			
	De	Descripción	Descripción	A		
MEA02.08 Ejecutar las iniciativas de aseguramiento. Ejecutar la iniciativa de aseguramiento planificada. Informar de los hallazgos identificados. Proveer opiniones de aseguramiento positivo, cuando sea oportuno, y recomendaciones de mejora relativas a los riesgos residuales identificados en el desempeño operacional, el cumplimiento externo y el sistema de control interno.	MEA02.04	Resultados de la evaluación y medidas correctivas	Informe de riesgos y recomendaciones	Interna		
	MEA02.07	Plan de compromiso actualizado				
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)						
1. Producir y emitir informes de gestión de riesgos cerrados.						

MEA03 Monitorear, Analizar y Valorar el Cumplimiento con los Requisitos Externos		Área: Gestión Dominio: Monitorear, Analizar y Valorar		
Descripción del Proceso Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general.				
Declaración del Propósito del Proceso Asegurar que la empresa cumple con todos los requisitos externos que le sean aplicables.				
MEA03 Metas y Métricas del Proceso específicas de Riesgos				
Metas del Proceso específicas de Riesgos		Métricas Relacionadas		
1. Las prácticas de gestión de riesgos se ajustan a los requisitos de cumplimiento externos; 2. Se monitorean los requisitos externos nuevos o revisados que tengan impacto en la gestión de riesgos.		<ul style="list-style-type: none"> Porcentaje de las prácticas de gestión de riesgos que satisfacen los requisitos de cumplimiento externos Número o porcentaje de proyectos iniciados por la función de riesgos para implementar nuevos requisitos externos 		
MEA03 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA03.01 Identificar requisitos externos de cumplimiento. Identificar y supervisar, de manera continuada, cambios en las legislaciones y regulaciones tanto locales como internacionales, así como otros requisitos externos de obligado cumplimiento en el área de TI.	Externo a COBIT 5 para Riesgos	Estándares y regulaciones de la gestión de riesgos	Requisitos externos de cumplimiento de la gestión de riesgos	MEA03.02
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Establecer mecanismos para monitorear el cumplimiento de la gestión de riesgos respecto a los requisitos externos; 2. Determinar los requisitos de cumplimiento externos que deben cumplirse (incluyendo legales, regulatorios, privados y contractuales); 3. Identificar los objetivos de cumplimiento de gestión de riesgos para los requisitos externos; 4. Identificar y comunicar las fuentes de materiales de gestión de riesgos para ayudar a satisfacer los requisitos de cumplimiento externos.				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA03.02 Optimizar la respuesta a requisitos externos. Revisar y ajustar políticas, principios, estándares, procedimientos y metodologías para asegurar la adecuada gestión y comunicación de los requisitos legales, regulatorios y contractuales. Considerar qué estándares sectoriales, códigos de buenas prácticas y guías de mejores prácticas pueden adoptarse y adaptarse.	MEA03.01	Los requisitos externos de cumplimiento de la gestión de riesgos	Requisitos externos actualizados	MEA03.03
	Externo a COBIT 5 para Riesgos	Normativas aplicable		
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Revisar y comunicar los requisitos externos a todas las partes interesadas.				

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

MEA03 Prácticas, Entradas/Salidas y Actividades específicas de Riesgos del Proceso (cont.)				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA03.03 Confirmar el cumplimiento de requisitos externos. Confirmar el cumplimiento de las políticas, los principios, los estándares, los procedimientos y las metodologías con los requisitos legales, regulatorios y contractuales.	MEA03.02	Requisitos externos actualizados	Informe de cumplimiento de gestión de riesgos	Interno
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Recopilar y analizar los datos de cumplimiento relacionados con la gestión de riesgos.				
Prácticas de Gestión	Entradas específicas de Riesgos (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgos (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
MEA03.04 Obtener garantía del cumplimiento de requisitos externos. Obtener y notificar garantías de cumplimiento y adherencia a políticas, principios, estándares, procedimientos y metodologías. Confirmar que las acciones correctivas para tratar las diferencias en el cumplimiento son cerradas a tiempo.			Informe de garantías de cumplimiento.	Interna
Actividades específicas de Riesgos (adicionales a las Actividades de COBIT 5)				
1. Obtener evidencias de terceros.				

Página dejada en blanco intencionadamente

B.3. Catalizadores: Estructuras Organizativas

Esta sección contiene las descripciones detalladas de las siguientes estructuras organizativas relevantes para la función del riesgo:

1. Comité de la gestión del riesgo de la empresa (de ahora en adelante ERM del inglés *Enterprise Risk Management*), **figura 56**
2. Grupo del riesgo de la empresa, **figura 57**
3. Función del riesgo, **figura 58**
4. Departamento de auditoría, **figura 59**
5. Departamento de cumplimiento, **figura 60**

Las descripciones detalladas de estas estructuras organizativas están destinadas a ser utilizadas como una guía genérica o ejemplos, por lo que no tienen en cuenta las situaciones específicas de las empresas. Por ejemplo, en el caso de una sociedad matriz con múltiples filiales, un comité de ERM puede existir o no en cada subsidiaria. El alcance del control de estas organizaciones subsidiarias puede ser limitado dentro de esta empresa específica y no cubrir todas las filiales del grupo.

Las estructuras organizativas descritas son ejemplos, no son preceptivas. De hecho, no todas las empresas - en función de su naturaleza, tamaño o cualquier otra circunstancia contextual - pueden haber implementado todas estas estructuras.

Los gráficos del 56 al 60 describen la composición de las estructuras organizativas a través de los roles y las funciones. La matriz RECI indica un ejemplo representativo de las prácticas de procesos donde la estructura organizativa posee responsabilidades. El nivel de aprobación dentro de una empresa depende del apetito al riesgo de cada empresa o de los requisitos legislativos geográficos. Se indican las entradas que la estructura necesita para cumplir con el mandato definido en el alcance del control. Estas entradas pueden ser elementos concretos de información, políticas o procedimientos, o decisiones de otras estructuras. Se indican las salidas que la estructura genera cumpliendo el mandato definido el ámbito del control. Las salidas pueden ser las decisiones, elementos particulares de información o políticas / procedimientos.

Figura 56—Comité de la Gestión del Riesgo de la Empresa (ERM)

Composición (cont.)	
Rol	Descripción
Responsable de la privacidad	Una persona responsable de supervisar el impacto y los riesgos que las leyes de privacidad tienen en el negocio y de orientar y coordinar la implementación de las políticas y actividades que garanticen el cumplimiento de las directivas de privacidad.
Responsable de la Seguridad de la Información (de ahora en adelante CISO, del inglés <i>Chief Information Security Officer</i>)	El más alto cargo en la empresa responsable de la seguridad de la información de la empresa en todas sus formas.
Representante del Departamento de RRHH	El más alto cargo en la empresa responsable de la planificación y las políticas de todos los recursos humanos de la empresa
Responsables de negocio (si lo requiere la agenda de los temas a tratar)	Un miembro de la alta dirección responsable de la operación de una unidad de negocio específica o subsidiaria. Esto incluye a los responsables de líneas claves para el negocio y a los directores de departamentos como ventas, marketing, recursos humanos, producción, etc.

Figura 56—Comité de la Gestión del Riesgo de la Empresa (ERM) (cont.)

Mandato, principios de funcionamiento, ámbito de control y nivel de autoridad		
Área	Descripción	
Mandato	Asistir a la junta directiva y el comité de auditoría en la supervisión de las actividades de ERM y asesorar al Consejo respecto al marco de gestión ERM.	
Principios de funcionamiento	<ul style="list-style-type: none"> • El comité de ERM se reunirá de forma periódica (por ejemplo, trimestralmente). Se pueden programar reuniones más frecuentes en el transcurso de iniciativas específicas o cuando haya problemáticas que deban ser tratadas de forma muy urgente. • Reportar a la Junta directiva de forma periódica (por ejemplo, trimestralmente) o según sea necesario y realizar recomendaciones sobre las actividades objeto de su mandato. • Elaborar las actas, incluyendo la agenda, las decisiones tomadas, la asistencia, acciones a acometer y los informes de estado que son aprobados por el comité (p.ej., al comienzo de la siguiente reunión) y conservados en conformidad con la política de gestión de documentos de la empresa. • Normas de gestión del comité: se nombrará un presidente y las reuniones se desarrollarán de acuerdo a un conjunto de principio guías tales como las “Robert’s Rules of Order”. 	
Ámbito del control	El comité de ERM da servicio a toda la entidad jurídica de la que la Junta es responsable.	
Nivel de autoridad/derechos de decisión	<p>Las responsabilidades del comité de ERM incluyen:</p> <ul style="list-style-type: none"> • Dirigir el sistema de gestión de riesgos, el marco de gestión y la metodología (p.ej., la estructura de la gobierno del riesgo, el método de evaluación, el apetito del riesgo) • Aprobar la política de ERM (bajo una delegación de la Junta) • Revisar la exposición al riesgo • Supervisar las actividades de riesgo para asegurar que están en consonancia con el apetito de riesgo definido por la Junta • Priorizar los riesgos y la estrategia <p>Revisar el estado de la respuesta a los riesgos y coordinar con los responsables del negocio la asignación de recursos.</p>	
Derechos de delegación	El comité de ERM tiene el derecho de delegar la propiedad del riesgo a los propietarios de los riesgos/ subcomités o a los dueños del negocio en función del tamaño y la complejidad de la empresa.	
Escalado	Todas las problemáticas claves y hallazgos que impactan a lo establecido por la Junta directiva deben ser escaladas al CEO y a la Junta.	
Matriz RECI		
Prácticas de Proceso		
Nivel de Implicación (RECI)		
Dirigir el sistema de gestión de riesgos, el marco de gestión y los métodos (por ejemplo, la estructura de gobierno del riesgo, el método de evaluación y el apetito de riesgo).		E
Revisar y aprobar la política de ERM.		R
Revisar la exposición y la tolerancia al riesgo, en consonancia con el apetito de riesgo de la empresa.		E
Institucionalizar el apetito de riesgo de la empresa.		E

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 56—Comité de la Gestión del Riesgo de la Empresa (ERM) (cont.)	
Composición	
Rol	Descripción
Función del Riesgo	El más alto cargo en la empresa responsable de todos los aspectos de la gestión de los riesgos en toda la empresa. Se puede establecer un responsable de la función de la gestión de los riesgos de las TI. En algunas empresas, cuando no se ha definido un rol específico de responsable de gestión del riesgo (de ahora en adelante CRO, del inglés Chief Risk Officer), el consejero delegado (de ahora en adelante CEO del inglés Chief Executive Officer) será el encargado de asistir al Comité, por delegación de la Junta, para supervisar los riesgos diarios en la empresa.,.
Responsable Financiero (de ahora en adelante CFO, del inglés <i>Chief Financial Officer</i>)	El más alto cargo en la empresa responsable de todos los aspectos de la gestión financiera, incluidos los riesgos y los controles financieros y la fiabilidad de las cuentas.
Responsable de Sistemas de Información (de ahora en adelante CIO, del inglés <i>Chief Information Officer</i>)	El más alto cargo en la empresa responsable de alinear las TI con la estrategia del negocio y de planificar y gestionar la entrega de los servicios y soluciones de TI que soportan los objetivos del negocio.
Responsable de Operaciones (de ahora en adelante COO, del inglés <i>Chief Operations Officer</i>)	El más alto cargo en la empresa responsable de las operaciones de la Organización.
Departamento de Cumplimiento Normativo (representante)	La función de la empresa responsable de la orientación sobre el cumplimiento legal, regulatorio y contractual.
Departamento de Auditoría (representante)	La función de la empresa responsable de la realización de las auditorías internas y de la coordinación de las auditorías externas

Figura 56— Comité de la Gestión del Riesgo de la Empresa (ERM) (cont.)

Matriz RECI (cont.)		
Prácticas de Proceso		Nivel de Implicación (RECI)
Dirigir y aprobar la priorización del riesgo y la estrategia.		E
Revisar el estado de eliminación del riesgo y coordinar con los responsables de negocio la asignación adecuada de los recursos.		E
Reportar la exposición al riesgo a la Junta.		E
Entradas / Salidas		
Entrada	Tipo	Origen
Indicadores Clave de Riesgo (de ahora en adelante KRIs del inglés <i>Key Risk Indicator</i>), Indicadores Clave de Rendimiento (de ahora en adelante KPIs, del inglés <i>Key Performance Indicator</i>) e Indicadores Clave de Objetivo (de ahora en adelante KGIs, del inglés <i>Key Goal Indicator</i>) de los riesgos	Información	Informes del desempeño
Informes de incidencias	Información	Proceso de incidencia
Estrategia del negocio (p. ej. tecnologías emergentes)	Información	Proceso de estrategia
Políticas	Decisión	Gobierno de la empresa
Informes de auditoría y otras revisiones	Información	<ul style="list-style-type: none"> • Informes de auditorías (internos y externos) • Evaluaciones y pruebas de seguridad, pruebas de continuidad del negocio y de la resiliencia de los servicios (de ahora en adelante BCRS, del inglés <i>business continuity and resiliency service</i>), etc.
Informes sobre los riesgos (estado actual y nivel de mitigación)	Decisión	Gestión del riesgo
Registro del riesgo	Información	Gestión del riesgo
Normas, leyes	Información	Legal y cumplimiento normativo
Inteligencia sobre las amenazas	Información	Proveedores de inteligencia sobre las (internos y externos)
Salida	Tipo	Destino
Tolerancia al riesgo	Información	Gestión del riesgo
Actas de reuniones externas según corresponda	Decisión	Gestión del riesgo
Estrategia de gestión del riesgo	Decisión	<ul style="list-style-type: none"> • Junta • Dueños del negocio
Acciones de mitigación del riesgo	Decisión	<ul style="list-style-type: none"> • Junta • Dueños del negocio • Propietarios de los procesos TI
Política (control del cambio)	Decisión	Comunicaciones

Figura 57—Grupo del Riesgo de la empresa

Composición	
Rol	Descripción
Función del riesgo	El más alto cargo en la empresa responsable de todos los aspectos de la gestión del riesgo en la empresa. Este rol requiere unos conocimientos técnicos específicos para gobernar los riesgos, capacidades para gestionar el grupo de gestión de riesgos, capacidades para comunicar e influenciar eficazmente en las interacciones con las partes interesadas.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 57—Grupo del Riesgo de la empresa (cont.)

Composición (cont.)	
Rol	Descripción
Gestores del riesgo	Este rol requiere unos conocimientos específicos de los riesgos para establecer, gestionar y sostener los procesos de gestión de los riesgos. Se requieren fuertes capacidades interpersonales para implicar a las partes interesadas como propietarios de los riesgos que gestionen los procesos asociados (como la identificación, evaluación y cuantificación de los riesgos, etc.). Se requieren habilidades de comunicación eficaces para presentar los resultados del análisis de riesgos al CRO e influir en el diseño e implementación de los controles.
Analistas del riesgo	Este rol requiere unos conocimientos específicos en el desglose de los datos de riesgos complejos, en el análisis de las interacciones y dependencias y en la comunicación eficaz de los hallazgos y tendencias. También requiere conocimientos y experiencia práctica con los marcos de gobierno del riesgo, las metodologías, los estándares más usados y las mejores prácticas en la gestión de riesgos.
Expertos técnicos (p.ej., seguridad TI, experto en Oracle®, expertos en procesos de negocio)	Este rol debe tener la experiencia técnica necesaria para analizar las áreas de riesgo y en términos de sus vulnerabilidades y amenazas, no sólo para entender cómo los eventos pueden conducir a incidentes (escenarios de riesgo), sino también para proporcionar información sobre las causas raíces de ciertos incidentes y sugerir los controles.
Mandato, principios de funcionamiento, ámbito de control y nivel de autoridad	
Área	Descripción
Mandato	El grupo de riesgo de la empresa se establece para considerar los riesgos de manera más detallada y asesorar al comité de ERM.
Principios de funcionamiento	A través del CRO, se informará al CEO y al comité ERM de forma periódica (por ejemplo, trimestralmente) sobre todas las problemáticas surgidas bajo el ámbito de este mandato. Se pueden programar reuniones más frecuentes cuando surjan asuntos urgentes.
Ámbito del control	El grupo de riesgo de la empresa da servicio a toda la entidad jurídica de la que la Junta es responsable.
Nivel de autoridad/derechos de decisión	Gestionar y ejecutar el programa de ERM: <ul style="list-style-type: none">• Identificar los riesgos• Analizar los riesgos para determinar el impacto• Evaluar el impacto del riesgo para el perfil del riesgo agregado• Analizar, conjuntamente con los propietarios de los procesos de negocio, el riesgo (e indicar las acciones apropiadas). Supervisar y analizar el entorno de riesgo.
Derechos de delegación	El grupo de riesgo de la empresa comparte responsabilidades sobre los riesgos en los procesos con los propietarios de los procesos de negocio.
Escalado	Todas las problemáticas claves y hallazgos que impactan a lo establecido por la Junta directiva deben ser escaladas al Comité ERM, al CEO y a la Junta.
Matriz RECI	
Prácticas de Proceso	
Nivel de Implicación (RECI)	
Investigar, definir y documentar los requisitos de la gestión de riesgos de la empresa.	R
Definir, gestionar y mejorar continuamente el sistema de ERM, los métodos, el marco de gobierno y las herramientas para ayudar a asegurar que las decisiones de aceptación del riesgo sean coherentes y eficaces.	R
Desarrollar la estrategia de ERM y poner en práctica el plan.	R
Desarrollar una política de gestión de riesgos, los procedimientos y otros documentos / plantillas.	R
Implementar y administrar el proceso de gestión de riesgos (APO12), las herramientas de soporte y lo repositorios del conocimiento.	R
Recopilar y comunicar las amenazas y la inteligencia sobre las vulnerabilidades.	R
Proporcionar pericia para identificar los riesgos actuales y futuros asociados con los posibles cambios en la estrategia de negocio.	R
Proporcionar un sistema para recoger, clasificar e informar de la exposición de la empresa a los riesgos alineándola a la estrategia de negocio y gestionando los riesgos de forma eficiente en costes.	R
Establecer una estrategia de comunicación para promover la colaboración, la comprensión de la propiedad de los riesgos y los comportamientos deseados con las partes interesadas en toda la empresa.	R

Figura 57—Grupo del Riesgo de la empresa (cont.)

Entradas / Salidas		
Entrada	Tipo	Origen
KRIs, KPIs y KGIs del riesgo	Información	Informes del desempeño
Apetito y tolerancia a los riesgos	Decisión	Comité ERM
Actas de reunión del Comité ERM	Decisión	Comité ERM
Estrategia de negocio (p. ej., tecnologías emergentes)	Información	Proceso de Estrategia
Políticas	Decisión	Gobierno de la empresa
Informes de auditoría y otras revisiones	Información	<ul style="list-style-type: none"> • Informes de auditorías (internas y externas) • Evaluaciones y pruebas de seguridad, pruebas de BCRS, etc.
Normas, leyes	Información	Legal y cumplimiento
Inteligencia de las amenazas	Información	Proveedores de la inteligencia de las amenazas (internos y externos)
Salida	Tipo	Destino
Informes de los riesgos (actuales y estado de mitigación)	Decisión	Comité ERM
Registro del riesgo	Información	<ul style="list-style-type: none"> • Comité ERM • Propietarios de los procesos de negocio
Acciones de mitigación del riesgo	Decisión	<ul style="list-style-type: none"> • Comité ERM • Propietarios de los procesos de negocio • Propietarios de los procesos TI

Figure 58—Función del Riesgo

Mandato, principios de funcionamiento, ámbito de control y nivel de autoridad	
Área	Descripción
Mandato	La responsabilidad total sobre el desarrollo y ejecución del programa de ERM
Principios de funcionamiento	<ul style="list-style-type: none"> • Garantizar un enfoque holístico a la gestión del riesgo • Establecer los parámetros del marco de gobierno de los riesgos, mantener el perfil de los riesgos e informar de forma periódica de los asuntos importantes asociados a los riesgos tanto al CEO como al Comité de ERM
Ámbito del control	Los riesgos que puedan afectar toda la Organización
Nivel de autoridad/derechos de decisión	Guiar y administrar el programa de ERM
Derechos de delegación	Asignar la propiedad y las responsabilidades de los riesgos
Escalado	Escalar al CEO y al Comité de ERM

Figura 58— Función del Riesgo (cont.)

Matriz RECI	
Prácticas de Proceso	Nivel de Implicación (RECI)
Investigar, definir y documentar los requerimientos de la gestión de riesgo de la empresa	R
Definir, gestionar y mejorar continuamente el sistema de ERM, los métodos, el marco de gobierno y las herramientas para ayudar a asegurar que las decisiones de aceptación del riesgo sean coherentes y eficaces.	R
Desarrollar la estrategia de ERM y poner en práctica el plan.	R
Desarrollar una política de gestión de riesgos, los procedimientos y otros documentos / plantillas.	E

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 58— Función del Riesgo (cont.)

Matriz RECI	
Prácticas de Proceso	Nivel de Implicación (RECI)
Implementar y administrar el proceso de gestión de riesgos (APO12) y las herramientas de soporte y los repositorios del conocimiento.	R
Recopilar y comunicar las amenazas y la inteligencia sobre las vulnerabilidades.	R
Proporcionar pericia para identificar los riesgos actuales y futuros asociados con los posibles cambios en la estrategia de negocio.	E
Proporcionar un sistema para medir e informar de la pérdida de exposición al riesgo mediante la alineación de la estrategia de negocio y la gestión eficaz de respuesta al riesgo.	E/R
Establecer una estrategia de comunicación para promover la colaboración, la comprensión de la propiedad de los riesgos y los comportamientos deseados con las partes interesadas en toda la empresa.	E/R
Definir un portfolio de acciones para la gestión del riesgo y gestionar las oportunidades para reducir los riesgos a un nivel aceptable.	E

Figura 59—Departamento de Auditoría

Mandato, principios de funcionamiento, ámbito de control y nivel de autoridad	
Área	Descripción
Mandato	Responsable de las pruebas, de la revisión y de la notificación de las condiciones de control dentro de la empresa. El mandato se determinará en el plan de auditoría. El departamento definirá y ejecutará un plan de auditoría basado en las consideraciones de riesgo del negocio.
Principios de funcionamiento	Independencia de las responsabilidades operativas. Los auditores deben garantizar su independencia de manera absoluta cuando desempeñan sus funciones de auditoría, pero, dentro de estos límites, pueden dar consejos, por ejemplo, sobre los riesgos relacionados con el negocio, el análisis de impacto en el negocio (BIA), etc.
Ámbito del control	El ámbito de control es toda la empresa. El Departamento de Auditoría está dando servicio a toda la entidad jurídica de la que la junta es responsable.
Nivel de autoridad / derechos de decisión	<ul style="list-style-type: none"> • Selección de los procesos y de las herramientas de auditoría • Establecer clasificaciones de los riesgos para los resultados de la auditoría <p>Reportar directamente a la Junta</p>
Derechos de delegación	Puede delegar algunas actividades de pruebas a otras partes de la Organización o a expertos externos siempre que puedan garantizar la calidad y la fiabilidad de las pruebas.
Escalado	Comité de Auditoría, la Junta y/o el CEO

Matriz RECI	
Prácticas de Proceso	Nivel de Implicación (RECI)
Desarrollar y ejecutar el plan de auditoría de la empresa alineado con la estrategia empresarial.	E/R
Planificar y realizar las auditorías.	E/R
Comunicar los hallazgos y validar los planes de mejoras resultantes.	E/R
Clasificar la severidad de los resultados de las auditorías.	E/R
Informar el estado de control de la empresa a la junta.	E/R
Presentar plan de auditoría para su aprobación por la Junta.	E/R
Implicar las partes interesadas.	E/R

Figura 60—Departamento de Cumplimiento Normativo

Mandato, principios de funcionamiento, ámbito de control y nivel de autoridad	
Área	Descripción
Mandato	Supervisar e informar sobre el estado de cumplimiento de la empresa respecto a las leyes y normas pertinentes.
Principios de funcionamiento	Asegurar que los requerimientos de cumplimiento sean comprendidos, comunicados, respetados y que se corrijan las áreas de incumplimiento.
Ámbito del control	Toda la empresa
Nivel de autoridad/derechos de decisión	<ul style="list-style-type: none"> • Establecer un programa de cumplimiento. • Recomendar las acciones a seguir a quienes tienen capacidad de decisión • Asignar la propiedad de las actividades de cumplimiento.
Derechos de delegación	N/A
Escalado	El Consejo General, el CEO, el Comité ERM y/o la Junta.
Matriz RECI	
Prácticas de Proceso	Nivel de Implicación (RECI)
Hacer seguimiento de las leyes y normas pertinentes.	E/R
Interpretar y comunicar los requerimientos de las leyes y normas pertinentes a las partes interesadas afectadas.	E/R
Facilitar las actividades de cumplimiento.	E/R
Colaborar con los organismos reguladores.	E/R
Facilitar las inspecciones que se establezcan en la regulación	E/R
Realizar auditorías internas de cumplimiento.	E/R
Comunicar los resultados de las auditorías de cumplimiento normativo a las partes interesadas pertinentes.	E/R
Hacer recomendaciones para lograr y mantener el cumplimiento normativo.	E/R
Comprender el impacto de la falta de cumplimiento en la organización.	E/R

B.4. Catalizadores: Cultura, ética y comportamiento

B.4.1 Influir en el comportamiento

En esta sección se describe cómo los comportamientos y conducta descritos en la sección 2A, capítulo 6 pueden ser influenciados por el liderazgo en los diferentes niveles de la empresa, es decir, a nivel de dirección ejecutiva, en la gestión de la función de riesgo y en el ámbito de los empleados.

Se puede influenciar en el comportamiento mediante:

- El uso de la comunicación y aplicación de normas
- Incentivos y premios
- Crear concienciación

Influir en la conducta a través de la comunicación y la aplicación de normas

El liderazgo utiliza la comunicación y la aplicación de normas para influir en el comportamiento de una empresa. La comunicación es siempre esencial para influir en cualquier tipo de comportamiento. El desarrollo y la implantación de una cultura de concienciación de los riesgos depende del grado de importancia de ese aspecto en la cultura. Las políticas y los procesos pueden ser utilizados para reforzar la acción interna donde las leyes y normas son obligatorias.

Los siguientes son algunos ejemplos de cómo la dirección puede utilizar la comunicación y la aplicación de normas para influenciar y promover un comportamiento deseable:

- Concienciar a la Gerencia - la dirección debe predicar con el ejemplo sobre el comportamiento adecuado.
- Las consideraciones y los factores de riesgo deben estar integrados en la planificación empresarial.
- Las políticas de la organización identifican claramente los requerimientos de cumplimiento normativo marcados y garantizan su cumplimiento.
- La alta dirección refuerza la transparencia proporcionando una comunicación adecuada en toda la empresa.
- Una actitud de tolerancia cero hacia los comportamientos no éticos indica que un comportamiento inadecuado tiene claras consecuencias.
- El CEO comunica a los responsables de las unidades de negocio que tengan una relación positiva con la función de cumplimiento.
- El CEO comunica a los responsables de las unidades de negocio la necesidad de implementar las recomendaciones que surjan del análisis de riesgo y fomentar el uso del análisis de la causa raíz.
- La alta dirección aprueba y comunica una política de seguridad documentada a partir de la cual se crean procedimientos, prácticas, normas y directrices que vienen difundidos y compartidos con todos los empleados pertinentes.
- La alta dirección fomenta la participación activa en las iniciativas empresariales.
- La alta dirección establece un proceso de comunicación anónima para promover y apoyar la denuncia de irregularidades.
- Los requerimientos de cumplimiento normativo relacionados con la ética son identificados y comunicados a todos los empleados y se incluyen en un código de ética.
- Se asigna un presupuesto para apoyar la formación, las herramientas y las directrices.
- Se define y se implementa un plan de comunicación para ayudar la gestión del cambio de la empresa cuando se pone en marcha un nuevo proyecto, procedimiento, programa, etc.
- Dentro de una empresa que ha establecido reglas formales, las estructuras informales pueden ser establecidas a través de una comunicación positiva. Estas estructuras informales dan un mayor alcance a las personas que rara vez están en contacto entre sí. Esto crea una sinergia positiva en la interacción diaria entre las personas.
- Las señales correctas pueden producir efectos positivos, las señales equivocadas pueden conducir a resultados indeseables. Una comunicación positiva puede dar resultados extraordinarios en los equipos de trabajo.

Influir en el comportamiento a través de iniciativas y recompensas

La Dirección influye en el comportamiento a través de medidas diseñadas que proporcionan una recompensa para las conductas deseadas y un castigo para los comportamientos que se desean disuadir. La ausencia de recompensas inhibe la adopción de una cultura de concienciación de los riesgos. La Dirección debe saber qué comportamiento de concienciación con los riesgos será recompensado; esto, a su vez, significa que debe manifestar de forma clara sus intenciones mediante el fomento de la aplicación de las respuestas apropiadas a los riesgos y promover las actitudes que constituyen una cultura de concienciación de los riesgos.

Los siguientes incentivos y recompensas pueden ser utilizados por los distintos niveles de gestión para influir en el comportamiento:

- El desempeño de la Dirección se alinea con los criterios de la gestión de los riesgos y apoya una cultura de concienciación de los riesgos.
- Se retribuyen los incentivos a los ejecutivos en conformidad a las buenas prácticas relacionadas con los riesgos y a los resultados esperados; se imponen sanciones y multas al demostrar un comportamiento opuesto.
- El compromiso con el riesgo es un requisito reconocido en la evaluación del desempeño de la Dirección.
- La Dirección tiene la política de reconocer y recompensar a los empleados que obtengan las certificaciones en el ámbito del gobierno de TI, el cumplimiento, la seguridad y el control.
- Se establece un plan estructurado y conocido de desarrollo de carrera. De este modo, los empleados saben que si hacen las cosas bien o proporcionan un valor añadido, pueden mejorar su carrera profesional.
- La Dirección fomenta entre el personal:
 - La participación activa es considerada como un atributo clave en la evaluación del desempeño individual.
 - El comportamiento ético es considerado un requisito fundamental en la evaluación del desempeño.
- El reconocimiento público es un premio de gran valor para aumentar la visibilidad y las relaciones con los directivos y compañeros.
- El reconocimiento financiero tiene que ser proporcional al nivel del valor:
 - Ser parte de la totalidad.
 - Su se considera una parte esencial de la maquinaria.
 - Están formalizados los objetivos de rendimiento personal, los objetivos generales, las recompensas y sanciones.

Influir en el comportamiento mediante la concienciación

Los programas de sensibilización deben tener un espacio, pero no son suficientes por sí mismos. Más que ser conscientes del riesgo de la información, las personas necesitan ser formados acerca de los riesgos y de su papel con ellos. Los diferentes niveles de gestión en una empresa pueden promover la concienciación a través de los siguientes medios.

La dirección ejecutiva puede crear conciencia a través de:

- Apoyar visiblemente el desarrollo, la ejecución y la finalización de los programas de formación para garantizar una cultura coherente de concienciación de los riesgos
- Comunicar periódicamente al personal la necesidad de la gestión de riesgos en toda la organización para hacer valer su conocimiento del entorno de riesgo como base para la toma de decisiones

La gestión del riesgo puede ser difundida y crear sensibilización a través de:

- La ejecución de talleres de sensibilización de riesgos con las principales partes interesadas para comunicar los impactos de los riesgos y sus probabilidades
- La creación de programas de sensibilización que forman la base de lo que se tiene que hacer una vez que el riesgo se materialice. Estas acciones son específicas de cada sector y organización, así como los planes de mitigación o acción a implementar en el caso de la materialización del riesgo.

Los profesionales del riesgo pueden incrementar la conciencia con:

- Casos de estudio que se utilizan para resaltar el impacto en el negocio de las faltas de concienciación de los riesgos o del cumplimiento
- El material/portal de la empresa que destacan aquellas personas que defienden los valores deseados

B.5. Catalizador: Información

Esta sección facilita detalles en relación al uso y optimización de ítems de información relacionados con el riesgo, basado en la introducción del facilitador Información visto en la sección 2a, capítulo 6.

Los ítems de información presentados incluyen:

- **Figura 61 – Perfil de riesgo**
- **Figura 63 – Plan de comunicación del riesgo**
- **Figura 64 – Informe de riesgo**
- **Figura 65 – Programa de concienciación sobre el riesgo**
- **Figura 66 – Mapa de riesgos**
- **Figura 67 – Universo, disposición y tolerancia de riesgo**
- **Figura 69 – Indicadores clave de riesgo**
- **Figura 71 – Aspectos y factores de riesgos emergentes**
- **Figura 72 – Taxonomía del riesgo**
- **Figura 73 – Análisis de impacto en el negocio**
- **Figura 74 – Eventos de riesgo**
- **Figura 75 – Matriz de actividad de riesgo y control**
- **Figura 76 – Análisis de riesgos**

Se discuten en detalle los ítems de información, y se presenta cada dimensión del modelo del facilitador Información. Esto permite al usuario considerar:

- Todos los objetivos o criterios de calidad para el ítem de información que quiere alcanzarse, permitiendo el desarrollo de aplicaciones y procedimientos apropiados.
- El ciclo de vida del ítem de información.
- Los grupos de interés que deben ser incluidos en el ciclo de vida de la información.

Figura 61—Perfil de riesgo

Un perfil de riesgo es una descripción de los riesgos globales (identificados) a los que la organización está expuesta. Un perfil de riesgo consiste en:

- Registro de riesgos
 - Escenarios de riesgo
 - Análisis de riesgos
- Plan de acción de riesgos
- Eventos de pérdidas (histórico y actual)
- Factores de riesgo
- Hallazgos en evaluaciones independientes

Ciclo de vida y grupos de interés	Etapa del ciclo de vida	Grupo de interés interno	Grupo de interés externo	Descripción / Interés
	Planificación de la información	Comité de gestión de riesgos empresariales (ERM), Consejo de administración	Auditores externos, regulador	<ul style="list-style-type: none"> • Grupos de interés internos: Iniciar y conducir la implementación y nombrar al Chief Risk Officer (CRO). Tener información adecuada del grado de exposición. • Grupos de interés externos: Sentirse cómodos en las competencias de gestión del riesgo
Diseño de la información	Función de riesgo, cumplimiento, CIO, CISO, propietarios de procesos de negocio, auditores internos			<ul style="list-style-type: none"> • CRO: Obtener información de los otros roles para facilitar una visión general a los órganos de gobierno • CIO: Para poder desarrollar un sistema de información adecuado • Otros roles: Para poder facilitar información relevante y asegurar integridad e idoneidad
Adquisición / Construcción de la información	Función de riesgo, auditoría interna			<ul style="list-style-type: none"> • CRO: Facilita los requerimientos funcionales y consulta a los otros • Auditoría interna: Provee servicios de aseguramiento de calidad en la implementación.
Uso/ operación de la información: guardar, compartir, usar	Consejo de administración, comité ERM, ejecutivos de negocio, CIO, función de riesgo, CISO, propietarios de procesos de negocio, cumplimiento, auditoría interna	Auditoría externa, regulador		<ul style="list-style-type: none"> • Propietarios de procesos de negocio, ejecutivos de negocio y CIO: Proveer eficientemente de información relevante • Consejo de administración y Comité ERM: Recibir información relevante y facilitar la toma de decisiones • Auditorías interna y externa, y regulador: Recibir información relevante • CRO: Supervisar la captación, proceso e interpretación de la información

Figura 61—Perfil de riesgo (cont.)

Ciclo de vida y grupos de interés	Etapa del ciclo de vida	Grupo de interés interno	Grupo de interés externo	Descripción / Interés
	Monitoreo de la información	Consejo de administración, comité ERM, función de riesgo, auditoría interna		<ul style="list-style-type: none"> • CRO: Monitoreo en curso de la idoneidad, integridad y exactitud de la información; evaluación semestral de rendimiento (MEA01) y controles (MEA02) para mantener la información • Auditoría interna: Validación anual de forma y nivel de contenidos
	Desecho de la información	Función de riesgo		<ul style="list-style-type: none"> • CRO: De acuerdo a la política de retención de datos, para asegurar la confidencialidad de la información y reducir el volumen de información

Figura 61—Perfil de riesgo (cont.)

Objetivos	Subdimensión y objetivos de calidad	Descripción-La extensión en la que la información es...	Relevancia	Objetivo															
	Intrínsecos	<table border="1"> <tr> <td>Exactitud</td> <td>Correcta y fiable</td> <td>Alta</td> <td>La fuente de información debe ser precisa (confirmada mediante auditoría) y debe estar englobada en la aplicación de gestión de riesgos de acuerdo a unas reglas fijadas.</td> </tr> <tr> <td>Objetividad</td> <td>Justa, sin prejuicios e imparcial</td> <td>Alta</td> <td>La información está basa en hechos verificables y comprobaciones, usando la visión común de riesgo establecida en la organización.</td> </tr> <tr> <td>Credibilidad</td> <td>Considerada como cierta y creíble</td> <td>Media</td> <td>Los informes son de total confianza.</td> </tr> <tr> <td>Reputación</td> <td>Considerada como procedente de una fuente cierta y creíble</td> <td>Media</td> <td>La información original es recolectada de fuentes competentes y reconocidas.</td> </tr> </table>	Exactitud	Correcta y fiable	Alta	La fuente de información debe ser precisa (confirmada mediante auditoría) y debe estar englobada en la aplicación de gestión de riesgos de acuerdo a unas reglas fijadas.	Objetividad	Justa, sin prejuicios e imparcial	Alta	La información está basa en hechos verificables y comprobaciones, usando la visión común de riesgo establecida en la organización.	Credibilidad	Considerada como cierta y creíble	Media	Los informes son de total confianza.	Reputación	Considerada como procedente de una fuente cierta y creíble	Media	La información original es recolectada de fuentes competentes y reconocidas.	
Exactitud	Correcta y fiable	Alta	La fuente de información debe ser precisa (confirmada mediante auditoría) y debe estar englobada en la aplicación de gestión de riesgos de acuerdo a unas reglas fijadas.																
Objetividad	Justa, sin prejuicios e imparcial	Alta	La información está basa en hechos verificables y comprobaciones, usando la visión común de riesgo establecida en la organización.																
Credibilidad	Considerada como cierta y creíble	Media	Los informes son de total confianza.																
Reputación	Considerada como procedente de una fuente cierta y creíble	Media	La información original es recolectada de fuentes competentes y reconocidas.																
Contextual y representacional	Relevancia	Aplicable y útil para las tareas a realizar	Alta	El perfil de riesgo está estructurado tal como está definido y el receptor confirma la relevancia de la información provista.															
	Completitud	No ausente y con suficiente profundidad y amplitud para las tareas a realizar	Alta	El perfil de riesgo abarca el alcance de toda la organización y el registro de riesgos completo. Aun así, no toda la información debe estar disponible y se tendrán que hacer suposiciones y corroborarlas.															
	Actualización	Suficientemente actualizada para las tareas a realizar	Baja	La necesidad de actualización para el perfil de riesgo viene dado por la frecuencia y el impacto de los cambios y dependiendo de los componentes.															
	Volumen de información	Es apropiada en volumen para las tareas a realizar	Alta	El volumen de información es apropiado a las necesidades del receptor y deberá ser definido en el diseño.															
	Representación concisa	Representada de forma concisa	Media	El perfil de riesgo está representado de forma concisa, se obtiene agregando datos de toda la organización y guardando sólo casos individuales de los umbrales definidos actualmente.															
	Representación congruente	Presentada en el mismo formato	Baja	El perfil de riesgo siempre se presenta de acuerdo a una plantilla acordada. Aun así, escenarios concretos pueden ser analizados de forma diferente si así se acuerda.															
	Interpretabilidad	En lenguajes, símbolos y unidades apropiados, y las definiciones son claras	Alta	Para la toma de decisiones fácil, el punto óptimo de la información ha de estar identificado y centrarse en él.															
	Comprensibilidad	Fácil de comprender	Alta	Para la toma de decisiones informadas, el perfil de riesgo debe ser comprendido por muchos grupos de interés.															
	Manipulación	Fácil de manipular y aplicar a diferentes tareas	Baja	Los escenarios pueden ser modificados y simulados.															
	Disponibilidad	Disponible cuando se requiere, o fácil y rápidamente recuperable	Media	El perfil de riesgo está siempre disponible para los grupos de interés; se acepta una indisponibilidad temporal en caso de un incidente.															
Seguridad	Acceso restringido	Restringida de manera apropiada a partes autorizadas	Alta	<p>El acceso al perfil de riesgo viene determinado por la función de riesgo, y está restringido así:</p> <ul style="list-style-type: none"> • Acceso de escritura: Función de riesgo (basado en las entradas de los colaboradores) • Acceso de lectura: El resto de grupos de interés 															

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 61—Perfil de riesgo (cont.)

	Atributo	Descripción	Valor
Buenas prácticas	Física	Soporte / medio de la información	El soporte de la información para el perfil de riesgo puede ser electrónico o documento impreso o un sistema de información (p.e. panel de control).
	Empírica	Canal de acceso a la información	El perfil de riesgo es accesible a través del portal de gestión de riesgos empresariales (ERM) o impreso en ubicaciones específicas.
	Sintáctica	Código / lenguaje	<p>El perfil de riesgo contiene los siguientes subapartados:</p> <ul style="list-style-type: none"> • Registro de riesgos (resultado del análisis de riesgos), que consiste en una lista de escenarios de riesgo y sus estimaciones asociadas para impacto y frecuencia (mapa de riesgo); ambos actualizados y el mapa de riesgo anterior debe estar incluido • Plan de acción de riesgo, incluyendo acciones, estado, responsable, fecha límite, etc. • Pérdidas de datos referentes a eventos ocurridos en los últimos períodos reportados • Factores de riesgo, incluyendo factores de riesgo contextual y factores de riesgo referidos a la capacidad (vulnerabilidades) • Resultados de aseguramientos independientes (p.e. hallazgos de auditoría, autoevaluaciones)
	Semántica	Tipo de información	Basada en un documento estructurado en una plantilla y/o un panel de control online con funcionalidad de examinar a fondo.
		Actualidad de la información	El perfil de riesgo contiene datos históricos, actuales y de previsiones.
		Nivel de información	El perfil de riesgo agrega información de toda la organización, representando sólo los riesgos más importantes de acuerdo a unos umbrales definidos y contemplando los cambios significativos respecto a períodos anteriores.
	Pragmática	Período de retención	El perfil de riesgo debe conservarse mientras los datos/información que reporta el riesgo deban ser conservados. Los cambios en el registro de riesgos deben guardarse en bitácora según los requerimientos legales, el uso de la información como evidencia o la necesidad de obtener aseguramiento independiente.
		Estado de la información	La instancia actual es operacional, las anteriores son datos históricos.
		Novedad	El perfil de riesgo combina varias fuentes de datos que generan una nueva instancia, por lo tanto son datos nuevos. Se actualiza regularmente (p.e. mensualmente).
		Contingencia	<p>El perfil de riesgo depende de la información siguiente estando disponible y siendo comprendido por el usuario:</p> <ul style="list-style-type: none"> • Disposición al riesgo de la organización • Factores de riesgo que aplican a la organización • Taxonomía de riesgo en uso en la organización
	Social	Contexto	El perfil de riesgo es principalmente significativo y se usa en el contexto del ERM, pero también puede usarse en otras circunstancias (p.e. en una fusión).

Figura 61—Perfil de riesgo (cont.)

Enlaces a otros facilitadores	
Procesos	<p>El perfil de riesgo se obtiene de las prácticas de gestión:</p> <ul style="list-style-type: none"> • APO12.03 Mantener un perfil de riesgo. • APO12.04 Articular el riesgo. <p>El registro de riesgos es una entrada para las prácticas de gestión:</p> <ul style="list-style-type: none"> • EDM03.02 Orientar la gestión de riesgos. • EDM05.02 Orientar la comunicación y reporte a los grupos de interés. • APO02.02 Evaluar el entorno actual, capacidades y rendimiento. • MEA02.08 Ejecutar iniciativas de aseguramiento. <p>Se usa en las siguientes prácticas de gestión:</p> <ul style="list-style-type: none"> • EDM03.03 Monitorear la gestión de riesgos. • APO12.06 Responder al riesgo. <p>Se menciona en el objetivo del proceso APO12 Gestionar el riesgo:</p> <ul style="list-style-type: none"> • Existe un perfil de riesgo completo y actualizado. <p>Y medido por las siguientes métricas:</p> <ul style="list-style-type: none"> • Porcentaje de procesos clave de negocio incluidos en el perfil de riesgo. • Completitud de atributos y valores en el perfil de riesgo.
Estructuras organizacionales	Bajo la responsabilidad del CRO, los siguientes roles son responsables de proveer / producir la información: <ul style="list-style-type: none"> • Propietarios de procesos de negocio • CIO (y personal de TI) • CISO
Infraestructura, aplicaciones y servicios	El perfil de riesgo es generado por una aplicación de gestión de riesgo o mantenido manualmente por el CRO.
Personas, habilidades y competencias	La generación del perfil de riesgo requiere una comprensión de los principios y habilidades de la gestión de riesgos. La provisión de información requiere experiencia en el tema y la presentación de información no debe requerir habilidades de gestión de riesgos pero permite a los órganos de gobierno el seguimiento de la gestión de riesgos y la toma de decisiones al respecto.
Cultura, ética y comportamiento	La disponibilidad del perfil de riesgos da soporte a la transparencia del riesgo como tendencia y a la cultura de conciencia respecto al riesgo.
Principios, políticas y marcos de trabajo	Principios relacionados: <ul style="list-style-type: none"> • Conexión con los objetivos de la organización • Alineamiento con la gestión de riesgos empresariales (ERM) • Balance coste / Beneficio del riesgo de TI • Estrategia consistente

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Un componente importante del perfil de riesgo es el registro de riesgos. La **Figura 62** contiene un ejemplo de plantilla para una entrada del registro de riesgos.

Figura 62—Plantilla de entrada del registro de riesgos								
Parte I - Resumen de datos								
Declaración del riesgo	.							
Propietario del riesgo								
Fecha del último análisis de riesgos								
Fecha esperada para la actualización del análisis de riesgos								
Categoría del riesgo	<input type="checkbox"/> ESTRÁTÉGICO (Facilita beneficio/valor de TI)		<input type="checkbox"/> ENTREGA DE PROYECTOS (Entrega de programas y proyectos de TI)		<input type="checkbox"/> OPERACIONAL (Operaciones TI y entrega de servicio)			
Clasificación del riesgo (copiado de los resultados del análisis de riesgos)	<input type="checkbox"/> BAJO		<input type="checkbox"/> MEDIO		<input type="checkbox"/> ALTO		<input type="checkbox"/> MUY ALTO	
Respuesta al riesgo	<input type="checkbox"/> ACEPTAR		<input type="checkbox"/> TRANSFERIR		<input type="checkbox"/> MITIGAR		<input type="checkbox"/> ELIMINAR	
Parte II - Descripción del riesgo								
Título								
Escenario de alto nivel (de la lista muestra de escenarios de alto nivel)								
Descripción detallada del escenario – Componentes del escenario	Actor							
	Tipo de amenaza							
	Evento							
	Activo / Recurso							
	Cadencia							
Otras informaciones del escenario								
Parte III - Resultados del análisis de riesgos								
Frecuencia del escenario (ocurrencias por año)	0	1	2	3	4	5		
	N≤0,01 <input type="checkbox"/>	0,001<N≤0,1 <input type="checkbox"/>	0,1<N≤1 <input type="checkbox"/>	1<N≤10 <input type="checkbox"/>	10<N≤100 <input type="checkbox"/>	100<N <input type="checkbox"/>		
Comentarios sobre frecuencia								
Impacto del escenario en el negocio	0	1	2	3	4	5		
1. Productividad	Pérdida en ingresos en un año							
Clasificación del impacto	$I \leq 0,1\%$ <input type="checkbox"/>	$0,1\% < I \leq 1\%$ <input type="checkbox"/>	$1\% < I \leq 3\%$ <input type="checkbox"/>	$3\% < I \leq 5\%$ <input type="checkbox"/>	$5\% < I \leq 10\%$ <input type="checkbox"/>	$10\% < I$ <input type="checkbox"/>		
Descripción detallada del impacto								
2. Coste de la respuesta	Gastos asociados con la gestión e las pérdidas del evento							
Clasificación del impacto	$I \leq 10K\$$ <input type="checkbox"/>	$10K\$ < I \leq 100K\$$ <input type="checkbox"/>	$100K\$ < I \leq 1M\$$ <input type="checkbox"/>	$1M\$ < I \leq 10M\$$ <input type="checkbox"/>	$10M\$ < I \leq 100M\$$ <input type="checkbox"/>	$100M\$ < I$ <input type="checkbox"/>		
Descripción detallada del impacto								
3. Ventaja competitiva	Clasificación informal de la satisfacción del cliente							
Clasificación del impacto	$I \leq 0,5$ <input type="checkbox"/>	$0,5 < I \leq 1$ <input type="checkbox"/>	$1 < I \leq 1,5$ <input type="checkbox"/>	$1,5 < I \leq 2$ <input type="checkbox"/>	$2 < I \leq 2,5$ <input type="checkbox"/>	$2,5 < I$ <input type="checkbox"/>		
Descripción detallada del impacto								

Figura 62—Plantilla de entrada del registro de riesgos (cont.)

4. Legal							Cumplimiento regulatorio - Multas						
Clasificación del impacto	Ninguna <input type="checkbox"/>	<1M\$ <input type="checkbox"/>	<10M\$ <input type="checkbox"/>	<100M\$ <input type="checkbox"/>	<1000M\$ <input type="checkbox"/>	>1000M\$ <input type="checkbox"/>							
Descripción detallada del impacto													
Clasificación global del impacto (media de 4 clasificaciones de impacto)													
Clasificación global del riesgo (obtenida combinando las clasificaciones de frecuencia e impacto del mapa de riesgos)	<input type="checkbox"/> BAJO		<input type="checkbox"/> MEDIO		<input type="checkbox"/> ALTO		<input type="checkbox"/> MUY ALTO						
Respuesta a este riesgo	<input type="checkbox"/> ACEPTAR		<input type="checkbox"/> TRANSFERIR		<input type="checkbox"/> MITIGAR		<input type="checkbox"/> ELIMINAR						
Justificación													
Descripción detallada de la respuesta (No en caso de ACEPTAR)	Acción de respuesta			Completada			Plan de acción						
	1.	<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>						
	2.	<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>						
	3.	<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>						
	4.	<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>						
	5.	<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>						
	6.	<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>						
Estado global del plan de acción de riesgos													
Aspectos principales del plan de acción de riesgos													
Estado global de las respuestas completadas													
Aspectos principales de las respuestas completadas													
Parte IV – Indicadores de riesgo													
Indicadores de riesgos principales para este riesgo	1. 2. 3. 4.												

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 63—Plan de comunicación del riesgo

Un plan de comunicación del riesgo define frecuencia, tipos y destinatarios de la información sobre el riesgo. El propósito principal del plan es reducir la sobrecarga de información no relevante (eliminando la probabilidad de “ruido sobre el riesgo”).

Ciclo de vida y grupos de interés	Etapa del ciclo de vida	Grupo de interés interno	Grupo de interés externo	Descripción / Interés
	Planificación de la información	Comité de gestión de riesgos empresariales (ERM), Comité de auditoría		<ul style="list-style-type: none"> • Asegurar que existe el plan de comunicación del riesgo y aprobarlo. • Asegurar que el riesgo se comunica de manera eficiente y oportuna.
	Diseño de la información	Función de riesgo		<ul style="list-style-type: none"> • Definir los diferentes aspectos a incluir en el plan de comunicación del riesgo (p.e. frecuencias / tipos / destinatarios). • Asegurar que el riesgo se comunica de manera eficiente y oportuna.
	Adquisición / Construcción de la información	Función de riesgo, propietarios de procesos de negocio / CIO		<ul style="list-style-type: none"> • Detallar los aspectos definidos del plan de comunicación del riesgo. • Asegurar que el plan de comunicación del riesgo incluye los requerimientos clave para la comunicación del riesgo.
	Uso/ operación de la información: guardar, compartir, usar	Consejo de administración, ejecutivos de negocio, CIO, función de riesgo, propietarios de procesos de negocio, cumplimiento, auditoría interna	Auditoría externa, regulador	La utilización efectiva del plan de comunicación de riesgo por parte de la función de riesgo asegura la disponibilidad reinformación correcta y concisa sobre el riesgo al resto de grupos de interés.
	Monitoreo de la información	Consejo de administración, comité de riesgo, comité de auditoría, función de riesgo	Auditoría externa	<ul style="list-style-type: none"> • Se toman las acciones oportunamente sobre el estado del riesgo y las capacidades ante el riesgo. • Se valida regularmente la adecuación del plan de comunicación del riesgo.
	Desecho de la información	Función de riesgo		Asegurar que la información se destruye de forma oportuna, segura y apropiada.

Figura 63—Plan de comunicación del riesgo (cont.)

Subdimensión y objetivos de calidad		Descripción-La extensión en la que la información es...	Relevancia	Objetivo-El plan de comunicación del riesgo...
Objetivos	Intrínsecos	Exactitud	correcta y fiable	Alta Debe definir exactamente tipo, frecuencia y destinatario de las comunicaciones del riesgo.
		Objetividad	justa, sin prejuicios e imparcial	Alta La información está basada en la cultura de riesgo de la organización.
		Credibilidad	considerada como cierta y creíble	Media Debe ser realista.
		Reputación	considerada como procedente de una fuente cierta y creíble	Media Concebida basándose en las aportaciones de la función de riesgo y de los propietarios de procesos de negocio, haciendo el plan de comunicación del riesgo apropiado.
	Contextual y representacional	Relevancia	aplicable y útil para las tareas a realizar	Alta Debe estar alineada con las necesidades de información del receptor.
		Completitud	no ausente y con suficiente profundidad y amplitud para las tareas a realizar	Alta Debe cubrir la estructura de la organización de principio a fin así como los grupos de interés externos.
		Actualización	suficientemente actualizada para las tareas a realizar	Baja No puede tener una antigüedad superior al año.
		Volumen de información	es apropiada en volumen para las tareas a realizar	Alta Debe contener frecuencias y tipos de comunicación, así como los destinatarios.
		Representación concisa	representada de forma concisa	Media Depende en la audiencia destinataria.
		Representación congruente	presentada en el mismo formato	Baja La información siempre debe ser presentada de acuerdo a formatos y plantillas preestablecidos.
	Interpretabilidad	en lenguajes, símbolos y unidades apropiados, y las definiciones son claras	Alta	Debe ser entendible para la audiencia destinataria.
		Comprensibilidad	fácil de comprender	Alta Debe ser comprensible para la audiencia destinataria.
	Manipulación	fácil de manipular y aplicar a diferentes tareas	Baja	Hecha a medida para cubrir las necesidades de los receptores que realizan diferentes tareas.
	Seguridad	Disponibilidad	disponible cuando se requiere, o fácil y rápidamente recuperable	Media Debe estar disponible en la frecuencia requerida para los grupos de interés clave. La información debe estar disponible 24x7 para la función de riesgo.
		Acceso restringido	restringida de manera apropiada a partes autorizadas	Alta Se indica que el acceso a esta información viene determinada por la función de riesgo, y se restringe así: • Acceso de escritura: Función de riesgo • Acceso de lectura: El resto de grupos de interés

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 63—Plan de comunicación del riesgo (cont.)

Buenas prácticas	Atributo	Descripción	Valor
	Física	Soporte / medio de la información	El soporte de la información para el plan de comunicación del riesgo puede ser electrónico o documento impreso.
	Empírica	Canal de acceso a la información	El plan de comunicación del riesgo es accesible a través del sistema de gestión documental, del portal de gestión de riesgos empresariales (ERM) o impreso en ubicaciones específicas.
	Sintáctica	Código / lenguaje	El plan de comunicación del riesgo contiene los siguientes subapartados: <ul style="list-style-type: none"> • Frecuencia y temporización de la comunicación • Tipo de comunicación • Audiencia destinataria y distribución
	Semántica	Tipo de información	Documento estructurado que facilita una clara visión de la comunicación requerida.
		Actualidad de la información	La información debe ser actual para su uso en la organización.
		Nivel de información	El plan de comunicación del riesgo debe detallar la información requerida para ser comunicada, dependiendo en la audiencia destinataria.
	Pragmática	Periodo de retención	De acuerdo con la política de retención de datos (y teniendo presentes los requerimientos de retención que establece la legislación local).
		Estado de la información	El plan de comunicación del riesgo generado debe ser actual, hasta que se genere uno de nuevo. Cuando de reemplace, pasa a ser una versión antigua (histórica).
		Novedad	Sólo se actualiza cuando se requiere. Aunque el plan debe ser actual.
		Contingencia	El portal de riesgo empresarial debe ofrecer la disponibilidad predefinida.
	Social	Contexto	El plan de comunicación del riesgo debe ser usado en el contexto del plan de comunicación del riesgo de TI.
Enlaces a otros facilitadores			
Procesos	El plan de comunicación del riesgo es una salida de las actividades de proceso: <ul style="list-style-type: none"> • EDM03.03 Monitorear la gestión de riesgo. • EDM05.01 Evaluar los requerimientos de reporte a los grupos de interés. • EDM05.02 Orientar la comunicación y reporte a los grupos de interés. • EDM05.03 Monitorear la comunicación con los grupos de interés. El plan de comunicación del riesgo es una entrada para las actividades de proceso: <ul style="list-style-type: none"> • APO12.01 Recolección de datos. • APO12.02 Análisis de riesgos. • APO12.04 Articular el riesgo. • APO12.06 Responder al riesgo. 		
Estructuras organizacionales	Los roles siguientes son responsables y ejecutores de (parcialmente) producir la información: <ul style="list-style-type: none"> • Responsables: Comité de gestión de riesgos empresariales (ERM) • Ejecutores: Función de riesgo • Consultados: Propietarios de procesos de negocio, CIO, consejo de administración, ejecutivos de gestión, cumplimiento, comité de auditoría, auditoría interna (ver también grupos de interés) 		
Infraestructura, aplicaciones y servicios	El plan de comunicación de riesgo se genera con el software habitual de gestión ofimática.		
Personas, habilidades y competencias	El universo de riesgo, disposición y tolerancia requiere las siguientes competencias: <ul style="list-style-type: none"> • Capacidad analítica • Competencias interpersonales • Pensamiento lateral (solución de problemas de forma creativa y no convencional) 		
Cultura, ética y comportamiento	El plan de comunicación del riesgo requiere los siguientes comportamientos: <ul style="list-style-type: none"> • Cultura que facilite y permita el riesgo • Actitud positiva respecto a las cuestiones emergentes • Aceptación del riesgo • Aceptación del riesgo por parte de las funciones de negocio 		
Principios, políticas y marcos de trabajo	Principios relacionados: <ul style="list-style-type: none"> • Promoción de una comunicación clara y abierta • Estrategia consistente 		

Figura 64—Informe de riesgo

Un informe de riesgo contiene información sobre la capacidad actual de gestión de riesgo, el estado actual y tendencias al respecto. Este informe se basará sobre el perfil de riesgo y se adaptará a los requisitos de los receptores

Ciclo de vida y Grupos de Interés	Estadio Ciclo de Vida	Grupo de interés Interno	Grupo de interés Externo	Descripción/Interés
	Planificación Información	Función de gestión de riesgos		Las capacidades de gestión de riesgo, el estado actual y las tendencias se comunican puntual y exactamente a las personas correctas basándose en sus necesidades y requisitos.
	Diseño Información	Función de gestión de riesgos		Las capacidades de gestión de riesgo, el estado actual y las tendencias se comunican puntual y exactamente a las personas correctas basándose en sus necesidades y requisitos.
	Desarrollo/ Adquisición Información	Función de gestión de riesgos, Propietarios procesos de negocio/CIO		Asegura que el informe de riesgos incluye la información más actual sobre capacidades de gestión de riesgo, últimas tendencias y estado respecto al riesgo de la totalidad de la organización
	Uso/Operativa Información; almacenar, compartir, usar	Consejo de Administración, gestión ejecutiva, CIO, Función de gestión de riesgos, Propietarios procesos de negocio/CIO, cumplimiento normativo y	Auditores externos, Agentes reguladores	Utilización efectiva y disponibilidad de los ítems de información por todos los implicados
	Monitoreo Información	Consejo de Administración, Comité de riesgo, Comité de auditoría, Función de gestión de riesgos, Propietarios procesos de negocio/CIO	Auditores externos	Verifica que la información se mantiene actualizada y alerta sobre cambios.
	Eliminación Información	Función de gestión de riesgos		Asegura que la información se elimina de forma segura, apropiada y en el momento adecuado.
	Subdimensión de Calidad y Metas	Descripción—Hasta qué punto la información es...	Relevancia	Meta- El Informe de riesgo.....
Metas Intrínsecas	Exactitud	Correcta y fiable	Alta	Debe definir con exactitud las capacidades de gestión de riesgo, el estado actual y tendencias sobre riesgo, desde un punto de vista que no produzca confusión.
	Objetividad	No sesgada, sin prejuicios e imparcial	Alta	Basa su información sobre la cultura de riego de la empresa y las observaciones la confirman.
	Credibilidad	Considerada como verdadera y fiable	Media	debe ser realista y preciso
	Reputación	Considerada que procede de fuentes verdaderas y fiables	Alta	Recoge la información de fuentes competentes y reconocidas.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 64—Informe Riesgo (cont.)

	Subdimensión de Calidad y Metas	Descripción—Hasta qué punto la información es...	Relevancia	Meta- El Informe de riesgo...
Metas Contextual y Formato	Relevancia	Aplicable y útil para las tareas a realizar	Alta	Está personalizado según los requerimientos de sus destinatarios.
	Integridad	Existe y tiene una profundidad y extensión acorde a las tareas a realizar	Alta	Cubre de principio a fin toda la estructura de la empresa así como a los grupos de interés externos
	Actualidad	Suficientemente actualizado para las tareas a realizar	Alta	No tiene más de un año de antigüedad ya que debe mantenerse actualizado
	Nivel de información	Apropiado para las tareas a realizar	Alta	Debe contener el nivel apropiado de información basándose en los requisitos de los receptores
	Presentación concisa	Presentado de forma compacta	Media	Depende de la audiencia destino
	Presentación consistente	Presentado en el mismo formato	Alta	Debe presentarse siempre siguiendo los formatos y plantillas predefinidos
	Inteligible	En un lenguaje apropiado, los símbolos, unidades y definiciones son claros.	Alta	Debe ser inteligible para la audiencia a la que se destina
	Comprensible	Fácilmente comprensible	Alta	Debe ser comprensible para la audiencia a la que se destina
	Manipulación	De fácil manipulación y aplicable a diferentes tareas	Media	Permite manipular la información para presentarla como diferentes informes de riesgo
	Disponibilidad	Disponible cuando se requiere, o fácil y rápidamente extraíble	Alta	Ha de estar disponible para los grupos de interés con la frecuencia que se requiera.
Buena Práctica	Acceso restringido	Apropiadamente restringido a las partes autorizadas	Alta	Tiene el acceso determinado por la función de gestión de riesgo con las restricciones siguientes: <ul style="list-style-type: none"> • Acceso de escritura: Función de gestión de riesgo • Acceso de lectura: Todos los otros grupos de interés
	Atributo	Descripción	Valor	
	Físico	Información soporte/medio	El soporte de la información del informe de riesgo puede ser un documento electrónico y/o impreso	
	Empírico	Información canal acceso	El informe de riesgo es accesible a través del portal de Gestión de Riesgo Empresarial, además está disponible impreso, en una ubicación específica.	
	Sintáctico	Código/lenguaje	El informe de riesgo contiene los apartados siguientes: <ul style="list-style-type: none"> • Estado de los ítems de riesgo • Acciones (respuesta a riesgos) • Capacidades gestión riesgos 	
	Semántico	Tipo información	Informes (de riesgo)	
		Actualidad información	La información debe estar actualizada para usarse en la organización	
		Nivel información	Depende de la audiencia a la que se dirige: para las funciones de Consejo de Administración y Comité de riesgo es adecuada una presentación del estado de riesgo y las capacidades de gestión de éste. Para los responsables de proceso un informe detallado de análisis de riesgos.	
	Pragmático	Periodo retención	Según la política de retención de datos (además considerando los requisitos que establezca la legislación local)	
		Estado información	La información producida debe ser actual. Cuando se reemplaza pasará a histórica	
		Novedad	Es actual, tal como el estado de riesgo se modifica a lo largo del tiempo	
		Contingencia	El portal de gestión de riesgo empresarial lo debe facilitar como y cuando sea necesario	
	Social	Contexto	Este ítem de información debe usarse en el contexto del plan de comunicación del riesgo TI	

Figura 64—Informe Riesgo (cont.)

Enlaces a otros facilitadores	
Procesos	<p>El informe de riesgo resulta de las actividades:</p> <ul style="list-style-type: none"> • APO12.01 Recogida de datos. • APO12.02 Analizar riesgos. • APO12.04 Articular riesgos • APO12.06 Respuesta a riesgos <p>El informe de riesgo se precisa para las actividades:</p> <ul style="list-style-type: none"> • EDM03.03 Monitorear gestión de riesgo. • EDM05.01 Evaluar los requisitos de los informes para los grupos de interés. • EDM05.02 Comunicación directa con los grupos de interés y preparación informes. • EDM05.03 Monitorear la comunicación a los grupos de interés
Estructuras organizativas	Los roles siguientes rinden cuentas y son responsables (parcialmente) de la producción de información: <ul style="list-style-type: none"> • Rinde cuentas: Función de gestión de riesgos • Responsable: Función de gestión de riesgos, Propietarios proceso de negocio/CIO • Consultados/Informados: Consejo de Administración, Comité Gestión Riesgo Empresarial, gestión ejecutiva, cumplimiento normativo, comité de auditoría, auditoría interna (ver también Grupos de interés)
Infraestructura, aplicaciones y servicios	El informe de riesgo se produce mediante el Portal de Gestión de Riesgo (herramienta CGR)
Personas, habilidades y competencias	La generación y uso del informe de riesgo requiere la comprensión de los principios y habilidades de gestión de riesgo.
Cultura, ética y conducta	El informe de riesgo precisa las conductas siguientes: <ul style="list-style-type: none"> • Cultura de riesgo activada/interiorizada
Principios, políticas y esquemas de trabajo	Principios relacionados <ul style="list-style-type: none"> • Alineamiento con Gestión de Riesgo Empresarial • Promover una comunicación imparcial y abierta • Funciona como parte de las actividades diarias • Aproximación consistente

Figura 65—Programa de Sensibilización de Riesgo

Un programa de sensibilización de riesgo es un plan clara y formalmente definido, tiene una aproximación estructurada, conteniendo un conjunto de actividades y procedimientos relacionados con el objetivo de realizar y mantener una cultura de conciencia de riesgo.

Ciclo de vida e grupos de interés	Estadio Ciclo de Vida	Grupo de interés Interno	Grupo de interés Externo	Descripción/Interés
	Planificación Información	Comité de Gestión del Riesgo Empresarial (ERM)		<ul style="list-style-type: none"> • Asegura que todos los grupos de interés comprenden el riesgo en general y las previsiones. • Crea una cultura de riesgo activada/interiorizada • Asegura que todas las decisiones relativas a riesgos están informadas.
Diseño Información	Función de gestión de riesgos			Diseña un programa efectivo para educación y concienciación entre las personas sobre los aspectos relacionados con riesgos.
Desarrollo/ Adquisición Información	Función de gestión de riesgos			Asegura que el programa de sensibilización de riesgo incluye actividades y procedimientos que alcanzan a todos los grupos de interés.
Uso/Operativa Información; almacenar, compartir, usar	Todos			Asegura que se comprenden las aspectos relacionados con riesgos
Monitoreo Información	Auditoría Interna, Función de gestión de riesgos			Monitorea que el plan continúa siendo adecuado para seguir creando la sensibilización de riesgo apropiada para todos los niveles de la empresa.
Eliminación Información	Función de gestión de riesgos			Asegura que la información se destruye de una manera puntual, segura y apropiada.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 65—Programa de Sensibilización de Riesgo (cont.)

	Subdimensión de Calidad y Metas	Descripción—Hasta qué punto la información es...	Relevancia	Meta- El Informe de riesgo...
Metas	Intrínseco	Exactitud	Alta	Se basa sobre la educación estándar en relación al riesgo
		Objetividad	Alta	Se basa en la cultura y disposición al riesgo en la organización.
		Credibilidad	Alta	Se adapta a la audiencia
		Reputación	Alta	Se ha preparado basándose sobre la política de riesgo aprobada por la empresa.
	Contextual y Formato	Relevancia	Alta	Se organiza orientado a la audiencia destino.
		Integridad	Alta	Cubre de principio a fin la estructura de la empresa así como a los grupos de interés externos.
		Actualidad	Media	Debe verificarse su adecuación cada seis meses.
		Nivel de Información	Media	Incluye información básica sobre gestión de riesgo y expectativas de los grupos de interés clave.
		Presentación Concisa	Media	Depende de la audiencia destino
		Presentación Constante	Media	Debe siempre presentarse según los formatos/ plantillas predefinidos y la audiencia destino.
	Seguridad	Interpretación	Media	Debe ser inteligible para la audiencia a la que se destina
		Comprendibilidad	Media	Debe ser comprensible para la audiencia a la que se destina
		Manipulación	Media	Las actividades y procedimientos deben ser adaptables, dependiendo de la audiencia destino
Buena Práctica	Disponibilidad	Disponible cuando se requiere, o fácil y rápidamente extraíble	Media	Ha de estar disponible para los grupos de interés clave con la frecuencia requerida (sesiones de trabajo sobre riesgo)
	Acceso restringido	Apropiadamente restringido a las partes autorizadas	Baja	Tiene el acceso determinado por la función de gestión de riesgo con las restricciones siguientes: <ul style="list-style-type: none"> • Acceso de escritura: Función de gestión de riesgo • Acceso de lectura: Todos los otros grupos de interés
	Atributo	Descripción		Valor
	Físico	Información soporte/medio		El soporte de la información del informe de riesgo puede ser un documento electrónico y/o impreso
	Empírico	Información canal acceso		El informe de riesgo es accesible a través de sistemas de gestión documental, el portal de Gestión de Riesgo Empresarial y a través de sesiones de trabajo
	Sintáctico	Código/lenguaje		El programa de sensibilización de riesgo contiene la formación relativa a riesgo, la frecuencia y la audiencia
	Semántico	Tipo información		Sensibilización/Educación sobre riesgo
		Actualidad información		El programa de sensibilización de riesgo debe estar actualizado para uso organizativo
		Nivel información		Un programa con frecuencia, contenido y destinatarios.
	Pragmático	Periodo retención		Según la política de retención de datos (además considerando los requisitos que establezca la legislación local)
		Estado información		La información producida debe ser actual. Cuando se convierte en histórica se ha de substituir.
		Novedad		Es actual, tal como el estado de riesgo se modifica en su momento
		Contingencia		El portal de gestión de riesgo empresarial lo debe facilitar como y cuando sea necesario
	Social	Contexto		El programa de sensibilización de riesgo debe usarse en el contexto de un requerimiento de educación de riesgo

Figura 65— Programa de Sensibilización de Riesgo (cont.)

Enlace a otros Catalizadores

Procesos	<p>El programa de sensibilización de riesgo es un resultado de la actividad:</p> <ul style="list-style-type: none"> • EDM03.02 Gestión directa de riesgo <p>El programa de sensibilización de riesgo es una entrada para la actividad:</p> <ul style="list-style-type: none"> • APO012 Gestionar riesgo.
Estructuras Organizativas	<p>Los roles siguientes rinden cuentas y son responsables (parcialmente) de la producción de información</p> <ul style="list-style-type: none"> • Rinde cuentas: Función de gestión de riesgos • Responsable: Función de gestión de riesgos, • Consultados: Consejo de Administración, Comité Gestión Riesgo Empresarial, gestión ejecutiva, cumplimiento normativo, comité de auditoría, auditoría interna • Informados: Todos (ver también Grupos de interés)
Infraestructura, Aplicaciones y Servicios	El programa de sensibilización de riesgo se prepara mediante una herramienta de gestión documental y/o un portal de riesgo empresarial.
Personas, Habilidades y Competencias	La generación y uso del programa de sensibilización de riesgo requiere la comprensión de los principios y habilidades de gestión de riesgo.
Cultura, Ética y Conducta	El programa de sensibilización de riesgo requiere establecer una cultura básica de riesgo e identificar la exposición a riesgos de la organización.
Principios, Políticas y Esquemas trabajo	<p>Principios relacionados</p> <ul style="list-style-type: none"> • Promover una comunicación imparcial y abierta • Funciona como parte de las actividades diarias

Figura 66—Mapa de Riesgos

Una técnica habitual, muy fácil e intuitiva, para presentar los riesgos es el mapa de riesgos. La presentación se realiza en un diagrama bidimensional con la frecuencia e impacto como dimensiones. La presentación del mapa de riesgos es potente y ofrece una vista completa sobre riesgos y áreas de actuación evidentes. Además, un mapa de riesgos permite definir zonas coloreadas indicando zonas deseables de significancia en modo gráfico. Una consideración práctica sería focalizarse sobre los 10-20 ítems de riesgo más importantes, o separarlos en categorías, de otra manera el mapa de riesgos puede no ser legible.

Ciclo de Vida e Grupos de interés	Estadio Ciclo de Vida	Grupo de interés Interno	Grupo de interés Externo	Descripción/Interés
	Planificación Información	Función de gestión de riesgos		El riesgo se comunica de manera planificada
	Diseño Información	Función de gestión de riesgos		<ul style="list-style-type: none"> • Diseño de mapas de riesgo según los requisitos del comité de Gestión de Riesgo Empresarial/Gestión ejecutiva • Asegura que el riesgo se presenta de manera comprensible.
	Desarrollo/ Adquisición Información	Función de gestión de riesgos, propietarios procesos de negocio/CIO		Recoger de los grupos de interés clave la información necesaria para llenar el mapa de riesgos.
	Uso/Operativa Información; almacenar, compartir, usar	Consejo de Administración, gestión ejecutiva, Función de gestión de riesgos, propietarios procesos de negocio/CIO, cumplimiento normativo, auditoría interna	Auditoría externa, Agencias reguladoras	Utilización efectiva del mapa de riesgos para dar soporte a la toma y ejecución de decisiones.
	Monitoreo Información	Consejo de Administración, comité de riesgo, comité de auditoría, Función de gestión de riesgos, propietarios procesos de negocio/CIO	Auditoría externa	<ul style="list-style-type: none"> • Monitorea si la información sobre el mapa de riesgos es la más actual • Asegura que el mapa de riesgos todavía es relevante para la empresa
	Eliminación Información	Función de gestión de riesgos		Asegura que la información se destruye de una manera puntual, segura y apropiada.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 66—Mapa de Riesgos (cont.)

	Subdimensión de Calidad y Metas	Descripción—Hasta que punto la información es.....	Relevancia	Meta —El mapa de riesgo...	
Metas	Intrínseco	Exactitud	Correcto y fiable	Alta	Debe definir con exactitud el estado de todos los ítems de riesgo
		Objetividad	Sin sesgo, ni prejuicios e imparcial	Alta	La información se recoge/confirma por múltiples fuentes en la empresa y externas a ésta, si aplica. La información puede almacenarse en una herramienta de Gestión Actual de Riesgos
		Credibilidad	Considerada, verdadera y creíble	Media	Su visión debe ser realista, considera las áreas evidentes para la acción, tiene en cuenta el estado actual y entorno de la empresa.
		Reputación	Se considera como procedente de fuentes verdaderas y creíbles	Alta	La información se recoge de fuentes competentes y reconocidas
	Contextual y Formato	Relevancia	Aplicable y útil para las tareas a realizar	Alta	Debe organizarse según categorías de riesgo para garantizar la posibilidad de comparaciones adecuadas
		Integridad	No falta y tiene la profundidad y amplitud suficientes para las tareas a realizar	Alta	Debe cubrir de principio a fin el espectro de la empresa.
		Actualidad	Suficientemente actualizado para las tareas a realizar.	Alta	Debe presentar el estado actual
		Nivel de Información	Apropiado para las tareas a realizar	Alta	Debe contener información de muy alto nivel. El volumen de la fuente de información debe ser el apropiado para dar soporte a la indicación en el mapa de riesgos
		Presentación Concisa	Presentado de forma compacta	Media	Debe siempre presentarse según los formatos y plantillas predefinidos.
		Presentación Constante	Presentado en el mismo formato	Alta	Debe siempre presentarse según los formatos y plantillas predefinidos.
	Seguridad	Interpretación	En un lenguaje apropiado, los símbolos, unidades y definiciones son claros.	Alta	Debe ser inteligible por la audiencia destino
		Comprendibilidad	Fácilmente comprensible	Alta	Debe ser comprensible por la audiencia destino
	Seguridad	Manipulación	De fácil manipulación y aplicable a diferentes tareas	Media	Su información puede manipularse para presentarla con diferentes métodos gráficos
		Disponibilidad	Disponible cuando se requiere, o fácilmente y rápidamente extraíble	Alta	Debe estar disponible 24X7
Buena Práctica	Práctica	Acceso restringido	Apropiadamente restringido a las partes autorizadas	Alta	Tiene el acceso determinado por la función de gestión de riesgo con las restricciones siguientes: <ul style="list-style-type: none"> • Acceso de escritura: Función de gestión de riesgo • Acceso de lectura: Todos los otros grupos de interés
		Atributo	Descripción	Valor	
		Físico	Información soporte/medio	El soporte del mapa de riesgos puede ser un documento electrónico y/o impreso	
		Empírico	Información canal acceso	El mapa de riesgos es accesible mediante el portal de Gestión de Riesgo Empresarial	
		Sintáctico	Código/lenguaje	El mapa de riesgos contiene los apartados siguientes: <ul style="list-style-type: none"> • Estado de los ítems de riesgo (indicados en el mapa de riesgos) • Áreas de actuación y, opcionalmente, una respuesta al riesgo 	
		Semántico	Tipo información	Estado de riesgos en formato gráfico	
			Actualidad información	La información debe estar actualizada para uso organizativo	
			Nivel información	Representación gráfica del estado del riesgo y área de acción	
		Pragmático	Periodo retención	Según la política de retención de datos (además considerando los requisitos que establezca la legislación local)	
			Estado información	El mapa de riesgos debe ser actual. Cuando se reemplaza se convierte en histórico	
			Novedad	Es actual ya que el mapa de riesgos está actualizado	
			Contingencia	El portal de riesgo empresarial debe suministrarlo como y cuando se requiera	
		Social	Contexto	El mapa de riesgos debe usarse en el contexto del plan de comunicación de riesgo TI	

Figura 66—Mapa de Riesgos (cont.)

Enlace a otros Catalizadores	
Procesos	<p>El mapa de riesgos es un resultado de las actividades:</p> <ul style="list-style-type: none"> • APO12.01 Recoger datos. • APO12.02 Analizar riesgo. • APO12.04 Articular riesgo. • APO12.06 Responder a riesgos. <p>El mapa de riesgos es una entrada de las actividades:</p> <ul style="list-style-type: none"> • EDM05.01 Evaluar los requisitos de los grupos de interés respecto a informes. • EDM05.02 Comunicación directa con los grupos de interés y preparación informes • EDM05.03 Monitorear la comunicación con los grupos de interés. • EDM03.03 Monitorear la gestión de riesgo.
Estructuras Organizativas	<p>Los roles siguientes rinden cuentas y son responsables (parcialmente) de la producción de información</p> <ul style="list-style-type: none"> • Rinde cuentas: Función de gestión de riesgos • Responsable: Función de gestión de riesgos, propietarios procesos de negocio/CIO • Consultados/Informados: Consejo de Administración, Comité Gestión Riesgo Empresarial, gestión ejecutiva cumplimiento normativo, comité de auditoría, auditoría interna (ver también Grupos de interés)
Infraestructura,	El mapa de riesgo se prepara mediante el portal de riesgo empresarial.(herramienta GRC)
Personas, Habilidades y Competencias	La generación y uso del mapa de riesgos requiere la comprensión de los principios y habilidades de gestión de riesgo.
Cultura, Ética y Conducta	El uso del mapa de riesgos requiere una cultura de habilitación/interiorización de riesgos
Principios, Políticas y Esquemas trabajo	<p>Principios relacionados:</p> <ul style="list-style-type: none"> • Conexión a los objetivos empresariales • Alineación con la Gestión de Riesgo Empresarial • Balance coste/beneficio del riesgo TI

Figura 67—Universo de Riesgo, Apetito y Tolerancia

- **Universo**—La cantidad total de riesgo, incluyendo el desconocido, que puede tener un impacto, bien positivo o negativo, en la capacidad de una empresa para conseguir su misión (o visión) a largo plazo.
- **Apetito**—La totalidad de riesgo, en diversos aspectos de una empresa, que se está dispuesto a aceptar en la persecución de su misión.
- **Tolerancia**—El nivel aceptable de variación de cualquier riesgo particular que la dirección está dispuesta a aceptar en la persecución de sus objetivos.

Ciclo de Vida y Partes Interesadas	Estado del Ciclo de Vida	Parte Interesada Interna	Parte Interesada Externa	Descripción/Interés
	Planificación de la información	Comité de dirección, director general		Las Partes Interesadas definen el universo, el apetito y la tolerancia.
	Diseño de la información	Función de riesgos		Diseña la descripción adecuada y precisa del universo y el apetito y define la información necesaria para poder establecer las tolerancias.
	Generación/ obtención de la información	Función de riesgos		Reúne (el resto de) la información requerida para establecer el universo, el apetito y las tolerancias.
	Uso/operación de la información: almacenamiento, compartición, uso	Comité de dirección, comité ejecutivo, función de riesgos, propietarios de los procesos de negocio/director de informática-sistemas (CIO), cumplimiento, auditoría interna	Auditoría externa, regulador	Utilización efectiva y disponibilidad del universo de riesgos, el apetito y las tolerancias.
	Supervisión de la información	Comité de dirección, comité de riesgos, comité de auditoría, función de riesgos, propietarios de los procesos de negocio/director de informática-sistemas (CIO)	Auditoría externa	Asegura que la aceptación del riesgo se mantiene en límites aceptables y adapta el universo de riesgos, el apetito y las tolerancias si es necesario.
	Eliminación de la información	Función de riesgos		Asegura que la información se elimina con puntualidad, de forma segura y apropiada.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 67—Universo de Riesgo, Apetito y Tolerancia (cont.)

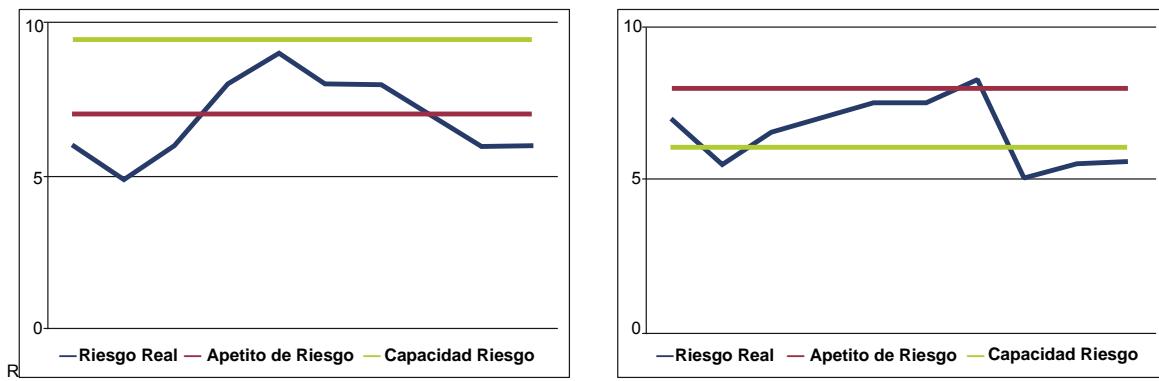
	Subdimensión de Calidad y Metas	Descripción—Hasta que punto la información es.....	Relevancia	Meta —El mapa de riesgo...
Objetivos	Intrínsecos	Exactitud	Alta	Debería articular los umbrales de forma precisa
		Objetividad	Alta	La información se recopila/confirma a través de múltiples fuentes en la empresa y fuera de ella si es aplicable
		Credibilidad	Media	Debería encontrarse alineado con la cultura de riesgo de la empresa
		Reputación	Alta	La información fuente se recopila en reuniones de trabajo con todas las partes interesadas necesarias
	Contextual y Representativo	Relevancia	Media	Se mantienen en plantillas pre-aprobadas
		Integridad	Alta	Las descripciones deberán considerar toda la información necesaria para describir de manera concisa los límites
		Vigencia	Alta	Deberá encontrarse en el estado actual
		Cantidad de Información	Alta	Deberá proporcionar información relevante para las decisiones informadas
		Representación concisa	Media	Deberá presentarse siempre de acuerdo a los formatos/plantillas predefinidos
		Representación consistente	Alta	Deberá presentarse siempre de acuerdo a los formatos/plantillas predefinidos
		Interpretabilidad	Alta	Debería ser inteligible para el público objetivo
		Comprensión	Media	Debería ser comprensible para el público objetivo
	Seguridad	Manejabilidad	Media	Debería estar escrito de tal forma que quede claro qué significa de forma específica para todos los departamentos, funciones, tareas, etc., en la empresa.
		Disponibilidad	Alta	Debería estar disponible 24x7
	Acceso restringido	Restringida adecuadamente a las partes autorizadas	Alta	El acceso lo determina la función de riesgos y se restringe como sigue: - Acceso de escritura: función de riesgos - Acceso de lectura: el resto de partes interesadas
Buena Práctica	Atributo	Descripción	Valor	
	Físico	Soporte de la información	El soporte de información para el universo, apetito y tolerancia al riesgo puede ser un documento electrónico o impreso.	
	Empírico	Canal de acceso a la información	El universo, apetito y tolerancia al riesgo son accesibles a través del portal de gestión de riesgos de la empresa (ERM).	
	Sintáctico	Código/lenguaje	El universo, apetito y tolerancia al riesgo contiene información histórica financiera, nivel de tolerancia/aceptación y un número de transacciones/actividades.	
	Semántico	Tipo de información	Plantilla estándar	
		Vigencia de la información	La información debería ser vigente para el uso de la organización.	
		Nivel de información	Descripciones detalladas del universo, apetito y tolerancia al riesgo, aplicable para el alcance de la organización.	
	Pragmático	Periodo de retención	Acorde a la política de retención de la información (y teniendo en cuenta los requisitos legales de retención locales).	
		Estado de la información	El universo, apetito y tolerancia al riesgo generados serían vigentes. Una vez sustituidos, pasan a histórico.	
		Novedad	Es vigente en tanto que el estado del riesgo se actualiza en el tiempo.	
		Contingencia	El portal de riesgos de la empresa (ERM) debería dar servicio cómo y cuándo se requiera.	
	Social	Contexto	El universo, apetito y tolerancia al riesgo deberían ser utilizados en el contexto de la política de riesgos.	

Figura 67—Universo de Riesgo, Apetito y Tolerancia (cont.)

Vínculo a otros catalizadores	
Procesos	<p>El universo, apetito y tolerancia son un resultado de las actividades de los procesos:</p> <ul style="list-style-type: none"> EDM03.01 Evaluar la gestión de riesgos. EDM03.03 Supervisar la gestión de riesgos. <p>El universo, apetito y tolerancia son una entrada para las actividades de los procesos:</p> <ul style="list-style-type: none"> APO12.03 Mantener un perfil de riesgo. APO12.04 Expresar el riesgo.
Estructuras Organizativas	<p>Las siguientes figuras son responsables y ejecutores (parcialmente) de producir la información:</p> <ul style="list-style-type: none"> Responsable: función de riesgos Ejecutor: función de riesgos Consultados/Informados: Comité de dirección, comité de gestión de riesgos de la empresa (ERM), comité de auditoría, propietarios de los procesos de negocio/director de informática-sistemas (CIO), auditoría interna (ver también las partes interesadas)
Infraestructura, Aplicaciones y Servicios	El universo, apetito y tolerancia al riesgo se encuentran disponibles en el portal de gestión de riesgos (herramienta GRC - Gobierno, gestión de Riesgo y Cumplimiento).
Personas, Habilidades y Competencias	El universo, apetito y tolerancia al riesgo requieren las siguientes competencias:
Cultura, Ética y Conducta	El universo, apetito y tolerancia al riesgo requieren los siguientes comportamientos:
Principios, Políticas y Marcos de Trabajo	Principios relacionados:

Sobre el Apetito, la Capacidad y la Tolerancia al Riesgo

En la discusión sobre el apetito de riesgo, el término ‘capacidad de riesgo’ también se utiliza en ocasiones. Esto se define como la cantidad objetiva de pérdidas que una empresa puede tolerar sin arriesgar la continuidad de su existencia. De este modo, es diferente del apetito de riesgo, que es más una decisión del comité de dirección/la gerencia sobre cuánto riesgo es deseable, tal como se muestra en la **figura 68**.

Figura 68—Capacidad de Riesgo, Apetito de Riesgo y Riesgo Real


En la **figura 68**:

- El diagrama de la izquierda muestra una situación relativamente sostenible en la que el apetito de riesgo es menor que la capacidad de riesgo, y en la que el riesgo real supera al apetito de riesgo en un número de situaciones, pero siempre está por debajo de la capacidad de riesgo.

- El diagrama de la derecha muestra una situación más bien insostenible, en la que la dirección establece el apetito de riesgo un nivel por encima de la capacidad de riesgo; esto significa que la dirección está preparada para aceptar un riesgo claramente superior a la capacidad objetiva para absorber pérdidas. Como resultado, el riesgo real excede la capacidad de riesgo sistemáticamente, incluso estando casi siempre por debajo del nivel de apetito de riesgo. Esto representa usualmente una situación insostenible.

Definiendo la Capacidad de Riesgo y el Apetito de Riesgo

La capacidad de riesgo y el apetito de riesgo son definidos por el comité de dirección y la dirección ejecutiva a nivel de empresa (EDM03). Existen diversos beneficios asociados a este enfoque:

- Soporta y proporciona evidencias del proceso de decisión basado en riesgos, porque todas las decisiones relativas a riesgos están basadas en el lugar donde reside el riesgo en el mapa de riesgos; por tanto, todas las acciones de respuesta al riesgo pueden ser trazadas y justificadas
- Soporta el entendimiento de cómo cada componente de la empresa contribuye a la totalidad del perfil de riesgo.
- Muestra cómo diferentes estrategias de ubicación de recursos pueden incrementar o disminuir la carga de riesgo, simulando diversas opciones de respuesta al riesgo
- Soporta la priorización y el proceso de aprobación de las acciones de respuesta al riesgo mediante presupuestos de riesgo; un presupuesto de riesgo permite a las empresas compensar tipos de riesgo (tiempo de lanzamiento al mercado frente a fiabilidad) y la aceptación del riesgo frente a la inversión para reducirlo. Por ejemplo, resulta útil entender cómo utilizar un presupuesto de riesgo destinado a mitigar elementos de riesgo ‘conocidos’ (p.ej., estabilidad operacional y disponibilidad de una infraestructura de realización de pedidos) para permitir la aceptación de un riesgo desconocido (p.ej., tarifas de entrada al mercado de nuevos productos)
- Identifica áreas específicas en las que debería producirse una respuesta al riesgo

El apetito de riesgo se traduce en un número de estándares y políticas, a fin de contener el nivel de riesgo dentro de los límites establecidos por el apetito de riesgo, por ejemplo:

- La dirección de una compañía de servicios financieros ha determinado que la plataforma y aplicaciones principales no pueden estar inoperativas por un periodo superior a las dos horas, y que el sistema debería ser capaz de soportar un incremento anual de transacciones de un 15 por ciento sin impacto en el rendimiento. La dirección de TI debe traducir esta información en requerimientos específicos de disponibilidad y redundancia para los servidores y resto de infraestructuras en las que se ejecutan las aplicaciones. A su vez, esto conlleva:
 - Requerimientos técnicos detallados de capacidad y previsiones
 - Procedimientos específicos de TI relacionados con la supervisión del rendimiento y planificación de la capacidad
 - La dirección ha determinado que el tiempo de lanzamiento al mercado de las nuevas iniciativas de negocio es crucial y que las aplicaciones TI que dan soporte a estas iniciativas no pueden ser entregadas con retrasos superiores a un mes – sin excepciones. La dirección de TI deberá traducir estos requisitos en requerimientos de recursos y procesos de desarrollo para todas las iniciativas de desarrollo.

De forma similar a la descripción del universo de riesgos y a las evaluaciones de riesgo de la empresa, el apetito de riesgo y los límites entre las diferentes franjas de significado deben ajustarse o confirmarse regularmente.

Tolerancia al Riesgo

Los niveles de tolerancia al riesgo son desviaciones tolerables del nivel establecido en las definiciones de apetito de riesgo, por ejemplo:

- Los estándares requieren que los proyectos se completen dentro del presupuesto y tiempo estimados, pero un exceso del 10 por ciento en presupuesto o el 20 por ciento en tiempo son tolerables.
- Los niveles de servicio requieren de la disponibilidad de los sistemas en funcionamiento del 99,5 por ciento de forma mensual; sin embargo, casos aislados del 99,4 por ciento serán tolerados.
- La empresa tiene una gran aversión al riesgo de seguridad y no quiere aceptar ninguna intrusión externa; sin embargo, intrusiones únicas aisladas con un daño limitado pueden ser toleradas.
- Existe un procedimiento de aprobación de perfiles de usuario, pero en algunos casos, si el procedimiento no se cumple en su totalidad, puede ser tolerado.

En los ejemplos previos, la tolerancia al riesgo se define usando métricas de TI o con la adhesión a procedimientos y políticas de TI definidos que son, a su vez, una traducción de los objetivos TI que necesitan ser alcanzados.

El apetito de riesgo y la tolerancia al riesgo van de la mano. La tolerancia al riesgo se define a nivel de empresa y se refleja en políticas establecidas por los ejecutivos; en niveles inferiores (tácticos) de la empresa, o en algunas instancias de la empresa, las excepciones pueden ser toleradas (o definidos diferentes umbrales), siempre y cuando a nivel de empresa la exposición total no exceda el apetito de riesgo establecido. Cualquier iniciativa de negocio

incluye un componente de riesgo, de forma que la dirección debería tener criterio para exceder los niveles de tolerancia al riesgo y perseguir nuevas oportunidades. En empresas en las que las políticas son más ‘grabados en piedra’ que ‘líneas en la arena’, puede haber una falta de agilidad e innovación para explotar nuevas oportunidades de negocio. De forma contraria, existen casos en los que las políticas se basan en requerimientos específicos legales, normativos o de la industria en los que lo apropiado es no tener tolerancia al riesgo en cuanto a su incumplimiento.

El apetito de riesgo y la tolerancia deberían ser definidos y aprobados por la alta dirección y comunicados claramente a todas las partes interesadas. Debería establecerse un proceso para revisar y aprobar cualquier excepción a dichos estándares. El apetito de riesgo es la traducción más estable de cuánto riesgo es aceptable con carácter general; la tolerancia al riesgo permite las excepciones individuales y justificadas. El apetito de riesgo y la tolerancia cambian con el tiempo. Nuevas tecnologías, nuevas estructuras organizativas, nuevas condiciones de mercado y muchos otros factores obligan a la empresa a reevaluar su cartera de riesgos a intervalos regulares, y también obligan a la empresa a reconfirmar su apetito de riesgos a intervalos regulares, provocando revisiones de la política de riesgos. A este respecto, una empresa también necesita comprender que cuanto mejor sea la gestión del riesgo, mayor será el riesgo que se puede asumir en la persecución de un retorno.

El coste de opciones de mitigación puede afectar a la tolerancia al riesgo; de hecho, podrían existir circunstancias en las que el impacto en coste/negocio de las opciones de mitigación excede las capacidades/recursos de la empresa, forzando de este modo una mayor tolerancia a una o más condiciones de riesgo. Por ejemplo, si una normativa establece que ‘la información sensible almacenada debe estar cifrada’, y no existiera una solución de cifrado viable o el coste de implementación de una solución tuviera un impacto extremadamente elevado, la empresa podría decidir aceptar el riesgo asociado al incumplimiento normativo.

Figura 69—¿Qué es un Indicador Clave de Riesgo?

Los indicadores de riesgo son métricas capaces de mostrar que la empresa está, o tiene una alta probabilidad de estar, sujeta a un riesgo que excede el apetito de riesgo definido. Estos son específicos para cada empresa, y su selección depende de un número de parámetros internos y externos, tales como el tamaño y complejidad de la empresa, si está operando en un mercado altamente regulado, y su enfoque estratégico.

Un indicador clave de riesgo (ICR/KRI – key risk indicator, en sus siglas en inglés) se caracteriza por ser altamente relevante y poseer una alta probabilidad de predecir o indicar un riesgo importante.

Círculo de Vida y Partes Interesadas	Estado del Ciclo de Vida	Parte Interesada Interna	Parte Interesada Externa	Descripción/Interés
	Planificación de la información	Comité de gestión de riesgos de la empresa		Elabora una descripción a alto nivel de los indicadores de riesgo necesarios para medir el apetito de riesgo de la empresa.
	Diseño de la información	Función de riesgos		Elabora los indicadores de riesgo en mayor detalle para llegar a una descripción detallada.
	Generación/ obtención de la información	Responsable de riesgos, analista de riesgos		Desarrolla los indicadores de riesgo con todo el detalle (identifica la información requerida) y asegura que estén listos para su uso (establece los flujos de aprovisionamiento de información).
	Uso/operación de la información: almacenamiento, compartición, uso	Comité de dirección, dirección ejecutiva, función de riesgos, propietarios de los procesos de negocio/director de informática-sistemas (CIO), cumplimiento, auditoría interna	Auditoría externa, regulador	Uso efectivo de los indicadores de riesgo.
	Supervisión de la información	Comité de dirección, comité de gestión de riesgos de la empresa (ERM), comité de auditoría, función de riesgos, propietarios de los procesos de negocio/director de	Auditoría externa	Supervisa los indicadores de riesgo para asegurar que se mantienen dentro de los límites definidos, de acuerdo al apetito de riesgo de la empresa.
	Eliminación de la información	Función de riesgos		Evaluá la relevancia de un indicador de riesgo oportunamente.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 69— Indicadores clave de Riesgo (cont.)

	Subdimensión de Calidad y Metas	Descripción—Hasta que punto la información es.....	Relevancia	Meta —Los indicadores de riesgo...
Intrínsecos	Exactitud	Correcta y fiable	Alta	Deben ser precisos y deberían articular los umbrales de forma precisa
	Objetividad	Objetiva, sin prejuicios e imparcial	Alta	Deberían estar basados en información objetiva—componentes medibles
	Credibilidad	Vista como cierta y creíble	Alta	Deberían indicar que las personas están convencidas de la correcta definición y la contribución a la percepción de la exposición al riesgo de la empresa
	Reputación	Vista como proveniente de una fuente veraz y creíble	Media	Las fuentes de información deberían citarse claramente, ser visibles para los usuarios y deberían provenir de una fuente fiable en la empresa
Objetivos	Relevancia	Aplicable y de ayuda para la tarea en cuestión	Alta	Deberían indicar que las personas se encuentran convencidas de su contribución a la percepción de la exposición de la empresa
	Integridad	Completa y tiene la suficiente profundidad y amplitud para la tarea en cuestión	Alta	Deberían contener todos los elementos clave que tienen influencia en el riesgo que el indicador está cuantificando
	Vigencia	Suficientemente actualizada para la tarea en cuestión	Alta	Las fuentes individuales deben estar tan actualizadas como sea posible para disponer de una referencia actualizada de la exposición
	Cantidad de Información	Adecuada para la tarea en cuestión	Baja	Dependen del número de elementos individuales
	Representación concisa	Representada de forma compacta	Baja	Son métricas y, por tanto, se representan de forma compacta por un número. Por otra parte, la explicación del indicador y las consecuencias potenciales pueden ser exhaustivas.
	Representación consistente	Presentada en el mismo formato	Media	Se representan con un formato estándar, aunque se pueden llevar a cabo modificaciones específicas para algunos indicadores
	Interpretabilidad	Con lenguaje, símbolos y unidades adecuadas, y con definiciones claras	Alta	La composición y los objetivos/significado deberían estar claros para el público objetivo
	Comprensión	Fácilmente comprensible	Alta	La composición y los objetivos/significado deberían estar claros para el público objetivo
	Manejabilidad	Fácil de manejar y aplicar a las diferentes tareas	Baja	Sólo pueden ser representados en un número limitado de formas, y un cambio en la presentación no debería tener impacto en cómo el indicador evalúa la exposición
Contextual y Representativo	Disponibilidad	Disponible cuando sea necesaria, o recuperable de forma fácil y rápida	Media	Debería estar disponible en todo momento, ya que algunos de ellos podrían estar vinculados a indicadores de negocio de alta fluctuación (p.ej., la Bolsa)
	Acceso restringido	Restringida apropiadamente a las partes autorizadas	Baja	Acceso: <ul style="list-style-type: none"> • Todo el mundo puede consultar los indicadores generales. El acceso a indicadores más específicos está restringido. • Un grupo seleccionado de personas dentro de la empresa recopilará la información necesaria y cumplimentará los indicadores. • El comité de riesgos de la empresa (ERM) y la función de riesgos tendrán derechos de acceso de modificación para la composición de los indicadores.
Seguridad				

Figura 69—Indicadores clave de riesgo (cont.)

	Atributo	Descripción	Valor
Buenas prácticas	Físico	Soporte de la información	El soporte de la información para los indicadores de riesgo puede ser un documento electrónico y/o impreso.
	Empírico	Canal de acceso a la información	Los indicadores de riesgo son accesibles a través del portal de gestión de riesgos de la empresa (con restricción de acceso implementada).
	Sintáctico	Código/lenguaje	Los indicadores de riesgo contienen métricas y explicaciones sobre su objetivo/significado.
	Semántico	Tipo de información	Composición fija de un indicador de riesgo.
		Vigencia de la información	Los indicadores de riesgo deberían estar actualizados para ser usados en la organización.
		Nivel de información	Los indicadores de riesgo recogen datos de toda la empresa para mostrar la exposición de un determinado proceso, producto o departamento.
	Pragmático	Periodo de retención	Mientras el indicador todavía proporcione correctamente el grado de exposición —esto es, que siguen presentes todos los elementos que son factores de influencia clave en el grado de exposición que se está midiendo— éste debe seguir retenido.
		Estado de la información	La información producida debería estar actualizada.
		Novedad	Es vigente, ya que utiliza el último estado de todos los elementos en el indicador.
		Contingencia	Esta información depende de que la siguiente información esté disponible y sea comprensible para el usuario: <ul style="list-style-type: none"> • Apetito de riesgo de la empresa • Composición del indicador de riesgo • Indicación que ofrece del apetito de riesgo de la empresa
	Social	Contexto	Esta información es útil para verificar si una cierta exposición excede el apetito de riesgo definido.
Vínculo a otros catalizadores			
Procesos	<p>Los indicadores de riesgo son un resultado de las actividades de los procesos:</p> <ul style="list-style-type: none"> • EDM03.01 Evaluar la gestión de riesgos. • EDM03.03 Supervisar la gestión de riesgos. <p>Los indicadores de riesgo son una entrada para las actividades de los procesos:</p> <ul style="list-style-type: none"> • APO12.03 Mantener un perfil de riesgo. • APO12.04 Expresar el riesgo. 		
Estructuras Organizativas	<p>Los siguientes figuras son responsables y ejecutores (parcialmente) de producir la información:</p> <ul style="list-style-type: none"> • Responsable: función de riesgos • Ejecutor: responsable de riesgos, analista de riesgos • Consultado/Informado: Comité de dirección, comité de gestión de riesgos de la empresa (ERM), comité de auditoría, propietarios de los procesos de negocio/ director de informática-sistemas (CIO), auditoría interna (ver también las partes interesadas) 		
Infraestructura, Aplicaciones y Servicios	<p>Los indicadores de riesgo se producen en el portal de gestión de riesgos (herramienta GRC – Gobierno, gestión de Riesgo y Cumplimiento).</p>		
Personas, Habilidades y Competencias	<p>Los indicadores de riesgo requieren de las siguientes competencias:</p> <ul style="list-style-type: none"> • Capacidad analítica • Pensamiento lateral (pensar creativamente) • Comprensión técnica • Experiencia en riesgo • Conocimiento de la organización y el negocio 		
Cultura, Ética y Conducta	<p>Los indicadores de riesgo requieren de los siguientes comportamientos:</p> <ul style="list-style-type: none"> • ICR se utilizan como una alerta temprana • Se actúa sobre los indicadores de riesgo o eventos que están fuera de la tolerancia • Las tendencias de riesgo se notifican a la dirección • La responsabilidad del riesgo es aceptada por la empresa • Reconocimiento de la exposición • Comportamientos transparentes • Mostrar esfuerzo para entender lo que el riesgo es para cada grupo de interés y su impacto en sus objetivos 		
Principios, Políticas y Marcos de Trabajo	<p>Principios relacionados:</p> <ul style="list-style-type: none"> • Establecer la actitud de la alta dirección (“tone at the top”) y la responsabilidad • Promover una comunicación clara y abierta 		

Indicadores clave de riesgo

Cualquier métrica que pueda ser usada para describir y seguir un riesgo es un indicador de ese riesgo. Los indicadores de riesgo son específicos de cada empresa. Hay muchos indicadores de riesgo disponibles y algunos son más apropiados para algunas empresas específicas. Su selección depende de un número de parámetros en el medio interno y externo, como el tamaño y la complejidad de la empresa, si está operando en un mercado altamente regulado, y el foco de su estrategia. Se debe tener en cuenta los siguientes aspectos (entre otros) en el proceso de identificación de los indicadores de riesgo:

- Considerar los diferentes grupos de interés en la empresa. Los indicadores de riesgo no deben centrarse únicamente en la visión operativa o en la vertiente estratégica del riesgo. Los indicadores de riesgo pueden y deben ser identificados por todas las partes interesadas. La participación de las partes interesadas adecuadas en la selección de los indicadores de riesgo también garantizará que sean más aceptados y mejor asumidos.
- Realizar una selección equilibrada de los indicadores de riesgo, que cubra los indicadores reactivos (que indican riesgo después de haber ocurrido los eventos), indicadores preventivos (que indican qué capacidades existen para prevenir que se produzcan los eventos) y tendencias (que analizan los indicadores en el tiempo o la correlación de los indicadores para una mejor percepción). Asegurarse de que los indicadores seleccionados profundizan hasta a la causa raíz de los acontecimientos (indicativos de la causa raíz y no sólo de los síntomas).

Una empresa puede desarrollar un amplio conjunto de indicadores que sirvan como indicadores de riesgo; sin embargo, no es ni posible ni viable mantener el conjunto completo de métricas como ICR. Los ICR se diferencian por ser de gran relevancia y por poseer una alta probabilidad de predecir o indicar un riesgo importante. Los criterios para seleccionar ICR incluyen:

- **Impacto** – Los indicadores para riesgos de alto impacto empresarial son más propensos a ser ICR.
- **Esfuerzo** (de implementar, medir y reportar) - Para los diferentes indicadores que son equivalentes en cuanto a sensibilidad, es preferible el que es más fácil de medir.
- **Fiabilidad** - El indicador debe poseer una alta correlación con el riesgo y ser un buen predictor o medidor del resultado.
- **Sensibilidad** - El indicador deberá ser representativo de los riesgos e indicar con precisión las variaciones en el riesgo.

Para ilustrar la diferencia entre la fiabilidad y la sensibilidad en la lista anterior usaremos el ejemplo de un detector de humo. Fiabilidad significa que el detector de humo hará sonar una alarma siempre que haya humo, y la sensibilidad significa que el detector de humo hará sonar la alarma precisamente cuando se alcanza un determinado umbral de densidad de humo.

El conjunto completo de ICR también debe equilibrar los indicadores de riesgo y los de causa raíz, así como los de impacto en el negocio. La selección del sistema correcto de ICR proporcionará los siguientes beneficios a la empresa:

- Proporcionar una alerta temprana (a futuro) de que un alto riesgo está surgiendo para que la dirección pueda tomar acciones proactivas (antes de que el riesgo genere una pérdida)
- Proporcionar una visión retrospectiva de los eventos de riesgo que se han producido, lo que permite dar respuestas y mejorar la gestión
- Habilitar la documentación y el análisis de las tendencias
- Proporcionar una indicación del apetito de riesgo de la empresa mediante el establecimiento de métricas (es decir, los umbrales de ICR)
- Aumentar la probabilidad de alcanzar los objetivos estratégicos de la empresa
- Ayudar a la optimización continua del gobierno del riesgo y la gestión del entorno

Algunos de los desafíos comunes que encontramos cuando se implementan con éxito ICR incluyen:

- Los ICR no están vinculados a elementos específicos de riesgo
- Los ICR son a menudo incompletos o inexactos en la especificación, es decir, demasiado genéricos
- Falta de alineación entre el riesgo, la descripción del ICR y la métrica del ICR
- Exceso de ICR
- Los ICR son difíciles de medir
- Dificultad para agregar, comparar e interpretar sistemáticamente ICR a nivel empresarial

Debido a que el ambiente interno y externo de la empresa está en constante cambio, el entorno de riesgo también es muy dinámico, y necesitará que el conjunto de ICR se actualice periódicamente. Cada ICR estará relacionado con el apetito y tolerancia al riesgo de manera que se puedan definir niveles de activación. Esto permitirá a las partes interesadas tomar las medidas adecuadas en el momento oportuno.

Además de indicar riesgo, los ICR son particularmente importantes durante la comunicación del riesgo. Facilitan el

diálogo sobre los riesgos dentro de la empresa, en base a hechos claros y medibles. Al mismo tiempo, los ICR se pueden utilizar para mejorar la concienciación sobre el riesgo en toda la empresa, debido a la naturaleza real de estos indicadores.

En el marco de COBIT 5, el gobierno y la gestión adecuada se consiguen mediante los catalizadores; debido a que se dispone de un modelo genérico de rendimiento de los catalizadores todos los componentes de este modelo son candidatos para servir como ICR, por ejemplo:

- Todas las métricas relacionadas con el logro de las metas catalizadoras, p. ej. metas de proceso, metas de estructura organizativa
- Todas las métricas relacionadas con la aplicación de buenas prácticas para catalizadores, p. ej. la aplicación de prácticas de proceso
- Todas las métricas relacionadas con la gestión del ciclo de vida de los catalizadores
- Métricas combinadas, p. ej. los niveles de capacidad de proceso (según la norma ISO / IEC 15504 evaluaciones basadas en procesos)

Adicionalmente, el marco de trabajo COBIT 5 incluye también la cascada de metas con distintos niveles de métricas (proceso de negocio, proceso de TI, práctica) diseñadas para medir operaciones exitosas y los resultados de los procesos de TI como soporte del negocio. A partir de estas métricas puede hacerse una selección para indicar la calidad de las prácticas del proceso (o para el caso cualquier otro catalizador) puesto en marcha para mitigar el riesgo.

La **figura 70** contiene un ejemplo de algunos ICR posibles para las diferentes partes interesadas. Se utilizan indicadores preventivos y reactivos. Esta no es una tabla completa (ni pretende serlo), sino que ofrece al lector algunas sugerencias e inspiración para su propio conjunto de ICR.

Las partes interesadas que aquí se consideran son:

- Director de informática-sistemas (CIO) - Esta función requiere visión de los riesgos de TI para la empresa.
- Función de riesgos - La función de riesgos exige una visión amplia sobre los riesgos de TI de todo el negocio, pero se puede considerar que tiene un enfoque más operativo.
- Director general ejecutivo (CEO)/ Comité de dirección - Estas entidades requieren de una visión del riesgo agregada de alto nivel.

Figura 70—Ejemplos de ICR

Fuente ⁷	Categoría del evento	CIO	Función de riesgos	CEO/Comité de dirección
EDM02, APO02, APO05, BAI01	Eventos relacionados con las decisiones de inversión o de proyecto	<ul style="list-style-type: none"> • Porcentaje de proyectos en tiempo, en presupuesto • Número y tipo de desviaciones del plan tecnológico de infraestructuras 	<ul style="list-style-type: none"> • Porcentaje de proyectos de TI revisados y firmados con garantía de calidad (GC) que cumplan con las metas y los objetivos de calidad • Porcentaje de proyectos con beneficio definido de antemano 	<ul style="list-style-type: none"> • Porcentaje de las inversiones en TI que excedan o cumplan el beneficio empresarial predefinido • Porcentaje de los gastos de TI que tienen trazabilidad directa a la estrategia de negocio
EDM01, EDM02, APO02, APO05	Eventos relacionados con la participación en el negocio	Grado de aprobación de los propietarios de negocio de los planes estratégicos / tácticos de TI	Frecuencia de las reuniones con participación de dirigentes de la empresa donde se discute la contribución de TI al valor	Frecuencia de los informes o la asistencia de los CIO a las reuniones del comité de dirección en las que se discute la contribución de TI a los objetivos empresariales
APO13, DSS05	Seguridad	Porcentaje de usuarios que no cumplen con las normas de contraseña	Número y tipo de violaciones de acceso presuntas y reales	Número de incidentes (de seguridad) con impacto en el negocio
APO07, DSS01, DSS02, DSS03, DSS04, BAI08, MEA03	Acto involuntario del personal: Destrucción	<ul style="list-style-type: none"> • Número de niveles de servicio impactados por incidentes operacionales • Porcentaje de miembros de TI que completan el plan de formación anual 	<ul style="list-style-type: none"> • Número de incidentes causados por documentación de usuario/operacional y formación deficientes • Número de procesos críticos de negocio que dependen de TI y no están cubiertos por el plan de continuidad de TI 	<ul style="list-style-type: none"> • Coste del incumplimiento normativo de TI, incluyendo acuerdos legales y multas • Número de casos de incumplimiento normativo denunciados ante el comité de dirección o que causan comentarios públicos o situaciones embarazosas

⁷ La fuente indica las referencias de procesos de COBIT 5.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 71—Problemas y factores de riesgo emergente				
Los problemas y factores de riesgo emergente son información de una futura o posible combinación de control, valor y amenazas que plantean un nivel significativo de riesgo de TI futuro				
	Etapa del ciclo de vida	Parte interesada interna	Parte interesada externa	Descripción/Interés
Ciclo de vida e interesados	Planificación de la información	Comité de gestión de riesgos de la empresa (ERM), director de informática-sistemas (CIO), función de riesgos	Auditor externo, regulador	Elabora una descripción de alto nivel de los problemas y factores de riesgo emergente que se consideran relevantes para la empresa.
	Diseño de la información	Director de informática-sistemas (CIO), función de riesgos		Elabora los problemas y factores de riesgo emergente con más detalle para llegar a un conocimiento profundo.
	Generación/obtención de la información	Director de informática-sistemas (CIO), función de riesgos, propietarios de los procesos de negocio, oficina de gestión de proyectos, director de seguridad de la información (CISO), jefe de arquitectura, jefe de desarrollo, jefe de operaciones de TI, jefe de administración de TI, jefe de servicio, jefe de seguridad de la información, jefe de continuidad de negocio, oficial de privacidad		Elabora los problemas y factores de riesgo emergente en todo detalle (identifica la información organizacional necesaria) y asegura que estén listos para ser supervisados por las partes interesadas.
	Uso/operación de la información: almacenamiento, compartición, uso	Función de riesgos, director de seguridad de la información (CISO), jefe de servicio, director de informática-sistemas (CIO), jefe de arquitectura, jefe de desarrollo, jefe de operaciones de IT, jefe de seguridad de la información, propietarios de los procesos de negocio, oficina de gestión de proyectos, cumplimiento, auditoría, jefe de administración de TI, jefe de continuidad de negocio, oficial de privacidad, director de operaciones (COO), ejecutivos de negocio	Auditor externo, regulador	Supervisión efectiva de todas las partes interesadas de las nuevas amenazas identificadas como relevantes para la empresa.
	Supervisión de la información	Director de informática-sistemas (CIO), auditoría	Auditor externo	Registro de las observaciones por las partes interesadas en relación a los problemas y factores de riesgo emergente y actualización de la evaluación de las mismas en consecuencia.
	Eliminación de la información	Director de informática-sistemas (CIO), función de riesgos		Evaluá periódicamente la relevancia de los problemas y factores de riesgo emergente.

Figura 71— Problemas y factores de riesgo emergente (cont.)

Figura 71— Problemas y factores de riesgo emergente (cont.)				
Objetivos	Subdimensión de Calidad y Metas	Descripción—En la medida que la información es...	Relevancia	Meta—Factores y cuestiones de riesgo emergentes ...
	Exactitud	Correcta y fiable	Alta	La información origen tiene que ser precisa (confirmar a través de auditoría) y necesita ser procesada, analizada y presentada en la aplicación de gestión de riesgo de acuerdo a las reglas establecidas
	Objetividad	Objetiva, sin prejuicios e imparcial	Alta	La información se basa en hechos y comprobaciones verificables, utilizando el punto de vista de riesgo común establecido en toda la empresa
	Credibilidad	Vista como cierta y creíble	Media	Puede ser tan nuevo para la empresa, especialmente en los mercados de alta tecnología, que no todas las partes interesadas considerarán la información como verdadera o creíble
	Reputación	Vista como proveniente de una fuente veraz y creíble	Alta	La información origen se obtiene de fuentes competentes y reconocidas
	Relevancia	Aplicable y de ayuda para la tarea en cuestión	Media	Se estructura de acuerdo con el atributo "sintaxis", y será confirmado por el director de informática-sistemas (CIO) y el responsable de riesgos (CRO) (APO12) que la información es relevante
	Integridad	Completa y tiene la profundidad y amplitud suficiente para la tarea en cuestión	Alta	Se referirá a la empresa completa y al registro de riesgos completo
	Vigencia	Suficientemente actualizada para la tarea en cuestión	Alta	La información no debe tener una antigüedad superior a un mes
	Cantidad de información	Adecuada para la tarea en cuestión	Media	Tienden a tener poca información disponible cuando se identifica por primera vez
	Representación concisa	Representada de forma compacta	Alta	Será presentada de forma concisa; esto se consigue mediante la recopilación, procesamiento y análisis de los datos relacionados con los riesgos para toda la empresa y mediante la detección y presentación solamente de cuestiones y factores emergentes
Contextual y Representativo	Representación consistente	Presentada en el mismo formato	Media	Siempre se presentarán de acuerdo con la plantilla establecida
	Interpretabilidad	Con lenguaje, símbolos y unidades adecuadas y con definiciones claras	Baja	Será nuevo para muchas partes interesadas y es necesario que sea fácilmente comprensible y por tanto utilizar símbolos y unidades de uso común
	Comprendión	Fácilmente comprensible	Alta	Será nuevo para muchas partes interesadas y es necesario que sea fácilmente comprensible
	Manejabilidad	Fácil de manejar y aplicar a diferentes tareas	Media	Al principio será considerado aplicable en muchos dominios y por tanto necesitará ser descrito de manera que se pueda aplicar a todas las diferentes tareas a las que se refiere
Seguridad	Disponibilidad	Disponible cuando sea necesaria, o recuperable de forma fácil y rápida	Media	Deberán estar en todo momento a disposición de las partes interesadas afectadas; una falta de disponibilidad de 24 horas es aceptable en el caso de incidentes
	Acceso restringido	Restringida adecuadamente a las partes autorizadas	Alta	El acceso lo determina la función de riesgos y director de informática-sistemas (CIO), y se restringe como sigue: Acceso de escritura: función de riesgos y CIO Acceso de lectura: el resto de partes interesadas

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 71— Problemas y factores de riesgo emergente (cont.)

	Atributo	Descripción	Valor
Buenas Prácticas	Físico	Soporte de la información	El soporte para problemas y factores de riesgo emergente puede ser un documento electrónico o impreso.
	Empírico	Canal de acceso a la información	Los problemas y factores de riesgo emergente están accesibles en el portal de gestión de riesgos de la empresa (ERM) o impresos en un área definida.
	Sintáctico	Código/lenguaje	Los problemas y factores de riesgo emergente contienen los siguientes apartados: Datos históricos analizados Problemas emergentes Factores emergentes Relaciones de perfiles de riesgo
	Semántico	Tipo de información	Estilo del informe de riesgo
		Vigencia de la Información	Los problemas y factores de riesgo emergente analizan información nueva y reciente e incluso consideran potenciales estados futuros.
		Nivel de Información	Los problemas y factores de riesgo emergente recogen datos de toda la organización, procesan y analizan los datos para detectar problemas y factores de riesgo emergente.
	Pragmático	Periodo de retención	Los problemas y factores de riesgo emergente tendrán el mismo periodo de retención que los datos/información de riesgo sobre los que se documenta (teniendo en cuenta requisitos legales locales de retención).
		Estado de la información	Todas las instancias producidas durante los tres últimos meses son operativas; las más antiguas son datos históricos.
		Novedad	Los problemas y factores de riesgo emergente combinan otras fuentes de datos que constituyen una nueva instancia; por lo tanto, se trata de datos nuevos. Se actualizan semanalmente.
		Contingencia	Los problemas y factores de riesgo emergente se basan en la disponibilidad de la siguiente información y en que sea comprensible por el usuario: Eventos de riesgo en la totalidad de la empresa Apetito de riesgo de la empresa Problemas de riesgo de la empresa Factores de riesgo que aplican a la empresa Taxonomía de riesgos en uso en la empresa
	Social	Contexto	Los problemas y factores de riesgo emergente solo tienen sentido y serán usados el en contexto de riesgo de la función de gestión de riesgos de la empresa.
Vínculo a otros catalizadores			
Procesos		Los problemas y factores de riesgo emergente son un resultado de la actividad del proceso: APO12.06 Respuesta al riesgo. Los problemas y factores de riesgo emergente son una entrada de la actividad de los procesos: MEA02.07 Estudiar las iniciativas de aseguramiento. MEA02.08 Ejecutar las iniciativas de aseguramiento.	
Estructuras organizativas		Los siguientes roles son responsables y ejecutores de producir (parcialmente) la información: Responsable: director de informática-sistemas (CIO) Ejecutor: Función de riesgos, propietarios de los procesos de negocio, oficina de gestión de proyectos, director de seguridad de la información (CISO), jefe de arquitectura, jefe de desarrollo, jefe de operaciones de TI, jefe de administración de TI, jefe de servicio, jefe de seguridad de la información jefe de continuidad del negocio, oficial de privacidad.	
Infraestructura, Aplicaciones y Servicios		Los problemas y factores de riesgo emergente pueden ser producidos por una aplicación de gestión de riesgo y pueden ser usados por aplicaciones de gestión de servicio, monitoreo, conformidad y auditoría.	
Personas, Habilidades y Competencias		La generación y uso de este elemento de información requiere de una comprensión básica de los principios y habilidades de la gestión del riesgo.	
Cultura, Ética y Conducta		Las partes interesadas deben ser educadas para la determinación de cuestiones de riesgos emergentes.	
Principios, Políticas y Marcos de Trabajo		Principios relacionados: Conectados a los objetivos de la empresa Alineados con la función de riesgos de la empresa (ERM)	

Figura 72—Taxonomía de Riesgos

Una taxonomía de riesgos ofrece una comprensión clara de terminologías y escalas para usar en las discusiones y comunicaciones sobre riesgo entre los Agentes Interesados. Para usar la Taxonomía de riesgos en un universo de estos precisa el compromiso de todos los interesados.

También contiene métodos y procedimientos sobre gestión de riesgos aplicados a la empresa (Identificación Evaluación sobre controles, Monitoreo, etc.)

Ciclo de Vida e Interesados	Estadio Ciclo de Vida	Interesado Interno	Interesado Externo	Descripción/Interés
	Planificación Información	Comité ERM Función relativa a riesgos		Inicia y conduce la implementación y planificación
	Diseño Información	Función relativa a riesgos, Todos los otros interesados pueden ser contribuyentes potenciales al diseño		<ul style="list-style-type: none"> La Función relativa a riesgos ha de obtener su información de fuentes externas y las necesidades de los comités /Funciones relevantes Basándose en las entradas, la Función de gestión de riesgos diseña la taxonomía más apropiada.
	Producir/Preparar Información	Función relativa a riesgos		<ul style="list-style-type: none"> Desarrolla una taxonomía adaptada a las necesidades de la empresa, comprensible y utilizable por los interesados. La Función relativa a riesgos prepara la taxonomía basada en su diseño y la acuerda con los interesados relevantes
	Uso/Operación Información: Almacenar, compartir, Usar	Todos los Interesados, en particular: Comité Directivo, Comité ERM, Función relativa a riesgos, Ejecutivos, CIO, CISO	Auditor Externo, Agentes Reguladores	Para utilizarse por todos los interesados estableciéndose una visión común y una terminología sobre gestión de riesgo aplicada a toda la empresa.
	Monitorear Información	Función relativa a riesgos, Auditoría Interna	Auditor Externo	<ul style="list-style-type: none"> Función relativa a riesgos Monitoreo regular sobre la adecuación, completitud y precisión de información; evaluación semi-anual del rendimiento (MEAD01) y controles (MEA02) para mantener la información. Auditoría interna; validación anual del formato y nivel de contenido
	Desechar Información	Función relativa a riesgos		Para disponer de una única taxonomía deben eliminarse las palabras obsoletas en caso de que se crean nuevas.
	Subdimensión de Calidad y Objetivos	Descripción—Hasta qué punto la información es...	Relevancia	Objetivo—La Taxonomía de riesgo...
Objetivos	Intrínseca	Exactitud	Medio	Es precisa pero no académica
		Objetividad	Alto	Es precisa y clara para todos los interesados
		Credibilidad	Alto	Es entendida como única verdad
		Reputación	Bajo	Está ajustada a la empresa
	Contextual y Formato	Relevancia	Medio	Tiene una terminología precisa y se comprenden las interdependencias
		Integridad	Alto	Clarifica las áreas clave y relaciones, así como los procedimientos a aplicar.
		Actualidad	Bajo	Se adecúa a las necesidades en información y guía de los interesados y las actualizaciones frecuentes son poco probables
		Nivel de información	Bajo	El nivel de detalle (definido durante el diseño) es apropiado para el usuario de la taxonomía
		Presentación concisa	Medio	Es corta y clara
		Presentación consistente	Alto	Está acordada en un panorama general.
		Inteligible	Alto	Es clara para todos los interesados
		Comprensible	Alto	Los interesados lo aplican de forma consistente, mostrando que la información es comprendida fácilmente.
		Manipulación	Medio	Con frecuencia reutiliza definiciones, símbolos, etc,...lo cual es un signo de que la información puede aplicarse a diferentes tareas de la empresa.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 72—Taxonomía de Riesgos								
Buena Práctica	Subdimensión de Calidad y Metas		Descripción—Hasta qué punto la información es.....	Relevancia	Objetivo—La Taxonomía de riesgo...			
	Seguridad	Disponibilidad	Disponible cuando se requiere, o fácilmente y rápidamente extraíble	Baja	Está siempre disponible para todos los interesados; en caso de incidentes se puede aceptar una indisponibilidad de 24 horas.			
	Acceso restringido	Apropiadamente restringido a las partes autorizadas		Baja	Está disponible para todos los interesados			
Atributo		Descripción	Valor					
Físico		Información soporte/medio	El soporte de la información de la taxonomía de riesgo precisa estar en formato electrónico o en un sistema de información (por ejemplo un cuadro de mando) y puede ser tener soporte impreso					
Empírico		Información canal acceso	La taxonomía de riesgos es accesible mediante el portal ERM o impresa					
Sintáctico		Código/lenguaje	La taxonomía de riesgo contiene las subpartes siguientes: - Análisis de datos históricos - Temas emergentes - Factores emergentes - Relación del perfil de riesgos					
		Tipo información	La taxonomía de riesgo contiene una lista de terminología comprensible para el conjunto de la empresa. También presenta un resumen de las escalas de riesgo, métodos y procedimientos que se han de utilizar.					
		Actualidad información	La información está actualizada para ser utilizada por la organización					
		Nivel información	La taxonomía de riesgo cubre todas las terminologías, escalas, métodos y procedimientos que son aplicables a toda la empresa.					
Pragmático		Periodo retención	Los ítems de información se mantienen mientras las terminologías/ escalas/ métodos /relaciones descritos son validos para la empresa (además teniendo en cuenta los requisitos legales respecto a su conservación)					
		Estado información	La información resultante debe ser actual					
		Novedad	La definición de la taxonomía de riesgo es nueva; no obstante no se esperan excesivos cambios durante el ciclo de vida de la empresa					
		Contingencia	La taxonomía de riesgo depende de la comprensión de la información siguiente por parte del usuario: • Terminología empleada • Escalas utilizadas • Métodos y procesos					
			Si se precisa una orientación, el departamento de riesgos de la empresa debe tener capacidad para dar a los usuarios un soporte adicional					
Social		Contexto	La taxonomía de riesgo solo es significativa y para usarse en un contexto de Gestión de riesgo empresarial.					
Enlace a otros Facilitadores								
Procesos		La Taxonomía de riesgo es una <u>salida</u> de las tareas de gestión:: • EDM03.01 Evaluar la gestión de riesgo. • EDM03.02 Gestión directa del riesgo.						
		La Taxonomía de riesgo es una <u>entrada</u> de las tareas de gestión • APO12.01 Recolección de datos. • APO12.02 Analizar riesgo • APO12.03 Mantener un perfil de riesgo. • APO12.04 Articular riesgo. • APO12.05 Definir un portfolio de acciones de gestión del riesgo • APO12.06 Responder al riesgo						
Estructuras Organizativas		Bajo la responsabilidad de la función de gestión de riesgo, el grupo correspondiente de la empresa es responsable del ajuste de la taxonomía de riesgo El resto de interesados de la empresa necesitan comprender y usar la taxonomía						
Infraestructura, Aplicaciones y Servicios		La función de gestión de riesgo y el grupo correspondiente de riesgo de la empresa, mantienen manualmente la taxonomía de riesgo vía el portal de gestión de riesgo						

Figura 72—Taxonomía de Riesgos (cont.)

Enlace a otros Facilitadores	
Personas, Habilidades y Competencias	Para encajar la taxonomía de riesgo, el grupo de gestión de riesgo precisa una comprensión técnica, experiencia en riesgo y conocimiento organizativo y del negocio. La taxonomía de riesgo debe explicarse de tal manera que el usuario tan solo precise una comprensión básica de gestión de riesgos para comprender la terminología, escalas, métodos y procedimientos
Cultura, Ética y Conducta	La disponibilidad de la taxonomía de riesgo da soporte a la transparencia de tendencias en riesgo así como a una cultura de conocimiento del riesgo
Principios, Políticas y Esquemas trabajo	Principio relacionado: • Aproximación consistente

Figura 73—Análisis Impacto en el Negocio (BIA)

Un Análisis del Impacto en el Negocio (BIA) es una actividad para desarrollar una comprensión compartida de los procesos de negocio que son específicos de cada unidad de negocio y críticos para la supervivencia de la empresa. El resultado de esta actividad es un documento BIA escrito.

Ciclo de Vida e Interesados	Estadio Ciclo de Vida	Interesado Interno	Interesado Externo	Descripción/Interés
	Planificación Información	Consejo de Administración, COO	Audit Externo, Regulador	Determina el ámbito de los procesos de negocio y el análisis esperado
	Diseño Información	Propietarios de procesos de negocio, gestor de la continuidad de negocio, responsable operaciones TI, gestor de servicios		Prepara el análisis identificando la información necesaria para su realización
	Producir/Preparar Información	COO, Propietarios de procesos de negocio, gestor de la continuidad de negocio, responsable operaciones TI, gestor de servicios, función relativa a riesgo		Realiza el análisis recopilando la información identificada y valorándola para determinar el impacto sobre los procesos de negocio.
	Uso/Operación Información: Almacenar, compartir, Usar	COO, Propietarios de procesos de negocio, CIO, función relativa a riesgo, responsable arquitectura, responsable operaciones TI, gestor de la continuidad de negocio	Audit Externo, Regulador	Confecciona el documento BIA disponible para todos los interesados relevantes.
	Monitorear Información	Gestor de la continuidad de negocio, función relativa a riesgo, Auditores.	Audit Externo	Monitorea los parámetros del análisis y lo actualiza si es necesario
	Desechar Información	COO, Propietarios de procesos de negocio, gestor de la continuidad de negocio, función relativa a riesgo		Desecha el documento BIA si la información ya no es relevante para la empresa
	Subdimensión de Calidad y Objetivos	Descripción—Hasta qué punto la información es.....	Relevancia	Objetivo—El BIA...
Metas Intrínsecas	Exactitud	Correcto y fiable	Alto	Su fuente de información precisa ser correcta (confirmado mediante los ejecutivos del negocio y ha de ser procesada, analizada y presentada en la gestión de riesgo y/o gestión de continuidad del negocio y/o aplicación GRC, según unas reglas prefijadas)
	Objetividad	No sesgada, sin prejuicios e imparcial	Alto	Su información se basa sobre hechos verificables, usando la visión de negocio común, establecida en la empresa.
	Credibilidad	Considerada como verdadera y fiable	Medio	No debe contener información contradictoria
	Reputación	Considerada que procede de fuentes verdaderas y fiables	Alto	Su fuente de información procede de los propietarios de los procesos de negocio, ejecutivos y otras fuentes competentes y reconocidas.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 73—Análisis Impacto en el Negocio (BIA) (cont.)

	Subdimensión de Calidad y Objetivos	Descripción—Hasta qué punto la información es...	Relevancia	Objetivo—El BIA...
Metas Contextual y Formato	Relevancia	Aplicable y útil para las tareas a realizar	Alto	Debe estructurarse según el atributo “sintáctico”, y el COO y CRO (BAI04) deben confirmar que la información es relevante
	Integridad	Existe y tiene una profundidad y extensión acorde a las tareas a realizar	Alto	Debe cubrir toda la empresa, todos los procesos/productos principales y todo el registro de riesgos.
	Actualidad	Suficientemente actualizado para las tareas a realizar	Alto	No debe tener una antigüedad mayor que seis meses
	Nivel de información	Apropiado para las tareas a realizar	Medio	La relevancia de la información es más importante que la cantidad, pero sin suficientes detalles el BIA será difícil de seguir por los interesados que no están involucrados en la preparación del análisis
	Presentación concisa	Presentado de forma compacta	Alto	La información debe presentarse de forma concisa, esto resulta de recopilar, procesar, analizar, evaluar los datos relativos al BIA respecto a toda la empresa
	Presentación consistente	Presentado en el mismo formato	Alto	Debe presentarse siempre siguiendo las plantillas actuales
	Inteligible	En un lenguaje apropiado, los símbolos, unidades y definiciones son claros.	Alto	Deberá distribuirse por toda la empresa llegando a los interesados relevantes, los cuales no están familiarizados con los aspectos descritos
	Comprensible	Fácilmente comprensible	Medio	Deberá distribuirse por toda la empresa llegando a los interesados relevantes, los cuales no están familiarizados con los aspectos descritos
	Manipulación	De fácil manipulación y aplicable a diferentes tareas	Bajo	Se focaliza sobre áreas específicas de la empresa y así probablemente solo afectará a un número seleccionado de tareas.
	Disponibilidad	Disponible cuando se requiere, o fácilmente y rápidamente extraíble	Alto	Debe estar siempre disponible para sus interesados; una indisponibilidad es aceptable en caso de incidentes
Seguridad	Acceso restringido	Apropiadamente restringido a las partes autorizadas	Alto	<p>El acceso está determinado por el COO, función de gestión de riesgo y gestor de continuidad del negocio y está restringido:</p> <ul style="list-style-type: none"> • Acceso escritura: COO, propietarios procesos de negocio, función de gestión de riesgo y gestor de continuidad del negocio. • Acceso lectura: toda la empresa
	Atributo	Descripción	Valor	
	Físico	Información soporte/medio	El soporte de la información del BIA puede estar en formato electrónico o en un documento impreso	
	Empírico	Información canal acceso	El BIA es accesible mediante el portal de gestión empresarial o impreso en una localización determinada	
	Sintáctico	Código/lenguaje	<p>El BIA contiene los apartados siguientes:</p> <ul style="list-style-type: none"> • Fuentes de datos relativos a la continuidad de negocio • Escenarios de riesgo • Funciones y procesos críticos • Análisis de vulnerabilidades 	
	Semántico	Tipo información	Informe de riesgo	
		Actualidad información	Para evaluar el impacto, el BIA maneja la información más reciente disponible	
		Nivel información	El BIA recopila datos de toda la empresa y los analiza	

Figura 73—Análisis Impacto en el Negocio (BIA) (cont.)

	Atributo	Descripción	Valor
Buena Práctica	Pragmático	Periodo retención	El BIA ha de mantenerse tanto tiempo como los datos/información sobre los cuales informa de necesidades de riesgo se mantienen actuales (y considerando los requerimientos legales)
		Estado información	Todas las instancias producidas en los últimos seis meses son operacionales, las anteriores son datos históricos
		Novedad	El BIA combina muchas otras fuentes de datos que constituyen una nueva instancia, por ello, son datos nuevos. Se actualiza con una periodicidad cuatrimestral
		Contingencia	El BIA se apoya en la información siguiente, que es comprensible y disponible para el usuario: <ul style="list-style-type: none"> • Continuidad de negocio • Impacto en el negocio • Escenarios de riesgo • Funciones y procesos críticos • Análisis de vulnerabilidades • Amenazas potencialmente disruptivas • Eventos de riesgo en toda la empresa relacionados con la continuidad del negocio • Tolerancia al riesgo de la empresa • Perfil de riesgo
	Social	Contexto	El BIA solo es adecuado y debe usarse en un contexto de continuidad empresarial y gestión de riesgo
Enlace a otros Facilitadores			
Procesos	El BIA es la salida de las actividades y procesos: <ul style="list-style-type: none"> • BAI04.02 Evaluación de riesgo de negocio. • DSS04.02 Mantenimiento de una estrategia de continuidad El BIA es la entrada de las actividades y procesos <ul style="list-style-type: none"> • APO12.02 Analizar riesgos. 		
Estructuras Organizativas	Los roles siguientes han de rendir cuentas y ser responsables (parcialmente) de la producción de la información: <ul style="list-style-type: none"> • Rendir cuentas: COO • Responsable: propietarios de procesos de negocio, gestor de continuidad del negocio, CIO, función de gestión de riesgo, responsable arquitectura, responsable operaciones TI 		
Infraestructura, Aplicaciones y Servicios	El BIA puede resultar de una aplicación de continuidad de negocio, de gestión de riesgo o de GRC y puede utilizarse por aplicaciones de gestión de servicios, monitoreo, cumplimiento normativo y auditoría		
Personas, Habilidades y Competencias	La preparación y uso de un BIA requiere una comprensión básica de los principios y habilidades de continuidad de negocio y gestión de riesgos		
Cultura, Ética y Conducta	Los interesados deben formarse en la comprensión y la realización de acciones adecuadas sobre el BIA		
Principios, Políticas y Esquemas trabajo	Principios relacionados: <ul style="list-style-type: none"> • Alineación con ERM • Balance coste/beneficio del riesgo TI 		

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 74—Evento de Riesgo

Un evento de riesgo es algo que puede ocurrir con una frecuencia desconocida en un lugar y tiempo futuros, también desconocidos, y que tendrá un impacto sobre el alcance de los objetivos empresariales.

	Estadio Ciclo de Vida	Interesado Interno	Interesado Externo	Descripción/Interés
Ciclo de Vida e Interesados	Planificación Información	Comité ERM, CIO, Función relativa a riesgos	Audit Externo, Regulador	Dermina el alcance de los eventos de riesgo. Tanto internos (Para qué procesos de negocio se monitorearan los eventos de riesgo?), como externos (Qué categorías externas o factores se han de considerar?)
	Diseño Información	CIO, Función relativa a riesgos		Diseñar y detallar que información se requiere cuando se identifica un evento de riesgo
	Producir/Preparar Información	CIO, Función relativa a riesgos, propietarios de procesos de negocio, oficina de gestión de proyectos, CISO, responsable de arquitectura, responsable de desarrollo, responsable de operaciones TI, responsable de administración TI, gestores servicios, gestor de seguridad de la información, gestor continuidad de negocio, responsale privacidad.		Identificar en su ámbito eventos de riesgo i recoger toda la información requerida sobre estos
	Uso/Operación Información: Almacenar, compartir, Usar	Toda la empresa	Audit Externo, Regulador	Utilizar el evento de riesgo identificado y realizar las acciones oportunas
	Monitorear Información	CIO, auditores	Audit Externo	Monitorear regularmente la evolución del evento de riesgo y verificar la exactitud de la información
	Desechar Información	CIO, Función relativa a riesgos		Borrar el evento de riesgo si ya no es relevante
Objetivos	Subdimensión de Calidad y Objetivos	Descripción—Hasta qué punto la información	Relevancia	Objetivo—El Evento de Riesgo...
	Exactitud	correcta y fiable	Alto	su fuente de información precisa ser correcta (confirmarlo mediante auditoria) y ha de ser procesada, analizada y presentada en la aplicación de gestión de riesgo de acuerdo con unas reglas fijadas.
	Objetividad	no sesgada, sin prejuicios e imparcial	Alto	su información se basa en hechos verificables y substanciones, usando la visión de riesgo común establecida en toda la empresa.
	Credibilidad	considerada como verdadera y fiable	Medio	cuento trata con muchos "desconocidos" puede no considerarse creible. Esto puede evitarse teniendo muchas fuentes (de confianza) sustentando las suposiciones. Los rangos y variables utilizados para mostrar la magnitud de los incidentes han de estar en un formato que la audiencia pueda comprender.

Figura 74—Evento de Riesgo (cont.)

Subdimensión de Calidad y Objetivos		Descripción—Hasta qué punto la información es...	Relevancia	Objetivo—El Evento de Riesgo...
Objetivos Contextual y Formato	Reputación Relevancia	Considerada que procede de fuentes verdaderas y fiables	Alto	Sus fuentes de información son competentes y reconocidas
		Aplicable y útil para las tareas a realizar	Medio	La información debe estructurarse según el atributo "sintaxis" y el CIO y la función relativa a riesgos (APO12) deben confirmar que la información es relevante.
	Integridad	Existe y tiene una profundidad y extensión acorde a las tareas a realizar	Alto	La información necesaria se determinará en el diseño, y precisa estar alineada con las necesidades de los usuarios en este aspecto.
	Actualidad	Suficientemente actualizado para las tareas a realizar	Alto	No debe ser superior a tres meses
	Nivel de información	Apropiado para las tareas a realizar	Bajo	Tiene muchos "desconocidos" que puedan imposibilitar recoger bastante información sobre el evento de riesgo.
	Presentación concisa	Presentado de forma compacta	Alto	Debe presentarse de forma concisa, esto se consigue recopilando, procesando y analizando los datos relacionados con riesgo en toda la empresa y presentando solo los eventos de riesgo relevantes
	Presentación consistente	Presentado en el mismo formato	Medio	Debe presentarse siempre formateado respecto a la plantilla actual
	Inteligible	En un lenguaje apropiado, los símbolos, unidades y definiciones son claros.	Medio	Y la información relacionada necesitan ser expresadas en términos que sean de comprensión amplia, ya que los eventos de riesgo han de ser utilizados por un amplio rango de trabajadores
	Comprensible	Fácilmente comprensible	Medio	Y la información relacionada necesitan ser expresadas en términos que sean de comprensión amplia, ya que los eventos de riesgo han de ser utilizados por un amplio rango de trabajadores
	Manipulación	De fácil manipulación y aplicable a diferentes tareas	Medio	Puede tener un gran impacto sobre la empresa, y por ello precisa ser descrito de tal manera que sea aplicable a las diferentes tareas sobre las que puede impactar el evento de riesgo
Seguridad	Disponibilidad	Disponible cuando se requiere, o fácil y rápidamente extraíble	Medio	Sus ítems deben estar disponibles para sus interesados, una indisponibilidad de 24 horas es aceptable en caso de incidentes
	Acceso restringido	Apropiadamente restringido a las partes autorizadas	Alto	El acceso al evento de riesgo está determinado por la función de gestión de riesgos y el CIO, y está restringida como sigue: <ul style="list-style-type: none"> • Acceso escritura: Función gestión de riesgos y CIO • Acceso lectura: Todos los otros interesados

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 74—Evento de Riesgo (cont.)			
Good Practice	Atributo	Descripción	Valor
	Físico	Información soporte/medio	El soporte de la información del evento de riesgo puede estar en formato electrónico o en un documento impreso.
	Empírico	Información canal acceso	El evento de riesgo es accesible en el portal ERM o impreso y ubicado en una localización precisa
	Sintáctico	Código/lenguaje	El evento de riesgo contiene las subpartes siguientes: <ul style="list-style-type: none">• Fuentes de datos relacionados con riesgos• Relaciones de perfiles de riesgo
	Semántico	Tipo información	Formato predefinido en un informe de riesgo de estilo resumen
		Actualidad información	El evento de riesgo analiza datos históricos y actuales y hace suposiciones sobre futuros eventos y estados
		Nivel información	Los datos se recogen de la totalidad de la empresa, y posteriormente se procesan y analizan para identificar los eventos de riesgo.
	Pragmático	Periodo retención	El evento de riesgo ha de ser conservado tanto tiempo como el evento sobre el que reporta riesgo precisa ser retenido (y teniendo en cuenta los requerimientos legales al respecto)
		Estado información	Todas las instancias producidas en los últimos 6 meses son operacionales; las anteriores son datos históricos, a menos que la aplicabilidad sea reconfirmada
		Novedad	El evento de riesgo combina muchas otras fuentes de datos constituyen una nueva instancia; por tanto, se trata de nuevos datos. Se actualiza semanalmente.
		Contingencia	El evento de riesgo se apoya sobre la información siguiente, la cual dispone y comprende el usuario: <ul style="list-style-type: none">• Eventos relacionados con riesgo en toda la empresa• Tolerancia al riesgo de la empresa• Perfil de riesgo• Taxonomía de riesgo en uso
	Social	Contexto	El evento de riesgo solo es significativo y se ha de usar en un contexto de ERM de riesgo
Enlace a otros Facilitadores			
Procesos	<p>El evento de riesgo es una <u>salida</u> de la actividad:</p> <ul style="list-style-type: none"> • APO12.01 Recoger datos <p>El evento de riesgo es una <u>entrada</u> para la actividad:</p> <ul style="list-style-type: none"> • Internas 		
Estructuras Organizativas	<p>Los roles siguientes han de rendir cuentas y responsables (parcialmente) en la producción de la información:</p> <ul style="list-style-type: none"> • Rendir cuentas: CIO • Responsables: Función de gestión de riesgo, propietarios de procesos de negocio, oficina de gestión de proyectos, CISO, responsable arquitectura, responsable operaciones TI, responsable administración TI, gestor servicios, gestor seguridad de la información, gestor continuidad de negocio, responsable privacidad. 		
Infraestructura, Aplicaciones y Servicios	Este ítem de información puede ser producido por la aplicación de gestión de riesgo y ser usado por gestión de servicios, monitoreo, cumplimiento normativo y aplicaciones de auditoría		
Personas, Habilidades y Competencias	La generación y uso de un evento de riesgo precisa de una comprensión básica de los principios y habilidades de gestión de riesgo.		
Cultura, Ética y Conducta	Los interesados deben formarse en la determinación de los eventos de riesgo		
Principios, Políticas y Esquemas trabajo	<p>Principios relacionados:</p> <ul style="list-style-type: none"> • Conexión a objetivos de la empresa • Alineación con ERM 		

Figura 75— Matriz de Actividad de Control y Riesgo (RCAM)

La matriz de Actividad de Control y Riesgo (RCAM de las siglas en inglés risk and control activity matrix) es un documento que contiene los riesgos identificados y su clasificación, así como las actividades de control que responden a cada riesgo, la descripción de su diseño y valoración de su efectividad operativa.

	Etapa del Ciclo de Vida (o proceso)	Propietario Interno	Propietario Externo	Descripción/Stake
Ciclo de vida y propietarios	Planificación de la Información	Comité ERM		Valida y refuerza la aplicabilidad de la RCAM como una herramienta de gestión del riesgo.
	Diseños de la Información	Función del riesgo		Identifica las áreas/procesos donde una RCAM podrá aplicarse.
	Construcción / adquisición de la información	Gestor del Riesgo, analistas del riesgo, expertos técnicos, propietarios de procesos de negocio, cumplimiento		Detalla el riesgo y diseña las acciones de control para cada proceso donde la RCAM se ha instalado.
	Utilización de la Información: almacenamiento, compartición, uso	propietarios de procesos de negocio, cumplimiento, auditoría interna	Auditor externo, regulador	Los propietarios de procesos de negocio serán los responsables de asegurar que las acciones de control son llevadas a cabo como se diseñaron y resolverán cualquier problemática de efectividad operacional.
	Control de la Información	cumplimiento, auditoría interna, grupo de riesgo de empresa, comité ERM	Auditor externo, regulador	<ul style="list-style-type: none"> Cumplimiento, auditoría interna y auditoría externa supervisarán la RCAM a fin de verificar si el riesgo identificado es en efecto relevante, si el diseño de las acciones de control están reflejando la realidad y si funcionan como se diseñaron. El Comité ERM y los reguladores actuarán sobre cualquiera de los hallazgos realizados por las anteriores intervenientes
	Disponibilidad de la información	grupo de riesgo de empresa, propietarios de procesos de negocio		El grupo de riesgo de empresa asegurará que la información en el RCAM está actualizada, conjuntamente con los propietarios de procesos de negocio, y acorde a eso adaptará el riesgo y los controles.
Objetivos	Subdimensión de Calidad y Objetivos	Descripción—El alcance de la que la información es ...	Relevancia	Objetivo
Intrínsecos	Exactitud	Correcta y fiable	Alta	<p>El riesgo debe ser descrito de forma precisa para valorar si los objetivos de control están diseñados de forma apropiada.</p> <p>Los objetivos de control deben ser descritos con precisión para que no haya posibilidad de interpretación en las operaciones de control</p>
	Objectividad	justa, sin prejuicios e imparcial	Alta	Los objetivos de riesgo y control deben ser descritos de una manera imparcial, libre de la tendencia al riesgo de la empresa.
	Credibilidad	Vista como verdadera y creíble	Alta	Las necesidades del riesgo identificado deben considerarse como creíbles en relación con el proceso. En otro caso, los objetivos de control que cubren el riesgo no se considerarán creíbles para reducir el riesgo de un proceso.
	Reputación	Vista como proveniente de una fuente verdadera y creíble	Baja	La fuente de información de la RCAM se obtiene de talleres y se introduce en el portal empresarial del riesgo.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 75— Matriz de Actividad de Control y Riesgo (RCAM)

	Subdimensión de Calidad y Objetivos	Descripción—El alcance de la que la información es ...	Relevancia	Objetivo
Objetivos Contextual y Representacional	Relevancia	aplicable y útil para la tarea en marcha	Media	La información requerida se detallará en una plantilla pre-aprobada y deberá ser aplicable a las tareas específicas en el alcance de la RCAM, sin que necesariamente sea única.
	Completitud	No perdida y con suficiente profundidad y amplitud para la tarea en marcha	Alta	Los controles deben ser completados con el fin de cubrir todos los riesgos identificados en un proceso.
	Actual	Suficientemente actual para la tarea en marcha	Alta	El riesgo y sus posteriores actividades y objetivos de control posterior deben de estar al día y reflejar en todo momento la realidad actual.
	Cantidad de información	Apropiada para la tarea en marcha	Media	La información en la RCAM debería proveer información relevante para ejecutar los controles y permitir una revisión de la efectividad del diseño de la RCAM.
	Representación concisa	Representada de forma compacta	Media	La información en el RCSE siempre se presenta de acuerdo con los formatos/plantillas predefinidas, vinculando un riesgo a un control con el objetivo de cubrir el riesgo.
	Representación Consistente	Presentada en el mismo formato	Alta	La información en el RCSE siempre se presenta de acuerdo con los formatos/plantillas predefinidas, vinculando un riesgo a un control con el objetivo de cubrir el riesgo.
	Interpretabilidad	Con el apropiado lenguaje, símbolos y unidades, siendo las definiciones claras y fácilmente comprensibles	Alta	La información de la RCAM no debe dejar lugar a la interpretación. El diseño de los controles ha de mostrar claramente que se dirigen a los riesgos identificados.
	Comprensión	Fácil de manipular y aplicar a las diferentes tareas	Media	El RCAM debe ser comprensible para el público objetivo, y podría requerir un mínimo de conocimiento de gestión de riesgos para su plena comprensión.
	Manipulación		Baja	Los controles están diseñados específicamente para un proceso para mitigar el riesgo identificado de ese proceso.
Seguridad	Disponibilidad	Disponible cuando se requiere, o fácilmente y rápidamente recuperable	Media	La RCAM debería tener una disponibilidad media; una indisponibilidad de 24 horas es aceptable.
	Acceso Restringido	Restringida de forma apropiada a las partes autorizadas	Alta	El acceso a la RCAM está restringido según: Acceso de escritura: grupo de riesgo de empresa Acceso de lectura: El resto de propietarios internos.
Buenas prácticas	Atributo	Descripción	Valor	
	Físico	Soporte/medio de la información	El soporte de información para la RCAM puede ser un documento electrónico y / o impreso.	
	Empírico	Canal de acceso a la información	La RCAM es accesible a través del portal de ERM y puede ser impresa por los propietarios de la RCAM.	
	Sintáctico	Código/lenguaje	La RCAM contiene los riesgos, su clasificación, descripciones de riesgo, objetivos de control y diseños de control con niveles de tolerancia relacionados sobre efectividad de la operación.	
	Semántico	Tipo de Información	Modelo tabulado estándar	
		Vigencia de la información	La información debe ser actual para el uso de la organización.	
		Nivel de información	Detallada para evitar malas interpretaciones.	
	Pragmático	Periodo de retención	Los RCAMs se conservan durante un año como máximo; momento en que se revisan y actualizan.	
		Estatus de las información	La información RCSE está al día en todo momento o debe actualizarse inmediatamente si no lo está.	
		Novedad	Está actualizada como el riesgo y los controles relacionados, se actualizan al mismo tiempo.	

Figura 75— Matriz de Actividad de Control y Riesgo (RCAM) (cont.)

Buenas prácticas	Atributo	Descripción	Valor
	Pragmático	Contingencia	La información debe ser clara para las partes interesadas que sólo requieren un conocimiento básico de las prácticas de gestión de riesgo.
	Social	Contexto	Esta RCAM debe utilizarse en las operaciones diarias para guiar a los controles necesarios para ser ejecutados en un proceso para prohibir que se produzca un riesgo identificado.
Enlace a otros facilitadores			
Procesos	<p>La RCAM es un resultado de los procesos:</p> <ul style="list-style-type: none"> • APO12.05 Definir una cartera de acciones de gestión de riesgos. <p>La RCAM es una entrada de los procesos:</p> <ul style="list-style-type: none"> • APO02.02 Evaluar el entorno actual, la capacidad y el rendimiento. • DSS01.01 Realizar procedimientos operacionales. 		
Estructuras Organizativas	<p>Los siguientes participantes son los responsables y ejecutores para la producción (parcial) de la información:</p> <ul style="list-style-type: none"> • Responsable: CRO, Comité ERM • Ejecutor: Grupo de riesgo de empresa, cumplimiento, propietarios de procesos de negocio • Consultado/Informado: Auditoría interna de negocio, auditoría externa, regulador (mirar propietarios) 		
Infraestructura, Aplicaciones y Servicios	La RCAM se elabora por el portal de gestión del riesgo (Herramienta GRC).		
Personal, Habilidades y Competencias	<p>La RCAM requiere las siguientes competencias:</p> <ul style="list-style-type: none"> • Capacidad analítica • Pensamiento lateral (pensar fuera de la caja) • Experiencia en riesgo 		
Cultura, Ética y Conducta	<p>La RCAM requiere los siguientes comportamientos:</p> <ul style="list-style-type: none"> • Reconocimiento de la exposición al riesgo. • Propiedad del riesgo es aceptado por el negocio • Obtención real del compromiso y asignación de recursos para la ejecución de las acciones • La dirección supervisa de forma proactiva el riesgo y el progreso del plan de acción. 		
Principios, Políticas y Marcos de trabajo	<p>Principios relacionados:</p> <ul style="list-style-type: none"> • Alineamiento con ERM • Función como parte de las actividades diarias • Acercamiento consistente 		

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 76— Evaluación del Riesgo

La valoración del Riesgo es la determinación de la relación de la exposición cuantitativa o cualitativa del riesgo a un escenario de riesgo. La valoración del riesgo es el resultado de esta tarea.

Ciclo de vida y propietarios	Etapa del Ciclo de Vida (o proceso)	Propietario Interno	Propietario Externo	Descripción/Stake
	Planificación de la Información	Comité ERM, función del riesgo,	Auditor externo, regulador	Identificar las categorías de escenarios de riesgo relevantes y los escenarios de riesgos para la empresa.
	Diseños de la Información	Función del riesgo, CIO		Determinar qué información se requiere para la evaluación de riesgos.
	Construcción / adquisición de la información	Función del riesgo, CIO, propietarios de procesos de negocio, oficina de gestión de proyectos, CISO, Responsable de arquitectura, Responsable de desarrollo, Responsable de operaciones TI, Responsable de operaciones IT, Responsable de administración IT, gestor de servicio, gestor de seguridad de la información, gestor de continuidad de negocio, oficial de privacidad		Recopilar la información necesaria para completar la evaluación del riesgo.
	Utilización de la Información: almacenamiento, compartición, uso	Toda la empresa	Auditor externo, regulador	Hacer uso de la evaluación del riesgo para determinar acciones en consecuencia.
	Control de la Información	CIO, auditoría		Evaluar en forma periódica la relevancia de la información en la evaluación de riesgos y la relevancia del escenario de riesgo en general.
	Disponibilidad de la información	CIO, función del riesgo		Eliminar la evaluación del riesgo si ya no es relevante.

Figura 76— Evaluación del Riesgo (cont.)

Objetivos Intrinsicos	Subdimensión de Calidad y Objetivos	Descripción—El alcance de la que la información es ...	Relevancia	Objetivo
	Exactitud	Correcta y fiable	Alta	La fuente de información tiene que ser precisa (confirmada mediante auditoría) y necesita ser procesada, analizada y presentada en la aplicación de gestión del riesgo de acuerdo a reglas fijas.
	Objectividad	Justa, sin prejuicios e imparcial	Alta	La información se basa en hechos y comprobaciones verificables, utilizando el punto de vista común del riesgo establecido en toda la empresa.
	Credibilidad	Vista como verdadera y creíble	Media	No debe contener información contradictoria.
	Reputación	Vista como proveniente de una fuente verdadera y creíble	Alta	La información de base se obtiene de fuentes competentes y reconocidas

Figura 76— Evaluación del Riesgo (cont.)

Objetivos Contextual y Representacional	Subdimensión de Calidad y Objetivos	Descripción—El alcance de la que la información es ...	Relevancia	Objetivo
	Relevancia	Aplicable y útil para la tarea en marcha	Alta	La información se estructurará de acuerdo con el atributo 'sintaxis', y será confirmado por la CRO (APO12) que la información es relevante
	Completitud	No perdida y con suficiente profundidad y amplitud para la tarea en marcha	Alta	Se referirá a toda la empresa con un registro de riesgos completo.
	Actual	Suficientemente actual para la tarea en marcha	Alta	No podrá ser mayor de seis meses
	Cantidad de información	Apropiada para la tarea en marcha	Media	Se recoge la información más relevante, permitiendo una mejor evaluación de un escenario de riesgo
	Representación concisa	Representada de forma compacta	Alta	La información deberá ser representada de forma concisa; esto se consigue mediante la recopilación, procesamiento y análisis de los datos relacionados con los riesgos para toda la empresa y mediante la detección y presentación únicamente de los riesgos relevantes.
	Representación Consistente	Presentada en el mismo formato	Alta	Siempre se presentará de acuerdo con la plantilla vigente.
	Interpretabilidad	Con el apropiado lenguaje, símbolos y unidades, siendo las definiciones claras y fácilmente comprensibles	Alta	Necesita ser descrito en términos que sean comprendidos de forma general, ya que será utilizado por una amplia tipología de empleados
	Comprensión		Alta	Necesita ser descrito en términos que sean comprendidos de forma general, ya que será utilizado por una amplia tipología de empleados
	Manipulación	Fácil de manipular y aplicar a las diferentes tareas	Media	Debe cubrir una amplia gama de posibles consecuencias, y por ello podría aplicarse a / impactar sobre diferentes tareas, pero la mayoría de las veces está delimitado a tareas / actividades identificadas.
Seguridad	Disponibilidad	Disponible cuando se requiere, o fácilmente y rápidamente recuperable	Alta	Deberá estar en todo momento disponibles para sus propietarios; una indisponibilidad de 24 horas es aceptable en caso de incidentes
	Acceso Restringido	Restringida de forma apropiada a las partes autorizadas	Alta	El acceso a la evaluación del riesgo es definido por la función del riesgo y está restringido según: <ul style="list-style-type: none"> • Acceso de escritura: función de riesgo • Acceso de lectura: El resto de propietarios internos.

Figura 76— Evaluación del Riesgo (cont.)

Buenas prácticas	Atributo	Descripción	Valor
	Físico	Soporte/medio de la información	El soporte de información para la evaluación de riesgos puede ser un documento electrónico o impreso.
	Empírico	Canal de acceso a la información	La evaluación de riesgos es accesible a través del portal de ERM.
	Sintáctico	Código/lenguaje	La evaluación de riesgos incluye las siguientes subpartes: <ul style="list-style-type: none"> • datos de origen relacionados con el riesgo • Relaciones Perfil de riesgo • Análisis de riesgos • análisis de riesgos de terceros
	Semántico	Tipo de Información	Plantilla de evaluación y escenario del riesgo
		Vigencia de la información	La evaluación de riesgos contiene datos históricos y actuales.
		Nivel de información	La evaluación del riesgo recoge datos de toda la empresa, procesos y analiza los datos y representa los datos pertinentes de forma completa en la evaluación de riesgos.

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 76— Evaluación del Riesgo (cont.)

	Atributo	Descripción	Valor
Buenas prácticas	Pragmático	Periodo de retención	La evaluación de riesgos se debe conservar tanto tiempo como el tiempo que los datos / información sobre la que informa del riesgo debe ser conservado (y considerando los requisitos legales de retención de datos).
		Estatus de las informaciones	Todos los casos producidos en los últimos 12 meses son operacionales, los datos más antiguos son considerados datos históricos.
		novedad	La evaluación del riesgo combina diversas otras fuentes de datos que conforman una nueva instancia; Por lo tanto, se trata de datos nuevos.
		Contingencia	La evaluación del riesgo se basa en que la siguiente información esté disponible y sea comprensible por el usuario: <ul style="list-style-type: none"> • Eventos relacionados con el riesgo en toda la empresa • El apetito al riesgo de la empresa • Análisis de riesgos • Evaluación de las actividades de gestión de riesgos • Las evaluaciones de las amenazas potenciales • Perfil de riesgo • taxonomía de riesgos en uso en la empresa
	Social	Contexto	La evaluación de riesgos sólo tiene sentido y para ser utilizado en un contexto de ERM.
Enlace a otros facilitadores			
Procesos		<p>La valoración del riesgo es un resultado de los procesos:</p> <ul style="list-style-type: none"> • APO02.05 Definir el plan estratégico y hoja de ruta. • APO12.02 Analizar el riesgo. • APO12.04 Articular el riesgo. • BAI01.10 Gestionar programa y riesgo del proyecto <p>La valoración del riesgo es una entrada de los procesos:</p> <ul style="list-style-type: none"> • EDM03.03 Supervisar la gestión del riesgo • APO01.03 Mantener los facilitadores del sistema de gestión • APO02.02 Valora el entorno actual, las capacidades y desempeño. • APO05.01 Establecer la diversidad de la inversión objetivo. • APO10.04 Gestionar el riesgo de los proveedores. • APO12.01 Recolectar datos. • BAI01.10 Gestionar programa y riesgo del proyecto • MEA02.01 Supervisar los controles internos. 	
Estructuras Organizativas		Las siguientes funciones son responsables y responsables de la producción parcialmente la información:	<ul style="list-style-type: none"> • Responsable: función de riesgos • Ejecutor: CIO, responsables de procesos de negocio, la oficina de gestión de proyectos, CISO, responsable de arquitectura, responsable de desarrollo, responsable de operaciones de TI, responsable de administración TI, gestor de servicio, gestor de seguridad de la información, gestor de continuidad de negocio, oficial de privacidad
Infraestructura, Aplicaciones y Servicios		La evaluación del riesgo puede ser elaborada por una aplicación de gestión de riesgos y puede ser utilizada por gestión de proyectos y portfolio, gestión de servicios, supervisión, cumplimiento y aplicaciones de auditoría.	
Personal, Habilidades y Competencias		La generación y el uso de una evaluación de riesgos requieren conocimiento básico de los principios y técnicas de gestión de riesgos.	
Cultura, Ética y Conducta		Las partes interesadas deben ser educadas sobre el significado y el uso de una evaluación de riesgos.	
Principios, Políticas y Marcos de trabajo		Principios relacionados:	<ul style="list-style-type: none"> • Conectar a los objetivos empresariales • Promover la comunicación justa y abierta • Establecer los principios en la dirección y la responsabilidad

B.6. Catalizadores: Servicios, Infraestructura y Aplicaciones

Para cada uno de los siguientes servicios, esta sección detalla la descripción, buenas prácticas (principios y puntos de vista sobre arquitectura, y consideraciones sobre el nivel de servicio) y las partes interesadas que están relacionadas:

- **Figura 77— Servicios de Asesoría de Riesgos de Programa/Proyecto**
- **Figura 78— Servicio de Gestión de Incidencias**
- **Figura 79— Servicios de Asesoría de Arquitectura**
- **Figura 80— Servicios de Inteligencia de Riesgos**
- **Figura 81— Servicios de Gestión de Riesgos**
- **Figura 82— Servicios de Gestión de Crisis**

Figura 77— Servicios de Asesoría de Riesgos de Programa/Proyecto

Descripción	Objetivo/Propósito	Beneficio
El conjunto de personas, procesos y tecnologías que ayudan a asegurar que los cambios o introducciones de estrategias de negocio, productos, procesos o tecnologías, no provocan niveles inaceptables de riesgo en la empresa.	Ayudar a la empresa a alcanzar/mantener el nivel de riesgo óptimo.	Al proporcionar este servicio antes de que se apliquen los cambios, la empresa va a ser proactiva en la gestión de riesgos y puede evitar costosas re-ingeniería para mitigar exposiciones a pérdidas evitables.
Buenas Prácticas		
Descripción	Buenas Prácticas	
Compra	Las empresas pueden escoger externalizar este servicio o implementar internamente las capacidades necesarias según corresponda a su cultura y recursos.	
Uso	<ul style="list-style-type: none"> • Establecer un proceso de clasificación para ayudar a garantizar que el servicio se aplica a los programas / proyectos con mayor potencial para la introducción de riesgos nuevos o mayores en la empresa. • Establecer un proceso de gobernanza para asegurar que los programas / proyectos no eluden indebidamente el servicio. Por ejemplo, el establecimiento de un proceso que sólo libera fondos para programas / proyectos después de conseguir los hitos de gestión de riesgos (por ejemplo, gestión del valor ganado). 	
Partes interesadas		
Partes interesadas	Descripción	
Usuarios	Ejecutivos de negocio, oficina de gestión de programas, CIO, función de riesgos, CTO, CISO	
Patrocinadores	CIO, oficina de estrategia de negocio, auditoría, cumplimiento	

Figura 78— Servicio de Gestión de Incidencias

Descripción	Objetivo/Propósito	Beneficio
El conjunto de personas, procesos y tecnologías que ayudan a minimizar las pérdidas que se materializan a partir de las incidencias.	Minimizar las pérdidas que se materializan a partir de las incidencias.	Menores pérdidas.
Buenas Prácticas		
Descripción	Buenas Prácticas	
Compra	<p>Las empresas pueden escoger externalizar este servicio o implementar internamente las capacidades necesarias según corresponda a su cultura y recursos.</p> <ul style="list-style-type: none"> • Las empresas deben asegurarse de que las partes interesadas pertinentes están involucradas en el equipo de gestión de incidencias (por ejemplo legal, privacidad, RRHH). • El servicio debe incluir procesos que documenten con precisión las medidas adoptadas para resolver las incidencias que se producen, para su posterior consulta (por ejemplo, en los procedimientos de defensa legal). • El servicio debe aprovechar los recursos forenses competentes según el caso. 	
Uso	El servicio debe documentar las pérdidas y los gastos en que se incurre para proporcionar evidencia empírica para posteriores análisis de riesgos.	
Partes interesadas		
Partes interesadas	Descripción	
Usuarios	Ejecutivos de negocio, CIO, la función de riesgos, CTO, CISO, gestión de la seguridad física	
Patrocinadores	CIO, auditoría, privacidad, legal, cumplimiento	

DETALLE DE LOS CATALIZADORES PARA EL GOBIERNO Y LA GESTIÓN DE LOS RIESGOS

Figura 79— Servicios de Asesoría de Arquitectura

Descripción	Objetivo/Propósito	Beneficio
El conjunto de personas, procesos y tecnologías que ayudan a asegurar que las introducciones o cambios de arquitecturas de negocio o de tecnología no provocan niveles inaceptables de riesgo a la empresa.	Ayudar a la arquitectura de empresa a dar soporte a un nivel de riesgo óptimo.	Reduce la posibilidad de cambios en la arquitectura para introducir niveles no deseados y / o inaceptables de riesgo.
Buenas Prácticas		
Descripción	Buenas Prácticas	
Compra	Las empresas pueden escoger externalizar este servicio o implementar internamente las capacidades necesarias según corresponda a su cultura y recursos.	
Uso	Las empresas deben asegurarse de que tienen fuentes efectivas de inteligencia con respecto a los cambios tácticos y estratégicos (emergentes) en el panorama de las amenazas y de las tecnologías.	
Partes interesadas		
Partes interesadas	Descripción	
Usuarios	CTO, CIO, ejecutivos de negocio, oficina de gestión de programas, función de riesgo, CISO	
Patrocinadores	CIO, CTO, CISO, oficina de estrategia de negocio, auditoría, cumplimiento	

Figura 80— Servicios de Inteligencia de Riesgos

Descripción	Objetivo/Propósito	Beneficio
El conjunto de personas, procesos y tecnología que ayudan a garantizar la disponibilidad de una inteligencia precisa y oportuna sobre amenazas, vulnerabilidades y activos. Esta inteligencia tiene que incluir información tanto táctica como estratégica (con una mayor perspectiva temporal).	Ayuda a los analistas y los responsables de toma de decisiones a tomar decisiones basadas en la mejor información disponible.	<ul style="list-style-type: none"> - Es menos probable que la empresa pase por alto o subestime aspectos clave de su entorno de riesgo. - La empresa es capaz de ser más proactiva en su toma de decisiones.
Buenas Prácticas		
Descripción	Buenas Prácticas	
Compra	Las empresas pueden escoger externalizar este servicio o implementar internamente las capacidades necesarias según corresponda a su cultura y recursos.	
Uso	La empresa necesita identificar fuentes de inteligencia de confianza e integrarlas en su proceso de análisis y de toma de decisión.	
Partes interesadas		
Partes interesadas	Descripción	
Usuarios	Ejecutivos de negocio, oficina de gestión de programas, CIO, función de riesgo, CTO, CISO	
Patrocinadores	CIO, oficina de estrategia de negocio, auditoría, cumplimiento	

Figura 81— Servicios de Gestión de Riesgos

Descripción	Objetivo/Propósito	Beneficio
El conjunto de personas, procesos y tecnología que ayudan a la empresa a garantizar la construcción / mantenimiento de un programa rentable para la gestión de riesgo a lo largo del tiempo.	Proporcionar experiencia en el tema a las partes interesadas clave en la gestión de riesgos	<ul style="list-style-type: none"> - Ayuda a asegurar que el programa de gestión de riesgos en la empresa es comprensible, consistente e integrado de manera efectiva en las líneas de negocio y sus procesos. - Proporciona una visión global sobre el riesgo en toda la empresa.
Buenas Prácticas		
Descripción	Buenas Prácticas	
Compra	Las empresas pueden escoger externalizar este servicio o implementar internamente las capacidades necesarias según corresponda a su cultura y recursos.	
Uso	Adoptar o desarrollar un marco estándar para la gestión de riesgos que se utilizará en toda la empresa.	

Partes interesadas	
Partes interesadas	Descripción
Usuarios	Todos los ejecutivos de las líneas de negocio, oficina de gestión de programas, CIO, función de riesgos, CTO, CISO
Patrocinadores	Consejo, CEO, CRO, auditoría

Figura 82— Servicios de Gestión de Crisis

Descripción	Objetivo/Propósito	Beneficio
El conjunto de personas, organizaciones, procesos y tecnología que ayudan a responder a cualquier tipo de crisis, como las que requieren la activación del PCN.	<ul style="list-style-type: none"> - Definir los principios generales de gestión de crisis aplicables: la organización de los acuerdos, los roles de los actores involucrados. - Especificar los procedimientos y procesos a ser implementados, los recursos logísticos que se utilizarán y los principios de mantenimiento en estado operativo de los servicios. 	<p>Reducir el impacto de los grandes eventos adversos y evitar problemas tales como:</p> <ul style="list-style-type: none"> - redundancia, retención y relevancia de la información - La ineficiencia de la empresa debido a la logística inadecuada - Centros de decisión múltiples y falta de respeto a la situación y la responsabilidad - Las malas decisiones debido a la falta de canales de comunicación hacia dirección

Buenas Prácticas

Descripción	Buenas Prácticas
Compra	Las empresas pueden escoger externalizar este servicio o implementar internamente las capacidades necesarias según corresponda a su cultura y recursos.
Uso	Los siguientes elementos deben ser previstos por los servicios de gestión de crisis: <ul style="list-style-type: none"> • Recursos físicos: activos, instalaciones y accesorios para salas de gestión de crisis • Recursos de información: memorándums, directorios, técnica y datos personales • Recursos técnicos: tecnologías de telecomunicación, plataformas remotas seguras • Recursos humanos especializados en gestión de crisis • Composición, funciones y detalles de contacto de los equipos de gestión de crisis

Partes interesadas

Partes interesadas	Descripción
Usuarios	Ejecutivos de negocio, CIO, función de riesgo, CTO, CISO, gestión de seguridad física, gestor de continuidad de negocio
Patrocinadores	Gestor de continuidad de negocio, función de riesgo, privacidad, legal y cumplimiento

B.7. Catalizador: Gente, Habilidades y Competencias

Los puestos directivos clave se describen en detalle en el marco de habilitador de las estructuras de la organización y, por lo tanto, no se elaboran en esta sección.

- Comité ERM
- Grupo de riesgo empresarial
- Función del riesgo
- Departamento de auditoría
- Departamento de cumplimiento

La siguiente sección describe además las habilidades y competencias de los dos roles específicos que tienen responsabilidades de gestión del riesgo:

- **Figura 83—Gestor del riesgo**
- **Figura 84—Analista del riesgo**

Figura 83—Gestor del riesgo

Los gestores del riesgo son responsables de la exitosa implementación y el seguimiento de la estrategia y el marco del riesgo. Los gestores del riesgo involucran a los implicados para asegurar que entienden los procesos, tienen los recursos suficientes, se implementan, y soportan los objetivos del negocio. Las consecuencias de los riesgos serán reportadas al CRO para que se incorporen en los perfiles y problemas globales del riesgo.

El rol trabaja con los gestores del negocio para asegurarse de que las tecnologías de la información apoyan con eficacia los objetivos estratégicos. El gestor del riesgo colabora con los departamentos de auditoría / segmento de negocio / riesgo corporativo para abordar los problemas con los planes de acción plausibles y fechas límite. Este rol actúa como el punto central para la recepción y distribución de la información importante del riesgo para las tecnologías de la información y se realimenta el flujo de información para la gestión del riesgo empresarial. El gestor del riesgo se asegura de que la tecnología de la información se adhiere a las políticas y procedimientos corporativos y de las unidades de negocio. Este rol debe tener en cuenta y estar al tanto de los riesgos asociados a la tecnología de la empresa. El rol puede o no puede tener responsabilidades de gestión.

Esta tabla describe la típica experiencia, la educación y las calificaciones para este rol específico. Estos no deben considerarse requisitos estrictos, sino una guía que se puede utilizar como punto de partida, por ejemplo, cuando se detallan posiciones de trabajo.

Experiencia, Educación y Calificaciones	
Requisito	Descripción
Experiencia	<ul style="list-style-type: none"> • Experiencia apropiada en la gestión y gobernanza de los riesgos de negocio y/o operaciones • Experiencia en la comunicación de los riesgos a miembros ejecutivos y/o dirección
Educación	Degree in management information systems with experience in IT, finance, economics, business or engineering
Calificaciones y certificaciones comunes	CISA, CISM, CRISC, CISSP, CPA
Conocimientos, habilidades técnicas y de conducta	
Conocimiento	<ul style="list-style-type: none"> • Tener un conocimiento profundo de la empresa y los sistemas de TI que soportan las funciones de la empresa, así como ser conscientes de los factores contextuales que influyen en ellos • Sólidos conocimientos de metodologías de riesgo, estándares de riesgo de uso común y buenas prácticas en la gestión del riesgo
Habilidades técnicas	<ul style="list-style-type: none"> • Tener conocimiento de los aspectos técnicos de los sistemas de TI que dan soporte a las funciones de la empresa
Habilidades de conducta	<ul style="list-style-type: none"> • Liderazgo • Comunicación • Influencia • Paciencia • Escalado

Figura 84—Analista del riesgo

<p>El analista del riesgo es el responsable de:</p> <ul style="list-style-type: none"> • Ejecutar globalmente el proceso de evaluación de riesgos de la empresa • Identificar y analizar las áreas de riesgos potenciales que amenazan los activos y la consecución de los objetivos de la organización • Proporcionar una evaluación específica de los escenarios de riesgo teniendo en cuenta tanto el negocio como una perspectiva técnica • Reportar sus hallazgos al gestor del riesgo o al CRO. <p>Esta tabla describe la típica experiencia, la educación y las calificaciones para este rol específico. Estos no deben considerarse requisitos estrictos, sino una guía que se puede utilizar como punto de partida, por ejemplo, cuando se detallan posiciones de trabajo.</p>	
Experiencia, Educación y Calificaciones	
Requisito	Descripción
Experiencia	<ul style="list-style-type: none"> • Experiencia contrastada en administración de empresas o de TI • Tener un conocimiento apropiado en arquitectura de sistemas, infraestructura, seguridad y aplicaciones
Educación	<ul style="list-style-type: none"> • Licenciatura en análisis financiero, TI, ingeniería, analista de sistemas • Master en disciplinas relacionadas, por ejemplo, matemáticas, estadística
Calificaciones y certificaciones comunes	CISM, CRISC, CISSP, FAIR
Conocimientos, habilidades técnicas y de conducta	
Conocimiento	<ul style="list-style-type: none"> • Conocimiento de las metodologías de riesgo, estándares de riesgo de uso común, las buenas prácticas de riesgo y análisis de riesgo cuantitativo y cualitativo • Conocimiento consistente de los procesos de negocio y su relación con la tecnología • El uso de herramientas y técnicas de evaluación de riesgos
Habilidades técnicas	<ul style="list-style-type: none"> • Profundo entendimiento del funcionamiento de TI y del negocio y amplio conocimiento de los dominios de TI, las amenazas y los activos • Capacidades analíticas, preferentemente con conocimientos de análisis estadístico y de probabilidades
Habilidades de conducta	<ul style="list-style-type: none"> • Capacidades comunicativas • Dotes para la presentación • Evaluaciones cruzadas • Capacidad de decisión • Delegación del trabajo a los expertos técnicos

APÉNDICE C

PRINCIPALES PROCESOS DE GESTIÓN DE RIESGOS EN COBIT5

Este apéndice contiene una guía más detallada sobre los procesos de gestión de riesgos principales que se identificaron en la sección 2B del capítulo 1.

Figura 85- Procesos de Gestión de Riesgos Principales	
COBIT 5 Proceso de Identificación	Justificación
EDM03 Asegurar la Optimización del Riesgo	Cubre la articulación y comunicación del apetito de riesgo y la tolerancia de la organización, y garantiza la identificación y gestión de los riesgos para el valor de la empresa relacionados con el uso de las TI.
APO12 Gestión de Riesgos	Cubre la identificación, evaluación y reducción de las actividades de riesgos.

Para cada proceso, se proporciona la siguiente información:

- Descripción del proceso y declaración del propósito del proceso (idéntica a *COBIT 5 Procesos Catalizadores*);
- Las metas y métricas del proceso;
- Las prácticas del proceso (idénticas a *COBIT 5 Procesos Catalizadores*), entradas y salidas;
- Las actividades del proceso incluyendo un nivel adicional de actividades detalladas. Esta información adicional específica de riesgo no está incluida en *COBIT 5 Procesos Catalizadores*.

EDM03 Asegurar la Optimización Específica de Riesgo		Área: Gobierno Dominio: Evaluar, Dirigir y Supervisar		
COBIT 5 Descripción del Proceso Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.				
COBIT 5 Declaración del Propósito del Proceso Asegurar que los riesgos relacionados con las TI de la empresa no exceden ni el apetito ni la tolerancia de riesgo, que el impacto de los riesgos de TI en el valor de la empresa se identifica y se gestiona y que el potencial fallo en el cumplimiento se reduce al mínimo.				
EDM03 Metas y Métricas específicas de Riesgo del Proceso No son relevantes para esta práctica metas y métricas específicas de riesgo. Las metas y métricas genéricas de COBIT 5 se pueden utilizar como orientación adicional.				
EDM03 Prácticas, Entradas/Salidas y Actividades específicas de Riesgo del Proceso				
Prácticas de Gobierno	Entradas específicas de Riesgo (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgo (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
EDM03.01 Evaluar la gestión de riesgos Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado.	No son relevantes para esta práctica entradas y salidas específicas de riesgo. Las entradas y salidas genéricas de COBIT 5 se pueden utilizar como orientación adicional.			
Actividades específicas de Riesgo (adicionales a las Actividades de COBIT 5)				
<p>1. Determinar el nivel de riesgos relacionados con las TI que la empresa está dispuesta a asumir para cumplir con sus objetivos (apetito de riesgo).</p> <p>1.1 Realizar la evaluación de riesgos de TI de la empresa;</p> <p>1.2 Patrocinar reuniones de trabajo con la dirección de negocio para discutir en toda su amplitud los riesgos que la empresa está dispuesta a aceptar para conseguir sus objetivos (apetito al riesgo);</p> <p>1.3 Ayudar a los responsables de negocio a entender los riesgos de TI en el contexto de los escenarios que afectan a su negocio y de los objetivos que más les afectan en su día a día;</p> <p>1.4 Analizar de arriba hacia abajo y extremo a extremo los servicios y procesos de negocio e identificar los principales puntos de soporte de TI. Identificar dónde se genera valor y es necesario protegerlo y sostenerlo;</p> <p>1.5 Identificar los eventos y condiciones relacionados con TI que puedan poner en riesgo su valor, afectar al rendimiento de la empresa y a la ejecución de las actividades críticas de negocio dentro de límites aceptables, o afectar de otro modo a los objetivos empresariales. Organizarlos en una jerarquía enfocada a negocio, compuesta de categorías y subcategorías de riesgo (dominios de riesgo TI) derivadas de los escenarios de riesgo de TI de alto nivel.</p> <p>1.6 Dividir los riesgos de TI por líneas de negocio, productos, servicios y procesos. Identificar potenciales cascadas y coincidencias de tipologías de amenazas y el efecto probable de concentración de riesgos y de correlación entre los diferentes silos;</p> <p>1.7 Entender cómo las capacidades de TI contribuyen a la capacidad de la empresa para generar valor y soportar la pérdida. Comparar la percepción de dirección de la importancia de las capacidades de TI respecto a la situación real;</p> <p>1.8 Considerar cómo las estrategias de TI, las iniciativas de cambio y los requisitos externos pueden afectar al perfil de riesgo;</p> <p>1.9 Identificar las áreas principales de riesgos, los escenarios, las dependencias, los factores de riesgo y las mediciones de riesgo que requieren atención de la dirección y un nuevo análisis y desarrollo.</p> <p>2. Evaluar y aprobar propuestas de umbrales de tolerancia al riesgo TI frente a los niveles de riesgo y oportunidad aceptables por la empresa.</p> <p>2.1 Establecer el nivel de riesgos TI de las líneas de negocio, productos, servicios, procesos, etc. que la empresa está dispuesta a asumir para cumplir con sus objetivos (apetito de riesgo);</p> <p>2.2 Definir límites expresados en medidas similares a los objetivos de negocio subyacentes y contraponerlos a impactos de negocio comerciales aceptables e inaceptables;</p> <p>2.3 Contemplar cualquier compensación que pueda ser requerida para lograr los objetivos clave en el contexto de un balance equilibrado de rentabilidad-riesgo;</p> <p>2.4 Proponer límites y medidas en el contexto de TI como facilitadoras de beneficio / valor, de programación y entrega de proyectos TI y de operación y prestación de servicios TI, contemplados en diferentes horizontes temporales;</p> <p>2.5 Evaluar los umbrales de tolerancia de riesgos TI propuestos frente al riesgo aceptable de la empresa y a las oportunidades existentes, teniendo en cuenta los resultados de la evaluación de riesgos TI corporativa y las compensaciones requeridas para lograr los objetivos clave en el contexto de un balance equilibrado rentabilidad-riesgo;</p>				

APÉNDICE C
PRINCIPALES PROCESOS DE GESTIÓN DE RIESGOS EN COBIT 5

EDM03 Prácticas, Entradas/Salidas y Actividades específicas de Riesgo del Proceso (cont.)
Actividades específicas de Riesgo (adicionales a las Actividades de COBIT 5) (cont.)
<p>2.6 Considerar los efectos potenciales de la concentración y correlación de riesgos TI transversales a las líneas de negocio, productos, servicios y procesos, y determinar si alguno de los umbrales de tolerancia específicos de una unidad debería ser aplicado a todas las líneas de negocio;</p> <p>2.7 Definir las tipologías de eventos (internos o externos) y los cambios en el ámbito de negocio o en el tecnológico que puedan requerir una modificación de la tolerancia al riesgo TI;</p> <p>2.8 Aprobar los umbrales de tolerancia de riesgos TI.</p>
<p>3. Determinar el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales.</p> <p>3.1 Codificar en la política, de forma transversal a toda la empresa, la tolerancia y el apetito por el riesgo TI;</p> <p>3.2 Aceptar que el riesgo TI es inherente a los objetivos de la empresa y documentar el valor de riesgo TI deseado y permitido en la obtención de esos objetivos;</p> <p>3.3 Documentar los principios de gestión de riesgos, las áreas de enfoque de riesgos y las medidas clave.</p> <p>3.4 Recomendar ajustes a la política de riesgos de TI basados en las cambiantes condiciones de riesgo y en las amenazas emergentes;</p> <p>3.5 Alinear la política operacional y los estándares adoptados con la tolerancia al riesgo.</p> <p>3.6 Realizar revisiones periódicas o programadas de la política operacional y estándares versus la política de riesgos de TI y la tolerancia. Allí donde se detecten lagunas, se han de establecer fechas objetivo teniendo como referencia los límites temporales de exposición al riesgo considerados aceptables y los recursos necesarios;</p> <p>3.7 Proponer ajustes de la tolerancia al riesgo en lugar de modificar políticas operacionales y estándares implementados y eficaces.</p>
<p>4. Evaluar proactivamente los factores de riesgo TI con anterioridad a la toma de decisiones estratégicas de la empresa que estén en proceso y asegurar que las decisiones de la empresa se toman siendo conscientes de los riesgos.</p> <p>4.1 Determinar los niveles de riesgo y de rendimiento del portfolio de aplicaciones TI en función del valor de los procesos de negocio o de las oportunidades que facilitan, para reequilibrar el portfolio corporativo basándolo en el riesgo, en el retorno y en la anticipación a los cambios en el entorno de TI;</p> <p>4.2 Ayudar a la dirección a tener en cuenta los efectos que los riesgos TI y la capacidad actual de gestión de riesgos (controles, capacidades, recursos) tendrán en las decisiones de negocio y el efecto que estas decisiones pueden tener sobre la exposición a riesgos TI actual y sobre la capacidad de gestionar los riesgos TI en el futuro;</p> <p>4.3 Ayudar a la dirección a entender los riesgos TI utilizando diferentes visiones del portfolio (por ejemplo, unidad de negocio, producto, proceso) y a valorar el impacto que las propuestas de inversiones TI tendrán en el perfil de riesgo global de la empresa (aumento o reducción de riesgos);</p> <p>4.4 Recalc当地 como condición para la aprobación de las decisiones de negocios, los costes y las oportunidades deben ser sopesadas versus la variación neta estimada de la exposición al riesgo TI (es decir, el impacto).</p>
<p>5. Determinar si el uso de TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes.</p> <p>5.1 Proporcionar entradas a los decisores de dirección derivadas del enfoque de análisis de riesgos de TI propuesto;</p> <p>5.2 Ilustrar cómo los resultados del análisis de riesgo pueden beneficiar a las decisiones importantes;</p> <p>5.3 Describir el nivel de calidad que deberían esperar los decisores, cómo interpretar los informes de análisis de riesgos, las definiciones de los términos clave (por ejemplo, probabilidades de riesgo, grado de error, factores de riesgo), y las limitaciones de las mediciones y estimaciones basadas en datos incompletos;</p> <p>5.4 Identificar las diferencias respecto a las expectativas de riesgo de la empresa;</p> <p>5.5 Determinar si el informe de análisis de riesgos proporciona suficiente información para comprender los problemas de riesgo y, en caso necesario, para evaluar las opciones de respuesta a los riesgos. Se debe hacer constar sus limitaciones para la toma de decisiones.</p>
<p>6. Evaluar las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la empresa para las pérdidas relacionadas con TI y la tolerancia de los líderes a los mismos.</p> <p>6.1 Determinar cómo debe definirse la gestión de riesgos relacionados con TI en el contexto de la protección y el mantenimiento de un proceso de negocio determinado o de una actividad de negocio;</p> <p>6.2 Adoptar y alinearse con el marco corporativo existente para los riesgos de negocio;</p> <p>6.3 Integrar datos específicos de TI en un único enfoque corporativo. Comprender las metas y objetivos de los riesgos empresariales y la combinación de problemas originados por la existencia de negocios competidores y limitaciones de recursos;</p> <p>6.4 Determinar cómo debe ser abordada la gestión de riesgos TI en el contexto del universo de riesgos de la empresa y de otros tipos de riesgos empresariales;</p> <p>6.5 Definir el rol del departamento de TI en las actividades de gestión de riesgos operacionales, en función del grado de dependencia de la empresa de TI y de la infraestructura física relacionada, para la consecución de los objetivos financieros, operativos y de satisfacción del cliente;</p> <p>6.6 Coordinar actividades de evaluación de riesgos y realizar informes integrados;</p> <p>6.7 Coordinar riesgos y problemas de clasificación; escalas de evaluación del riesgo y jerarquías de las políticas basadas en riesgos.</p>

EDM03 Prácticas, Entradas/Salidas y Actividades específicas de Riesgo del Proceso y Actividades Detalladas de Riesgo (cont.)								
Práctica de Gobierno	Entradas específicas de Riesgo (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgo (adicionales a las Salidas de COBIT 5)					
	De	Descripción	Descripción	A				
EDM03.02 Orientar la gestión de riesgos. Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que el riesgo en TI actual no excede el apetito de riesgo del Consejo.	No son relevantes para esta práctica entradas y salidas específicas de riesgo. Las entradas y salidas genéricas de COBIT 5 se pueden utilizar como orientación adicional.							
Actividades específicas de Riesgo (adicionales a las Actividades de COBIT 5)								
<p>1. Promover una cultura consciente de los riesgos TI e impulsar a la empresa a una identificación proactiva de riesgos TI, oportunidades e impactos potenciales en el negocio.</p> <ul style="list-style-type: none"> 1.1 Alentar a los empleados para hacer frente a problemas de riesgos TI antes de que se requiera una escalada formal; 1.2 Entrenar al personal de negocio y de TI sobre las amenazas, los impactos y las respuestas establecidas por la empresa a los eventos de riesgo específicos; 1.3 Comunicar mensajes de "por qué deberías preocuparte" a las áreas de enfoque de riesgo, y explicar cómo tomar acciones consecuentes con los riesgos en las situaciones no especificadas en las políticas; 1.4 Repasar escenarios para las áreas no directamente cubiertas por la política, y reforzar las expectativas de comprensión de la política general de la dirección y del uso del sentido común; 1.5 Mostrar una actitud que fomente la discusión y la aceptación del nivel apropiado de riesgo, es decir, ser positivo sobre la promoción de una adecuada cultura de riesgo de TI alineada con la cultura de concienciación de riesgos de la empresa. <p>2. Orientar la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones empresariales estratégicas.</p> <ul style="list-style-type: none"> 2.1 Organizar los métodos de gestión riesgos de TI existentes necesarios para: 1) entender el contexto de negocio de TI (por ejemplo, el análisis de la dependencia de TI del negocio, el análisis de escenarios), 2) identificar los riesgos de TI (por ejemplo, modelos de datos, vías de escalado), 3) gobernar el riesgo TI, y 4) gestionar el riesgo TI (por ejemplo, seleccionar los indicadores clave de riesgo adecuados para los objetivos de rendimiento de negocio adecuados y definir los procedimientos de escalado); 2.2 Comprender las expectativas actividades y métodos de la gestión de riesgos empresarial general (ERM) que son relevantes para la gestión de riesgos TI; 2.3 Identificar las lagunas y las prácticas específicas de gestión de riesgos de TI que deben actualizarse o crearse para satisfacer las expectativas de ERM; 2.4 Identificar las actividades de riesgo empresarial que deberían añadirse o actualizarse para tener plenamente en cuenta los riesgos TI; 2.5 Identificar qué otras funciones hacer, o que sean necesarias hacer, para facilitar los objetivos y la gestión de riesgos TI corporativos; 2.6 Priorizar y trazar los esfuerzos para cubrir las lagunas entre los riesgos TI y ERM, y mejorar la eficacia y la eficiencia (por ejemplo, optimizar los controles, agilizar la evaluación de riesgos, coordinar los indicadores clave de riesgo y los disparadores de escalado, integrar informes). <p>3. Orientar la elaboración de planes de comunicación de riesgos (cubriendo todos los niveles de la empresa), así como los planes de acción de riesgo.</p> <ul style="list-style-type: none"> 3.1 Establecer y mantener un plan de comunicación de riesgos que cubra la política de riesgos TI, las responsabilidades, la rendición de cuentas y el panorama de riesgos. Organizar el contenido del plan para hacerlo claro, conciso, útil y dirigido a los destinatarios adecuados; 3.2 Mantener una comunicación frecuente y regular entre la dirección de TI y los líderes de negocio relativa al estado, preocupaciones y exposiciones de problemas de riesgos de TI; 3.3 Fundamentar las comunicaciones de la dirección de negocio y de TI en un enfoque predefinido con los siguientes objetivos: <ul style="list-style-type: none"> • Alinear las comunicaciones de riesgos TI con la terminología de riesgos de la empresa; • Priorizar de forma consistente los problemas de riesgos TI de forma que se alineen con la manera corporativa de definir los riesgos empresariales; • Expresar los riesgos de TI en términos estratégicos y operativos del negocio; • Comunicar claramente cómo los eventos negativos relacionados con TI pueden afectar a los objetivos de negocio; • Incentivar a los altos directivos y ejecutivos de TI a comprender la situación actual de riesgos de TI para ayudarlos a asignar los recursos adecuados para responder a los riesgos TI en base al apetito y a la tolerancia. <p>4. Orientar la implantación de mecanismos apropiados para responder rápidamente a los riesgos cambiantes y notificar inmediatamente a los niveles adecuados de la dirección, soportados por principios de escalado acordados (qué informar, cuándo, dónde y cómo).</p> <ul style="list-style-type: none"> 4.1 Identificar los responsables y los rendidores de cuentas de la gestión de riesgos TI en toda la empresa. Para los ejecutivos de máximo nivel que rindan cuentas de riesgos TI, establecer una expectativa de rendimiento para incorporar la conciencia de riesgo en la cultura empresarial. 4.2 Garantizar que existen las estructuras necesarias (por ejemplo, comité de riesgos de la empresa, consejo de riesgos TI, oficiales de riesgos TI) para involucrar al negocio en las decisiones conscientes de riesgo/retorno y en las operaciones del día a día; 4.3 Distinguir entre los roles de las unidades de negocio (que poseen y gestionan el riesgo en el día a día), de las funciones de control de riesgos (que ofrecen evaluación experta y asesoramiento en la materia) y de la auditoría interna (que ofrece aseguramiento independiente); 4.4 Asignar roles para la gestión de dominios específicos de riesgo de TI (por ejemplo, capacidades del sistema, personal de TI, selección de programas TI). Asignar a cada dominio un nivel de criticidad en función del riesgo/retorno. Cuando sea necesario, asignar responsabilidades adicionales de gestión de riesgos (por ejemplo, específicas de un sistema) en los niveles inferiores. 								

APÉNDICE C
PRINCIPALES PROCESOS DE GESTIÓN DE RIESGOS EN COBIT 5

EDM03 Prácticas, Entradas/Salidas y Actividades específicas de Riesgo del Proceso y Actividades Detalladas de Riesgo (cont.)						
Actividades específicas de Riesgo (adicionales a las Actividades de COBIT 5) (cont.)						
4.5 Examinar el inventario de actividades de respuesta al riesgo para identificar las que tienen una mayor probabilidad de reducir el riesgo a nivel global. Cuantificar el efecto global esperado en la frecuencia y magnitud probables de los escenarios de riesgo relacionados mediante la aplicación prevista de controles, capacidades y recursos.						
4.6 En función de dimensiones como el nivel de riesgo actual y el ratio eficacia / coste, clasificar y equilibrar las respuestas (por ejemplo, resultados rápidos, oportunidades, los esfuerzos diferidos) que puede requerir un caso de negocio;						
4.7 Hacer hincapié en los proyectos específicos con relativamente mayores probabilidades de:						
<ul style="list-style-type: none"> • Reducir las concentraciones de riesgo (por ejemplo, las mejoras de la arquitectura, la segregación de las unidades operacionales y sistemas); • Implementar controles que afronten directamente varios tipos de riesgo y que sean rentables; • Implementar controles que mejoren la eficacia de los procesos y que eviten la adopción de excesivos riesgos. 						
4.8 Registrar los motivos, las limitaciones y la forma en que las decisiones impulsan cambios en la política publicada, en los controles operacionales, en las capacidades, en los despliegues de recursos y en los planes de comunicación. En su caso, registrar los motivos para exceder o no alcanzar el apetito de riesgo y la tolerancia.						
5. Orientar para que el riesgo, las oportunidades, los problemas y preocupaciones puedan ser identificados y notificados por cualquier persona en cualquier momento. El riesgo debería ser gestionado de acuerdo con las políticas y procedimientos publicados y escalados a los decisores relevantes.						
5.1 Utilizando los umbrales de tolerancia de riesgos establecidos como guía, decidir si se acepta el nivel de exposición al riesgo residual;						
5.2 Considerar la información relevante de los informes de análisis de riesgo, tales como las probabilidades y rangos de pérdida, las alternativas de respuesta al riesgo, las expectativas de coste / beneficio, y los potenciales efectos de la agregación de riesgos. Plantear y examinar conjuntamente con los propietarios de procesos de negocio afectados los ratios riesgo / retorno, y determinar dónde gastar el presupuesto de riesgo en riesgos "conocidos" para permitir la aceptación de los riesgos desconocidos;						
5.3 Obtener la conformidad de negocio de la aceptación de riesgos o, si no se acepta, los requisitos de respuesta a los riesgos correspondientes. Documentar cómo se valoró el riesgo en la decisión y las justificaciones a cualquier excepción a la tolerancia al riesgo (por ejemplo, importante oportunidad de negocio estratégica);						
5.4 Garantizar que las decisiones de aceptación del riesgo y los requisitos de respuesta al riesgo se comunican de forma transversal a todas las líneas de la organización conforme a los riesgos corporativos establecidos y a las políticas y procedimientos de gobierno corporativo.						
6. Identificar los objetivos e indicadores clave de los procesos de gobierno y gestión de riesgos a ser monitoreados y aprobar los enfoques, métodos, técnicas y procesos para capturar y notificar la información de medición.						
6.1 Establecer medidas de rendimiento y procesos de generación de informes con los niveles adecuados de reconocimiento, aprobación, incentivos y sanciones;						
6.2 Identificar a los gestores de negocio con atribuciones para afrontar los problemas de riesgos TI a través de facilitar el beneficio / valor de TI, programas y ejecución de proyectos TI, y operaciones y prestación de servicios TI. Establecer las expectativas de estos gestores respecto a las seleccionadas políticas, estándares, controles y actividades de monitoreo del cumplimiento (por ejemplo, definición y monitoreo de KRI);						
6.3 Establecer y evaluar los objetivos de rendimiento en función de la toma de decisiones conscientes de riesgo -retorno (por ejemplo, la capacidad de los directivos para integrar y equilibrar la gestión del rendimiento con la gestión de riesgos a través de su ámbito competencial).						
Prácticas de Gobierno	Entradas específicas de Riesgo (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgo (adicionales a las Salidas de COBIT 5)			
	De	Descripción	Descripción			
EDM03.03 Supervisar la gestión de riesgos. Supervisar las metas y métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución.	No son relevantes para esta práctica entradas y salidas específicas de riesgo. Las entradas y salidas genéricas de COBIT 5 se pueden utilizar como orientación adicional.					
Actividades específicas de Riesgo (adicionales a las Actividades de COBIT 5)						
No es relevante para esta práctica una guía específica de riesgo. Las actividades genéricas de COBIT 5 se pueden utilizar como orientación adicional.						

AP012 Gestionar el Riesgo		Área: Gestión Dominio: Alinear, Planificar y Organizar		
COBIT 5 Descripción del Proceso Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.				
COBIT 5 Declaración del Propósito del Proceso Integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI.				
APO12 Metas y Métricas Específicas de Riesgo del Proceso				
No son relevantes para esta práctica metas y métricas específicas de riesgo. Las metas y métricas genéricas de COBIT 5 se pueden utilizar como orientación adicional.				
APO12 Prácticas, Entradas/Salidas, Actividades y Actividades Detalladas específicas de Riesgo del Proceso				
Prácticas de Gestión	Entradas específicas de Riesgo (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgo (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO12.01 Recopilar datos. Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.	No son relevantes para esta práctica entradas y salidas específicas de riesgo. Las entradas y salidas genéricas de COBIT 5 se pueden utilizar como orientación adicional.			
Actividades específicas de Riesgo (adicionales a las Actividades de COBIT 5)				
1. Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con los riesgos de TI, con capacidad para varios tipos de eventos, múltiples categorías de riesgos de TI y de múltiples factores de riesgo. 1.1 Establecer y mantener un modelo para la recogida, clasificación y análisis de datos sobre los riesgos de TI; 1.2 Acomodar múltiples tipos de eventos y varias categorías de riesgos de TI; 1.3 Incluir filtros y vistas para ayudar a determinar cómo los factores de riesgo específicos pueden afectar el riesgo; 1.4 El modelo debería apoyar la medición y evaluación de los atributos de riesgo a través de dominios de riesgo de TI y proporcionar información útil para el establecimiento de incentivos para una cultura de concienciación de riesgos.				
2. Registrar los datos pertinentes acerca del entorno corporativo interno y externo que puedan desempeñar un papel importante en la gestión de riesgos de TI. 2.1 Registrar los datos del entorno operativo de la empresa que puedan desempeñar un papel importante en la gestión de riesgos de TI; 2.2 Consultar fuentes internas de la empresa, departamento jurídico, de auditoría, de cumplimiento y la oficina del CIO; 2.3 Cubrir las principales fuentes de ingresos, los sistemas externos de TI, la responsabilidad del producto, el panorama de regulación, la competencia dentro de la industria, las tendencias de TI, la alineación del competidor con los puntos de referencia clave, la relativa madurez en los negocios clave y en las capacidades de TI, y los problemas geopolíticos; 2.4 Estudiar y organizar los datos históricos de riesgos TI y la experiencia de pérdidas por parte de colegas del sector a través de registros de eventos basados en el sector, bases de datos y acuerdos del sector para la divulgación de eventos comunes.				
3 Estudiar y analizar los datos históricos de riesgos TI y la experiencia de pérdidas obtenida de datos y tendencias externos que estén disponibles, colegas del sector a través de registros de eventos basados en el sector, bases de datos y acuerdos del sector para la divulgación de eventos comunes; 3.1 Según el modelo de recogida de datos, registrar datos sobre eventos de riesgo que hayan causado o puedan causar impactos a los catalizadores del beneficio/valor de TI, a la entrega de proyectos y programas de TI, y / o a las operaciones y a la prestación de servicios de TI; 3.2 Recopilar información relevante de los asuntos relacionados, incidentes, problemas e investigaciones.				
4. Registrar datos sobre eventos de riesgo que hayan causado o puedan causar impactos a los catalizadores del beneficio/valor de TI, a la entrega de programas y proyectos de TI, y / o a las operaciones y a la prestación de servicios de TI. Capturar la información relevante de los asuntos relacionados, incidentes, problemas e investigaciones. 4.1 Organizar los datos recopilados y destacar los factores determinantes; 4.2 Determinar la existencia/no existencia de condiciones específicas cuando se experimentaron eventos de riesgo y cómo estas condiciones pueden haber afectado a la frecuencia de eventos y a la magnitud de las pérdidas; 4.3 Determinar los factores determinantes comunes presentes en múltiples eventos. Realizar análisis periódicos de eventos y de factores de riesgo para identificar problemas de riesgos nuevos o emergentes y para obtener una comprensión plena de los factores de riesgo internos y externos asociados.				

APÉNDICE C
PRINCIPALES PROCESOS DE GESTIÓN DE RIESGOS EN COBIT 5

APO12 Prácticas, Entradas/Salidas, Actividades y Actividades Detalladas específicas de Riesgo del Proceso (cont.)				
Prácticas de Gestión	Entradas específicas de Riesgo (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgo (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO12.02 Analizar el riesgo. Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo.	No son relevantes para esta práctica entradas y salidas específicas de riesgo. Las entradas y salidas genéricas de COBIT 5 se pueden utilizar como orientación adicional.			
Actividades específicas de Riesgo (adicionales a las Actividades de COBIT 5)				
<p>1. Definir el alcance y la profundidad adecuada de las actividades de análisis de riesgos teniendo en cuenta todos los factores de riesgo y la criticidad de los activos de negocio. Establecer el alcance del análisis de riesgos después de realizar un análisis de coste / beneficio.</p> <p>1.1 Definir el alcance de los análisis de riesgos de IT. Decidir sobre la amplitud y la profundidad esperada de los esfuerzos de análisis de riesgos. Considerar una amplia gama de opciones de alcance;</p> <p>1.2 Mapear los factores de riesgo relevantes y la criticidad del negocio con los activos / recursos y factores desencadenantes dentro del alcance;</p> <p>1.3 Focalizarse en el valor óptimo de los esfuerzos de análisis de riesgo, favoreciendo el alcance basado en procesos productivos y productos de la empresa por encima de las estructuras internas que no están directamente relacionados con los resultados del negocio;</p> <p>1.4 Establecer el alcance de análisis de riesgos después de un examen de la criticidad del negocio, el coste de la medida contra el valor esperado de la información y la reducción de la incertidumbre, y todos los requisitos fundamentales reguladores.</p> <p>2. Construir y actualizar periódicamente los escenarios de riesgo de TI, incluidos los escenarios compuestos de cascada y / o los tipos de amenazas coincidentes, y desarrollar expectativas para las actividades de control específicas, para las capacidades de detección y para otras medidas de respuesta.</p> <p>2.1 Estimar el riesgo de TI. Estimar la frecuencia probable y la magnitud probable de la pérdida o ganancia asociada con escenarios de riesgo de TI influenciados por los factores de riesgo aplicables;</p> <p>2.2 Estimar la cantidad máxima de daño que se pudiera sufrir o la oportunidad que se pudiera obtener;</p> <p>2.3 Considerar los escenarios compuestos de cascada y / o tipos de amenazas coincidentes;</p> <p>2.4 Sobre la base de los escenarios más importantes, desarrollar expectativas para los controles específicos, para la capacidad de detectar y para otras medidas de respuesta;</p> <p>2.5 Evaluar controles de operación conocidos y su efecto sobre la frecuencia probable, y la probable magnitud y los factores de riesgo aplicables;</p> <p>2.6 Estimar los niveles de exposición de riesgo residual y compararlos con la tolerancia al riesgo aceptable para identificar las exposiciones que pueden requerir una respuesta al riesgo.</p> <p>3. Estimar la frecuencia y la magnitud de la pérdida o ganancia asociada con los escenarios de riesgo de TI. Considerar todos los factores de riesgo aplicables, evaluar los controles operativos conocidos y estimar los niveles de riesgo residual.</p> <p>3.1 Identificar las opciones de respuesta a los riesgos. Examinar el rango de opciones de respuesta al riesgo, tales como evitar, reducir / mitigar, transferir / compartir, aceptar y explotar / aprovechar;</p> <p>3.2 Documentar la justificación y posibles compensaciones en toda la gama;</p> <p>3.3 Especificar requisitos de alto nivel para proyectos o programas que, basados en la tolerancia al riesgo, mitigarán el riesgo a niveles aceptables; identificar los costes, los beneficios y la responsabilidad de la ejecución del proyecto;</p> <p>3.4 Desarrollar los requisitos y expectativas de los controles materiales en los puntos más adecuados, o donde se espera que se produzcan para dar visibilidad significativa.</p> <p>4. Comparar el riesgo residual con la tolerancia al riesgo aceptable e identificar las exposiciones que pueden requerir una respuesta al riesgo.</p> <p>4.1 Realizar una revisión por homólogos de análisis de riesgos de TI. Realizar una revisión por homólogos de los resultados del análisis de riesgos antes de enviarlos a la gerencia para su aprobación y uso en la toma de decisiones.</p> <p>4.2 Confirmar que el análisis se documenta en función de los requisitos empresariales;</p> <p>4.3 Revisar las bases de las estimaciones de las probabilidades de pérdida / ganancia y de rangos;</p> <p>4.4 Verificar que los estimadores humanos fueron adecuadamente preparados de antemano y buscar evidencias de "jugar con el sistema", es decir, de elecciones conscientes o sospechosas de entradas que puedan originar un resultado deseado o esperado;</p> <p>4.5 Verificar que el nivel de experiencia y credenciales del analista eran apropiados para el alcance y la complejidad de la revisión;</p> <p>4.6 Proporcionar una opinión sobre si se logró la reducción esperada de la incertidumbre y de si el valor de la información obtenida supera el coste de la medición.</p>				

APO12 Prácticas, Entradas/Salidas, Actividades y Actividades Detalladas específicas de Riesgo del Proceso (cont.)				
Prácticas de Gestión	Entradas específicas de Riesgo (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgo (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO12.03 Mantener un perfil de riesgo. Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.	No son relevantes para esta práctica entradas y salidas específicas de riesgo. Las entradas y salidas genéricas de COBIT 5 se pueden utilizar como orientación adicional.			
Actividades específicas de Riesgo (adicionales a las Actividades de COBIT 5)				
<p>1. Los procesos de negocio de inventario, incluyendo personal de soporte, aplicaciones, infraestructura, instalaciones, registros manuales críticos, proveedores, suministradores y subcontratistas, y documentar la dependencia de los procesos de gestión de servicios de TI y de los recursos de la infraestructura de TI.</p> <p>1.1 Comprender la dependencia de las actividades clave del negocio respecto a los procesos de gestión de servicios de TI y los recursos de la infraestructura de TI.</p> <p>2. Determinar y acordar qué servicios de TI y qué recursos de infraestructura de TI son esenciales para mantener el funcionamiento de los procesos de negocio. Analizar las dependencias e identificar los eslabones débiles.</p> <p>2.1 Determinar qué servicios de TI y qué recursos de la infraestructura de TI son necesarios para mantener el funcionamiento de los servicios esenciales y los procesos críticos de negocio;</p> <p>2.2 Analizar las dependencias y los eslabones débiles a través de la "pila llena", es decir, desde la capa superior bajando hasta las instalaciones físicas;</p> <p>2.3 Obtener el consenso del negocio y el liderazgo de TI en la información más valiosa de la empresa y los activos relacionados con la tecnología.</p> <p>3. Agregar escenarios de riesgos actuales por categoría, línea de negocio y área funcional.</p> <p>3.1 Inventariar y evaluar la capacidad de procesado de TI, las habilidades y el conocimiento de las personas, y los resultados del desempeño de TI en todo el espectro de riesgos de TI (por ejemplo, la habilitación del beneficio / valor de TI, la entrega de programas y proyectos de TI, la operación y la prestación de servicios de TI);</p> <p>3.2 Determinar dónde la ejecución normal del proceso puede o no puede proporcionar los controles adecuados y la capacidad de tomar el nivel de riesgo aceptable;</p> <p>3.3 Identificar dónde reduciendo la variabilidad de resultados del proceso se puede contribuir a una estructura de control interno más sólida, mejorar las TI y el rendimiento del negocio y explotar / aprovechar las oportunidades.</p> <p>4. Regularmente, recopilar toda la información de los perfiles de riesgo y consolidarla en un perfil de riesgo agregado.</p> <p>4.1 Revisar la colección de atributos y valores a través de los componentes de escenarios de riesgos de TI y sus conexiones inherentes a las categorías de impacto empresarial.</p> <p>4.2 Ajustar las entradas basadas en las condiciones de riesgo cambiantes y las amenazas emergentes para la activación del beneficio / valor de las TI, la entrega de programas y proyectos de TI y la operación y prestación de servicios de TI.</p> <p>4.3 Actualizar distribuciones y rangos basados en la criticidad de los activos / recursos, los datos del entorno operacional y los datos de eventos de riesgo. Relacionar tipos de eventos con categorías de riesgo y con categorías de impacto empresarial.</p> <p>4.4 Agregar tipos de eventos por categoría, sector empresarial y área funcional.</p> <p>4.5 Como mínimo, actualizar los componentes de escenarios de riesgos de TI en respuesta a cualquier cambio interno o externo significativo, y revisarlas anualmente.</p> <p>5. Definir un conjunto de indicadores de riesgo, basado en todos los datos de los perfiles de riesgo, que permita la rápida identificación y seguimiento del riesgo actual y de las tendencias del riesgo.</p> <p>5.1 Capturar el perfil de riesgo mediante herramientas tales como un registro de riesgos de TI y un mapa de riesgos de TI;</p> <p>5.2 Construir el perfil de riesgo a través de los resultados de la evaluación de los riesgos de TI de la empresa, los componentes de escenarios de riesgos, la recopilación de datos de eventos de riesgo, análisis de riesgos en curso y los resultados de evaluación independientes de TI;</p> <p>5.3 Para las entradas de registro de riesgos de TI individuales, actualizar los atributos clave como el nombre, descripción, propietario, frecuencia esperada/actual y la magnitud potencial / real de escenarios asociados, el impacto en el negocio potencial / actual y la disposición.</p> <p>6. Capturar información sobre eventos de riesgo de TI que se han materializado, para su inclusión en el perfil de riesgos de TI de la empresa.</p> <p>6.1 Diseñar métricas o indicadores que puedan apuntar a los eventos e incidentes relacionados con las TI que pueden afectar significativamente el negocio;</p> <p>6.2 Basar los indicadores en un modelo de lo que pone en peligro la exposición y la capacidad de gestión de riesgos;</p> <p>6.3 Ofrecer una gestión con una comprensión de los indicadores de riesgo útiles y potencialmente claves;</p> <p>6.4 Revisar periódicamente los indicadores clave de riesgo en uso por la dirección, y recomendar ajustes ante cambios de las condiciones internas y externas.</p>				

APÉNDICE C
PRINCIPALES PROCESOS DE GESTIÓN DE RIESGOS EN COBIT 5

APO12 Prácticas, Entradas/Salidas, Actividades y Actividades Detalladas específicas de Riesgo del Proceso (cont.)				
Prácticas de gestión	Entradas específicas de Riesgo (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgo (adicionales a las Salidas de COBIT 5)	
	De	Descripción	Descripción	A
APO12.04 Expresar el riesgo. Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada.	No son relevantes para esta práctica entradas y salidas específicas de riesgo. Las entradas y salidas genéricas de COBIT 5 se pueden utilizar como orientación adicional.			
Actividades específicas de Riesgo (adicionales a las Actividades de COBIT 5)				
<p>1. Reportar los resultados de análisis de riesgos a todas las partes interesadas afectadas en los términos y formatos útiles para respaldar las decisiones empresariales. Siempre que sea posible, incluir las probabilidades y los rangos de pérdida o ganancia, junto con los niveles de confianza que permiten a la dirección equilibrar el ratio retorno-riesgo.</p> <ul style="list-style-type: none"> 1.1 Coordinar la actividad de análisis de riesgo adicional como es requerido por los tomadores de decisiones (por ejemplo, informe de rechazo, ajuste de alcance); 1.2 Comunicar claramente el contexto de riesgo-retorno; 1.3 Identificar los impactos negativos de los eventos / escenarios, que deberían conducir las decisiones de respuesta, y los efectos positivos de eventos / escenarios que representan la gestión de oportunidades, que deberían canalizarse de nuevo en la estrategia y el proceso de establecimiento de objetivos. <p>2. Ayudar a los tomadores de decisiones a comprender los peores casos y los escenarios más probables, las exposiciones de debida diligencia y la reputación significativa, consideraciones legales o reglamentarias.</p> <p>2.1 En este esfuerzo, incluir lo siguiente:</p> <ul style="list-style-type: none"> • Los componentes clave de riesgo (por ejemplo, la frecuencia, magnitud, impacto) y los factores de riesgo clave y sus efectos estimados; • Magnitud de pérdida probable estimada o probable ganancia futura; • Estimación del extremo superior de la pérdida / ganancia potencial y escenario/s más probable/s de pérdida / ganancia (por ejemplo, una frecuencia probable pérdida de entre tres y cinco veces al año, y una magnitud probable de pérdida de entre \$50.000 y \$100.000, con un 90 por ciento de confianza); • Información relevante adicional para apoyar las conclusiones y recomendaciones del análisis. <p>3. Reportar el perfil actual de riesgos a todas las partes interesadas, incluida la eficacia del proceso de gestión de riesgos, el control de la eficacia, las lagunas, incoherencias, redundancias, estado de remediación, y sus impactos sobre el perfil de riesgo.</p> <p>3.1 Conocer las necesidades de informes de riesgo de las diversas partes interesadas (por ejemplo, dirección, comité de riesgos, funciones de control de riesgos, dirección de unidades de negocio) mediante la aplicación de los principios de pertinencia, eficiencia, puntualidad y exactitud de los informes;</p> <p>3.2 Incluir lo siguiente en el informe: el control de eficacia y rendimiento, problemas y carencias, el estado de la remediación, eventos e incidentes y sus impactos en el perfil de riesgo, el rendimiento de los procesos de gestión de riesgos;</p> <p>3.3 Proveer entradas para informes empresariales integrados.</p> <p>4. Revisar los resultados de las evaluaciones objetivas de terceros, de la auditoría interna y de las revisiones de controles de calidad y asignarlos al perfil de riesgo. Revisar las lagunas identificadas y las exposiciones para determinar la necesidad de un análisis de riesgo adicional.</p> <p>4.1 Extraer las lagunas y las exposiciones de la empresa para valorar su disposición o la necesidad de un análisis de riesgos;</p> <p>4.2 Ayudar a la empresa a comprender cómo los planes de acción correctivos afectarán el perfil de riesgo global;</p> <p>4.3 Identificar oportunidades para la integración con otros esfuerzos de remediación y las actividades de gestión de riesgos en curso.</p> <p>5. De forma periódica, para zonas con riesgo relativo y capacidad de riesgo paritarias, identificar oportunidades relacionadas con TI que permitan la aceptación de un mayor riesgo y mayor crecimiento y rentabilidad.</p> <p>5.1 Buscar oportunidades donde las TI se puedan utilizar para:</p> <ul style="list-style-type: none"> • Aprovechar los recursos empresariales en la creación de ventajas competitivas (por ejemplo, utilizar la información existente en formas nuevas, aprovechar mejor los recursos humanos y empresariales; • Reducir los costes de coordinación de la empresa; • Aprovechar las economías de escala y de alcance en ciertos recursos estratégicos clave comunes a varias líneas de negocio; • Aprovechar las diferencias estructurales con los competidores; • Coordinar las actividades entre las unidades de negocio o en la cadena de valor; 				

APO12 Prácticas, Entradas/Salidas, Actividades y Actividades Detalladas específicas de Riesgo del Proceso (cont.)							
Prácticas de gestión	Entradas específicas de Riesgo (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgo (adicionales a las Salidas de COBIT 5)				
	A	Descripción	Descripción	A			
APO12.05 Definir un portafolio de acciones para la gestión de riesgos. Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.	No son relevantes para esta práctica entradas y salidas específicas de riesgo. Las entradas y salidas genéricas de COBIT 5 se pueden utilizar como orientación adicional.						
Actividades específicas de Riesgo (adicionales a las Actividades de COBIT 5)							
<p>1. Mantener un inventario de las actividades de control implantadas para gestionar el riesgo y que permita que los riesgos se adecúen al apetito de riesgo y a la tolerancia. Clasificar las actividades de control y asignarlas a las declaraciones de riesgo de TI específicas y a las agregaciones de riesgos de TI.</p> <p>1.1 A través de las áreas de enfoque de riesgo, inventariar los controles establecidos para gestionar riesgos y permitir que los riesgos se adecúen al apetito de riesgo y a la tolerancia;</p> <p>1.2 Clasificar los controles (por ejemplo, predictivo, preventivo, detectivo, correctivo) y asignarlos a las declaraciones de riesgo de TI específicas y a las agregaciones de riesgos de TI.</p> <p>2. Determinar si cada entidad organizativa monitorea el riesgo y acepta la responsabilidad de operar dentro de sus niveles de tolerancia tanto individual como de portafolio.</p> <p>2.1 Supervisar la alineación operacional con los umbrales de tolerancia al riesgo;</p> <p>2.2 Asegurar que cada línea de negocio acepta la responsabilidad de operar dentro de sus niveles de tolerancia tanto individual como de portafolio y de incorporar las herramientas de monitoreo en los procesos operativos clave;</p> <p>2.3 Supervisar el rendimiento del control, y medir la variación de los umbrales respecto de los objetivos.</p> <p>3. Definir un conjunto equilibrado de propuestas de proyectos destinados a reducir el riesgo y / o proyectos que faciliten las oportunidades empresariales estratégicas, teniendo en cuenta el coste / beneficio, los efectos sobre el perfil de riesgo actual y la regulación.</p> <p>3.1 Responder a la exposición al riesgo y a las oportunidades descubiertas;</p> <p>3.2 Seleccionar controles de TI candidatos basándose en amenazas específicas, el grado de exposición al riesgo, la pérdida probable y los requisitos obligatorios especificados en los estándares de TI;</p> <p>3.3 Supervisar los cambios en los perfiles de riesgo operacional de negocio subyacentes y ajustar la clasificación de los proyectos de respuesta a los riesgos;</p> <p>3.4 Comunicar con los grupos de interés clave al principio del proceso;</p> <p>3.5 Realizar pruebas piloto y revisar los datos de rendimiento para verificar el funcionamiento respecto al diseño;</p> <p>3.6 Mapear controles operativos nuevos y actualizados para monitorear mecanismos que permitan medir el rendimiento de control a través del tiempo y una rápida acción correctiva de la gerencia cuando sea necesario;</p> <p>3.7 Identificar y capacitar al personal en los nuevos procedimientos que se han implementado;</p> <p>3.8 Informar acerca del progreso del plan de acción de riesgos de TI. Monitorear los planes de acción de riesgos de TI a todos los niveles para garantizar la eficacia de las acciones necesarias y para determinar si se obtuvo la aceptación del riesgo residual;</p> <p>3.9 Garantizar que las acciones comprometidas son propiedad del o de los dueños del proceso afectado y que las desviaciones son reportadas a la alta dirección.</p>							

APÉNDICE C
PRINCIPALES PROCESOS DE GESTIÓN DE RIESGOS EN COBIT 5

APO12 Prácticas, Entradas/Salidas, Actividades y Actividades Detalladas específicas de Riesgo del Proceso (cont.)								
Prácticas de Gestión	Entradas específicas de Riesgo (adicionales a las Entradas de COBIT 5)		Salidas específicas de Riesgo (adicionales a las Salidas de COBIT 5)					
	De	Descripción	Descripción	A				
APO12.06 Responder al riesgo. Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.	No son relevantes para esta práctica entradas y salidas específicas de riesgo. Las entradas y salidas genéricas de COBIT 5 se pueden utilizar como orientación adicional.							
Actividades específicas de Riesgo (adicionales a las Actividades de COBIT 5)								
<p>1. Preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave. Asegurar que los planes incluyan vías de escalado a través de la empresa.</p> <p>1.1 Prepararse para la materialización de las amenazas a través de planes que documenten los pasos específicos a seguir cuando un evento de riesgo pueda causar un impacto a nivel operativo, en el desarrollo y / o estrategia de negocio (es decir, incidentes relacionados con IT) o cuando ya haya causado un impacto en el negocio;</p> <p>1.2 Mantener una comunicación abierta acerca de la aceptación del riesgo, las actividades de gestión de riesgos, técnicas de análisis y resultados disponibles para ayudar en la preparación del plan;</p> <p>1.3 En el desarrollo de planes de acción, tener en cuenta el tiempo que puede estar la empresa expuesta así como el tiempo que puede tardar en recuperarse;</p> <p>1.4 Definir las vías de escalado en toda la empresa, desde la línea de dirección a los comités ejecutivos.</p> <p>1.5 Verificar que los planes de respuesta a incidentes de procesos altamente críticos son adecuados.</p>								
<p>2. Categorizar incidentes, y comparar la exposición real respecto a los umbrales de tolerancia al riesgo. Comunicar los impactos de negocio a los tomadores de decisiones en el marco de presentación de informes, y actualizar el perfil de riesgo.</p> <p>2.1 Monitorear los riesgos de TI. Monitorear el entorno.</p> <p>2.2 Cuando un límite de control se ha incumplido, escalar al siguiente paso o confirmar que la medida está de nuevo dentro de los límites.</p> <p>2.3 Garantizar que la política se sigue y que existe una clara responsabilidad para las acciones de seguimiento.</p>								
<p>3. Aplicar el plan de respuesta adecuado para minimizar el impacto cuando se produzcan incidentes de riesgo.</p> <p>3.1 Iniciar la respuesta a incidentes;</p> <p>3.2 Adoptar medidas para minimizar el impacto de un incidente en curso;</p> <p>3.3 Identificar la categoría del incidente y seguir los pasos en el plan de respuesta;</p> <p>3.4 Informar a todas las partes interesadas y a las partes afectadas de que se está produciendo un incidente;</p> <p>3.5 Identificar la cantidad de tiempo necesaria para llevar a cabo el plan y hacer los ajustes, según sea necesario, para la situación en cuestión;</p> <p>3.6 Asegurar que se adoptan las medidas adecuadas.</p>								
<p>4. Examinar los eventos / pérdidas adversos pasados y la pérdida de oportunidades y determinar las causas raíz. Comunicar la causa raíz, los requisitos adicionales de respuesta al riesgo y las mejoras en los procesos a los procesos de gobierno de riesgos y a los tomadores de decisiones adecuados;</p> <p>4.1 Comunicar las lecciones aprendidas de los eventos de riesgo;</p> <p>4.2 Examinar últimos eventos / pérdidas adversas y las oportunidades perdidas;</p> <p>4.3 Determinar si hubo una falla derivada de la falta de conciencia, la capacidad o motivación;</p> <p>4.4 Investigar la causa raíz de eventos de riesgo similares y la eficacia relativa de las acciones tomadas antes y ahora;</p> <p>4.5 Determinar la magnitud de cualquier problema subyacente;</p> <p>4.6 Identificar correcciones tácticas; potenciales inversiones en proyectos; o ajustes en los procesos globales de riesgos en materia de gobierno, evaluación y / o respuesta;</p> <p>4.7 Integrarse con el proceso de soporte de escritorio y de respuesta a incidentes de TI y con el proceso de gestión de problemas de TI para identificar y corregir la causa raíz subyacente;</p> <p>4.8 Identificar la causa raíz de los incidentes que afecten a la prestación de beneficio / valor de TI y la entrega de programas y proyectos de TI a través de la comunicación abierta con el negocio en conjunto y con las funciones de TI. Solicitar análisis de riesgos adicionales cuando sea necesario.</p> <p>4.9 Comunicar la causa raíz, los requisitos adicionales de respuesta al riesgo y las mejoras en los procesos a los procesos de gobierno de riesgos y a los tomadores de decisiones adecuados.</p>								

Página dejada en blanco intencionadamente

APÉNDICE D

EL USO DE CATALIZADORES DE COBIT5 PARA REDUCIR LOS ESCENARIOS DE RIESGO EN TI

Introducción

En este apéndice se ofrece una serie de ejemplos sobre cómo COBIT 5 facilitadores pueden utilizarse para responder a situaciones de riesgo. Los escenarios de riesgo se identificaron en la sección 2B, en el capítulo 3 de esta publicación.

En el proceso de respuesta al riesgo, la mitigación del riesgo se identifica como una de las opciones para responder a cualquier riesgo excesivo. Mitigación de riesgos de TI es equivalente a la aplicación de una serie de controles de TI. En COBIT 5 términos, controles de TI puede ser cualquier facilitador, por ejemplo, la puesta en marcha de una estructura de organización, puesta en marcha de ciertas prácticas o actividades de gobierno o de gestión, etc

Para cada una de las categorías de riesgo, las acciones de mitigación potenciales relacionados con los siete COBIT 5 facilitadores se proporcionan, con una referencia, el título y la descripción de cada capacitador que pueden ayudar a mitigar el riesgo.

Al utilizar los ejemplos en este apéndice, el lector debe tener en cuenta que:

- Las tablas no sustituyen el ejercicio de análisis de riesgo. Las categorías de riesgo que aquí se presentan son de carácter genérico y en sí mismos pueden cubrir muchos escenarios derivados y variables. Toda empresa necesita primero para personalizar y definir su propio conjunto de escenarios de riesgo.
- Las tablas deben ser personalizados. Cada situación es única y necesita todos los riesgos y todos los factores de riesgo que rodean a considerar antes se definen las medidas de mitigación de riesgos.
- Los controles sugeridos no son absolutos. Ellos deben ser sopesados en términos de costo / beneficio, es decir, qué tan efectivos serán en la reducción del riesgo y el costo es de implementar. El efecto de la acción atenuante sobre el potencial impacto y frecuencia del riesgo debe ser estimado y depende de la madurez de la ejecución, el contexto de la empresa, etc. Cuando se estima el efecto en el impacto y frecuencia de ser "alto", la acción puede ser considerado "esencial" para la empresa.
- La lista sugerida de los controles puede no ser completa para una situación particular, por lo que el usuario debe estar preparado para analizar cuidadosamente si los controles se deben agregar (o quitado) en función de cada situación. Para algunos escenarios, puede ser necesaria una guía adicional y más detallada. Ejemplos de ello son elementos de información de riesgos y controles de seguridad, tales como la gestión de vulnerabilidad o de análisis de seguridad de la aplicación.

El valor de esta sección se enlaza con:

- **Análisis de evaluación de riesgos** -Cuando la frecuencia y el impacto deben ser evaluados, los controles / facilitadores deben tenerse en cuenta para determinar el impacto y debe realizarse una evaluación realista de su frecuencia. Medidas de control inapropiadas son factores de riesgo importantes.
- **Disminución del riesgo**- Cuando se requiere disminuir el riesgo, es decir, cuando estén definidos e implementados los controles / facilitadores. Los siguientes cuadros nos presentan una serie de controles sugeridos que pueden ayudar a mitigar el riesgo en cuestión.

Nota: Las tablas que relacionan cada categoría de riesgo a un conjunto de los facilitadores atenuantes, se mantiene en un nivel muy genérico, proporcionando así un punto de partida para el análisis y mitigación de riesgos. Cada empresa tendrá que adaptar el conjunto de estos facilitadores necesarios para analizar y mitigar cada escenario de riesgo específicos que tenga que manejar.

D.1. Escenario 1: Establecimiento y Mantenimiento de la cartera		
Categoría del Escenario del Riesgo	Cartera de establecimiento y de mantenimiento	
Principios, políticas y marcos facilitadores		
Referencia	Contribución para dar respuesta a la situación	
Política de gestión del programa/proyecto	Para hacer cumplir el uso de la metodología general del programa / proyecto, incluyendo la política corporativa en caso de negocio o la debida diligencia a fin de mejorar la visibilidad del valor relativo de los programas (en comparación con los demás). Esta política debe describir los umbrales de inversión de aprobación para el valor del programa.	
Procesos facilitadores para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
EDM02.01	Evaluar la optimización de la valoración	Evaluar continuamente la cartera de inversiones, servicios y activos de TI habilitados para determinar la probabilidad de alcanzar los objetivos de la empresa y la entrega de valor a un costo razonable. Identificar y hacer un juicio sobre cualquier cambio en la dirección que hay que conceder a la gestión para optimizar la creación de valor.
EDM02.02	Optimización de la valoración directa.	Principios y prácticas de gestión de valor directo para permitir la realización del valor óptimo de TIC disponible para las inversiones a lo largo de su ciclo de vida económico.
EDM02.03	Supervisar la valoración optimizada	Supervisar las metas y las métricas clave para determinar el grado en que el negocio está generando el valor y los beneficios para la empresa de inversiones y servicios posibilitados por TI esperado. Identificar los problemas importantes y considerar las acciones correctivas.
APO01.01	Definir la estructura organizativa.	Establecer una estructura organizativa interna y extendida que refleje las necesidades y prioridades del negocio de TI. Poner en marcha las estructuras de gestión necesarias (por ejemplo, comités) que permitan la toma de decisiones para que la gestión se lleve a cabo de la manera más eficaz y eficiente.
APO01.04	Gestionar la comunicación de los objetivos y su desviación	Comunicar la conciencia y comprensión de los objetivos y la dirección de TIC a las partes interesadas y a los usuarios apropiados a lo largo de la empresa.
APO02.03	Definir las capacidades TI destinadas al negocio.	Definir las capacidades TIC y los servicios de TIC que requiere el negocio. Basándose en la comprensión del medio y las necesidades de la empresa; evaluando los procesos de negocio actual y el entorno TIC y los problemas; considerándose las normas de referencia, las mejores prácticas y el arte de las tecnologías emergentes o las propuestas de innovación.
APO04.03	Supervisar y analizar el entorno tecnológico	Lleve a cabo un control sistemático y la exploración de entorno externo de la empresa para identificar las tecnologías emergentes que tienen el potencial de crear valor (por ejemplo, mediante la realización de la estrategia empresarial, la optimización de costes, evitando la obsolescencia, y mejor capacitación de Servicios y procesos de TIC). Vigilar el mercado, el entorno competitivo, los sectores de la industria, y las tendencias legales y reglamentarias para poder analizar las tecnologías emergentes o ideas de innovación en el contexto empresarial.
APO05.01	Establecer la combinación de inversiones destinadas al negocio	Revisar y asegurar la claridad de la empresa y las estrategias de TIC y servicios actuales. Defina una combinación de inversiones adecuada basada en el precio, la alineación con la estrategia y las medidas financieras tales como el costo y el retorno de la inversión esperado durante el ciclo de vida económico, el grado de riesgo, y el tipo de beneficio para los programas de la cartera. Ajuste la empresa y en su caso las estrategias de TI.
APO05.03	Evaluación y seleccionar los programas para financiar..	Sobre la base de las necesidades globales en la cartera de inversión, se evalúa y se da prioridad a los casos de negocios del programa, y se decide sobre las propuestas de inversión. Asignándose fondos para iniciar los programas.
APO05.05	Mantener cartera.	Mantener carteras de programas y proyectos, servicios de TIC y de los activos de TIC de inversión.
APO06.02	Priorizar la asignación de recursos.	Implementar un proceso de toma de decisiones para priorizar la asignación de recursos y las reglas para las inversiones discretionales por unidades de negocio individuales. Se incluye el uso potencial de los proveedores de servicios externos y se consideran la compra, el desarrollo y la opciones de alquiler.
BAI02.01	Definir y mantener los requisitos comerciales funcionales y técnicos	Basado en el modelo de negocio, identificar, priorizar, especificar y acordar información comercial, requisitos funcionales, técnicas y de control que cubren el alcance / comprensión de todas las iniciativas necesarias para alcanzar los resultados esperados de la solución de negocio habilitado para TI propuesto.

EL USO DE FACILITADORES DE COBIT 5 PARA REDUCIR LOS ESCENARIOS DE RIESGO EN TI

D.1. Escenario 1: Establecimiento y Mantenimiento de la cartera (cont.)	
Catalizador de estructuras organizativas	
Referencia	Contribución para dar respuesta a la situación
Oficina de Gestión de Programas y Proyectos (PMO)	Responsable de la calidad de los casos de negocios
Junta	Se requiere la aprobación cuando los programas superan un determinado umbral de valor y nivel de riesgo.
CFO	Ayuda con la alineación de la estrategia y las prioridades, visión general sobre los programas.
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta	
Referencia	Contribución para dar respuesta a la situación
Selección de programas que incluya decisiones basadas en datos	La emoción y la política no será un factor dominante en la toma de decisiones.
Compromiso con las partes interesadas	Se tomará la gama completa de los factores de éxito a la hora de seleccionar los programas.
Centrarse en los objetivos empresariales	Asegurar la alineación con la estrategia y las prioridades de la empresa.
Catalizador para alcanzar los objetivos de información	
Referencia	Contribución para dar respuesta a la situación
Programa del caso de negocio	Mejora la visibilidad del valor relativo de los programas (en comparación con el uno al otro)
Definir las combinaciones de inversión	Mejora la visibilidad del valor relativo de los programas (en comparación con el uno al otro)
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones	
Referencia	Contribución para dar respuesta a la situación
Cartera de herramientas de gestión	Reducir la complejidad y aumentar la visión general de los programas y proyectos.
Facilitado para alcanzar los objetivos de las personas, sus habilidades y competencias	
Referencia	Contribución para dar respuesta a la situación
Habilidades financieras del programa/proyecto	Crear visibilidad sobre el valor del programa.
Análisis del negocio	Transparencia en la estrategia empresarial, los requisitos y las prioridades del negocio relacionados
Habilidades relacionadas con el marketing	Crear visibilidad sobre el valor del programa.

D.2. Escenario 2: Gestión del Ciclo de Vida del Programa/Proyecto		
Categoría del escenario de riesgo		Gestión del ciclo de vida del programa / proyecto (iniciación del programa / proyecto, la economía, la entrega, la calidad y la terminación)
Catalizador para alcanzar los objetivos de los principios, políticas y los libros de acuerdos		
Referencia	Contribución para dar respuesta a la situación	
Política de gestión del programa/proyecto	<p>El grado de visibilidad y el grado de transparencia i vigencia para los tomadores de las decisiones, su medición debe estar basado en un lenguaje y metodología comunes:</p> <ul style="list-style-type: none"> - Conciencia respecto de los proyectos que fallan (en términos de costo, los retrasos, la corrupción del alcance, cambió de las prioridades del negocio, etc) y crear flujos de información para inducir a una acción correctiva. - Para evitar la falla en los cambios en el alcance de los proyectos existentes deben administrarse de forma estricta 	
Proceso facilitador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
EDM02.03	Supervisar la valoración optimizada	Supervisar las metas y las métricas clave para determinar el grado en que el negocio está generando el valor y los beneficios para la empresa de inversiones y servicios posibilitados por las TIC. Identificar los problemas importantes y considerar las acciones correctivas.

D.2. Escenario 2: Gestión del Ciclo de vida del Programa/Proyecto (cont.)

Proceso facilitador para alcanzar el objetivo(cont.)		
Referencia	Título	Práctica de Gestión
APO01.01	Definir la estructura organizativa.	Establecer una estructura organizativa interna y extendida que refleje las necesidades y prioridades del negocio de TIC. Poner en marcha las estructuras de gestión necesarias (por ejemplo, comités) que permitan la toma de decisiones para que la gestión se lleve a cabo de la manera más eficaz y eficiente.
APO06.04	Modelar y asignar costos.	Establecer y utilizar un modelo de TIC de costes basados en la definición del servicio, asegurando que la asignación de los costes de los servicios sea identificable, medible y predecible, para fomentar el uso responsable de los recursos incluidos los proporcionados por los proveedores de servicios. Revisar periódicamente y comparar la adecuación del modelo de costes / devolución de cargo para mantener su pertinencia e idoneidad de las actividades de TIC empresarial y cambiante.
APO06.05	Administrar los costes.	Implementar un proceso de gestión de costes que compare los costos reales con los presupuestados. Los costes deben ser supervisados y reportados y, en el caso de desviaciones, identificar en forma oportuna, su impacto en los procesos y servicios de la empresa evaluada.
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 actividades de toma de decisiones y de gestión de la entrega centrándose en la realización del valor y en los objetivos (requisitos, riesgos, costos, horario, calidad) para el negocio con la gobernanza de manera coherente y con la revisión por parte de la dirección.
BAI01.02	Iniciar un programa	Iniciar un programa para confirmar los beneficios esperados y obtener la autorización para proceder. Esto incluye acordar el patrocinio del programa, se confirma el mandato del programa a través de la aprobación del modelo de negocio conceptual, se nombra a al consejo del programa o miembros del comité, la producción breve del plan del programa, la revisión y la actualización del modelo de negocio, el desarrollo de un plan de generación de beneficios, y se procede a obtener la aprobación de los patrocinadores.
BAI01.03	Gestionar los grupos de interés.	Administrar los grupos de interés para asegurar un intercambio activo de información precisa, coherente y oportuna que llegue a todos los interesados pertinentes. Esto incluye la planificación, la identificación y participación de los interesados y la gestión de sus expectativas.
BAI01.04	Desarrollar y mantener la planificación del programa	Formular un programa para preparar el terreno inicial y posicionarlo para la ejecución exitosa de la formalización del alcance del trabajo a realizar y la identificación de los entregables que satisfagan sus objetivos y ofrecer valor. Mantener y actualizar el plan del programa y modelo de negocio en todo el ciclo de vida económico del programa, lo que garantiza la alineación con los objetivos estratégicos y reflejará la situación actual y las perspectivas actualizadas obtenidas hasta la fecha.
BAI01.05	Iniciar y ejecutar el programa	Iniciar y ejecutar el programa para adquirir y dirigir los recursos necesarios para lograr los objetivos y beneficios del programa tal como se define en el plan del programa. De acuerdo con la etapa para liberar los criterios de revisión, y prepararse para la siguiente etapa, de iteración o liberar opiniones para informar sobre la marcha del programa y para ser capaz de hacer que el caso alcance su financiación hasta la etapa siguiente para liberar la revisión.
BAI01.06	Supervisar, controlar e informar sobre los resultados del programa.	Supervisión y control del programa (entrega de la solución) y de la empresa (valor / resultado) el rendimiento contra el plan en todo el ciclo de vida económico de la inversión. Señalar este rendimiento con el comité directivo del programa y de los patrocinadores.
BAI01.07	Puesta en marcha e iniciar los proyectos dentro de un programa.	Definir y documentar la naturaleza y el alcance del proyecto para confirmar y desarrollar entre las partes interesadas una comprensión común del alcance del proyecto y cómo se relaciona con otros proyectos dentro del programa general de inversión en TIC. La definición debe ser aprobada formalmente por el programa y los patrocinadores del proyecto.
BAI01.08	Planificación de los proyectos.	Establecer y mantener un plan formal, aprobado integrada de proyectos (que abarca los negocios y los recursos de TIC) para guiar la ejecución del proyecto y el control a lo largo de la vida del proyecto. El alcance de los proyectos debe estar claramente definido y ligado a la construcción o mejora de la capacidad empresarial.
BAI01.09	Administrar los programas y la calidad del proyecto. .	Elaborar y ejecutar un plan de gestión de la calidad, los procesos y las prácticas, en línea con el SGC que describe el programa y el enfoque de la calidad del proyecto y cómo se implementará. El plan debe ser revisado y acordado por todas las partes interesadas y luego incorporados en el programa integrado y planes de proyecto formalmente.
BAI01.10	Administrar los programas y el riesgo del proyecto.	Eliminar o minimizar los riesgos específicos asociados a los programas y proyectos a través de un proceso sistemático de planificación, identificación, análisis, respuesta y seguimiento y control de las áreas o eventos que tienen el potencial de causar un cambio no deseado. Los riesgos que enfrentan los programas y la gestión del proyecto debe ser establecido y registrado de forma centralizada.

EL USO DE FACILITADORES DE COBIT 5 PARA REDUCIR LOS ESCENARIOS DE RIESGO EN TI

D.2. Escenario 2: Gestión del Ciclo de vida del Programa/Proyecto (cont.)		
Proceso facilitador para alcanzar el objetivo(cont.)		
Referencia	Título	Práctica de Gestión
BAI01.11	Supervisar y controlar proyectos	Medir el desempeño del proyecto contra los criterios clave de rendimiento del proyecto, tales como plazos, calidad, costo y riesgo. Se Identifica cualquier desviación de lo esperado. Evaluando el impacto de las desviaciones sobre el proyecto y el programa en general, y se comunica los resultados a las partes interesadas clave.
BAI01.12	Administrar los recursos del proyecto y los paquetes de trabajo. .	Administrar los paquetes de trabajo del proyecto mediante la colocación de los requisitos formales relativos a la autorización y aceptación de los paquetes de trabajo y la asignación y coordinación de negocio adecuado y los recursos de TIC.
BAI01.13	Cerrar un proyecto y sus iteraciones	Al final de cada proyecto, la liberación o la iteración, requiere a los interesados en el proyecto para determinar si el proyecto, la liberación o la iteración entregan los resultados y los valores previstos. Se Identifican y comunican las actividades pendientes necesarias para alcanzar los resultados planificados del proyecto y los beneficios del programa, y se identifican y documentan las lecciones aprendidas para su uso en futuros proyectos, comunicados, iteraciones y programas.
Catalizador de estructuras organizativas		
Referencia	Contribución para dar respuesta a la situación	
Oficina de Gestión de Programas y Proyectos (PMO)	Garantizar la coherencia de planteamientos en el seguimiento del programa / proyecto.	
CIO	Toma las medidas correctivas si es necesario	
Promotor del programa/proyecto	En general, el responsable de seguimiento del presupuesto y en la demostración del valor	
Dirección del programa o proyecto	En general, el responsable de seguimiento del presupuesto y en la demostración del valor	
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta		
Referencia	Contribución para dar respuesta a la situación	
La supervisión del programa / proyecto incluye actividades orientadas a medir datos	Las emociones y la política no será un factor dominante en la toma de decisiones	
Admitir que las malas noticias sean resueltas por la alta dirección	Permite avanzarse a la toma de decisiones y minimiza el impacto	
Programa que beneficie la realización del plan	Esta entrada le proporcionará los datos necesarios para realizar un seguimiento del progreso y estimar el potencial rebasamiento.	
Registro de los beneficios y presupuesto del programa	Esta entrada le proporcionará los datos necesarios para realizar un seguimiento del progreso y estimar el potencial rebasamiento.	
Informe sobre la situación del programa	Medición de la visibilidad y del estado real de los tomadores de decisiones que deben estar basadas en un lenguaje y una metodología comunes.	
Catalizadores para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones		
Referencia	Contribución para dar respuesta a la situación	
Cartera de herramientas de gestión	Aumentar la transparencia de la situación presupuestaria.	
Catalizadores para alcanzar los objetivos de las personas, sus habilidades y competencias		
Referencia	Contribución para dar respuesta a la situación	
Rendimiento de las habilidades en control presupuestario	Las habilidades analíticas correctas permiten la estimación de las consecuencias de los proyectos que fallan por posibles excesos de presupuesto.	

D.3. Escenario 3: Toma de decisiones de inversión en TIC		
Categoría del escenario de riesgo	La toma de decisiones de inversión en TIC	
Catalizadores para alcanzar los objetivos de los principios, políticas y los libros de acuerdos		
Referencia	Contribución para dar respuesta a la situación	
Política de gestión del programa/proyecto	La política debe definir quién debe participar en las decisiones de inversión y de la cadena de aprobación.	
Proceso facilitador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
APO05.06	Gestione el beneficio de los logros	Supervisar los beneficios de proporcionar y mantener los servicios y capacidades de TIC adecuados, en base a lo acordado y en el actual caso de negocio.
APO06.02	Priorizar la asignación de recursos.	Implementar un proceso de toma de decisiones para priorizar la asignación de recursos y las reglas para las inversiones discrecionales por unidades de negocio individuales. Se incluye el uso potencial de los proveedores de servicios externos y considerar la compra, el desarrollo y las opciones de alquiler.
APO06.03	Crear y mantener presupuestos	Preparar un presupuesto que refleje las prioridades de inversión en apoyo de los objetivos estratégicos en base a la cartera TIC habilitando programas y servicios de TIC.
APO07.01	Mantener la dotación de personal suficiente y adecuado.	Evaluando las necesidades de personal en forma regular o en cambios importantes en la empresa u operativos o entornos TIC para garantizar que la empresa cuenta con los recursos humanos suficientes para apoyar las metas y objetivos de la empresa. En el personal se incluye tanto los recursos internos como los externos.
BAI01.03	Gestionar los grupos de interés.	Administrar los grupos de interés para asegurar un intercambio activo de información precisa, coherente y oportuna que llegue a todos los interesados pertinentes. Esto incluye la planificación, la identificación y participación de los interesados y la gestión de sus expectativas.
BAI03.04	Adquirir componentes que resuelvan las necesidades.	Adquirir los componentes para dar solución, basándose en el plan de adquisición de acuerdo con los requisitos y diseños detallados, los principios y estándares de arquitectura, y los procedimientos globales de la empresa en la adquisición y contratación, los requisitos de control de calidad y las normas de homologación. Asegúrese que todos los requisitos legales y contractuales han sido identificados y abordados por el proveedor.
Catalizador de estructuras organizativas		
Referencia	Contribución para dar respuesta a la situación	
CIO	Responsable de la toma de decisión de inversión adecuada	
CFO	Responsable de la toma de decisión de inversión adecuada	
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta		
Referencia	Contribución para dar respuesta a la situación	
Proceso de toma de decisiones a partir de la medición de datos	Las emociones y la política no deben ser un factor dominante en la toma de decisiones.	
Catalizadores para alcanzar los objetivos de información		
Referencia	Contribución para dar respuesta a la situación	
Casos de negocio	Aclarar el propósito, el coste y el retorno sobre la inversión de las iniciativas de TIC.	
Priorizar y clasificar las iniciativas TIC	Información general de las iniciativas de TIC para facilitar la selección	
Presupuestos y planificación TIC	Información general sobre el presupuesto TIC disponible y las directrices	
N/A	N/A	
Catalizadores para alcanzar los objetivos de las personas, sus habilidades y competencias		
Referencia	Contribución para dar respuesta a la situación	
Asignación de presupuestos y costes	Capacidad de los aspectos financieros en detalle de las iniciativas de TIC	
Análisis de los casos de negocio	Aclarar el propósito, el coste y el retorno sobre la inversión de las iniciativas de TIC.	

EL USO DE FACILITADORES DE COBIT 5 PARA REDUCIR LOS ESCENARIOS DE RIESGO EN TI

D.4. Escenario 4: Habilidades y experiencia en TIC		
Categoría del escenario de riesgo	Habilidades y experiencia en TIC	
Catalizadores para alcanzar los objetivos de los principios, políticas y los libros de acuerdos o convenios		
Referencia	Contribución para dar respuesta a la situación	
Política de RRHH	Describe el desarrollo de los requisitos para la selección y evaluación de perfiles de IT en toda la carrera.	
Proceso facilitador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
APO01.01	Definir la estructura organizativa.	Establecer una estructura organizativa interna y extendida que refleje las necesidades y prioridades del negocio de TIC. Poner en marcha las estructuras de gestión necesarias (por ejemplo, comités) que permitan la toma de decisiones para qué la gestión se lleve a cabo de la manera más eficaz y eficiente.
APO01.04	Comunicar los objetivos de gestión y dirección	Comunicar la conciencia y comprensión de los objetivos y la dirección de TIC a las partes interesadas y los usuarios apropiados a lo largo de la empresa.
APO02.01	Comprender la dirección de la empresa	Considere el entorno actual de la empresa y los procesos de negocio, así como la estrategia de la empresa y los objetivos futuros. Tenga en cuenta también el entorno externo de la empresa (impulsores de la industria, las regulaciones pertinentes, la competencia).
APO03.01	Desarrollar la visión de la arquitectura empresarial.	La visión de la arquitectura proporciona un primer corte, descripción de alto nivel de las arquitecturas de referencia y los objetivos, que abarcan los dominios de negocios, información, datos, aplicaciones y tecnología. La visión de la arquitectura proporciona al patrocinador de una herramienta clave para vender los beneficios de la capacidad de propuesta a las partes interesadas en la empresa. La visión de la arquitectura describe cómo la nueva capacidad será cumplir con las metas propuestas por la empresa y los objetivos estratégicos y las preocupaciones de las partes interesadas de la dirección cuando se implemente.
APO07.01	Mantener la dotación de personal suficiente y adecuado.	Evaluando las necesidades de personal en forma regular o en cambios importantes en la empresa u operativos o entornos de TI para garantizar que la empresa cuenta con los recursos humanos suficientes para apoyar las metas y objetivos de la empresa. En el personal se incluye tanto los recursos internos como los externos.
APO07.02	Identificar el personal clave en TIC	Identificar al personal clave de TI y reducir al mínimo la dependencia en un solo individuo que realiza una función de trabajo crítico a través de captura de conocimiento (documentación), debe fomentarse el intercambio de conocimientos, planificar la sucesión y conseguir sustituir al personal.
APO07.03	Mantener las habilidades y competencias del personal.	Definir y gestionar las habilidades y competencias necesarias del personal. Regularmente verificar que el personal tenga las competencias necesarias para cumplir sus funciones sobre la base de su educación, formación y / o experiencia, y verificar que se mantienen estas competencias, mediante programas de certificación de calificación y, en su caso. Proporcionar a los empleados con el aprendizaje y oportunidades para mantener sus conocimientos, habilidades y competencias a un nivel necesario para alcanzar las metas de la empresa en marcha.
APO07.04	Evaluando el desempeño laboral de los empleados.	Realizar evaluaciones de desempeño a tiempo sobre una base regular con los objetivos individuales derivados de los objetivos de la empresa, las normas establecidas, las responsabilidades específicas del trabajo, y las habilidades y el marco de competencias. Los empleados deben recibir el entrenamiento en el rendimiento y llevarlo a cabo siempre que sea apropiado..
APO07.05	Planificar y realizar el seguimiento del uso de las herramientas TIC y de negocio por parte de los recursos humanos	Comprender y realizar un seguimiento de la demanda actual y futura de los negocios y de TIC de los recursos humanos con competencias para las TIC corporativas. Identificar carencias y aportaciones de los planes de abastecimiento y de TIC, para la empresa, e identificar carencias y aportaciones de los planes en los procesos de contratación de abastecimiento y de negocios y de los procesos de contratación TIC.
Catalizador de estructuras organizativas		
Referencia	Contribución para dar respuesta a la situación	
CIO	Responsable de análisis de las carencias en cuanto a capacidades y competencias de TI	
Jefe de RRHH	Responsable de establecer las expectativas con respecto al personal	
Dirección de gestión de funciones TIC específicas	Responsable de identificar los requisitos específicos	
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta		
Referencia	Contribución para dar respuesta a la situación	
Conocimiento de las actividades empresariales por parte del personal TIC	El personal de TI debe conocer las actividades de negocio de la empresa que soportan.	
Fomentar el desarrollo de competencias con el personal TIC	El desarrollo continuo de las habilidades de TI existentes.	

D.4. Escenario 4: Habilidades y experiencia en TIC (cont.)

Catalizador para alcanzar los objetivos de información	
Referencia	Contribución para dar respuesta a la situación
Matriz de competencias y habilidades	Describa las habilidades y competencias existentes dentro de la organización de TIC y permitir el análisis de las deficiencias
Carrera competencial y planes para desarrollar habilidades	Describir la evolución necesaria de los perfiles específicos de TIC.
Descripción de funciones genéricas	Describir las habilidades / experiencia y requisitos de conocimiento de los perfiles genéricos dentro de las organizaciones de TIC.
Repositorios de conocimiento	Reducir al mínimo el efecto de la falta de disponibilidad parcial de los recursos mediante el intercambio de conocimientos sobre procesos, tecnología, etc
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones	
Referencia	Contribución para dar respuesta a la situación
N/A	N/A
Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias	
Referencia	Contribución para dar respuesta a la situación
Habilidades de los RRHH	Manejo de habilidades y competencias
Análisis de negocio	Coincidencia de las necesidades del negocio con las habilidades de TIC necesarias

D.5. Escenario 5: Operaciones del personal

Categoría del escenario de riesgo		
Operaciones del personal (errores humanos y malas intenciones)		
Catalizador para alcanzar los objetivos de los principios, políticas y de los libros de acuerdos o convenios		
Referencia		Contribución para dar respuesta a la situación
Política de RRHH		Describe las restricciones que se siguen después de salir de la organización.
Políticas de seguridad de la información		Define las limitaciones técnicas en el intercambio y uso de información.
Políticas de Ética		Reglas de comportamiento, el uso aceptable de la tecnología y las precauciones necesarias
Proceso facilitador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
APO07.01	Mantener la dotación de personal suficiente y adecuado.	Evaluar las necesidades de personal de forma regular o sobre cambios importantes en la empresa u operativos o entornos de TIC para garantizar que la empresa cuenta con los recursos humanos suficientes para apoyar las metas y objetivos de la empresa. En el personal se incluye tanto los recursos internos como los externos.
APO07.03	Mantener las habilidades y las competencias del personal.	Definir y gestionar las habilidades y competencias necesarias del personal. Regularmente verificar que el personal tenga las competencias necesarias para cumplir sus funciones sobre la base de su educación, formación y / o experiencia, y verificar que se mantienen estas competencias, mediante programas de certificación de calificación y, en su caso. Proporcione a los empleados en curso de aprendizaje y oportunidades para mantener sus conocimientos, habilidades y competencias a un nivel necesario para alcanzar las metas de la empresa.
APO07.06	Gestión de los contratos del personal.	Comprobar que los consultores y el personal contratado que apoyan a la empresa con las habilidades de TI conocen y cumplen con las políticas de la organización y conocen y suscriben los requisitos contractuales.
BAI03.07	Preparar las pruebas de selección.	Establecer un plan de pruebas y entornos necesarios para probar los componentes de la solución individuales e integrados, incluidos los procesos de negocio y los servicios de apoyo, las aplicaciones y la infraestructura.
DSS01.01	Realizar los procedimientos operacionales.	Mantener y llevar a cabo los procedimientos operativos y las tareas operativas de forma fiable y consistente.
DSS01.04	Gestión del Medio ambiente.	Mantener las medidas de protección frente a factores ambientales. Instalar equipos y dispositivos especializados para supervisar y controlar el medio ambiente.

EL USO DE FACILITADORES DE COBIT 5 PARA REDUCIR LOS ESCENARIOS DE RIESGO EN TI

D.5. Escenario 5: Operaciones del personal (cont.)		
Proceso facilitador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
DSS01.05	Gestión de las instalaciones.	Administrar las instalaciones, incluyendose los equipos de comunicaciones y de energía, de acuerdo con las leyes y reglamentos, requisitos técnicos y comerciales, las especificaciones del fabricante, y las directrices de seguridad e higiene.
DSS04.03	Desarrollar e implementar una respuesta a la continuidad del negocio	Desarrollar un plan de continuidad del negocio (BCP) sobre la base de la estrategia que documente que los procedimientos y la información en tratamiento estén disponibles para su uso cuando surja un incidente permitiendo a la empresa continuar con sus actividades críticas.
DSS04.04	Ejercicio, prueba y revisión del Plan de Continuidad del Negocio BCP	Prueba de los mecanismos de continuidad de forma regular como ejercicio en los planes de recuperación frente a los resultados predeterminados, permita soluciones innovadoras para su desarrollo posterior y cronometre las pruebas para comprobar que el plan va a funcionar tal y como se esperaba.
DSS05.05	Gestión del acceso físico a los activos TIC.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, a los edificios y a las áreas de acuerdo a las necesidades del negocio, incluidas las emergencias. El acceso a las instalaciones, a los edificios y a las áreas debe justificarse, autorizarse,y deben estar registrada y supervisada. Esto debería aplicarse a todas las personas que entren en las instalaciones, incluido el personal, personal temporal, clientes, proveedores, visitantes o cualquier otro tercero.
DSS06.02	Control de los procesos de la información	Opera la ejecución de las actividades del proceso de negocio y los controles relacionados, con base en el riesgo de la empresa, para asegurar que el procesamiento de la información sea válido, completa, exacta, oportuna y segura (es decir, refleje el uso del negocio legítimo y autorizado).
DSS06.03	Gestión de los roles, responsabilidades, privilegios de acceso y niveles de autoridad.	Gestionar las funciones de negocio, las responsabilidades, los niveles de autoridad y la segregación de funciones necesarias para apoyar los objetivos del proceso de negocio. Autorizar el acceso a los activos de información relacionados con los procesos de información de negocios, incluyendo aquellos bajo la custodia comercial, informático y de terceros. Esto asegura que la empresa sabe cuales son los datos y quien se encarga de los datos en su nombre.
Catalizador de estructuras organizativas		
Referencia	Contribución para dar respuesta a la situación	
Gestor de la Seguridad de la Información	Responsable de la protección técnica de los activos y de la información	
Jefe de RRHH	Responsable de establecer las expectativas con respecto al personal	
Jefe de Operaciones TIC	Responsable de la gestión del entorno operativo	
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta		
Referencia	Contribución para dar respuesta a la situación	
Todos son responsables de la protección de la información dentro de la empresa	Predicar con el ejemplo	
Respeto de las personas a la importancia de las políticas y los procedimientos	La prevención de errores y accidentes	

D.5. Escenario 5: Operaciones del personal (cont.)	
Catalizador para alcanzar los objetivos de información	
Referencia	Contribución para dar respuesta a la situación
Contratos del personal	Las obligaciones contractuales, las restricciones y los derechos del personal
Acceso y registro de eventos	Detectar la actividad ilícita.
Roles asignados y responsabilidades / niveles de autoridad	Proporcionar claridad en la distribución de la organización.
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones	
Referencia	Contribución para dar respuesta a la situación
Control de acceso	Para impedir el acceso físico no autorizado
Supervisión del sistema de seguridad y de alarmas	Para impedir el acceso físico no autorizado
Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias	
Referencia	Contribución para dar respuesta a la situación
Habilidades de seguridad	Evitar las malas intenciones.

EL USO DE FACILITADORES DE COBIT 5 PARA REDUCIR LOS ESCENARIOS DE RIESGO EN TI

D.6 Escenario 6: Información		
Categoría del escenario de riesgo	Información (daños, fugas y acceso)	
Catalizador para alcanzar los objetivos de los principios, políticas y de los libros de acuerdos o convenios		
Referencia	Contribución para dar respuesta a la situación	
Política de seguridad física	El acceso sólo se puede proporcionar al personal autorizado.	
Política de copias de seguridad	Las copias de seguridad están disponibles.	
Políticas de Continuidad de Negocio y de recuperación ante desastres	Validar la recuperabilidad de los datos.	
Políticas de seguridad de la información	Define las limitaciones técnicas en el intercambio y en el uso de la información.	
Proceso facilitador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
APO01.06	Definir el propietario de los datos y del sistema de información.	Definir y mantener las responsabilidades de la propiedad de la información (datos) y de los sistemas de información. Asegúrese que los propietarios toman las decisiones clasificando la información y los sistemas y revisan la protección de acuerdo con dicha clasificación.
BAI02.01	Definir y mantener los requisitos funcionales y técnicos de negocio	Basado en el modelo de negocio, identificar, priorizar, especificar y acordar la información comercial, los requisitos funcionales, técnicos y de control que cubren el alcance o comprensión de todas las iniciativas necesarias para alcanzar los resultados esperados de la solución de negocio TIC propuesta.
BAI04.05	Investigar y dirigir los problemas de disponibilidad, de rendimiento y capacidad..	Dirigir las desviaciones mediante la investigación y la resolución de problemas de disponibilidad, rendimiento y capacidad ya identificadas.
DSS01.01	Realizar los procedimientos operacionales.	Mantener y llevar a cabo los procedimientos operativos y las tareas operativas de forma fiable y consistente.
DSS01.05	Gestión de las instalaciones.	Administrar las instalaciones, incluyéndose los equipos de comunicaciones y de energía, de acuerdo con las leyes y reglamentos, requisitos técnicos y comerciales, las especificaciones del fabricante, y las directrices de seguridad e higiene.
DSS04.03	Desarrollar e implementar una respuesta a la continuidad del negocio	Desarrollar un plan de continuidad del negocio (BCP) sobre la base de la estrategia que documente que los procedimientos y la información en tratamiento estén disponibles para su uso cuando surja un incidente permitiendo a la empresa continuar con sus actividades críticas.
DSS04.04	Ejercicio, prueba y revisión del Plan de Continuidad del Negocio BCP	Pruebe los mecanismos de continuidad de forma regular como ejercicio para comprobar que los planes de recuperación frente a los resultados predeterminados, permitiendo dar soluciones innovadoras para desarrollar posteriormente y cronometrar que el plan va a funcionar como se esperaba.
DSS05.02	Gestión de la seguridad de la red y conectividad	Utilice las medidas de seguridad y procedimientos de gestión relacionados para proteger la información para todos los métodos de conectividad.
DSS05.05	Gestión del acceso físico a los activos TIC.	Definir e implementar los procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo a las necesidades del negocio, incluidas las emergencias. Acceso a las instalaciones, edificios y áreas que deben justificar su acceso, de forma autorizada, registrada y supervisada. Esto debería aplicarse a todas las personas que entren en las instalaciones, incluido el personal, personal temporal, clientes, proveedores, visitantes o cualquier otro tercero.
DSS05.06	Gestión de documentación sensible y salida de dispositivos.	Establecer las garantías apropiadas físicas, las prácticas contables junto con la gestión de inventario de los activos TIC sensibles, como formularios especiales, instrumental biométrico, impresoras de propósito especial o tokens de seguridad.
DSS06.04	Gestión de errores y excepciones	Administración de las excepciones de los procesos de negocio y de los errores para facilitar su corrección. Se incluye escalado de errores en los procesos de negocio y las excepciones con la ejecución de las medidas correctoras ya definidas. Esto proporciona una garantía en la exactitud y en la integridad del proceso de información del negocio.
DSS06.05	Asegurar la trazabilidad de los eventos de su información y su contabilización.	Asegúrese de que la información comercial proviene del evento de negocios de origen y de las partes responsables. Esto permite disponer de la trazabilidad de la información partiendo del propio ciclo de vida y de los procesos relacionados. Esto garantiza que la información que maneja el negocio sea confiable y se haya tratado de acuerdo con los objetivos definidos.

D.6 Escenario 6: Información (cont.)

Catalizador de estructuras organizativas	
Referencia	Contribución para dar respuesta a la situación
Gestor de la Seguridad de la Información	Proporcionar la orientación sobre los controles y las medidas de protección de datos y hardware apropiados.
Jefe de Operaciones TIC	Responsable de la implementación de los controles y las medidas de protección de datos y hardware apropiados
Proceso facilitador para alcanzar el objetivo de Cultura, Ética y Conducta	
Referencia	Contribución para dar respuesta a la situación
La seguridad de la información se practique en las operaciones diarias	Seleccione siempre la opción más segura con respecto a las operaciones diarias.
Necesidad de acceso único	Limitar el acceso del personal sin afectar al rendimiento.
Todos son responsables de la protección de la información dentro de la empresa	Predicar con el ejemplo.
Catalizador para alcanzar los objetivos de información	
Referencia	Contribución para dar respuesta a la situación
Informes de las copias de seguridad	Describe el estado en cuanto a las copias de seguridad.
Campaña de prevención en la pérdida de información	Aumentar el conocimiento dentro de la empresa.
Acuerdos de confidencialidad	Por contrato proteger la propiedad intelectual, al disuadir al personal divulgar información a terceros malintencionados.
Registro de acceso y eventos	Detectar la actividad ilícita.
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones	
Referencia	Contribución para dar respuesta a la situación
Control de acceso	Para impedir el acceso físico no autorizado
Sistemas de copias de seguridad	Asegurar una correcta recuperación en caso de pérdida, modificación o alteración de los datos.
Infraestructura para la protección de datos y de aplicaciones	Encriptación, contraseñas, control del correo electrónico, etc, para aplicar el principio de necesidad de conocer
Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias	
Referencia	Contribución para dar respuesta a la situación
Habilidades técnicas	En cuanto a los controles y las medidas de protección de datos y hardware (por ejemplo, copia de seguridad de datos, almacenamiento) adecuados
Políticas de seguridad de la información	Define las limitaciones técnicas en el intercambio y uso de información.

D.7. Escenario 7: Arquitectura		
Categoría del escenario de riesgo	Arquitectura (visión y diseño arquitectónico)	
Catalizador para alcanzar los objetivos de los principios, políticas y de los libros de acuerdos o convenios		
Referencia	Contribución para dar respuesta a la situación	
Principios de la arquitectura	Los principios de la arquitectura definen las normas y directrices para el uso y despliegue de todos los recursos y activos de TIC en toda la empresa general o delegación.	
Procesos de excepción	En casos específicos, excepcionales a las reglas arquitectónicas existentes se puede permitir. Casos excepcionales y de procedimiento a seguir para su aprobación deben describirse.	
Proceso facilitador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
APO02.01	Comprender la dirección de la empresa	Considere el entorno actual de la empresa y de los procesos de negocio, así como la estrategia de la empresa y los objetivos futuros. Tenga en cuenta también el entorno externo de la empresa (impulsores de la industria, las regulaciones pertinentes, la competencia).
APO02.03	Definir las capacidades TIC necesarias.	Definir las capacidades TIC y los servicios de TIC que requiere el negocio. Basándose en la comprensión del medio y las necesidades de la empresa; evaluando los procesos de negocio actual y el entorno TIC y los problemas; considerándose las normas de referencia, las mejores prácticas y el arte de las tecnologías emergentes o las propuestas de innovación.
APO03.01	Desarrollar la visión de la arquitectura empresarial.	La visión de la arquitectura proporciona un primer corte, descripción de alto nivel de las arquitecturas de referencia y los objetivos, que abarcan los dominios de negocios, información, datos, aplicaciones y tecnología. La visión de la arquitectura proporciona al patrocinador de una herramienta clave para vender los beneficios de la capacidad de propuesta a las partes interesadas en la empresa. La visión de la arquitectura describe cómo la nueva capacidad será cumplir con las metas propuestas por la empresa y los objetivos estratégicos y las preocupaciones de las partes interesadas de la dirección cuando se implemente.
APO03.02	Definir la arquitectura de referencia	La arquitectura de referencia describe las arquitecturas actuales y objetivo para los dominios de negocios, información, datos, aplicaciones y tecnología.
APO03.03	Seleccionar oportunidades y soluciones	Racionalizar las brechas entre las arquitecturas de referencia y los objetivos, teniendo en cuenta tanto los negocios y las perspectivas técnicas, y, lógicamente, agruparlos en paquetes de trabajo del proyecto. Integrar el proyecto con todos los programas de inversión TIC relacionados para asegurar que las iniciativas arquitectónicas están alineadas y permitir estas iniciativas como parte de un cambio global de la empresa. Haga de esto un esfuerzo de colaboración con las partes clave interesadas de la empresa de negocio y de TIC para evaluar la transformación y la disposición 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 un plan de migración alineado con el programa y el catálogo de proyectos. Asegúrese que el plan está estrechamente coordinado para asegurar que el valor se entrega y los recursos necesarios están disponibles para completar el trabajo encomendado.
APO03.05	Proveer de los servicios necesarios para la arquitectura empresarial.	La prestación de servicios de arquitectura empresarial dentro de la empresa incluye los servicios de orientación y supervisión de los proyectos en ejecución, formalización de las formas de trabajar a través de contratos de arquitectura, medir y comunicar el valor añadido e inspección del cumplimiento de la arquitectura.
APO04.03	Supervisar y analizar el entorno tecnológico	Llevar a cabo un control sistemático y la exploración del entorno externo de la empresa para identificar las tecnologías emergentes que tienen el potencial de crear valor (por ejemplo, al realizar la estrategia empresarial, la optimización de costes, evitando la obsolescencia, y mejorar la capacitación de los Servicios y los procesos tecnológicos). Vigilar el mercado, el entorno competitivo, los sectores de la industria, y las tendencias legales y reglamentarias para poder analizar las tecnologías emergentes o ideas de innovación dentro del contexto empresarial.
APO04.04	Evaluuar el potencial de las tecnologías emergentes y las ideas de innovación.	Analizar las tecnologías emergentes identificadas y / o otras sugerencias de innovación de TIC. Trabajar con las partes interesadas para validar las hipótesis sobre el potencial de las nuevas tecnologías y la innovación.
APO04.06	Supervisar la implementación y el uso de la innovación.	Supervisar la implementación y el uso de tecnologías e innovaciones emergentes durante la integración, la adopción y durante todo el ciclo de vida económico para garantizar que los beneficios prometidos se realizan e identificar las lecciones aprendidas.

D.7. Escenario 7: Arquitectura (cont.)

Catalizador de estructuras organizativas	
Referencia	Contribución para dar respuesta a la situación
Consejo de arquitectura	Garantizar el cumplimiento de la arquitectura resultante y permitir excepciones cuando sea necesario.
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta	
Referencia	Contribución para dar respuesta a la situación
Respeto con las normas	La empresa debe estimular el uso de los estándares generalmente aceptados
Catalizador para alcanzar los objetivos de información	
Referencia	Contribución para dar respuesta a la situación
Modelo de Arquitectura	Modelo de la Arquitectura resultante
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones	
Referencia	Contribución para dar respuesta a la situación
CMDB	Base de datos de la gestión de la configuración
Software para el Modelado de la Arquitectura	El modelado de la aplicación optimizará el desarrollo de la arquitectura y minimizará el esfuerzo al analizar el impacto de la arquitectura en caso de excepciones o cambios.
Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias	
Referencia	Contribución para dar respuesta a la situación
Liderazgo y comunicación	Aclarar las razones de la arquitectura y las posibles consecuencias..
Experiencia en arquitectura	Desarrollar una arquitectura eficiente y eficaz alineada con los requerimientos del negocio. .

D.8. Escenario 8: Infraestructura		
Categoría del escenario de riesgo	Infraestructura (hardware, sistema operativo, tecnología de control) (Selección o implementación, operaciones y clausura))	
Catalizador para alcanzar los objetivos de los principios, políticas y los libros de acuerdos		
Referencia	Contribución para dar respuesta a la situación	
Principios de la arquitectura	Definir las normas generales subyacentes y las directrices para el uso y despliegue de todos los recursos y activos de TIC en toda la empresa.	
Política de gestión de cambios	Guía con los cambios y las evoluciones en la infraestructura.	
Proceso catalizador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
APO02.03	Definir las capacidades TIC necesarias.	Definir del negocio a estudio, las capacidades de TIC y los servicios requeridos de TIC. Esto debe basarse en la comprensión del entorno y de las necesidades de la empresa; previa a una evaluación de los procesos de negocio actuales y del entorno tecnológico, averiguando los problemas actuales; considerando las normas de referencia, las mejores prácticas y las tecnologías emergentes validadas o las nuevas propuestas de innovación.
APO04.03	Supervisar y analizar el entorno tecnológico	Lleve a cabo un control sistemático y de la exploración del entorno externo de la empresa para identificar que tecnologías emergentes tienen el potencial de crear valor (por ejemplo, al realizar la estrategia empresarial, la optimización de costes, evitando la obsolescencia, y mejorar la capacitación de Servicios y procesos TIC). Supervise el mercado, el entorno competitivo, los sectores de la industria, y las tendencias legales y reglamentarias para poder analizar las tecnologías emergentes o ideas de innovación en el contexto empresarial.
BAI03.03	Desarrollar soluciones con componentes .	Desarrollar componentes de la solución progresivamente según diseños detallados siguientes métodos de desarrollo y con los estándares de documentación, los requisitos de garantía de calidad (QA) y los estándares de aprobación. Asegúrese que se aborden todos los requisitos de control de los procesos de negocio, el apoyo a aplicaciones y a los servicios de infraestructura, servicios y los productos de tecnología de socios o proveedores.
BAI04.01	Evaluar la disponibilidad actual, el rendimiento y la capacidad y crear una línea maestra.	Evaluar la disponibilidad, el rendimiento y la capacidad de los servicios y recursos necesarios para garantizar que la capacidad y el rendimiento-coste justificable están disponibles para apoyar las necesidades del negocio y entregar contra los SLAs. Crear líneas maestras sobre la disponibilidad, rendimiento y capacidad para futuras comparaciones.
BAI04.02	Evaluar el impacto del negocio	Identificar importantes servicios para la empresa, el mapa de servicios y recursos a los procesos de negocio, e identificar las dependencias empresariales. Asegúrese que el impacto de los recursos no disponibles está totalmente de acuerdo y aceptado por el cliente. Velar por que, para las funciones vitales del negocio, los requisitos de disponibilidad SLA puedan ser satisfechas.
BAI04.03	Plan para nuevos requerimientos o cambios del servicio	Planificar y priorizar las implicaciones sobre la disponibilidad, rendimiento y capacidad de las cambiantes necesidades de negocio y requerimientos del servicio.
BAI04.04	Supervisar y revisar el rendimiento y capacidad.	Supervisar, medir, analizar, informar y revisar la disponibilidad, el rendimiento y la capacidad. Identificar las desviaciones de las líneas de base establecidas. Informes de análisis de las tendencias de la opinión que identifican cualquier problema y las diferencias más importantes, que inician acciones en caso necesario, y garantizar que todas las cuestiones pendientes sean objeto de seguimiento.
BAI04.05	Investigar y dirigir los problemas de disponibilidad, de rendimiento y capacidad.	Dirigir las desviaciones mediante la investigación y la resolución de problemas de disponibilidad, rendimiento y capacidad identificadas.
BAI10.04	Elaborar informes de estado y configuración	Definir y elaborar informes de configuración con 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 la integridad y exactitud con la meta deseada.

D.8. Escenario 8: Infraestructura (cont.)

Proceso catalizador para alcanzar el objetivo

Referencia	Título	Práctica de Gestión
DSS05.05	Gestión del acceso físico a los activos TIC.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo a las necesidades del negocio, incluidas las emergencias. El acceso a las instalaciones, a edificios y a las áreas debe justificarse, estar autorizadas, registrada y supervisada. Esto debería aplicarse a todas las personas que entren en las instalaciones, incluido el personal, personal temporal, clientes, proveedores, visitantes o cualquier otro tercero.

Catalizador de estructuras organizativas

Referencia	Contribución para dar respuesta a la situación
Jefe de Operaciones TIC	Responsable de la gestión y mantenimiento de la infraestructura de TIC
Jefe de Arquitectura	El diseño de la arquitectura de una manera óptima

Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta

Referencia	Contribución para dar respuesta a la situación
Respetar los activos disponibles	Se requiere a todo el personal para mantener los activos de una manera apropiada

Catalizador para alcanzar los objetivos de información

Referencia	Contribución para dar respuesta a la situación
Modelo de Arquitectura	Modelo de Arquitectura resultante
Actualizar el inventario de activos	El seguimiento de todos los activos en toda la empresa
Mantener el plan	Planificación del mantenimiento de la infraestructura de TIC
Informe del estado de la configuración	Seguimiento de cambios en la configuración

Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones

Referencia	Contribución para dar respuesta a la situación
CMDB	Ayuda a identificar las áreas de mejora.

Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias

Referencia	Contribución para dar respuesta a la situación
Experiencia en arquitectura	Desarrollar una arquitectura eficiente y eficaz alineada con los requerimientos del negocio. .
Habilidades técnicas	La gestión de los diferentes componentes de la infraestructura

D.9. Escenario 9: Software		
Categoría del escenario de riesgo	Software (selección/implementación, operación y clausura)	
Catalizador para alcanzar los objetivos de los principios, políticas y los libros de acuerdos		
Referencia	Contribución para dar respuesta a la situación	
Política de gestión de cambios	Cambios rectores y evoluciones en la infraestructura	
Procedimiento de emergencia	Directrices en el caso de retroceder al retirar los cambios	
Principios de la arquitectura	Los principios de la arquitectura definen las normas y directrices para el uso y despliegue de todos los recursos y activos TIC en toda la empresa y delegaciones.	
Proceso catalizador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
BAI03.01	Diseño de soluciones de alto nivel.	Desarrollar y documentar los diseños de alto nivel utilizando técnicas de desarrollo ágil apropiadas de forma gradual o rápida según lo acordado y, asegurar que está alineado con la estrategia TIC y con la arquitectura de la empresa. Vuelva a evaluar y actualizar los diseños cuando se produzcan problemas significativos durante el diseño detallado o durante las fases de construcción a medida que evoluciona la solución. Asegúrese que las partes interesadas participen activamente en el diseño y aprueban cada versión.
BAI03.02	Diseño de soluciones con componentes detallado	Desarrollar, documentar y elaborar diseños progresivamente con el uso de técnicas de desarrollo ágil apropiadas de forma gradual o rápida según lo acordado y, dirigiéndose a todos los componentes (procesos de negocio y los controles automatizados y manuales relacionados, el apoyo a las aplicaciones informáticas, servicios de infraestructura y a los productos de tecnología de socios o proveedores). Asegúrese que en el diseño detallado se incluye los SLA y OLA internos y externos.
BAI03.03	Desarrollar soluciones con componentes.	Desarrollar componentes de la solución progresivamente según diseños detallados siguiendo los métodos de desarrollo y los estándares de documentación, cumpliendo con los requisitos de garantía de calidad (QA) y los estándares de aprobación. Asegúrese que se aborden todos los requisitos de control de los procesos de negocio, se da continuación a las aplicaciones y a los servicios de infraestructura, a los servicios y productos de tecnología de socios o proveedores.
BAI03.05	Construir soluciones.	Instalación y configuración de soluciones y la integración con las actividades del proceso de negocio. Implementar medidas de control, seguridad y auditabilidad durante la configuración, y durante la integración de hardware y software de infraestructura, para proteger los recursos y garantizar la disponibilidad y la integridad de los datos. Actualizar el catálogo de servicios para reflejar las nuevas soluciones.
BAI03.06	Realizar controles de calidad (QA)	Desarrollar, recursos y ejecutar un plan de control de calidad en consonancia con el SGC para obtener la calidad especificada en la definición de los requisitos y las políticas y procedimientos de calidad de la empresa.
BAI03.07	Preparar las pruebas de selección.	Establecer un plan de pruebas y entornos necesarios para probar los componentes de las soluciones individuales e integradas, incluidos los procesos de negocio y los servicios de apoyo, las aplicaciones y la infraestructura.
BAI03.08	Ejecutar las pruebas de soluciones	Ejecutar pruebas de forma continua durante el desarrollo, incluidas las pruebas de control, de conformidad con el plan de pruebas definido y prácticas de desarrollo en el entorno adecuado. Involucrar a los dueños de procesos de negocio y a los usuarios finales en el equipo de pruebas. Identificar, registrar y dar prioridad a los errores y los problemas detectados durante las pruebas.
BAI03.09	Gestión de los cambios a nuevos requerimientos.	Realizar el seguimiento del estado de las necesidades individuales (incluyendo todos los requerimientos rechazados) durante todo el ciclo de vida del proyecto y gestionar la aprobación de los cambios en los requisitos.
BAI03.10	Mantener soluciones.	Desarrollar y ejecutar un plan para el mantenimiento de la solución y los componentes de la infraestructura. Incluye revisiones periódicas en contra de las propias necesidades del negocio y de los requisitos operacionales.
BAI05.05	Habilitar la operativa y el uso.	Planificar e implementar todos los aspectos técnicos, de explotación y uso de tal manera que todos los que están involucrados en el futuro entorno del nuevo estado puedan ejercer su responsabilidad
BAI06.01	Evaluar, priorizar y autorizar peticiones de cambio.	Evaluar todas las solicitudes de cambio para determinar el impacto en los procesos de negocio y en los servicios TIC, y para evaluar si el cambio va a afectar negativamente al entorno operativo y presentar un riesgo inaceptable. Asegúrese que los cambios se registran, se priorizan, se clasifican, se evalúan, son autorizados, se planifican y son programados.

D.9. Escenario 9: Software (cont.)
Proceso catalizador para alcanzar el objetivo

Referencia	Título	Práctica de Gestión
BAI06.02	Gestionar cambios de emergencia.	Manejar con cuidado los cambios de emergencia para minimizar nuevos incidentes y asegurarse que el cambio está controlado y se lleva a cabo de forma segura. Compruebe que los cambios de emergencia sean evaluados y autorizados después de realizar el cambio de manera apropiada.
BAI06.03	Seguimiento e informe del estado del cambio	Mantener un sistema de seguimiento y presentación de informes para documentar los cambios rechazados, comunicar el estado de los cambios aprobados y en proceso de fabricación, y los cambios completados. Asegúrese que se aprobaron los cambios y se implementen según lo previsto.
BAI06.04	Cerrar y documentar los cambios.	Siempre que se apliquen los cambios, actualizar en consecuencia la solución y documentación del usuario, adjuntando los procedimientos afectados por el cambio.
BAI07.01	Establecer un plan de implementación.	Establecer un plan de implementación que cubra el sistema y la conversión de los datos, criterios de prueba de aceptación, la comunicación, la formación, la preparación de liberación, la promoción de la producción, el apoyo a la producción temprana, un plan de reserva o de cancelación, y una revisión posterior a la implementación. Obtener la aprobación por las partes implicadas.
BAI07.03	Aceptación del Plan de pruebas	Establecer un plan de pruebas basados en los estándares de toda la empresa que definen criterios de roles, responsabilidades, y procesos de entrada y salida. Asegurándose que el plan sea aprobado por las partes interesadas.
BAI07.05	Realizar las pruebas de aceptación	Prueba de los cambios realizados de forma independiente, de acuerdo con el plan de pruebas definido antes de la migración para el entorno operativo en real.
BAI07.08	Realizar una revisión posterior a la implementación	Llevar a cabo una revisión posterior a la implementación para confirmar los resultados y con los resultados, identificar las lecciones aprendidas, y desarrollar un plan de acción. Evaluar y comprobar si el rendimiento real y los resultados del nuevo servicio o servicio modificado funcionan con el desempeño esperado y dan los resultados previstos (es decir, si corresponde al servicio esperado por el usuario o cliente).
BAI08.01	Nutrir y facilitar una cultura de intercambio de conocimientos	Diseñar e implementar un plan para fomentar y facilitar una cultura de intercambio de conocimientos.
BAI08.04	Utilizar y compartir el conocimiento.	Propagar los recursos de conocimiento a disposición de las partes interesadas pertinentes y comunicar cómo se pueden usar estos recursos para hacer frente a las diferentes necesidades (por ejemplo, la resolución de problemas, aprendizaje, planificación estratégica y toma de decisiones).
BAI10.04	Elaborar informes de estado y configuración	Definir y elaborar informes de configuración con 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 la integridad y exactitud con la meta deseada.

Catalizador de estructuras organizativas

Referencia	Contribución para dar respuesta a la situación
Jefe de desarrollo	Responsable del diseño y desarrollo adecuado de los componentes de software
Jefe de Arquitectura	Diseña la arquitectura de una manera óptima

Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta

Referencia	Contribución para dar respuesta a la situación
Las pruebas se realizan en todos los niveles adecuados	Los usuarios y desarrolladores colaboren para efectuar pruebas de los componentes de software.

Catalizador para alcanzar los objetivos de información

Referencia	Contribución para dar respuesta a la situación
Modelo de Arquitectura	Modelo de Arquitectura resultante
Especificaciones de diseño	Aclarar las necesidades de los usuarios
Plan de Aseguramiento de la Calidad (plan de pruebas y procedimientos)	Definir los pasos a seguir con el fin de asegurar la calidad
Mantener el plan	Planificación del mantenimiento del software

D.9. Escenario 9: Software (cont.)	
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones	
Referencia	Contribución para dar respuesta a la situación
Entorno de desarrollo integrado (IDE)	Facilitar el desarrollo y que consiste en un editor de código fuente, construir herramientas de automatización y un depurador
Repositorios de conocimiento	Compartir y sobre el conocimiento coordinar las actividades de desarrollo
Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias	
Referencia	Contribución para dar respuesta a la situación
Experiencia en arquitectura	Desarrollar una arquitectura eficiente y eficaz alineada con los requerimientos del negocio.
Habilidades técnicas	Diseño y desarrollo de los componentes de software adecuados

D.10. Escenario 10: Propietario del Negocio de TIC		
Categoría del escenario de riesgo		Propietario del Negocio de TIC
Catalizador para alcanzar los objetivos de los principios, políticas y de los libros de acuerdos o convenios		
Referencia		Contribución para dar respuesta a la situación
Principios que guian la gobernanza empresarial		La participación de las empresas y de las TIC
Principios de informes y de comunicación		Clarificar los medios de comunicación
Proceso facilitador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
EDM01.01	Evaluar el sistema de gobierno.	Continuamente identificar y comprometer a las partes interesadas de la empresa, documentar la comprensión de las necesidades, y hacer un juicio sobre el diseño actual y futuro de la gobernanza de la TIC de la empresa.
EDM01.02	Dirigir el sistema de gobierno	Informar a los líderes y obtener su apoyo, aceptación y compromiso. Guiar de las estructuras, procesos y prácticas de la gobernanza de TIC estén en línea con los principios acordados en la gobernanza, en su diseño, en los modelos de toma de decisiones y en los niveles de autoridad. Definir la información requerida para la toma de decisiones informada.
EDM01.03	Supervisar el sistema de gobierno.	Supervisar la efectividad y el desempeño de la gobernanza de la empresa de TIC. Evaluar si el sistema de gobierno y los mecanismos implementados (incluyendo las estructuras, los principios y los procesos) funcionan con eficacia y proporciona una supervisión adecuada de las TI.
APO01.04	Dirección y gestión de la comunicación de objetivos.	Comunicar en la toma de conciencia y comprensión de los objetivos y la dirección de TIC a las partes interesadas y a los usuarios apropiados a lo largo de la empresa.
APO02.01	Comprender la dirección de la empresa	Considere el entorno actual de la empresa y los procesos de negocio, así como la estrategia de la empresa y los objetivos futuros. Tenga en cuenta también el entorno externo de la empresa (impulsores de la industria, las regulaciones pertinentes, la competencia).
APO05.06	Gestione el beneficio de los logros	Supervisar los beneficios de proporcionar y mantener los servicios y las capacidades de TIC adecuadas, en base a lo acordado y en el caso de un negocio actual.
APO09.03	Definir y preparar los acuerdos de servicio.	Definir y preparar los acuerdos de servicios basados en las opciones de los catálogos de servicios, en los que se incluya los acuerdos operativos internos.
APO09.04	Supervisar e informar de los niveles de servicio.	Supervisar los niveles de servicio, informar sobre los logros e identificar tendencias. Proporcionar la información de gestión adecuada para mejorar la gestión del rendimiento.
BAI01.03	Gestionar los grupos de interés.	Administrar los grupos de interés para asegurar un intercambio activo de información precisa, coherente y oportuna que llegue a todos los interesados pertinentes. Esto incluye la planificación, la identificación y participación de los interesados y la gestión de sus expectativas.
BAI02.01	Definir y mantener los requisitos comerciales funcionales y técnicos	Basado en el modelo de negocio, identificar, priorizar, especificar y acordar información comercial, requisitos funcionales, técnicas y de control que cubren el alcance o la comprensión de todas las iniciativas necesarias para alcanzar los resultados esperados de la solución de negocio que ofrece la propuesta TIC.
Catalizador de estructuras organizativas		
Referencia	Contribución para dar respuesta a la situación	
Oficina de Gestión de Programas y Proyectos (PMO)	Proporcionar una metodología común, utilizada por el negocio y TIC, para definir los requisitos adecuados.	
Oficina de gestión de Oportunidades que aportan valor(VMO)	VMO, o similar función, consiste en la colección de actividades, necesarias para proporcionar una metodología común, utilizada por el negocio y las TIC, con la finalidad de evaluar las oportunidades en términos de valor para la empresa.	
Comité de estrategia (ejecutivos TIC)	Estructura clave que tiene la responsabilidad sobre el negocio y en la cooperación empresarial	
Junta	Responsable de configurar la normativa de gobierno en la empresa y su mantenimiento	

D.10. Escenario 10: Propietario del Negocio TIC (cont.)	
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta	
Referencia	Contribución para dar respuesta a la situación
Negocio y TIC trabajan juntos como socios	Negocios tiene en cuenta las dificultades que se enfrenta en el uso de las TIC, debe de aprender para dar solución a los problemas del negocio.
Catalizador para alcanzar los objetivos de información	
Referencia	Contribución para dar respuesta a la situación
Estrategia TIC	La alineación de los planes de TIC con los objetivos empresariales llevará a una rendición de cuentas más eficiente de la empresa en el uso de las TIC.
Niveles de autoridad	Clarificar las responsabilidades en la toma de decisiones
SLAs (Niveles de Servicio Acordado)	Acuerdos de nivel de servicio
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones	
Referencia	Contribución para dar respuesta a la situación
N/A	N/A
Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias	
Referencia	Contribución para dar respuesta a la situación
Habilidades en la gestión de relaciones	Las herramientas TIC debe tener las habilidades adecuadas para construir las relaciones con las partes interesadas relevantes en el negocio
Habilidades /afinidades relacionadas con TIC	Los representantes empresariales deben ser capacitados , o bien seleccionados en base a una afinidad mínima requerida con el uso de las TIC

D.11. Escenario 11: Proveedores		
Categoría del escenario de riesgo		Proveedores (selección, realización, cumplimiento contractual, la finalización del servicio y transferencia)
Catalizador para Alcanzar los objetivos de los principios, políticas y de los libros de acuerdos o convenios		
Referencia		Contribución para dar respuesta a la situación
Política de contratación		Proporcionar un enfoque conjunto para la selección de los proveedores, incluyendo los criterios de aceptación en términos de negocio
Principios de la arquitectura		Los principios de la arquitectura definen las normas y directrices para el uso y despliegue de todos los recursos y activos de TIC en toda la empresa y sus delegaciones o empresas con activos subyacentes.
Políticas de seguridad de la información		Define las limitaciones técnicas en el intercambio y uso de información.
Proceso facilitador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
APO10.02	Selección de proveedores.	Seleccionar proveedores de acuerdo con una práctica justa y formal para garantizar un mejor ajuste viable en base a los requisitos especificados. Los requisitos deben ser optimizados con la colaboración de los proveedores potenciales.
APO10.03	Gestión de la relación con proveedores y contratación.	Formalizar y gestionar la relación con los proveedores para cada proveedor. Administrar, mantener y supervisar los contratos y la prestación de servicios. Asegúrese de que los contratos nuevos o modificados se ajustan a las normas de la empresa y los requisitos legales y reglamentarios. Encaja con las disputas contractuales.
APO10.04	Gestión del riesgo con proveedores..	Identificar y gestionar los riesgos relacionados con la capacidad de los proveedores para proporcionar continuamente la prestación de servicios segura, eficiente y eficaz.
APO10.05	Supervisión del rendimiento de proveedores y cumplimiento.	Revisar periódicamente el desempeño general de los proveedores, el cumplimiento de los requisitos del contrato, y la relación calidad-precio, y las cuestiones identificadas direcciones.
Catalizador de estructuras organizativas		
Referencia		Contribución para dar respuesta a la situación
Grupo Legal		Revisión de los términos propuestos del negocio
Propietario del proceso de negocio		Los requisitos de ajuste, los indicadores de desempeño y garantizar las expectativas adecuadas son incorporados en los contratos
Departamento de compras		Proporcionar el apoyo y acercamiento a participar de manera eficiente con los proveedores.
CIO		Responsable de la gestión con los proveedores
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta		
Referencia		Contribución para dar respuesta a la situación
Respeto al procedimiento de contratación		Se requieren nuevos esfuerzos para garantizar una protección mínima en relación con los proveedores.
El enfoque a la cultura de transparencia y de participación es un punto importante..		Para optimizar el resultado de la relación con el proveedor
Catalizador para alcanzar los objetivos de información		
Referencia		Contribución para dar respuesta a la situación
Requisitos de servicio		Saber lo que quieres, te permite una posición razonable para la negociación.
Estrategia TIC		Definir los límites y los objetivos de la empresa a considerar durante la negociación de contrato
Catálogo de proveedores		Una presentación estructurada de los proveedores conocidos, incluyéndose su rendimiento anterior
SLAs		Acuerdos de nivel de servicio
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones		
Referencia		Contribución para dar respuesta a la situación
Sistema de gestión de proveedores		Establecer un sistema para realizar un seguimiento de la evolución de la exposición al riesgo durante todo el proceso, desde la selección hasta la terminación del servicio.

D.11. Escenario 11: Proveedores (<i>cont.</i>)	
Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias	
Referencia	Contribución para dar respuesta a la situación
Habilidades de negociación	Garantizar que los requisitos mínimos son soportados.
Destrezas en la litigación	Una vez que se inicia la demanda, se requieren de las habilidades adecuadas para minimizar el impacto legal.
Habilidades en la interpretación y análisis legal.	Apoyo a la cooperación con los proveedores.

D.12. Escenario 12: Cumplimiento Legal		
Categoría del escenario de riesgo		Cumplimiento de normativas
Catalizador para alcanzar los objetivos de los principios, políticas y los libros de acuerdos		
Referencia		Contribución para dar respuesta a la situación
Políticas específicas en el dominio		Políticas tales como las de privacidad , las de seguridad y las de salud
Políticas de cumplimiento		Guia la identificación de los requisitos de cumplimiento externo
Proceso facilitador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
MEA03.01	Identificar los requisitos de cumplimiento externo.	Sobre una base continua, identificar y vigilar los cambios en las leyes, reglamentos y otros requerimientos externos locales e internacionales que deben cumplirse a partir de una perspectiva de TIC.
MEA03.02	Optimizar la respuesta a los requerimientos externos.	Revisar y ajustar las políticas, principios, normas, procedimientos y metodologías para asegurar que los requisitos legales, reglamentarios y contractuales se tratan y comunican. Considere la posibilidad de estándares de la industria, códigos de buenas prácticas y guía de prácticas recomendadas para la adopción y adaptación.
MEA03.03	Confirmar cumplimiento externo.	Confirmar el cumplimiento de las políticas, principios, normas, procedimientos y metodologías con los requisitos legales, reglamentarios y contractuales.
Catalizador de estructuras organizativas		
Referencia		Contribución para dar respuesta a la situación
Responsable de seguridad de datos personales		Vigilar los impactos de las leyes y hacer que se cumplan las directivas de privacidad.
Departamento Legal		Proporciona orientación sobre el cumplimiento legal, regulatorio y contractual. Seguimiento de los cambios y nueva legislación.
Grupo Legal		Soporte legal durante el análisis y el litigio
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta		
Referencia	Contribución para dar respuesta a la situación	
La cultura del riesgo y del cumplimiento está presente en toda la empresa incluye la identificación proactiva y escalar el riesgo.	Todos los miembros de la empresa tienen la facultad de facilitar el cumplimiento normativo.	
El cumplimiento está integrado en las operaciones diarias	Todos los miembros de la empresa tienen la facultad de facilitar el cumplimiento normativo.	
Catalizador para alcanzar los objetivos de información		
Referencia	Contribución para dar respuesta a la situación	
La tolerancia o apetencia al riesgo	Equilibrar el cumplimiento de la empresa al riesgo / tolerancia	
Informes de garantía	Por ejemplo, SAS 70	
Acuerdos de control interno	Optimizar la eficiencia del control interno.	
Análisis de los nuevos requisitos de cumplimiento legislativos y regulatorios	La regulación impuesta por el gobierno necesita ser analizado.	
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones		
Referencia	Contribución para dar respuesta a la situación	
Bases de datos jurídicas y regulatorias	Facilitar el seguimiento de los requisitos de cumplimiento	
Herramientas para la Garantía del Cumplimiento y regulación (GRC)	Descripción general de los controles y prácticas para asegurar el cumplimiento	

D.12. Escenario 12: Cumplimiento Legal	
Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias	
Referencia	Contribución para dar respuesta a la situación
Destrezas en la litigación	Una vez que se inicia la denuncia, se requieren las habilidades adecuadas para minimizar el impacto legal.
Habilidades en la interpretación y análisis legal.	Comprender las expectativas del legislador local.
Habilidades en la planificación de contingencias	Mantener opciones necesarias para ofrecer un servicio continuo.
Control interno	Evaluuar el cumplimiento con la reglamentación pertinente.

D.13. Escenario 13: Geopolítico		
Categoría del escenario de riesgo		Geopolítico
Catalizador para alcanzar los objetivos de los principios, políticas y de los libros de acuerdos o convenios		
Referencia		Contribución para dar respuesta a la situación
Principio de puerto seguro (Safe harbour)		Acuerdos de puerto seguro reducen la probabilidad de intercepción.
Proceso facilitador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
DSS04.02	Mantener una estrategia de continuidad	Evaluar las opciones de gestión de continuidad de negocio y elegir una estrategia de continuidad rentable y viable que garantice la recuperación de la empresa y la continuidad frente a un desastre o incidente importante o de interrupción.
MEA03.01	Identificar los requisitos de cumplimiento externo.	Sobre una base continua, identificar y supervisar los cambios legislativos, reglamentos y otros requerimientos externos locales e internacionales que deben cumplirse a partir de una perspectiva de TIC.
MEA03.02	Optimizar la respuesta a los requerimientos externos.	Revisar y ajustar las políticas, principios, normas, procedimientos y metodologías para asegurar que los requisitos legales, reglamentarios y contractuales se tratan y comunican. Considere la posibilidad de estándares de la industria, códigos de buenas prácticas y guía de prácticas recomendadas para su adopción y adaptación.
Catalizador de estructuras organizativas		
Referencia	Contribución para dar respuesta a la situación	
Responsable de seguridad de datos personales	Vigilar los impactos de la legislación vigente y hacer que se cumplan las directivas de privacidad.	
Departamento Legal y Normativo	Orientación sobre el cumplimiento legal, regulatorio y contractual	
Grupo Legal	Soporte legal durante el análisis y el litigio	
Plan de recuperación de Continuidad y desastre del Negocio	Mantener las opciones necesarias para ofrecer servicio continuo.	
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta		
Referencia	Contribución para dar respuesta a la situación	
Controlar el crecimiento y la expansión	Asegúrese que la legislación vigente y los requisitos externos estén integrados	
Catalizador para alcanzar los objetivos de información		
Referencia	Contribución para dar respuesta a la situación	
Análisis de nuevas regulaciones	La legislación impuesta por el gobierno local debe ser analizada.	
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones		
Referencia	Contribución para dar respuesta a la situación	
Servicios legales externos	Obtener consejo sobre la nueva legislación de los gobiernos locales y el impacto que tienen sobre la empresa.	
Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias		
Referencia	Contribución para dar respuesta a la situación	
Destrezas en la litigación	Una vez que se inicia la denuncia, se requieren de las habilidades adecuadas para minimizar el impacto legal.	
Habilidades en la interpretación y análisis legal.	Comprender las expectativas de la legislación local.	
Habilidades en la planificación de contingencias	Mantener las opciones necesarias para ofrecer un servicio continuo.	

EL USO DE FACILITADORES DE COBIT 5 PARA REDUCIR LOS ESCENARIOS DE RIESGO EN TI

D.14. Escenario 14: Infraestructura Robo o Destrucción		
Categoría del escenario de riesgo	Robo o destrucción de la infraestructura (por terceros fuera de la empresa)	
Catalizador para alcanzar los objetivos de los principios, políticas y los libros de acuerdos		
Referencia	Contribución para dar respuesta a la situación	
Políticas de seguridad de la información física y medio ambientales	Restringir el acceso físico a la infraestructura con el fin de evitar la destrucción de la misma.	
Políticas de Recuperación de desastres y Continuidad del Negocio	Validar la recuperabilidad de la información, de los servicios, de las aplicaciones y de la infraestructura.	
Proceso facilitador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
DSS01.04	Gestión del Medio ambiente.	Mantener las medidas de protección frente a los factores ambientales. Instalar equipos y dispositivos especializados para supervisar y controlar la calidad del medio ambiente.
DSS01.05	Gestión de las instalaciones.	Administrar las instalaciones, incluyéndose los equipos de comunicaciones y de energía, de acuerdo con las leyes y reglamentos, requisitos técnicos y comerciales, las especificaciones del fabricante, y las directrices de seguridad e higiene.
DSS05.05	Gestión del acceso físico a los activos TIC.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo a las necesidades del negocio, incluidas las emergencias. Los accesos a las instalaciones, edificios y áreas deben justificarse, autorizar, registrar y deben supervisarse. Esto debería aplicarse a todas las personas que entren en las instalaciones, incluido el personal, personal temporal, clientes, proveedores, visitantes o cualquier otro tercero.
Catalizador de estructuras organizativas		
Referencia	Contribución para dar respuesta a la situación	
Gestor de la Seguridad de la Información	La implementación de medidas de seguridad	
Jefe de Operaciones TIC	En respuesta al robo y a la destrucción de infraestructuras	
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta		
Referencia	Contribución para dar respuesta a la situación	
La seguridad de la información se practica habitualmente en las operaciones diarias	Para impedir el acceso físico no autorizado	
Las personas respetan la importancia de los principios y políticas de la seguridad de la información.	Para impedir el acceso físico no autorizado	
Las partes interesadas son conscientes de la manera de identificar y responder frente a las amenazas a la empresa.	Para reducir el impacto en el robo y la destrucción de infraestructuras	
Catalizador para alcanzar los objetivos de información		
Referencia	Contribución para dar respuesta a la situación	
Petición de acceso	Supervisar el acceso a las instalaciones	
Registros de acceso	Presentación de informes de acceso integral	
Informes de evaluación de las instalaciones	La empresa es consciente del estado y el riesgo de las instalaciones.	
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones		
Referencia	Contribución para dar respuesta a la situación	
Control de acceso	Para impedir el acceso físico no autorizado	
Supervisión del sistema de seguridad y de alarmas	Para impedir el acceso físico no autorizado	
Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias		
Referencia	Contribución para dar respuesta a la situación	
Habilidades de seguridad de la información	Prevenir y reducir el impacto en las infraestructuras ante el robo y la destrucción	

D.15. Escenario 15: Software mal intencionado		
Categoría del escenario de riesgo	Software mal intencionado	
Catalizador para alcanzar los objetivos de los principios, políticas y los libros de acuerdos		
Referencia	Contribución para dar respuesta a la situación	
Políticas de seguridad de la información	Describe las medidas de seguridad de la información dentro de la empresa.	
Políticas de prevención de software mal intencionado.	Detalles de las medidas de prevención, detección y medidas correctivas vigentes en toda la empresa para proteger los sistemas de información y la tecnología del software mal intencionado.	
Principios de la arquitectura	Los requisitos de seguridad de la información son parte intrínseca de la arquitectura de la empresa y se traducen en una arquitectura formal de seguridad de la información.	
Políticas de Continuidad de Negocio y de recuperación ante desastres	Validar la recuperabilidad de la información, de los servicios, las aplicaciones y la infraestructura.	
Proceso catalizador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
APO01.03	Mantener los catalizadores de la gestión del sistema	Mantener los catalizadores del sistema de gestión y crear un ambiente de control con las TIC corporativas, y asegurarse que están integrados y alineados con la gobernanza y la gestión como parte de la filosofía de la empresa y del estilo operativo. Estos catalizadores comunicaran claramente las expectativas o las necesidades. El sistema de gestión debe estimular la cooperación y el trabajo en equipo entre las distintas divisiones, promover el cumplimiento y la mejora continua, y manejar las desviaciones del proceso (incluyendo los fallos).
APO01.08	Mantener el cumplimiento con las políticas y los procedimientos.	Establecer los procedimientos para mantener el cumplimiento y la medición del desempeño de las políticas y otros facilitadores que posibiliten mejorar la estructura de control, y sancionar el incumplimiento o el cumplimiento defectuoso. Realizar un seguimiento de las tendencias y su rendimiento y considerar estos en diseños futuros y mejorar el marco de control.
DSS05.01	Protegerse contra el software mal intencionado.	Implementar y mantener las medidas de prevención, detección y corrección actualizados y vigentes (especialmente los parches de seguridad actualizados y control de las firmas de virus) en toda la empresa, para proteger los sistemas de información y tecnología de software malicioso (por ejemplo, virus, gusanos, software espía, correo no deseado).
DSS05.07	Supervisar la infraestructura de los eventos relacionados con la seguridad	El uso de herramientas de detección de intrusos, con el fin de supervisar la infraestructura del acceso no autorizado y garantizar que los eventos queden integrados con la supervisión general de eventos y la gestión de incidencias.
Catalizador de estructuras organizativas		
Referencia	Contribución para dar respuesta a la situación	
Gestor de la Seguridad de la Información	La implementación de medidas de seguridad	
Jefe de Operaciones TIC	Al frente del equipo de gestión de respuesta para restablecer el servicio en el momento oportuno	
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta		
Referencia	Contribución para dar respuesta a la situación	
La seguridad de la información se practica de forma habitual en las operaciones cotidianas.	Para prevenir la instalación de software malicioso	
Las personas respetan la importancia de los principios y políticas de la seguridad de la información.	Para prevenir la instalación de software malicioso	
Las partes interesadas son conscientes de la manera de identificar y responder frente a las amenazas a la empresa.	Para minimizar el impacto de la instalación de software malicioso	
Sensibilizar e informar sobre el uso del software mal intencionado, el uso del correo electrónico e Internet.	Para evitar la instalación de software malicioso	

D.15. Escenario 15: Software mal intencionado (cont.)	
Catalizador para alcanzar los objetivos de información	
Referencia	Contribución para dar respuesta a la situación
Información fente a la amenaza	Inteligencia en relación con los tipos de ataques
Informes de supervisión.	Identificación de los intentos de ataque, eventos de amenaza, etc
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones	
Referencia	Contribución para dar respuesta a la situación
Protección perimetral	Protección contra el software mal intencionado
SIEM	Seguridad de la Infomación y gestión de eventos.
Herramientas de protección de software mal intencionado.	Protección contra el software mal intencionado
Supervisión y servicios de alerta	Ser notificado a tiempo de las amenazas potenciales
Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias	
Referencia	Contribución para dar respuesta a la situación
Habilidades de seguridad de la Información	La prevención y la reducción del impacto por el software malintencionado.
Habilidades técnicas en TIC	Configuración de la infraestructura TIC, tales como cortafuegos o protección perimetral, etc, y la revisión de los productos entregados por los proveedores

D.16. Escenario 16: Ataques lógicos		
Categoría del escenario de riesgo	Ataques lógicos	
Catalizador para alcanzar los objetivos de los principios, políticas y los libros de acuerdos		
Referencia	Contribución para dar respuesta a la situación	
Políticas de seguridad de la información	Describe las medidas de seguridad de la información dentro de la empresa.	
Políticas y procedimientos técnicos en seguridad	Detalla las consecuencias técnicas de la política de seguridad de la información.	
Principios de la arquitectura	Los requisitos de seguridad de la información son parte intrínseca de la arquitectura de la empresa y se traducen en una arquitectura formal de seguridad de información.	
Políticas de Continuidad de Negocio y de recuperación ante desastres	Validar la recuperabilidad de la información, de los servicios, de las aplicaciones y la infraestructura.	
Proceso catalizador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
APO13.01	Establecer y mantener el sistema de gestión de la seguridad de la información (ISMS).	Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo de la gestión de seguridad de información, permitiendo asegurar que los procesos tecnológicos y empresariales estén alineados con los requerimientos del negocio y la gestión de seguridad de la empresa.
APO13.03	Supervisar y revisar el ISMS	Mantener y comunicar regularmente la necesidad y los beneficios de instaurar procesos de mejora continua en la seguridad de la información. Recopilar y analizar los datos sobre el SGSI, y mejorar la eficacia del SGSI. Corregir las no conformidades para prevenir la recurrencia. Promover una cultura de la seguridad y de la mejora continua.
BAI03.07	Preparar las pruebas de selección.	Establecer un plan de pruebas y entornos necesarios para probar cada uno de los componentes de la solución individualizada e integrada, incluyendo a todos los procesos de negocio y a los servicios de apoyo, las aplicaciones y la infraestructura
DSS01.03	Supervisar la infraestructura TIC.	Supervisar la infraestructura TIC y los ventos relacionados. Almacenar la información necesaria y suficiente de forma cronológica en los registros de operaciones para permitir la reconstrucción, revisión y análisis secuencial y temporal de todas las operaciones y el resto de las actividades que respaldan cada una de dichas operaciones.
DSS04.03	Desarrollar e implementar una respuesta a la continuidad del negocio	Desarrollar un plan de continuidad del negocio (BCP) sobre la base estratégica que documente los procedimientos y prepara la información para su uso en un incidente y permite a la empresa continuar con sus actividades críticas.
DSS05.01	Protegerse contra el software mal intencionado.	Implementar y mantener las medidas de prevención, detección y corrección actualizados y vigentes (especialmente los parches de seguridad actualizados y control de las firmas de virus) en toda la empresa, para proteger los sistemas de información y tecnología de software malicioso (por ejemplo, virus, gusanos, software espía, correo no deseado).
DSS05.02	Gestión de la seguridad de la red y conectividad	Utiliza las medidas de seguridad y procedimientos de gestión relacionados para proteger la información sobre todos los métodos de conectividad.
DSS05.07	Supervisar la infraestructura de los eventos relacionados con la seguridad	El uso de herramientas de detección de intrusos, permite supervisar la infraestructura en el acceso no autorizado y garantiza que los eventos se integren con la supervisión general de eventos y la gestión de incidencias.
Catalizador de estructuras organizativas		
Referencia	Contribución para dar respuesta a la situación	
Gestor de la Seguridad de la Información	Implementa las medidas de seguridad	
Jefe de Operaciones TIC	Al frente del equipo de respuesta de operaciones para restablecer el servicio en el momento oportuno	
Gestor del servicio	En caso de que los ataques tengan éxito, se comunica con el usuario final y le ayuda a gestionar la respuesta.	
Jefe de arquitectura de seguridad	Diseña y mide la seguridad	

D.16. Escenario 16: Ataques lógicos (cont.)	
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta	
Referencia	Contribución para dar respuesta a la situación
La seguridad de la información se practica habitualmente en las operaciones diarias	Para prevenir ataques lógicos
Las personas respetan la importancia de los principios y las políticas de la seguridad de la información.	Para evitar ataques lógicos
Las partes interesadas son conscientes de la manera de identificar y responder frente a las amenazas a la empresa.	Para minimizar el impacto de los ataques lógicos
Catalizador para alcanzar los objetivos de información	
Referencia	Contribución para dar respuesta a la situación
SLAs	Detallar las acciones a realizar en caso de recibir un ataque
Amenaza de la información	Inteligencia en relación con los tipos de ataques
Informes de supervisión.	Identificación de los intentos de ataque, eventos de amenaza, etc
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones	
Referencia	Contribución para dar respuesta a la situación
Protección perimetral	Prevenir de los ataques lógicos exitosos.
SIEM	Gestión de la seguridad de la información y de los eventos
Scanners de vulnerabilidad y herramientas de gestión de la red	La identificación de los puntos débiles
Supervisión y servicios de alerta	Ser notificado a tiempo de las amenazas potenciales
Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias	
Referencia	Contribución para dar respuesta a la situación
Habilidades de seguridad de la Información.	Prevenir y reducir el impacto de los ataques lógicos
Habilidades técnicas TIC	Configuración de la infraestructura TIC, tales como firewalls, componentes críticos de la red, etc

D.17. Escenario 17: Acción Industrial		
Categoría del escenario de riesgo	Acción industrial	
Catalizador para alcanzar los objetivos de los principios, políticas y de los libros de acuerdos o convenios		
Referencia	Contribución para dar respuesta a la situación	
Política de RRHH	Definir los derechos y obligaciones de todo el personal, en el que se detalle el comportamiento aceptable e inaceptable por los empleados, y al hacerlo, se gestione el riesgo que está relacionado con el comportamiento humano.	
Política de gestión de proveedores	Definir la sustitución o las opciones de prestación de servicios en caso de emergencia.	
Proceso facilitador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
APO01.01	Definir la estructura organizativa	Establecer una estructura organizativa interna y externa que refleje las necesidades y prioridades del negocio de TI. Poner en marcha las estructuras de gestión necesarias (por ejemplo, comités) que permitan la toma de decisiones para que la gestión se lleve a cabo de la manera más eficaz y eficiente.
APO07.01	Mantener la dotación de personal suficiente y adecuado.	Evaluar las necesidades de personal de forma regular o en cambios importantes en la empresa u operativos o entornos de TI para garantizar que la empresa cuenta con los recursos humanos suficientes para apoyar las metas y objetivos de la empresa. El personal se incluye tanto en los recursos internos, como en los externos.
APO07.02	Identificar el personal clave en TIC	Identificar al personal clave de TI y reducir al mínimo la dependencia en un solo individuo que realiza una función de trabajo crítico a través de captura de conocimiento (documentación), debe fomentarse el intercambio de conocimientos, planificar la sucesión y conseguir sustituir al personal.
APO07.05	Planificar y realizar el seguimiento del uso de las herramientas TIC y de negocio por parte de los recursos humanos	Comprender y realizar un seguimiento de la demanda actual y futura de los negocios y de TIC de recursos humanos con competencias para las TIC corporativas. Identificar carencias y aportaciones a futuros planes de abastecimiento, en los procesos de contratación de suministro y de negocios, y en procesos de contratación TIC
Catalizador de estructuras organizativas		
Referencia	Contribución para dar respuesta a la situación	
Jefe de RRHH	Responsable de establecer las expectativas del personal y para el personal	
Grupo Legal	Apoya a la contratación inicial y a demandar en casos de malos usos o vicios.	
Junta	Responsable del buen funcionamiento de la empresa, es la estructura organizativa de primer nivel para comunicarse con los interesados	
Ejecutivo del negocio	Facilitar la comunicación entre las partes.	
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta		
Referencia	Contribución para dar respuesta a la situación	
El enfoque a la cultura de transparencia y de participación es un punto importante.	Para evitar acciones laborales que puedan producirse	
Catalizador para alcanzar los objetivos de información		
Referencia	Contribución para dar respuesta a la situación	
Convenios con el personal	Definición clara de las responsabilidades, de los derechos y de las obligaciones de todo el personal.	
Contratos de suministro	Definición clara de responsabilidades, de derechos y de las obligaciones en los acuerdos específicos con los proveedores	
Repositorios de conocimiento	Reducir al mínimo el efecto de la falta de disponibilidad parcial de los recursos mediante el intercambio de conocimientos sobre procesos, tecnología, etc	
Ánalysis de déficit de recursos	Ánalysis claro que determine el nivel crítico de los recursos	
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones		
Referencia	Contribución para dar respuesta a la situación	
Servicios de copia de seguridad de terceros	Acción de ayuda industrial en caso temporal	

D.17. Escenario 17: Acción Industrial (cont.)	
Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias	
Referencia	Contribución para dar respuesta a la situación
Habilidades de los RRHH	Manejo de habilidades y competencias
Habilidades de negociación	Facilitar la máxima comunicación entre las partes y garantizar que se cumplan los requisitos operativos mínimos.
Destrezas en la litigación	Una vez que se inicia la demanda, se requieren disponer de las habilidades adecuadas para defender los intereses de la empresa.

D.18. Escenario 18: Medio Ambiente		
Categoría del escenario de riesgo		Medio ambiente
Catalizador para alcanzar los objetivos de los principios, políticas y de los libros de acuerdos o convenios		
Referencia		Contribución para dar respuesta a la situación
Políticas de Ética		La conciencia medioambiental debe ser parte de la política general de la ética empresarial.
Política de gestión de proveedores		La conciencia medioambiental debe incluirse en todos los contratos y acuerdos con los proveedores.
Reglas de comportamiento (Usos aceptables)		Los usuarios deben ser conscientes de su impacto individual en este sentido.
Proceso catalizador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
APO02.03	Definir las capacidades TI destinadas al negocio.	Definir el negocio de destino y las capacidades de TI y requirió los servicios de TI. Esto debe basarse en la comprensión del medio ambiente y las necesidades de la empresa; la evaluación de los procesos de negocio actual y entorno de TI y los problemas; y la consideración de las normas de referencia, las mejores prácticas y tecnologías emergentes validados o propuestas de innovación.
APO04.03	Supervisar y analizar el entorno tecnológico	Llevar a cabo un control sistemático y explorar el entorno externo de la empresa para identificar las tecnologías emergentes que tienen el potencial de crear valor (por ejemplo, mediante la realización de la estrategia empresarial, la optimización de costes, evitando la obsolescencia, y mejor capacitación de los servicios y los procesos de TI). Supervisar el mercado, el entorno competitivo, los sectores de la industria, y las tendencias legales y reglamentarias para poder analizar las tecnologías emergentes o ideas de innovación en el contexto empresarial.
BAI03.04	Adquirir componentes que resuelvan las necesidades.	Adquirir los componentes para dar solución, basándose en el plan de adquisición de acuerdo con los requisitos y diseños detallados, los principios y estándares de arquitectura, y los procedimientos globales de la empresa en la adquisición y contratación, los requisitos de control de calidad y las normas de homologación. Asegúrese que todos los requisitos legales y contractuales han sido identificados y abordados por el proveedor.
DSS01.04	Gestión del Medio ambiente.	Mantener las medidas de protección frente a factores ambientales. Instalar equipos y dispositivos especializados para supervisar y controlar el medio ambiente.
DSS01.05	Gestión de las instalaciones.	Administrar las instalaciones, incluyéndose los equipos de comunicaciones y de energía, de acuerdo con las leyes y reglamentos, requisitos técnicos y comerciales, las especificaciones del fabricante, y las directrices de seguridad e higiene.
Catalizador de estructuras organizativas		
Referencia	Contribución para dar respuesta a la situación	
Jefe de Operaciones TIC	Responsable de la gestión del entorno TIC e instalaciones	
Jefe de arquitectura	Diseño de medidas favorables al medio ambiente	
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta		
Referencia	Contribución para dar respuesta a la situación	
Una clara definición de la estructura para la responsabilidad ética y una cultura que promueva que la contabilidad específica se desarrolle y mantiene con normalidad.	La gente está involucrada y es consciente de las consecuencias de los problemas ambientales y están facultados para manejar de acuerdo a las normas éticas.	
Catalizador para alcanzar los objetivos de información		
Referencia	Contribución para dar respuesta a la situación	
Estrategia TIC	La conciencia ambiental debe ser parte de la estrategia de TI.	
Registro de activos	Para evaluar el impacto medioambiental de la tecnología utilizada	
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones		
Referencia	Contribución para dar respuesta a la situación	
CMDB	Base de datos de gestión de configuración utilizada en la asistencia en la identificación de áreas de mejora	

D.18. Escenario 18: Medio Ambiente (cont.)	
Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias	
Referencia	Contribución para dar respuesta a la situación
Desarrollo de la arquitectura	El desarrollo arquitectónico permite ayudar a reducir el impacto medioambiental de la tecnología.
Sistemas ergonómicos	La racionalización y la optimización de la tecnología utilizada

D.19. Escenario 19: Causas de fuerza mayor		
Categoría del escenario de riesgo		Causas de fuerza mayor
Catalizador para alcanzar los objetivos de los principios, políticas y los libros de acuerdos		
Referencia		Contribución para dar respuesta a la situación
Política de copias de seguridad		Disponibilidad de las copias de seguridad.
Políticas de continuidad del negocio y recuperación ante desastres		Validar la recuperación de los datos.
Proceso catalizador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
DSS01.04	Gestión del Medio ambiente.	Mantener las medidas de protección frente a factores ambientales. Instalar equipos y dispositivos especializados para supervisar y controlar el medio ambiente.
DSS01.05	Gestión de las instalaciones.	Administrar las instalaciones, incluyéndose los equipos de comunicaciones y de energía, de acuerdo con las leyes y reglamentos, requisitos técnicos y comerciales, las especificaciones del fabricante, y las directrices de seguridad e higiene.
DSS04.03	Desarrollar e implementar una respuesta a la continuidad del negocio	Desarrollar un plan de continuidad del negocio (BCP) sobre la base de la estrategia que documente que los procedimientos y la información en tratamiento estén disponibles para su uso cuando surja un incidente permitiendo a la empresa continuar con sus actividades críticas.
DSS04.04	Ejercicio, prueba y revisión del Plan de Continuidad del Negocio BCP	Ejercicios de prueba de los mecanismos de continuidad que de forma regular se ejecutan dentro de los planes de recuperación, frente a los resultados predeterminados, permite dar soluciones innovadoras para desarrollarse y contribuye a comprobar durante el transcurso de la prueba que el plan va a funcionar como se esperaba.
DSS05.05	Gestión del acceso físico a los activos TIC.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas de acuerdo a las necesidades del negocio, incluidas las emergencias. El acceso a las instalaciones, a los edificios y a las áreas debe justificarse, autorizarse, registrarse y deben ser supervisadas. Esto debería aplicarse a todas las personas que entren en las instalaciones, incluido el personal, personal temporal, clientes, proveedores, visitantes o cualquier otro tercero.
Catalizador de estructuras organizativas		
Referencia	Contribución para dar respuesta a la situación	
Gestión de la Continuidad del Negocio	Responsable del plan de Continuidad del Negocio (BCP)	
Jefe de Operaciones TIC	Responsable de la gestión del entorno TIC y de las instalaciones	
CIO	Responsable del desarrollo e implementación de dar respuesta a la continuidad del negocio	
Propietario del proceso de negocios	Responsable del desarrollo e implementación de dar respuesta a la continuidad del negocio	
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta		
Referencia	Contribución para dar respuesta a la situación	
Las partes interesadas son conscientes de cómo identificar y responder a las amenazas	La gente está involucrada y es consciente de cómo debe reaccionar cuando se produce un incidente.	
Los gestores de los negocios colaboran en procesos de mejora continua para permitir que los programas de continuidad del negocio sean más eficientes y eficaces.	El negocio toma el compromiso y es proactivo a contribuir a la mitigación del riesgo.	
Catalizador para alcanzar los objetivos de información		
Referencia	Contribución para dar respuesta a la situación	
Informes de pólizas de seguro	Están vigentes los Seguros en caso de actos naturales.	
Informes de evaluación de las instalaciones	La empresa es consciente del estado y el riesgo en las instalaciones.	
Acciones de respuesta y comunicación frente a incidentes.	La gente es consciente de cómo debe reaccionar cuando se produce un incidente.	

D.19. Escenario 19: Causas de fuerza mayor (cont.)	
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones	
Referencia	Contribución para dar respuesta a la situación
Supervisión y servicios de alerta	Ser notificado con antelación a las amenazas potenciales
Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias	
Referencia	Contribución para dar respuesta a la situación
Gestión de riesgo de la información.	Identificar y formular la respuesta al riesgo de la información relativa a actos naturales.
Conocimiento técnico	Experiencia técnica en relación con actos específicos y relevantes a la propia naturaleza

D.20. Escenario 20: Innovación		
Categoría del escenario de riesgo	Innovación	
Catalizador para alcanzar los objetivos de los principios, políticas y los libros de acuerdos		
Referencia	Contribución para dar respuesta a la situación	
Principios de la arquitectura	Los principios de la arquitectura definen las normas y directrices para su uso y el despliegue de todos los recursos y activos TIC en toda la empresa generales y subyacentes.	
Proceso facilitador para alcanzar el objetivo		
Referencia	Título	Práctica de Gestión
APO02.01	Comprender la dirección de la empresa	Considere el entorno actual de la empresa y los procesos de negocio, así como la estrategia de la empresa y los objetivos futuros. Tenga en cuenta también el entorno externo de la empresa (impulsores de la industria, las regulaciones pertinentes, que son la base para la competencia).
APO02.03	Definir las capacidades TIC destinadas al negocio.	Definir las capacidades TIC y los servicios de TIC que requiere el negocio. Basándose en la comprensión del medio y las necesidades de la empresa; evaluando los procesos de negocio actual y el entorno TIC y los problemas; considerándose las normas de referencia, las mejores prácticas y el arte de las tecnologías emergentes o las propuestas de innovación.
APO03.01	Desarrollar la visión de la arquitectura empresarial.	La visión de la arquitectura proporciona un primer corte, la descripción de alto nivel de las arquitecturas de referencia y objetivos, los dominios de negocios que abarcan, la información, los datos, las aplicaciones y la tecnología. La visión desde el punto de vista de arquitectura proporciona al promotor una herramienta clave para vender los beneficios de la capacidad de la propuesta a las partes interesadas en la empresa. La visión de la arquitectura describe cómo la nueva capacidad cumplirá con las metas de la empresa y los objetivos estratégicos y resolverá las preocupaciones de las partes interesadas de la dirección cuando se implemente.
APO04.01	Crear un ambiente propicio para la innovación	Crear un entorno que sea favorable a la innovación, teniendo en cuenta cuestiones tales como la cultura, la recompensa, la colaboración, foros de tecnología, y los mecanismos de promoción y la captura de las ideas de los empleados.
APO04.02	Mantener una comprensión del entorno empresarial	Trabajar conjuntamente con las partes interesadas relevantes para entender sus retos. Mantener una adecuada comprensión de la estrategia de la empresa y el entorno competitivo o de otras restricciones para que las oportunidades que posibilitan las nuevas tecnologías puedan ser identificadas.
APO04.03	Supervisar y analizar el entorno tecnológico	Realizar un control sistemático y explorar el entorno externo de la empresa para identificar las tecnologías emergentes que tengan el potencial de crear valor (por ejemplo, mediante la consecución de la estrategia empresarial, la optimización de costes, evitando la obsolescencia, y mejorar la capacitación de servicios y procesos de TIC). Explorar el mercado, el entorno competitivo, los sectores de la industria, y las tendencias legales y reglamentarias para poder analizar las tecnologías emergentes o ideas de innovación en el contexto empresarial.
APO04.04	Evaluuar el potencial de las tecnologías emergentes y las ideas de innovación.	Analizar las tecnologías emergentes identificadas y / o otras sugerencias de innovación de TIC. Trabajar con las partes interesadas para validar las hipótesis sobre el potencial de las nuevas tecnologías y la innovación.
APO04.05	Recomendar nuevas iniciativas apropiadas	Evaluuar y supervisar los resultados de las iniciativas durante la prueba de concepto y, si es favorable, generar recomendaciones de nuevas iniciativas y lograr el apoyo de las partes interesadas
APO04.06	Supervisar la implementación y el uso de la innovación.	Supervisar la implementación y el uso de tecnologías e innovaciones emergentes durante la integración, la adopción y durante todo el ciclo de vida económico con el fin de garantizar que los beneficios prometidos sean realizados e identificar las lecciones aprendidas.
Catalizador de estructuras organizativas		
Referencia	Contribución para dar respuesta a la situación	
CEO	Responsable de la creación de un entorno propicio para la innovación	
Comité estratégico	Responsable de llevar adelante y realizar un seguimiento de las iniciativas de innovación favorables.	
CIO	Responsable de la identificación de innovaciones de base tecnológica y evaluar su potencial	
Grupo de innovación	Responsable de identificar las oportunidades de innovación y desarrollar nuevos casos de negocio para las iniciativas de innovación.	

D.20. Escenario 20: Innovación (cont.)	
Proceso facilitador para alcanza el objetivo de Cultura, Ética y Conducta	
Referencia	Contribución para dar respuesta a la situación
Voluntad de asumir riesgos	La innovación, por definición, consiste en un nuevo uso de las nuevas tecnologías y de nuevas formas de trabajo, lo que resulta una resistencia potencial ya que los supuestos beneficios no quedan seguros. Sin embargo, al no tener la voluntad de asumir riesgos se excluye anticipadamente cualquier potencial de innovación.
Soporte por parte de la alta dirección a las iniciativas de innovación	Se requiere apoyo de la dirección para financiar las iniciativas de innovación y apoyarlos para superar la resistencia inicial.
Actitud a aceptar los fracasos	No todos los proyectos de innovación o las iniciativas suelen ser un éxito, y un cierto grado de fracaso debe aceptarse como parte del precio a pagar por las iniciativas exitosas.
Catalizador para alcanzar los objetivos de información	
Referencia	Contribución para dar respuesta a la situación
Plan de innovación	Las innovaciones están claramente establecidas para que puedan ser supervisadas y se incorporen en los planes estratégicos de la empresa.
Programa de reconocimiento	La innovación debe ser recompensada adecuadamente, de acuerdo con un plan acordado de mano y formalizado.
Evaluar las iniciativas de innovación	La evaluación formal de las iniciativas de innovación facilita la toma de decisiones ejecutivas.
Catalizador para alcanzar los objetivos de Infraestructuras, Servicios y Aplicaciones	
Referencia	Contribución para dar respuesta a la situación
N/A	N/A
Catalizador para alcanzar los objetivos de las personas, sus habilidades y competencias	
Referencia	Contribución para dar respuesta a la situación
Liderazgo y comunicación	Aclarar las razones de la arquitectura y las posibles consecuencias..
Experiencia en arquitectura	Desarrollar una arquitectura eficiente y eficaz alineada con los requerimientos del negocio.

Página dejada en blanco intencionadamente

APÉNDICE E
COMPARATIVA DE RIESGOS DE TI CON COBIT 5

APÉNDICE E
COMPARATIVA DE RIESGOS DE TI CON COBIT 5

Este apéndice contiene una comparativa entre las partes más destacadas de la guía de Riesgos de TI (ambos *El marco de Riesgos de TI* y *La guía profesional de Riesgos de TI*) y sus equivalentes en COBIT 5, *COBIT 5: Procesos Catalizadores* o *COBIT 5 para Riesgos*.

E.1 Comparativa del Marco de Riesgos de TI con COBIT 5				
Capítulo Marco de Riesgos en TI	Subsección	COBIT 5	COBIT 5: Procesos Catalizadores	COBIT 5 para Riesgos
3. Principios de Riesgos TI: • Conectar con los objetivos de negocio • Alinear la gestión de riesgos de TI con ERM • Balance coste/beneficio de Riesgos de TI • Promover una comunicación justa y abierta • Establecer el tono al inicio • Funcionar como parte de las actividades diarias		La optimización de riesgos es uno de los tres componentes básicos del valor objetivo de la empresa.	N/A	Los principios de riesgo se incluyen en los Catalizadores de Principios, Políticas y Marcos (sección 2A, capítulo 2). En el apéndice B.1 se incluye una descripción más detallada de los principios de riesgo.
4. El Marco de Riesgos de TI		Los procesos relacionados con los riesgos de TI se han integrado en el Modelo de Referencia de Procesos de COBIT 5		N/A
5. Fundamentos de gobierno del riesgo	A. Apetito y tolerancia al Riesgo	N/A	El apetito y tolerancia al Riesgo está (parcialmente) cubierto por el proceso EDM03.	El apetito y tolerancia al Riesgo se definen como ejemplos del catalizador de la Información (sección 2A, capítulo 6). En el apéndice B.5 se ha incluido una descripción más detallada de la capacidad, apetito y tolerancia al Riesgo. Esta sección también incluye orientaciones sobre cómo establecer y comunicar estos umbrales.
	B. Responsabilidades y rendición de cuentas sobre la gestión de riesgos de TI	Las responsabilidades y la rendición de cuentas son parte de la gráfica RACI en la descripción del proceso	Las responsabilidades y la rendición de cuentas son parte de la gráfica RACI en la descripción del proceso	Las responsabilidades y la rendición de cuentas de la gestión de riesgos de TI están definidas como parte del catalizador de Estructuras Organizacionales (sección 2A, capítulo 4)
	C. Sensibilización y comunicación	Cultura, Ética y Conducta se incluyen ahora como un catalizador independiente en el marco de COBIT 5, incluyendo como prácticas tanto la sensibilización como la comunicación	La sensibilización y la comunicación del Riesgo está cubierta (parcialmente) por el proceso EDM03	La sensibilización y la comunicación están definidas como parte del catalizador de Cultura, Ética y Conducta (sección 2A, capítulo 5)
	D. Cultura de Riesgos	Cultura, Ética y Conducta se incluyen ahora como un catalizador independiente en el marco de COBIT 5	La cultura del Riesgo está cubierta por la práctica EDM03.02	El catalizador de Cultura, Ética y Conducta se describe en la sección 2A, capítulo 5. Una descripción más detallada de los comportamientos deseados y como conseguirlos se incluye en el apéndice B.4

E.1 Comparativa del Marco de Riesgos de TI con COBIT 5 (cont.)				
Capítulo Marco de Riesgos en TI	Subsección	COBIT 5	COBIT 5: Procesos Catalizadores	COBIT 5 para Riesgos
6. Fundamentos de evaluación del riesgo	A. Describiendo impactos en el negocio	Principio 1: La cobertura de necesidades de las partes interesadas, cubre la cascada de objetivos de COBIT 5. Es el mecanismo para convertir las necesidades de las partes interesadas en metas específicas y acciones concretas y personalizadas de la empresa, objetivos relacionados con TI y objetivos del catalizador	El impacto en el negocio está cubierto por el proceso EDM03	El impacto en el negocio se incluye en la elaboración de los catalizadores de Procesos en el apéndice B.2.
	B. Escenarios de Riesgos de TI	N/A	Los escenarios de riesgo están cubiertos en las prácticas APO12.03/04	Toda la información sobre los escenarios de riesgos de TI se ha incluido en la sección 2B, capítulo 2. Una descripción más detallada de los escenarios de riesgos de TI y cómo responder ante ellos utilizando COBIT 5 se ha incluido en el apéndice D.
7. Fundamentos de respuesta al riesgo	A. Indicadores clave de riesgos	N/A	Los KRIs están cubiertos (parcialmente) por el proceso EDM03	Los KRIs se han definido como ejemplos de catalizador de Información (sección 2A, capítulo 6) Una descripción más detallada de los KRIs se ha incluido en el apéndice B.5.
	B. Selección y priorización de respuestas ante riesgos	N/A	La selección y priorización de respuestas ante riesgos está cubierta en la práctica APO12.06	Toda la información respecto a respuestas ante riesgos se ha incluido en la sección 2B, capítulo 5.
8. Gestión de riesgos y oportunidades utilizando COBIT, Val TI y Risk TI		Principio 3: La aplicación de un único marco integrado, implica que todo el conocimiento cubierto en los anteriores marcos de ISACA se ha integrado en COBIT 5	N/A	Una descripción más detallada de los escenarios de riesgos de TI y cómo responder ante ellos utilizando COBIT 5 se ha incluido en el apéndice D.
12. El Marco de Riesgos de TI	RG1	Los procesos relacionados con los riesgos de TI se han integrado en el Modelo de Referencia de Procesos de COBIT 5	EDM03, APO12	Más detalles del proceso se han incluido en la descripción detallada del apéndice B.2 del Catalizador de Procesos.
	RG2		EDM03, EDM04, APO07	
	RG3		EDM01, EDM03	
	RE1		APO12.01	
	RE2		APO12.02	
	RE3		APO12.02, APO12.03	
	RR1		APO12.04	
	RR2		APO12.05	
	RR3		APO12.06	
Apéndice 2. Comparación de alto nivel con otros marcos de gestión de riesgos	N/A	N/A	N/A	Apéndice C

APÉNDICE E
COMPARATIVA DE RIESGOS DE TI CON COBIT 5

E.2 Comparativa de la Guía Profesional de Riesgos de TI con COBIT 5				
Capítulo de la Guía Profesional de Riesgos en TI	Subsección	COBIT 5	COBIT 5: Procesos Catalizadores	COBIT 5 para Riesgos
1. Definición del universo de riesgos y determinación del alcance de la gestión de riesgos		El marco de COBIT 5 se utiliza para establecer los límites del universo GEIT de la empresa, es decir, todos los aspectos del universo GEIT deben ser considerados desde una perspectiva de gobierno y gestión.	El universo de riesgos y la determinación del alcance de los mismos está cubierto (parcialmente) por el proceso EDM03.	COBIT 5 para Riesgos guía a las empresas en el uso de COBIT para considerar y abordar GEIT desde una perspectiva de gobierno y gestión del riesgo y apoya a los profesionales de riesgos de la empresa en el uso de COBIT en el desempeño de sus actividades.
2. Apetito y tolerancia al riesgo		N/A	El Apetito y tolerancia al Riesgo está (parcialmente) cubierto por el proceso EDM03.	El Apetito y tolerancia al Riesgo se definen como ejemplos del catalizador de la Información (sección 2A, capítulo 6). En el apéndice B.5 se ha incluido una descripción más detallada de la capacidad, Apetito y tolerancia al Riesgo. Este apéndice también incluye orientaciones sobre cómo establecer y comunicar estos umbrales.
3. Sensibilización ante el riesgo, comunicación y presentación de informes	A. Sensibilización y comunicación	Cultura, Ética y Conducta se incluyen como un catalizador independiente en el marco de COBIT 5	La sensibilización y comunicación del Riesgo está cubierta (parcialmente) por el proceso EDM03	La sensibilización y la comunicación están definidas como parte del catalizador de Cultura, Ética y Conducta (sección 2ª, capítulo 5)
	B. Indicadores clave y presentación de informes de riesgos	N/A	Los KRIs y la presentación de informes de riesgos están cubiertos (parcialmente) por el proceso EDM03	Los KRIs se han definido como ejemplos de catalizador de información (sección 2A, capítulo 6). En el apéndice B.5 se incluye una descripción más detallada de los KRIs.
	C.Perfil de riesgo	N/A	El perfil de riesgo está cubierto en la práctica APO12.03	Los perfiles de riesgo se han definido como ejemplos de catalizador de información (sección 2A, capítulo 6). En el apéndice B.5 se incluye una descripción más detallada de los perfiles de riesgo.
	D.Agregación de riesgos	N/A	La agregación de riesgos está cubierta (parcialmente) por el proceso EDM03	La agregación de riesgos está explicada en la sección 2B, capítulo 4.
	E.Cultura de riesgos	Cultura, Ética y Conducta se incluyen como un catalizador independiente en el marco de COBIT 5	La cultura de riesgos está cubierta por la práctica EDM03.02	El catalizador de Cultura, Ética y Conducta se describe en la sección 2A, capítulo 5. En el apéndice B.4 se incluye una descripción más detallada de los comportamientos deseados y cómo conseguirlos.

E.2 Comparativa de la Guía Profesional de Riesgos de TI con COBIT 5 (cont.)

Capítulo de la Guía Profesional de Riesgos en TI	Subsección	COBIT 5	COBIT 5: Procesos Catalizadores	COBIT 5 para Riesgos
4. Expresando y describiendo riesgos	A. Expresión de impacto en términos de negocio	Principio 1: la reunión de necesidades de las partes interesadas cubre la cascada de objetivos de COBIT 5. Es el mecanismo para trasladar las necesidades de las partes interesadas en metas específicas y acciones concretas y personalizadas de la empresa, así como los objetivos relacionados con TI y con el catalizador.	El impacto en el negocio está cubierto por el proceso EDM03.	El impacto en el negocio se incluye en la elaboración de los catalizadores de Procesos en el apéndice B.2.
	B. Describiendo riesgos – expresando frecuencias	N/A	La expresión de frecuencias está cubierta en la práctica APO12.02	La expresión de frecuencias se incluye en la elaboración de los catalizadores de Procesos en el apéndice B.2. No se incluyen orientaciones con el mismo nivel de detalle o ejemplos detallados como en la Guía Profesional de Riesgos de TI.
	C. Describiendo riesgos – expresando impacto	N/A	La expresión de impactos está cubierta en la práctica APO12.02	La expresión de impactos se incluye en la elaboración de los catalizadores de Procesos en el apéndice B.2. No se incluyen orientaciones con el mismo nivel de detalle o ejemplos detallados como en la Guía Profesional de Riesgos de TI.
	D. Comparación de COBIT objetivo de negocio con otros criterios de impacto	N/A	El impacto en el negocio está cubierto por el proceso EDM03.	El impacto en el negocio se incluye en la elaboración de los catalizadores de Procesos en el apéndice B.2. No se incluyen orientaciones con el mismo nivel de detalle o ejemplos detallados como en la Guía Profesional de Riesgos de TI.
	E. Mapa de riesgos	N/A	La utilización de un mapa de riesgos está cubierto en las prácticas APO12.03/04	Los mapas de riesgos se han definido como ejemplos de catalizador de información (sección 2A, capítulo 6) En el apéndice B.5 se incluye una descripción más detallada de los elementos de información del mapa de riesgos. No se incluyen orientaciones con el mismo nivel de detalle o ejemplos detallados como en la Guía Profesional de Riesgos de TI.

APÉNDICE E
COMPARATIVA DE RIESGOS DE TI CON COBIT 5

E.2 Comparativa de la Guía Profesional de Riesgos de TI con COBIT 5 (cont.)				
4. Expresando y describiendo riesgos	F. Registro de riesgos	N/A	La utilización de un registro de riesgos está cubierta en las prácticas APO12.03/04	Un registro de riesgos se define como parte del perfil de riesgo (sección 2A, capítulo 6). En el apéndice B.5 se incluye una descripción más detallada de los perfiles de riesgo. Esta sección también contiene una plantilla para la entrada de registros de riesgos.
5. Escenarios de riesgo	A. Escenarios de riesgo explicados	N/A	N/A	Toda la información respecto a escenarios de riesgos de TI está incluida en la sección 2B, capítulos 1 a 3. En el apéndice D se incluye una descripción más detallada de los escenarios de riesgos de TI y cómo darles respuesta utilizando los catalizadores de COBIT 5.
	B. Ejemplo de escenarios de riesgo	N/A	N/A	En la sección 2B, capítulo 3 se enumeran ejemplos de escenarios de riesgo. En el apéndice D se incluye una descripción más detallada de los escenarios de riesgos de TI y cómo darles respuesta utilizando los catalizadores de COBIT 5.
	C. Factores de riesgo de capacidad en el proceso de análisis de riesgos	N/A	N/A	Toda la información respecto a escenarios de riesgos de TI está incluida en la sección 2B, capítulos 1 a 2. En el apéndice D se incluye una descripción más detallada de los escenarios de riesgos de TI y cómo darles respuesta utilizando los catalizadores de COBIT 5.
	D. Factores de riesgo del entorno en el proceso de análisis de riesgos	N/A	N/A	Toda la información respecto a escenarios de riesgos de TI está incluida en la sección 2B, capítulos 1 a 2. En el apéndice D se incluye una descripción más detallada de los escenarios de riesgos de TI y cómo darles respuesta utilizando los catalizadores de COBIT 5.
6. Respuesta y priorización ante riesgos	N/A	La respuesta ante riesgos está cubierta por el proceso APO12.	Toda la información respecto a escenarios de riesgos de TI está incluida en la sección 2B, capítulo 5.	
7. Flujo de trabajo en el análisis de riesgos	N/A	El flujo de trabajo en el análisis de riesgos está cubierto por el proceso APO12.	N/A	

E.2 Comparativa de la Guía Profesional de Riesgos de TI con COBIT 5 (cont.)

8. Mitigación de riesgos utilizando COBIT y Val IT	N/A	N/A	El apéndice D contiene una descripción detallada sobre cómo responder a cada una de las categorías de escenarios de riesgo identificados (20) utilizando los catalizadores de COBIT 5.
--	-----	-----	--

APÉNDICE F
PLANTILLA EXHAUSTIVA PARA ESCENARIOS DE RIESGOS

APÉNDICE F
PLANTILLA EXHAUSTIVA PARA ESCENARIOS DE RIESGOS

Este apéndice contiene una completa plantilla para la gestión de un escenario de riesgo —desde su inicio hasta la respuesta y monitoreo— como soporte de los procesos centrales de gestión de riesgos de una empresa.

Plantilla para Escenarios de Riesgos	
Título	
Categoría Descripción de la categoría de riesgo a alto nivel	<input type="checkbox"/> 01-Definición y mantenimiento del catálogo <input type="checkbox"/> 02-Gestión del ciclo de vida de programas /proyectos <input type="checkbox"/> 03-Toma de decisiones de inversiones TI <input type="checkbox"/> 04-Experiencia y habilidades en TI <input type="checkbox"/> 05-Personal de operaciones <input type="checkbox"/> 06-Información <input type="checkbox"/> 07-Arquitectura <input type="checkbox"/> 08-Infraestructura <input type="checkbox"/> 09-Software <input type="checkbox"/> 10-Apropiación de TI por el negocio no efectiva <input type="checkbox"/> 11-Selección / desempeño de proveedores externos <input type="checkbox"/> 12-Cumplimiento normativo <input type="checkbox"/> 13-Geopolítico <input type="checkbox"/> 14-Robo de infraestructura <input type="checkbox"/> 15-Software malicioso (malware) <input type="checkbox"/> 16-Ataque lógico <input type="checkbox"/> 17-Conflicto laboral <input type="checkbox"/> 18-Medioambiental <input type="checkbox"/> 19-Desastre natural <input type="checkbox"/> 20-Innovación
Describa el escenario de riesgo / oportunidad, incluyendo el detalle de los impactos negativos y positivos del escenario. La descripción explica el tipo de amenaza / vulnerabilidad e incluye los actores, eventos, activos y elementos cronológicos.	
Tipo de amenaza La naturaleza del evento—¿Es malicioso? En caso contrario, ¿es accidental, o defecto de un proceso bien definido? ¿Es un evento natural o tiene una causa externa?	<input type="checkbox"/> Malicioso <input type="checkbox"/> Accidental <input type="checkbox"/> Error <input type="checkbox"/> Defecto <input type="checkbox"/> Natural <input type="checkbox"/> Causa externa
Actor ¿Quién genera la amenaza que explota una vulnerabilidad? Los actores pueden ser internos o externos, humanos o no humanos.	<input type="checkbox"/> Actores internos, que se encuentran dentro de la empresa, p.ej. personal, contratistas. <input type="checkbox"/> Actores externos, que incluyen intrusos, competidores, reguladores y el Mercado.
Evento ¿Procede de la revelación (de información confidencial), interrupción (de un sistema o un proyecto), robo o destrucción? El desencadenante incluye también el diseño no eficaz (de sistemas, procesos, etc.), la utilización inadecuada, cambios en normas y regulaciones que impactan materialmente a un sistema, o la ejecución ineficaz de procesos, p.ej., procedimientos de gestión de cambios, procedimientos de adquisición, procesos de priorización de proyectos.	<input type="checkbox"/> Revelación <input type="checkbox"/> Interrupción <input type="checkbox"/> Modificación <input type="checkbox"/> Robo <input type="checkbox"/> Destrucción <input type="checkbox"/> Diseño ineficaz <input type="checkbox"/> Ejecución ineficaz <input type="checkbox"/> Normas y regulaciones <input type="checkbox"/> Uso inadecuado

Plantilla para Escenarios de Riesgos (cont.)

Activo Un activo es cualquier elemento de valor para la empresa que puede ser afectado y causar un impacto en el negocio. (Los activos y los recursos pueden ser idénticos, p.ej., el hardware TI es un recurso importante porque todas las aplicaciones TI lo utilizan y, al mismo tiempo, es un activo porque tiene cierto valor para la empresa.)	<ol style="list-style-type: none"> 1. Procesos, p.ej., modelizados como procesos de COBIT 5 o como procesos de negocio 2. Personas y Habilidades 3. Estructura Organizativa 4. Infraestructura Física (instalaciones, equipos, etc.) 5. Infraestructura TI (incluyendo hardware, redes, middleware) 6. Información 7. Aplicaciones
Recurso Un recurso es un elemento que contribuye a conseguir una meta. (Los activos y los recursos pueden ser idénticos, p.ej., el hardware TI es un recurso importante porque todas las aplicaciones TI lo utilizan, y al mismo tiempo, es un activo porque tiene un cierto valor para la empresa.)	<ol style="list-style-type: none"> 1. Procesos, p.ej., modelizados como procesos de COBIT 5 o como procesos de negocio 2. Personas y Habilidades 3. Estructuras Organizativas 4. Infraestructura Física (instalaciones, equipo, etc.) 5. Infraestructura TI (incluyendo hardware de computación, redes, middleware [sistemas medios]) 6. Información 7. Aplicaciones
Título	
Plazos	<ol style="list-style-type: none"> 1. Momento del suceso (crítico, no crítico—¿Ocurre el evento en un momento crítico?) 2. Duración (total—La duración del evento, p.ej., interrupción prolongada de un servicio o centro de datos) 3. Detección (lenta, moderada, instantánea) 4. Intervalo temporal (inmediato, diferido—tiempo transcurrido entre el evento y la consecuencia; ¿Hay una consecuencia inmediata [p.ej., fallo de red, inactividad inmediata, o consecuencia diferida] o una incorrecta arquitectura de TI con alto coste acumulado en el plazo de varios años?)
Tipo de riesgo Describa el tipo de riesgo. Incluya si el tipo de riesgo es primario o secundario, p.ej., alto o bajo nivel de adecuación de TI. Tipologías de riesgo:	<ul style="list-style-type: none"> • Realización de beneficios / valores de TI: Se asocia con oportunidades [perdidas] de utilizar la tecnología para mejorar la eficiencia o eficacia de los procesos de negocio, o como un catalizador para nuevas iniciativas de negocio <ul style="list-style-type: none"> – La tecnología como catalizador de nuevas iniciativas de negocio – La tecnología como catalizador para la eficiencia operativa • Entrega de Programas y Proyectos TI: Se asocia con la contribución de TI a soluciones de negocio nuevas o mejoradas, normalmente en forma de proyectos y programas como parte de carteras de inversión. <ul style="list-style-type: none"> – Calidad del proyecto – Relevancia del proyecto – Desviación del proyecto • Operaciones y Entrega de Servicios de TI: Se asocia con todos los aspectos del rendimiento habitual de los sistemas y servicios de TI, que pueden conllevar una destrucción o reducción del valor para la empresa. <ul style="list-style-type: none"> – Interrupciones de servicios TI – Problemas de seguridad – Cuestiones de cumplimiento normativo
Respuesta al Riesgo Describa cómo la empresa responderá al riesgo. El objetivo de definir una respuesta al riesgo es alinear el riesgo con el apetito y nivel de tolerancia definido en la empresa:	<ul style="list-style-type: none"> • Aceptación del riesgo • Transferencia / compartición del riesgo • Mitigación del riesgo • Evitar el riesgo

APÉNDICE F
PLANTILLA EXHAUSTIVA PARA ESCENARIOS DE RIESGOS

Plantilla para Escenarios de Riesgos (cont.)					
Mitigación del riesgo utilizando Catalizadores de COBIT 5 (ver apéndice D en COBIT 5 para Riesgos) Describa cómo la empresa evitará que el riesgo se materialice. Para conocer las posibilidades de mitigación de riesgos, utilice las prácticas de gestión de COBIT 5 (catalizadores). Facilite la siguiente información:					
Referencia a Práctica de Gestión	Título	Práctica de Gestión	Efecto en Frecuencia	Efecto en Impacto	Indispensable
Indicadores Clave de Riesgo Identifique una serie de métricas para detectar y monitorear el escenario de riesgo y la respuesta al riesgo.					

Página dejada en blanco intencionadamente