

Objetivos de gobierno y gestión

Acerca de ISACA

Con casi 50 años de vida, ISACA® (isaca.org) es una asociación global que ayuda tanto a individuos como a empresas a alcanzar el potencial positivo de la tecnología. La tecnología impulsa al mundo actual e ISACA proporciona a los profesionales el conocimiento, las credenciales, la educación y la comunidad para avanzar en sus carreras profesionales y transformar sus organizaciones. ISACA aprovecha la experiencia de su medio millón de dedicados profesionales en información y ciberseguridad, gobierno, aseguramiento, riesgo e innovación, así como su filial de desempeño empresarial, el instituto CMMI®, para contribuir a una mayor innovación a través de la tecnología. ISACA está presente en más de 188 países, con más de 217 capítulos y oficinas, tanto en Estados Unidos como en China.

Descargo de responsabilidad

ISACA ha diseñado y creado el *Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión* (el «Trabajo») fundamentalmente como un recurso educativo para los profesionales de gobierno de información y Tecnología empresarial (GEIT), aseguramiento, riesgo y seguridad. ISACA no asume ninguna responsabilidad acerca de que el uso de cualquier parte del Trabajo garantice un resultado exitoso. No debe considerarse que el Trabajo incluye toda la información, procedimientos y pruebas correctas, ni que excluye otra información, procedimientos y pruebas que estén orientadas razonablemente hacia la obtención de los mismos resultados. Para determinar la conveniencia de cualquier información específica, procedimiento o prueba, los profesionales de aseguramiento, gobierno, riesgo y seguridad deben aplicar su propio criterio profesional a las circunstancias específicas presentadas por los sistemas específicos o por el entorno de tecnología de la información.

Copyright

© 2018 ISACA. Todos los derechos reservados. Para acceder a las instrucciones de uso, visite www.isaca.org/COBITuse.

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA
Teléfono: +1.847.660.5505
Fax: +1.847.253.1755
Contacto: <https://support.isaca.org>
Sitio web: www.isaca.org

Participar en los foros en línea de ISACA: <https://engage.isaca.org/onlineforums>

Twitter: <http://twitter.com/ISACANews>

LinkedIn: <http://linkd.in/ISACAOOfficial>

Facebook: www.facebook.com/ISACAHQ

Instagram: www.instagram.com/isacanews/

Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión

ISBN 978-1-60420-790-3

En memoria: John Lainhart (1946-2018)

Dedicado a John Lainhart, Presidente del Consejo de Administración de ISACA, 1984-1985. John fue una figura clave en la creación del marco de referencia COBIT® y en los últimos años ejerció como presidente del grupo de trabajo de COBIT® 2019, que culminó con la creación de este trabajo. Durante sus cuatro décadas en ISACA, John participó en distintos aspectos de la organización, además de contar con las certificaciones CISA, CRISC, CISM y CGEIT de ISACA. John deja un increíble legado personal y profesional, y su trabajo ha tenido un gran impacto en ISACA.

Página dejada intencionalmente en blanco

Agradecimientos

ISACA desea agradecer a:

COBIT Working Group (2017-2018)

John Lainhart, Chair, CISA, CRISC, CISM, CGEIT, CIPP/G, CIPP/US, Grant Thornton, EE. UU.

Matt Conboy, Cigna, EE. UU.

Ron Saull, CGEIT, CSP, Great-West Lifeco & IGM Financial (jubilado), Canadá

Equipo de desarrollo

Steven De Haes, Ph.D., Antwerp Management School, University of Antwerp, Bélgica

Matthias Goorden, PwC, Bélgica

Stefanie Grijp, PwC, Bélgica

Bart Peeters, PwC, Bélgica

Geert Poels, Ph.D., Ghent University, Bélgica

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

Revisores expertos

Sarah Ahmad Abedin, CISA, CRISC, CGEIT, Grant Thornton LLP, EE. UU.

Floris Ampe, CISA, CRISC, CGEIT, CIA, ISO27000, PRINCE2, TOGAF, PwC, Bélgica

Elisabeth Antonssen, Nordea Bank, Suecia

Krzysztof Baczkiewicz, CHAMP, CITAM, CSAM, Transpectit, Polonia

Christopher M. Ballister, CRISC, CISM, CGEIT, Grant Thornton, EE. UU.

Gary Bannister, CGEIT, CGMA, FCMA, Austria

Graciela Braga, CGEIT, Auditor and Advisor, Argentina

Ricardo Bria, CISA, CRISC, CGEIT, COTO CICSA, Argentina

Sushil Chatterji, CGEIT, Edutech Enterprises, Singapur

Peter T. Davis, CISA, CISM, CGEIT, COBIT 5 Assessor, CISSP, CMA, CPA, PMI-RMP, PMP, Peter Davis+Associates, Canadá

James Doss, CISM, CGEIT, EMCCA, PMP, SSGB, TOGAF 9, ITvalueQuickStart.com, EE. UU.

Yalcin Gerek, CISA, CRISC, CGEIT, ITIL Expert, Prince2, ISO 20000LI, ISO27001LA, TAC AS., Turquía

James L. Golden, Golden Consulting Associates, EE. UU.

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

Jimmy Heschl, CISA, CISM, CGEIT, Red Bull, Austria

Jorge Hidalgo, CISA, CISM, CGEIT, Chile

John Jasinski, CISA, CRISC, CISM, CGEIT, COBIT 5 Assessor, CSM, CSPO, IT4IT-F, ITIL Expert, Lean IT-F, MOF, SSBB, TOGAF-F, EE. UU.

Joanna Karczewska, CISA, Polonia

Glenn Keaveny, CEH, CISSP, Grant Thornton, EE. UU.

Eddy Khoo S. K., CGEIT, Kuala Lumpur, Malasia

Joao Souza Neto, CRISC, CGEIT, Universidad Católica de Brasilia, Brasil

Tracey O'Brien, CISA, CISM, CGEIT, IBM Corp (jubilada), EE. UU.

Zachy Olorunjojon, CISA, CGEIT, PMP, BC Ministry of Health, Victoria, BC Canadá

Opeyemi Onifade, CISA, CISM, CGEIT, BRMP, CISSP, ISO 27001LA, M.IoD, Afenoid Enterprise Limited, Nigeria

Andre Pitkowski, CRISC, CGEIT, CRMA-IIA, OCTAVE, SM, APIT Consultoria de Informatica Ltd., Brasil

Abdul Rafeq, CISA, CGEIT, FCA, Managing Director, Wincer Infotech Limited, India

Dirk Reimers, Entco Deutschland GmbH, A Micro Focus Company

Steve Reznik, CISA, CRISC, ADP, LLC., EE. UU.

Bruno Horta Soares, CISA, CRISC, CGEIT, PMP, GOVaaS - Governance Advisors, as-a-Service, Portugal

Dr. Katalin Szenes, Ph.D., CISA, CISM, CGEIT, CISSP, John von Neumann Faculty of Informatics, Obuda University, Hungría

Peter Tessin, CISA, CRISC, CISM, CGEIT, Discover, EE. UU.

Mark Thomas, CRISC, CGEIT, Escoute, EE. UU.

John Thorp, CMC, ISP, ITCP, The Thorp Network, Canadá

Greet Volders, CGEIT, COBIT Assessor, Voqual N.V., Bélgica

Agradecimientos (continuación)

Revisores expertos (continuación)

Markus Walter, CISA, CISM, CISSP, ITIL, PMP, TOGAF, PwC Singapur/Suiza

David M. Williams, CISA, CAMS, Westpac, Nueva Zelanda

Greg Witte, CISM, G2 Inc., EE. UU.

Consejo de dirección de ISACA

Rob Clyde, Presidente, CISM, Clyde Consulting LLC, EE. UU.

Brennan Baybeck, Vicepresidente, CISA, CRISC, CISM, CISSP, Oracle Corporation, EE. UU.

Tracey Dedrick, Former Chief Risk Officer con Hudson City Bancorp, EE. UU.

Leonard Ong, CISA, CRISC, CISM, CGEIT, COBIT 5 Implementer and Assessor, CFE, CIPM, CIPT, CISSP, CITBCM, CPP, CSSLP, GCFA, GCIA, GCIH, GSNA, ISSMP-ISSAP, PMP, Merck & Co., Inc., Singapur

R.V. Raghu, CISA, CRISC, Versatilist Consulting India Pvt. Ltd., India

Gabriela Reynaga, CISA, CRISC, COBIT 5 Foundation, GRCP, Holistics GRC, México

Gregory Touhill, CISM, CISSP, Cyxtera Federal Group, EE. UU.

Ted Wolff, CISA, Vanguard, Inc., EE. UU.

Tichaona Zororo, CISA, CRISC, CISM, CGEIT, Asesor de COBIT 5, CIA, CRMA, EGIT, Enterprise Governance of IT, Sudáfrica

Theresa Grafenstine, CISA, CRISC, CGEIT, CGAP, CGMA, CIA, CISSP, CPA, Deloitte & Touche LLP, EE. UU., Presidenta del Consejo de Administración de ISACA, 2017-2018

Chris K. Dimitriadis, Ph.D., CISA, CRISC, CISM, INTRALOT, Grecia, Presidente del Consejo de Administración de ISACA, 2015-2017

Matt Loeb, CGEIT, CAE, FASAE, Chief Executive Officer, ISACA, EE. UU.

Robert E Stroud (1965-2018), CRISC, CGEIT, XebiaLabs, Inc., EE. UU., Presidente del Consejo de Administración de ISACA, 2014-2015

ISACA lamenta profundamente el fallecimiento de Robert E Stroud en septiembre de 2018.

ÍNDICE

Capítulo 1. Introducción a COBIT® 2019	9
1.1 COBIT como marco de gobierno de la información y la tecnología	9
1.1.1 ¿Qué es COBIT y qué no es?	9
1.2 Visión general de COBIT® 2019	10
1.3 Terminología y conceptos clave del marco de referencia COBIT	11
1.3.1 Objetivos de gobierno y gestión	11
1.3.2 Componentes del sistema de gobierno	12
1.3.3 Áreas prioritarias	14
Capítulo 2. Estructura de esta publicación y público destinatario	15
2.1 Estructura de esta publicación	15
2.2 Público destinatario	15
Capítulo 3. Estructura de objetivos de gobierno y gestión COBIT	17
3.1 Introducción	17
3.2 Objetivos de gobierno y gestión	17
3.3 Cascada de metas	18
3.4 Componente: Proceso	19
3.5 Componente: Estructuras organizativas	20
3.6 Componente: Flujos y elementos de información	22
3.7 Componente: Personas, habilidades y competencias	24
3.8 Componente: Políticas y procedimientos	25
3.9 Componente: Cultura, ética y comportamiento	25
3.10 Componente: Servicios, infraestructura y aplicaciones	25
Capítulo 4. Objetivos de gobierno y gestión de COBIT: Guía detallada	27
Modelo Core de COBIT	27
4.1 Evaluar, Dirigir y Monitorizar (EDM en inglés)	27
4.2 Alinear, Planificar y Organizar (APO)	53
4.3 Construir, Adquirir e Implementar (BAI)	151
4.4 Entregar, Dar Servicio y Soporte (DSS)	229
4.5 Monitorizar, Evaluar y Valorar (MEA)	271
Apéndices	297
A.1 Apéndice A: Cascada de metas: Tablas de cruce	297
A.2 Apéndice B: Estructuras organizativas: Visión general y descripciones	299
A.3 Apéndice C: Lista de referencias detallada	300

LISTA DE FIGURAS

Capítulo 1. Introducción a COBIT® 2019

Figura 1.1—Visión general de COBIT 10

Figura 1.2—Modelo Core de COBIT 12

Figura 1.3—Componentes COBIT de un sistema de gobierno 13

Capítulo 3. Estructura de objetivos de gobierno y gestión de COBIT

Figura 3.1—Presentación de objetivos de gobierno y gestión..... 18

Figura 3.2—Presentación de metas empresariales y de alineamiento aplicables 18

Figura 3.3—Presentación de metas aplicables y métricas modelo 19

Figura 3.4—Presentación del componente de procesos 19

Figura 3.5—Niveles de capacidad para los procesos..... 20

Figura 3.6—Presentación del componente de estructuras organizativas 21

Figura 3.7—Presentación del componente flujos y elementos de información..... 23

Figura 3.8—Salidas a procesos múltiples 23

Figura 3.9—Presentación del componente de personas, habilidades y competencias 24

Figura 3.10—Presentación del componente de políticas y procedimientos 25

Figura 3.11—Presentación del componente de cultura, ética y comportamiento..... 25

Figura 3.12—Presentación del componente de servicios, infraestructura y aplicaciones 25

Apéndices

Figura A.1—Cruce de metas empresariales y metas de alineamiento 297

Figura A.2—Cruce de objetivos de gobierno y gestión a metas de alineamiento 298

Figura A.3—Roles y estructuras organizativas de COBIT 299

Capítulo 1

Introducción a COBIT® 2019

1.1 COBIT como marco de gobierno de la información y la tecnología

Con el paso de los años, se han desarrollado y promocionado marcos de referencia de mejores prácticas para contribuir al proceso de conocimientos, diseño e implementación del gobierno empresarial de TI (GETI). COBIT® 2019 integra y se basa en más de 25 años de desarrollo en este campo, no solo mediante la incorporación de los nuevos conocimientos de la ciencia, sino también con la aplicación de estos conocimientos en la práctica.

Desde su nacimiento dentro de la comunidad de la auditoría de TI, COBIT® se ha convertido en un marco de gobierno y gestión de información y tecnología más amplio y completo y continua estableciéndose como un marco de referencia generalmente aceptado para el gobierno de I&T.

1.1.1 ¿Qué es COBIT y qué no es?

Antes de describir el marco de referencia actualizado de COBIT, es importante explicar qué es COBIT y qué no es:

COBIT es un marco de referencia para el gobierno y la gestión de la información y la tecnología, dirigido a toda la empresa. La I&T empresarial significa toda la tecnología y procesamiento de la información que la empresa utiliza para lograr sus objetivos, independientemente de dónde ocurra dentro de la empresa. En otras palabras, la información y la tecnología (I&T) empresarial no se limita al departamento de TI de una organización, aunque este está indudablemente incluido.

El marco de referencia COBIT hace una distinción clara entre gobierno y gestión. Estas dos disciplinas abarcan distintos tipos de actividades, requieren distintas estructuras organizativas y sirven diferentes propósitos.

- **El Gobierno** asegura que:

- Las necesidades, condiciones y opciones de las partes interesadas se evalúan para determinar objetivos empresariales equilibrados y acordados.
- La dirección se establece a través de la priorización y la toma de decisiones.
- El rendimiento y el cumplimiento se monitorean en relación con la dirección y los objetivos acordados.

En la mayoría de las empresas, el gobierno es responsabilidad del consejo de dirección bajo el liderazgo del presidente. Ciertas responsabilidades específicas del gobierno se pueden delegar a estructuras organizativas especiales a un nivel adecuado, en particular, en empresas más grandes y complejas.

- **La Gestión** planifica, construye, ejecuta y monitorea actividades en alineación con la dirección establecida por el órgano de gobierno para alcanzar los objetivos de la empresa.

En la mayoría de las empresas, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del director general ejecutivo (CEO).

COBIT define los componentes para crear y sostener un sistema de gobierno: procesos, estructuras organizativas, políticas y procedimientos, flujos de información, cultura y comportamientos, habilidades e infraestructura.¹

COBIT define los factores de diseño que la empresa debería considerar para crear un sistema de gobierno más adecuado.

COBIT trata asuntos de gobierno mediante la agrupación de componentes de gobierno relevantes dentro de objetivos de gobierno y gestión que pueden gestionarse según los niveles de capacidad requeridos.

¹ Estos componentes se denominaron como habilitadores/catalizadores en COBIT® 5.

Debemos disipar algunos conceptos erróneos acerca de COBIT:

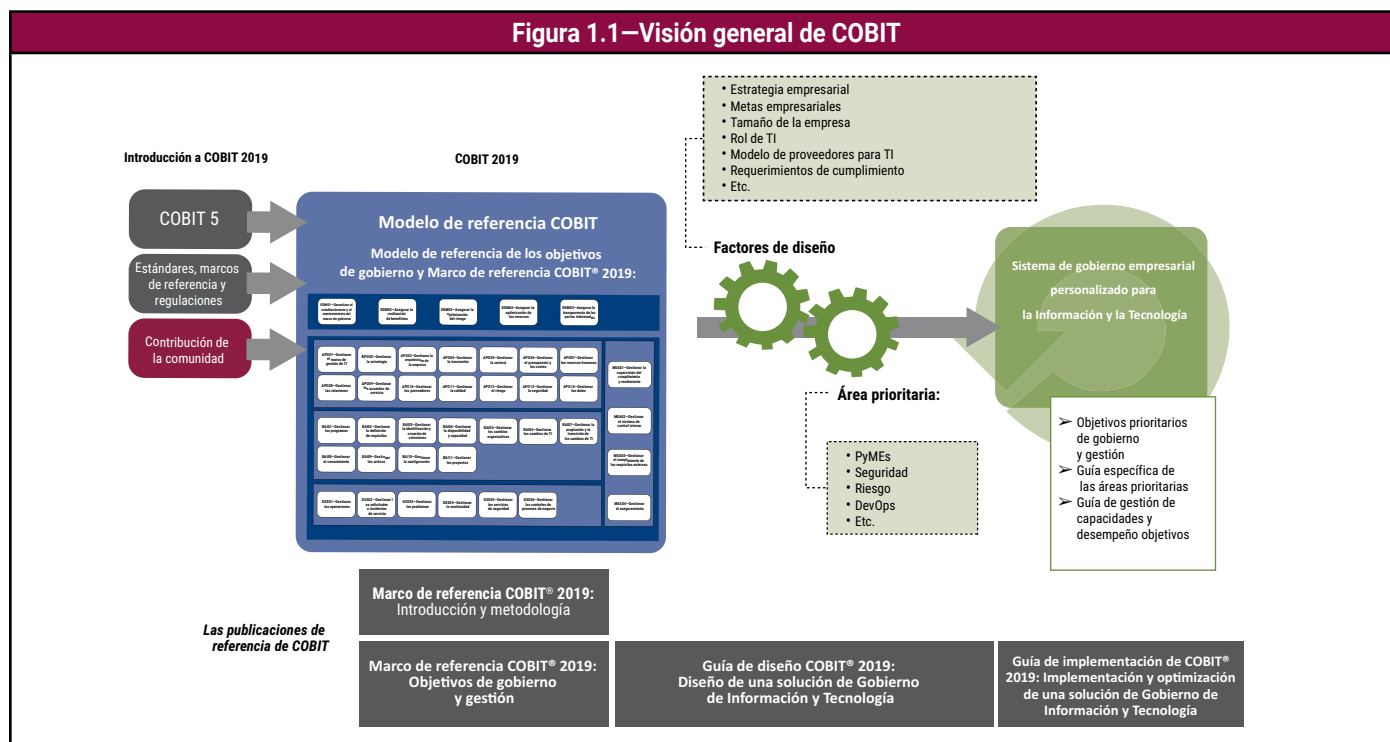
- COBIT no es una descripción completa de todo el entorno de TI de una empresa.
- COBIT no es un marco de referencia para organizar procesos de negocio.
- COBIT no es un marco de referencia técnico (de TI) para gestionar toda la tecnología.
- COBIT no toma ni prescribe ninguna decisión relacionada con las TI. No decidirá cuál es la mejor estrategia de TI, cuál es la mejor arquitectura, o cuánto puede o debería costar la TI. Por el contrario, COBIT define todos los componentes que describen qué decisiones deberían tomarse, cómo deberían tomarse y quién debería tomarlas.

1.2 Visión general de COBIT® 2019

La familia de productos COBIT® 2019 es abierta y se ha diseñado para la personalización. En la actualidad, están disponibles las publicaciones siguientes.²

- **Marco de Referencia COBIT® 2019: Introducción y metodología** presenta los conceptos clave de COBIT® 2019.
- **Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión** describe de forma exhaustiva los 40 objetivos principales del gobierno y la gestión, los procesos incluidos en ellos y otros componentes relacionados. Esta guía también hace referencia a otros estándares y marcos de referencia.
- **Guía de diseño COBIT® 2019: Diseño de una solución de Gobierno de Información y Tecnología** explora los factores de diseño que pueden influir en el gobierno e incluye un flujo de trabajo para la planificación de un sistema de gobierno personalizado para la empresa.
- **Guía de implementación de COBIT® 2019: Implementación y optimización de una solución de gobierno de Información y Tecnología** representa una evolución de la guía de *Implementación de COBIT 5®* y desarrolla una hoja de ruta para la mejora continua del gobierno. Puede usarse en combinación con la Guía de diseño COBIT® 2019.

La **figura 1.1** muestra una visión general de COBIT® 2019 e ilustra cómo distintas publicaciones de esta serie cubren diversos aspectos.



² En el momento de la publicación de este documento *Marco de referencia COBIT® 2019: Objetivos de gobierno y gestión*, se planean títulos adicionales de la familia de productos COBIT® 2019, que aún no se han publicado.

El contenido identificado como áreas prioritarias en la **figura 1.1** incluirá una guía más detallada sobre determinados aspectos.³

En el futuro, COBIT acudirá a su comunidad de usuarios para que proponga actualizaciones de contenido, que se apliquen a modo de contribuciones controladas de forma continua, para que COBIT esté al día de las últimas ideas y evoluciones.

Las secciones siguientes explican los conceptos y términos clave que se usan en COBIT® 2019.

1.3 Terminología y conceptos clave del marco de referencia COBIT

1.3.1 Objetivos de gobierno y gestión

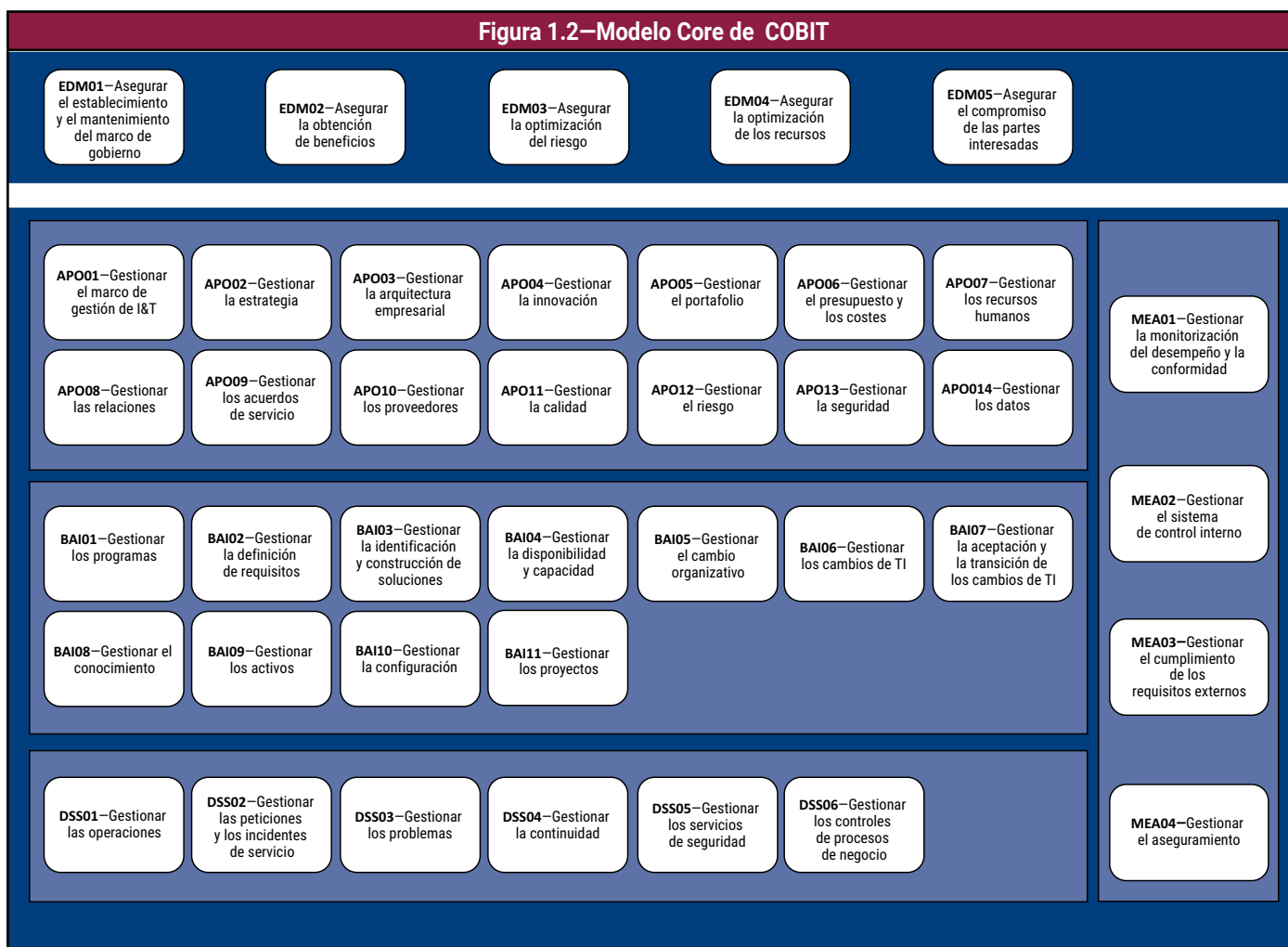
Para que la información y la tecnología contribuyan a los objetivos de la empresa, deberían alcanzarse una serie de objetivos de gobierno y gestión. Los conceptos básicos relacionados con los objetivos de gobierno y gestión son:

- Un objetivo de gobierno o gestión **siempre está relacionado con un proceso** (con un nombre idéntico o similar) y una serie de componentes relacionados de otros tipos para contribuir a lograr el objetivo.
- Un objetivo de gobierno está relacionado con un proceso de gobierno (mostrado en el fondo azul oscuro de la **figura 1.2**), mientras que un objetivo de gestión está relacionado con un proceso de gestión (mostrado en el fondo azul claro de la **figura 1.2**). Los consejos de administración y la dirección ejecutiva suelen rendir cuentas sobre los procesos de gobierno, mientras que los procesos de gestión pertenecen al dominio de la alta y media gerencia.

Los objetivos de gobierno y gestión de COBIT se agrupan en cinco dominios. Los dominios se nombran mediante verbos que expresan el propósito clave y las áreas de actividad de los objetivos que los contienen:

- Los objetivos de gobierno se agrupan en el dominio **Evaluar, Dirigir y Monitorizar** (EDM en inglés). En este dominio, el órgano de gobierno evalúa las opciones estratégicas, guía a la alta gerencia con respecto a las opciones estratégicas elegidas y monitoriza el logro de la estrategia.
- Los objetivos de gestión se agrupan en cuatro dominios:
 - **Alinear, Planificar y Organizar** (APO) aborda la organización general, estrategia y actividades de apoyo para la información y la tecnología (I&T).
 - **Construir, Adquirir e Implementar** (BAI) se encarga de la definición, adquisición e implementación de soluciones y su integración en los procesos de negocio.
 - **Entregar, Dar Servicio y Soporte** (DSS) aborda la entrega operativa y el soporte de los servicios de información y tecnología (I&T), incluida la seguridad.
 - **Monitorizar, Evaluar y Valorar** (MEA) aborda la monitorización del rendimiento y la conformidad de I&T con los objetivos de rendimiento internos, los objetivos de control interno y los requisitos externos.

³ Algunas de estas guías de contenido de áreas prioritarias ya están preparándose; y otras están previstas. Esta serie de guías de áreas prioritarias es abierta y seguirá evolucionando. Para obtener la información más reciente sobre las publicaciones disponibles y previstas en la actualidad, así como otros contenidos, puede visitar www.isaca.org/cobit.



1.3.2 Componentes del sistema de gobierno

Para satisfacer los objetivos de gobierno y gestión, cada empresa necesita establecer, personalizar y sostener un sistema de gobierno creado a partir de una serie de componentes.

- Estos componentes son factores que, de forma individual y colectiva, contribuyen al buen funcionamiento del sistema de gobierno de la empresa en cuanto a I&T.
- Los componentes interactúan entre sí, lo que da lugar a un sistema de gobierno holístico de I&T.
- Los componentes pueden ser de diversos tipos. Los más comunes son los procesos. Sin embargo, los componentes de un sistema de gobierno incluyen también estructuras organizativas; políticas y procedimientos; elementos de información; cultura y comportamiento; habilidades y competencias; y servicios, infraestructura y aplicaciones (**figura 1.3**).
 - Los **Procesos** describen una serie de prácticas y actividades organizadas para lograr determinados objetivos y producir una serie de salidas que contribuyan a la consecución de la totalidad de los objetivos relacionados con las TI.
 - Las **Estructuras organizativas** son las entidades claves de toma de decisiones en una empresa.
 - Los **Principios, Políticas y Marcos de referencia** convierten el comportamiento deseado en una aplicación práctica para la gestión diaria.
 - La **Información** es generalizada a través de cualquier organización e incluye toda la información producida y utilizada por la empresa. COBIT se centra en la información requerida para el funcionamiento eficaz del sistema de gobierno de la empresa.

- La **Cultura, Ética y Comportamiento** de individuos y de la empresa son, a menudo, subestimados como un factor de éxito en las actividades de gobierno y gestión.
- Las **Personas, habilidades y competencias** son necesarias para tomar buenas decisiones, ejecutar medidas correctivas y completar satisfactoriamente todas las actividades.
- Los **Servicios, infraestructura y aplicaciones** incluyen la infraestructura, la tecnología y las aplicaciones que brindan a la empresa un sistema de gobierno para el procesamiento de I&T.

Figura 1.3—Componentes COBIT de un sistema de gobierno



Los componentes de cualquier tipo pueden ser genéricos o variantes de los componentes genéricos:

- Los componentes **Genéricos** se describen en el modelo core de COBIT (ver **figura 1.2**) y se aplican, en principio, a cualquier situación. Sin embargo, su naturaleza es genérica y suelen requerir una personalización antes de que se puedan implementar de forma práctica.
- Las **Variantes** se basan en componentes genéricos, pero se adaptan para un propósito o contexto específico dentro de un área prioritaria (p. ej.: para seguridad de la información, DevOps, una regulación específica).

1.3.3 Áreas prioritarias Un **área prioritaria** describe un determinado tema de gobierno, dominio o problema que puede ser abordado por una colección de objetivos de gobierno y gestión y sus componentes. Algunos de los ejemplos de áreas prioritarias incluye pequeñas y medianas empresas, ciberseguridad, transformación digital, computación en la nube, privacidad, y DevOps.⁴

El modelo core de COBIT es el objeto de esta publicación, y proporciona los componentes genéricos de gobierno. Las áreas prioritarias pueden incluir una combinación de componentes de gobierno genéricos y variantes en algunos componentes personalizados para el tópico de esa área prioritaria.

La cantidad de áreas prioritarias es prácticamente ilimitada. Esto hace que COBIT sea abierto. Se pueden añadir nuevas áreas prioritarias conforme sea necesario o conforme los expertos y especialistas en la materia contribuyan al modelo COBIT abierto.

Algunas de estas guías de contenido de áreas de prioritarias ya están preparándose; y otras están previstas. Para obtener la información más reciente sobre las publicaciones disponibles y previstas en la actualidad, así como otros contenidos, puede visitar www.isaca.org/cobit.

⁴ DevOps es un ejemplo tanto de una variante de componente como de un área prioritaria. ¿Por qué? DevOps es un tema de actualidad en el mercado y requiere indudablemente una directriz específica, lo que lo convierte en un área prioritaria. DevOps incluye una serie de objetivos de gobierno y gestión genéricos del modelo core de COBIT, junto con una serie de variantes de desarrollo, procesos relacionados con la operación y monitorización y las estructuras organizativas.

Capítulo 2

Estructura de esta publicación y público destinatario

2.1 Estructura de esta publicación

Esta publicación proporciona una descripción exhaustiva de los 40 objetivos de gobierno y gestión principales definidos en el modelo Core de COBIT (**figura 1.2**), los procesos incluidos en ella, otros componentes relacionados, y referencias a guías relacionadas, como otros estándares y marcos de referencia. En el Apéndice C se incluye una lista detallada de las fuentes de las referencias incluidas.

El resto de este documento contiene las secciones y apéndices:

- El Capítulo 3 explica la estructura que se utiliza para detallar la guía para los 40 objetivos de gobierno y gestión a través de los componentes.
- El Capítulo 4 proporciona una descripción exhaustiva de los 40 objetivos de gobierno y gestión principales definidos en el modelo core de COBIT (**figura 1.2**), los procesos incluidos en ella, otros componentes relacionados, y referencias a guías relacionadas, como otros estándares y marcos de referencia.
- Los apéndices incluyen más información sobre:
 - Las tablas de cruce en las que se basa la cascada de metas
 - Descripciones de estructuras organizativas
 - Lista de referencias fuente

2.2 Público destinatario

Esta guía se ha escrito para profesionales del mundo empresarial, incluidos personas del negocio, auditores, seguridad, gestión de riesgos, TI y otros profesionales que se beneficiarán de una guía detallada de los 40 objetivos de gobierno y gestión del modelo core de COBIT. Se requiere un cierto nivel de experiencia y conocimiento para adaptar COBIT a prácticas de gobierno personalizadas y prioritarias para la empresa.

Página dejada en blanco intencionadamente

Capítulo 3

Estructura de objetivos de gobierno y gestión de COBIT

3.1 Introducción

Este capítulo describe la estructura usada para detallar cada uno de los objetivos de gobierno y gestión de COBIT. Para cada objetivo de gobierno y gestión, el capítulo 4 de esta publicación proporciona información relacionada con cada uno de los **componentes de gobierno** aplicables a ese objetivo de gobierno o gestión:

- Proceso
- Estructura organizativa
- Flujos y elementos de información
- Personas, habilidades y competencias
- Políticas y procedimientos
- Cultura, ética y comportamiento
- Servicios, infraestructura y aplicaciones

La estructura de esta información se detalla en las secciones siguientes

3.2 Objetivos de gobierno y gestión

Como se ha explicado anteriormente, COBIT® 2019 incluye 40 objetivos de gobierno y gestión, organizados en cinco dominios (ver **figura 1.2**).

- Dominio de **Gobierno**
 - Evaluar, Dirigir y Monitorizar (EDM en inglés)
- Dominios de **Gestión**
 - Alinear, Planificar y Organizar (APO)
 - Construir, Adquirir e Implementar (BAI)
 - Entrega, Dar Servicio y Soporte (DSS)
 - Monitorizar, Evaluar y Valorar (MEA)

La información general detallada para cada objetivo (**figura 3.1**) incluye:

- Nombre del dominio
- Área prioritaria (en el caso de esta publicación, se trata del modelo core de COBIT)
- Nombre del objetivo de gobierno o gestión
- Descripción
- Declaración de propósito

Figura 3.1—Presentación de objetivos de gobierno y gestión

Dominio: <NOMBRE> Objetivo de gobierno/gestión: <NOMBRE>		Área prioritaria: <NOMBRE>
Descripción <TEXTO>		
Propósito <TEXTO>		

3.3 Cascada de metas

Cada objetivo de gobierno o gestión apoya el logro de metas de alineamiento que están relacionadas con metas empresariales más importantes (ver Sección 4.6 del *Marco de referencia COBIT® 2019: Introducción y metodología* para obtener más información y ver las tablas de cruce de la cascada de metas en el Apéndice A, a modo de ejemplo).

Las metas de alineamiento que tienen una vinculación primordial con el objetivo de gobierno o gestión en cuestión se enumeran en el margen derecho de la sección de guía detallada que cubre las metas (figura 3.2).

Figura 3.2—Presentación de metas empresariales y de alineamiento

El objetivo de gobierno/gestión respalda el logro de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales • <EG REF> <DESCRIPCIÓN DE METAS>	➔	Metas de alineamiento • <AG REF> <DESCRIPCIÓN DE METAS>

Las metas de alineamiento incluyen:

- AG01: Cumplimiento y soporte de I&T para el cumplimiento empresarial con las leyes y regulaciones externas
- AG02: Gestión de riesgo relacionado con I&T
- AG03: Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T
- AG04: Calidad de la información financiera relacionada con la tecnología
- AG05: Prestación de servicios de I&T conforme a los requisitos del negocio
- AG06: Agilidad para convertir los requisitos del negocio en soluciones operativas
- AG07: Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad
- AG08: Habilitar y dar soporte a procesos de negocio mediante la integración de aplicaciones y tecnología
- AG09: Ejecución de programas dentro del plazo, sin exceder el presupuesto, y que cumplen con los requisitos y estándares de calidad
- AG10: Calidad de la información sobre gestión de I&T
- AG11: Cumplimiento de I&T con las políticas internas
- AG12: Personal competente y motivado con un entendimiento mutuo de la tecnología y el negocio
- AG13: Conocimiento, experiencia e iniciativas para la innovación empresarial

Las metas empresariales que tienen una vinculación primaria con las metas de alineamiento enumeradas se incluyen en el margen izquierdo de la guía detallada del Capítulo 4 que cubre las metas. Las metas empresariales incluyen:

- EG01: Portafolio de productos y servicios competitivos
- EG02: Gestión de riesgo de negocio

- EG03: Cumplimiento con las leyes y regulaciones externas
- EG04: Calidad de la información financiera
- EG05: Cultura de servicio orientada al cliente
- EG06: Continuidad y disponibilidad del servicio del negocio
- EG07: Calidad de la información sobre gestión
- EG08: Optimización de la funcionalidad de procesos internos del negocio
- EG09: Optimización de costes de los procesos del negocio
- EG10: Habilidades, motivación y productividad del personal
- EG11: Cumplimiento de las políticas internas
- EG12: Gestión de programas de transformación digital
- EG13: Innovación de productos y negocios

En las tablas también se proporcionan métricas de ejemplo para metas empresariales y metas de alineamiento. (figura 3.3).

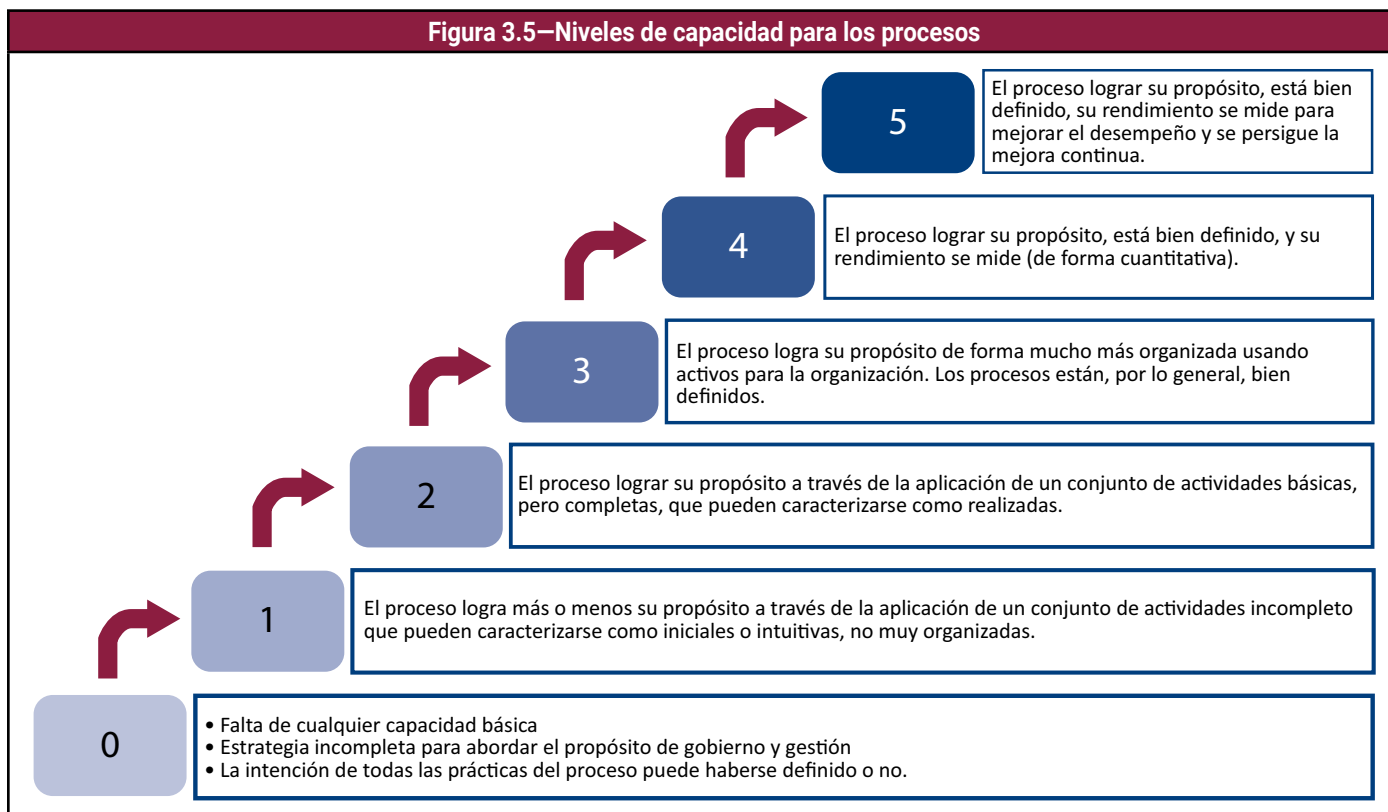
Figura 3.3—Presentación de metas aplicables y métricas modelo	
El objetivo de gobierno/gestión respalda el logro de una serie de metas empresariales y de alineamiento primordiales:	
Metas empresariales	Metas de alineamiento
<EG REF> <DESCRIPCIÓN DE METAS>	<AG REF> <DESCRIPCIÓN DE METAS>
Métricas modelo para metas empresariales	Métricas modelo para metas de alineamiento
<EG REF> • <MÉTRICA>	<AG REF> • <MÉTRICA>
<EG REF> • <MÉTRICA>	<AG REF> • <MÉTRICA>

3.4 Componente: Proceso

Cada objetivo de gobierno y gestión incluye varias prácticas de proceso. Cada proceso incluye una o más actividades. Cada práctica de proceso viene acompañada por un número limitado de métricas modelo para medir el logro de la práctica y su contribución al alcance del objetivo en su conjunto (figura 3.4).

Figura 3.4—Presentación del componente de procesos		
A. Componente: Proceso		
Práctica de gobierno/gestión	Métricas modelo	
<REF> <NOMBRE> <DESCRIPCIÓN>	<MÉTRICA>	
Actividades		Nivel de capacidad
1. <TEXT0>		<NR>
2. <TEXT0>		<NR>
n. <TEXT0>		<NR>
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
<NOMBRE DEL ESTÁNDAR>	<TEXT0>	
<NOMBRE DEL ESTÁNDAR>	<TEXT0>	

Se asigna un nivel de capacidad a todas las actividades del proceso, permitiendo una clara definición de los procesos con distintos niveles de capacidad. Un proceso alcanza un cierto nivel de capacidad siempre que todas las actividades de ese nivel se realicen de forma satisfactoria. COBIT® 2019 respalda la Integración del Modelo de Madurez de la Capacidad® (CMMI)-, basado en un esquema de capacidad de los procesos que va de 0 a 5. El nivel de capacidad es una medida de lo bien que un proceso se ha implementado y funciona. La **figura 3.5** muestra el modelo, los niveles de capacidad incrementales y las características generales de cada uno.



Ver el Capítulo 6 del *Marco de referencia COBIT® 2019: Introducción y metodología* para obtener más información acerca de la gestión del desempeño y la medición de la capacidad.

Cuando procede, también se han incorporado referencias a otros estándares y guías en esta sección (ver la **figura 3.4**). La Documentación relacionada menciona todos los estándares, marcos de referencia y requisitos de cumplimiento y otras guías relevantes para el proceso en cuestión. En las referencias específicas se mencionan capítulos o secciones específicas dentro de la Documentación relacionada. En el Apéndice C se incluye una lista completa de recursos para la Documentación relacionada.

Si no aparece una documentación relacionada para un componente determinado, significa que no se conocen referencias aplicables de las fuentes cruzada. Se promueve que la comunidad de profesionales sugiera las guías correspondientes.

3.5 Componente: Estructuras organizativas

El componente de gobierno de las estructuras organizativas sugiere niveles de responsabilidad y rendición de cuentas para las prácticas de los procesos (**figura 3.6**). Los cuadros incluyen roles individuales, así como estructuras organizativas, tanto del negocio como de TI.

Figura 3.6—Presentación del componente de estructuras organizativas

B. Componente: Estructuras organizativas								
	Estructura organizativa 1	Estructura organizativa 2	Estructura organizativa 3	Estructura organizativa 4	Estructura organizativa 5	Estructura organizativa 6	Estructura organizativa 7	Estructura organizativa 8, etc.
Práctica clave de gobierno/gestión								
<REF> <NOMBRE>								

Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
<NOMBRE DEL ESTÁNDAR>	<TEXTO>
<NOMBRE DEL ESTÁNDAR>	<TEXTO>

Se han definido los siguientes roles y estructuras organizativas dentro del contexto de COBIT® 2019:

- Consejo de Administración
- Comité Ejecutivo
- Director general ejecutivo (CEO)
- Director general financiero (CFO)
- Director de operaciones (COO)
- Director de riesgos (CRO)
- Director de TI (CIO)
- Director de tecnología (CTO)
- Director de tecnologías digitales (CDO)
- Consejo de gobierno de I&T
- Consejo de Arquitectura
- Comité de riesgos empresariales
- Director de seguridad de la información (CISO)
- Dueño del proceso de negocio
- Gestor de Portafolio
- Comité Estratégico (Programas/Proyectos)
- Gestor de programas
- Gestor de proyecto
- Oficina de gestión de proyectos
- Función de gestión de datos
- Director de recursos humanos
- Gestor de relaciones

- Jefe de arquitectura
- Jefe de desarrollo
- Jefe de operaciones de TI
- Jefe de administración de TI
- Gestor de servicios
- Gestor de seguridad de la información
- Gestor de continuidad del negocio
- Director de privacidad
- Asesor legal
- Cumplimiento
- Auditoría

En el Apéndice B se incluye una descripción detallada de estos roles y estructuras organizativas. Los distintos niveles de participación incluidos para estas estructuras pueden dividirse en niveles de responsabilidad y de rendición de cuentas.

- Los roles de **Responsable (R)** tienen la función operativa principal de completar la actividad y generar el resultado esperado. ¿Quién realiza la tarea? ¿Quién dirige la tarea?
- Los roles de **Quien rinde cuentas (A)** conllevan toda la rendición de cuentas. Como principio, el rol de quien rinde cuentas no se puede compartir. ¿Quién rinde cuentas por el éxito y la consecución de la tarea?

Cada dominio describe las estructuras organizativas que tienen la responsabilidad y/o rinden cuentas en dicho dominio. Se incluye una descripción detallada de cada rol y estructura organizativa. Se han omitido otras estructuras que no corresponden a responsables ni a quienes rinden cuentas para simplificar la lectura del cuadro.

Los profesionales pueden completar cuadros añadiendo dos niveles de participación para roles y estructuras organizativas. Visto que la atribución de los roles de consultado e informado depende del contexto y las prioridades organizativas, estos no se han incluido en esta guía detallada.

- Los roles de **Consultado (C)** proporcionan información para la actividad. ¿Quién está proporcionando información?
- Los roles de **Informado (I)** reciben información de los logros y/o entregables de la práctica. ¿Quién está recibiendo información?

Las empresas deberían revisar los niveles de responsable, quien rinde cuentas, consultado e informado y actualizar los roles y estructuras organizativas del cuadro conforme al contexto, prioridades y terminología preferida de la empresa.

Cuando procede, también se han incorporado referencias a otros estándares y guías en la sección de componentes de la estructura organizativa. La documentación relacionada menciona todas los estándares, marcos de referencia y requisitos de cumplimiento y otras guías relevantes para las estructuras organizativas en cuestión y sus niveles de participación en el proceso. En las referencias específicas se alude a capítulos o secciones específicas dentro de la documentación relacionada. En el Apéndice C se incluye una lista completa de fuentes.

3.6 Componente: Flujos y elementos de información

El tercer componente de gobierno proporciona una guía sobre los flujos y elementos de información vinculados con las prácticas de los procesos. Cada práctica incluye entradas y salidas, con indicaciones de origen y destino.

En general, cada salida se envía a un único destino o una serie limitada de destinos, por lo general, otra práctica de proceso de COBIT. Esa salida se convierte entonces en entrada para su destino ((**figura 3.7**).

Figura 3.7—Presentación del componente flujos y elementos de información

C. Componente: Flujos y elementos de información				
Práctica de gobierno/gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
<REF> <NOMBRE>	<REF>	<TEXTO>	<TEXTO>	<REF>

Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
<NOMBRE DEL ESTÁNDAR>	<TEXTO>
<NOMBRE DEL ESTÁNDAR>	<TEXTO>

Sin embargo, algunas salidas tienen muchos destinos (p. ej. todos los procesos de COBIT o todos los procesos dentro de un dominio). Para facilitar la lectura, estas salidas no se han relacionado como entradas en los procesos objetivo. En la **figura 3.8** se incluye una lista completa de dichas salidas.

Para algunas entradas/salidas, se menciona «interno» como destino si la entrada y la salida se comparten entre actividades dentro del mismo proceso.

Figura 3.8—Salidas a múltiples procesos

Salidas a todos los procesos		
De la Práctica clave	Descripción de la salida	Destino
AP013.02	Plan de tratamiento del riesgo de seguridad de la información	Todos los EDM, todos los APO; todos los BAI, todos los DSS; todos los MEA
De la Práctica de gobierno	Descripción de la salida	Destino
EDM01.01	Principios rectores del gobierno empresarial	Todos los EDM
EDM01.01	Modelo de toma de decisiones	Todos los EDM
EDM01.02	Comunicación del gobierno de la empresa	Todos los EDM
EDM01.01	Niveles de autoridad	Todos los EDM
EDM01.03	Retroalimentación sobre la eficacia y el rendimiento del gobierno	Todos los EDM
Salidas a todos los procesos de gestión		
De la Práctica de gestión	Descripción de la salida	Destino
AP001.01	Diseño del sistema de gestión	Todos los APO; todos los BAI; todos los DSS; todos los MEA
AP001.01	Objetivos prioritarios del gobierno y la gestión	Todos los APO; todos los BAI; todos los DSS; todos los MEA
AP001.02	Comunicación de los objetivos de I&T	Todos los APO; todos los BAI; todos los DSS; todos los MEA
AP001.02	Reglas básicas de comunicación	Todos los APO; todos los BAI; todos los DSS; todos los MEA
AP001.03	Análisis de la brecha del modelo objetivo	Todos los APO; todos los BAI; todos los DSS; todos los MEA
AP001.11	Oportunidades de mejora del proceso	Todos los APO; todos los BAI; todos los DSS; todos los MEA
AP002.05	Estrategia y objetivos de I&T	Todos los APO; todos los BAI; todos los DSS; todos los MEA
AP002.06	Paquete de comunicación	Todos los APO; todos los BAI; todos los DSS; todos los MEA
AP011.03	Estándares de gestión de calidad	Todos los APO; todos los BAI; todos los DSS; todos los MEA
AP011.04	Calidad del proceso de las metas y métricas del servicio	Todos los APO; todos los BAI; todos los DSS; todos los MEA
AP011.05	Comunicaciones sobre mejora continua y mejores prácticas	Todos los APO; todos los BAI; todos los DSS; todos los MEA
AP011.05	Ejemplos de buenas prácticas a compartir	Todos los APO; todos los BAI; todos los DSS; todos los MEA
AP011.05	Resultados del benchmark de revisión de calidad	Todos los APO; todos los BAI; todos los DSS; todos los MEA

Figura 3.8—Salidas a múltiples procesos (continuación)

Salidas a todos los procesos de gestión		
De la Práctica de gestión	Descripción de la salida	Destino
MEA01.02	Objetivos de monitorización	Todos los APO; todos los BAI; todos los DSS; todos los MEA
MEA01.04	Informes de desempeño	Todos los APO; todos los BAI; todos los DSS; todos los MEA
MEA01.05	Acciones y tareas de remediación	Todos los APO; todos los BAI; todos los DSS; todos los MEA
MEA02.01	Resultados de la revisión y monitorización del control interno	Todos los APO; todos los BAI; todos los DSS; todos los MEA
MEA02.01	Resultados del benchmarking y otras evaluaciones	Todos los APO; todos los BAI; todos los DSS; todos los MEA
MEA02.03	Resultados de las revisiones de las autoevaluaciones	Todos los APO; todos los BAI; todos los DSS; todos los MEA
MEA02.03	Planes y criterios de autoevaluación	Todos los APO; todos los BAI; todos los DSS; todos los MEA
MEA02.04	Deficiencias del control	Todos los APO; todos los BAI; todos los DSS; todos los MEA
MEA02.04	Acciones remediales	Todos los APO; todos los BAI; todos los DSS; todos los MEA
MEA03.02	Comunicación de cambios en los requisitos de cumplimiento	Todos los APO; todos los BAI; todos los DSS; todos los MEA
MEA04.02	Planes de aseguramiento	Todos los APO; todos los BAI; todos los DSS; todos los MEA
MEA04.08	Informes de revisión de aseguramiento	Todos los APO; todos los BAI; todos los DSS; todos los MEA
MEA04.08	Resultados de la revisión de aseguramiento	Todos los APO; todos los BAI; todos los DSS; todos los MEA
MEA04.09	Acciones remediales	Todos los APO; todos los BAI; todos los DSS; todos los MEA

Cuando procede, se han incorporado referencias a otros estándares y guías en el componente de flujos y elementos de información. En la documentación relacionada se alude a todos los estándares, marcos de referencia y requisitos de cumplimiento y otras guías relevantes para el elemento de información en cuestión. En las referencias detalladas se alude a capítulos o secciones específicas dentro de la documentación relacionada. En el Apéndice C se incluye una lista completa de fuentes.

3.7 Componente: Personas, habilidades y competencias El componente de gobierno de personas, habilidades y competencias identifica los recursos humanos y las habilidades requeridas para alcanzar el objetivo de gobierno o gestión. COBIT® 2019 basó esta guía en el marco Skills Framework for the Information Age (SFIA®) V6 (versión 6).⁵ Todas las habilidades enumeradas se describen detalladamente en el marco de referencia SFIA. La referencia específica proporciona un código único que corresponde con la guía SFIA de la habilidad (**figura 3.9**). Además, se incluyen referencias para varios objetivos de gobierno y gestión en el *e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework*⁶ y «Core Principles for the Professional Practice of Internal Auditing» del Institute of Internal Auditors.⁷

Figura 3.9—Presentación del componente de personas, habilidades y competencias

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
<NOMBRE>	Skills Framework for the Information Age, V6 (SFIA 6), 2015	<CÓDIGO SFIA>
<NOMBRE>	Skills Framework for the Information Age, V6 (SFIA 6), 2015	<CÓDIGO SFIA>

⁵ SFIA Foundation, “SFIA V6, the sixth major version of the Skills Framework for the Information Age,” <https://www.sfia-online.org/en/framework/sfia-6>

⁶ Comité europeo de normalización (CEN), e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework, EN 16234-1:2016, https://standards.cen.eu/dyn/www/f?p=204:110:0:::FSP_PROJECT:41798&cs=13E00999DD92E702F0E171397CF76EC87

⁷ The Institute of Internal Auditors® (IIA®), “Core Principles for the Professional Practice of Internal Auditing,” <https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Core-Principles-for-the-Professional-Practice-of-Internal-Auditing.aspx>

3.8 Componente: Políticas y procedimientos

Este componente proporciona una guía detallada de las políticas y procedimientos relevantes para el objetivo de gobierno y gestión. Se incluye el nombre de políticas y procedimientos relevantes, con una descripción del propósito y contenido de la política (**figura 3.10**).

Cuando procede, también se han incorporado referencias a otros estándares y guías. En la documentación relacionada se alude a capítulos o secciones específicas dentro de la documentación relacionada donde puede consultarse más información. En el Apéndice C se incluye una lista completa de fuentes.

Figura 3.10—Presentación del componente de políticas y procedimientos			
E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
<NOMBRE>	<DESCRIPCIÓN>	<NOMBRE DEL ESTÁNDAR>	<TEXTO>

3.9 Componente: Cultura, ética y comportamiento

El componente de gobierno de cultura, ética y comportamiento proporciona una guía detallada sobre los elementos culturales deseados dentro de la organización que respaldan la consecución de un objetivo de gobierno o gestión (**figura 3.11**). Cuando procede, también se han incorporado referencias a otros estándares y guías. En la documentación relacionada se alude a capítulos o secciones específicas dentro de la documentación relacionada donde puede consultarse más información. En el Apéndice C se incluye una lista completa de fuentes.

Figura 3.11—Presentación del componente de cultura, ética y comportamiento		
F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
<NOMBRE>	<NOMBRE DEL ESTÁNDAR>	<TEXTO>

3.10 Componente: Servicios, infraestructura y aplicaciones

El componente de gobierno de servicios, infraestructura y aplicaciones proporciona una guía detallada sobre los servicios, tipos de infraestructura y categorías de aplicaciones de terceros que pueden utilizarse para respaldar la consecución de un objetivo de gobierno o gestión. La guía es genérica (para evitar nombrar a proveedores o productos concretos); sin embargo, las entradas proporcionan una orientación para que las empresas construyan su sistema de gobierno para I&T (**figura 3.12**).

Figura 3.12—Presentación del componente de servicios, infraestructura y aplicaciones	
G. Componente: Servicios, infraestructura y aplicaciones	
<CATEGORÍA DE SERVICIOS, INFRAESTRUCTURA O APLICACIONES>	

Página dejada en blanco intencionadamente

Capítulo 4

Objetivos de gobierno y gestión de COBIT: Guía detallada

Modelo Core de COBIT

4.1 EVALUAR, DIRIGIR Y MONITORIZAR (EDM)

- 01 Asegurar el establecimiento y el mantenimiento del marco de gobierno
- 02 Asegurar la obtención de beneficios
- 03 Asegurar la optimización del riesgo
- 04 Asegurar la optimización de los recursos
- 05 Asegurar el compromiso de las partes interesadas

Página dejada en blanco intencionadamente

Dominio: Evaluar, Dirigir y Monitorizar Objetivo de gobierno: EDM01 – Asegurar el establecimiento y el mantenimiento del marco de gobierno		Área prioritaria: Modelo Core de COBIT
Descripción		
Analizar y articular los requisitos para el gobierno de la I&T de la empresa. Establecer y mantener componentes de gobierno claros con respecto a la autoridad y las responsabilidades para lograr la misión, las metas y los objetivos de la empresa.		
Propósito		
Proporcionar un enfoque consistente integrado y alineado con el enfoque de gobierno de la empresa. Las decisiones relacionadas con I&T deben hacerse en línea con las estrategias y objetivos de la empresa y para alcanzar el valor deseado. En este sentido, debe asegurarse de que los procesos relacionados con la I&T se supervisen de forma eficaz y transparente; que se cumpla con los requisitos legales, contractuales y regulatorios; y que se cumplan los requisitos de gobierno para los miembros del consejo de dirección.		
El objetivo de gobierno respalda el logro de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales		Metas de alineamiento
<ul style="list-style-type: none"> • EG03 Cumplimiento de leyes y regulaciones externas • EG08 Optimización de la funcionalidad de procesos internos del negocio • EG12 Gestión de programas de transformación digital 		<ul style="list-style-type: none"> • AG01 Cumplimiento y soporte de I&T para el cumplimiento empresarial con las leyes y regulaciones externas • AG03 Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG03 a. Coste de incumplimiento regulatorio, incluidos acuerdos y multas b. Número de problemas de incumplimiento regulatorio que causan comentarios públicos o publicidad negativa c. Número de problemas de incumplimiento señalados por los reguladores d. Número de problemas de incumplimiento regulatorio en relación con acuerdos contractuales con socios de negocio		AG01 a. Coste de incumplimiento de TI, incluidos acuerdos y multas, y el impacto de la pérdida reputacional b. Número de problemas de incumplimiento relacionados con la TI notificados al consejo de administración o que causan comentarios o vergüenza pública c. Número de problemas de incumplimiento relacionados acuerdos contractuales con los proveedores de servicios de TI
EG08 a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso del negocio b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores externos con las capacidades de la cadena de suministro		AG03 a. Porcentaje de inversiones posibilitadas por la I&T en las que los beneficios previstos se cumplen o exceden b. Porcentaje de servicios de I&T para los que se han logrado los beneficios esperados (indicados en los acuerdos de nivel de servicio)
EG12 a. Número de programas ejecutados a tiempo y dentro del presupuesto b. Porcentaje de partes interesadas satisfechas con la ejecución del programa c. Porcentaje de programas de transformación del negocio suspendidos d. Porcentaje de programas de transformación del negocio con actualizaciones de estado informadas regularmente		

A. Componente: Proceso		
Práctica de gobierno	Métricas modelo	
EDM01.01 Evaluar el sistema de gobierno Identificar e involucrarse continuamente con las partes interesadas de la empresa, documentar una comprensión de los requisitos y evaluar el diseño actual y futuro del gobierno de I&T empresarial.	a. Número de principios guía definidos para el gobierno y la toma de decisiones de I&T b. Número de altos ejecutivos implicados en establecer el rumbo del gobierno para I&T	
Actividades	Nivel de capacidad	
1. Analizar e identificar los factores ambientales internos y externos (obligaciones legales, regulatorias y contractuales), así como las tendencias en el entorno de negocio que pueden influir en el diseño del gobierno.	2	
2. Determinar la importancia de I&T y su papel con respecto al negocio.		
3. Considerar las regulaciones, leyes, y obligaciones contractuales externas y determinar cómo deberían aplicarse dentro del gobierno de I&T de una empresa.		
4. Determinar las implicaciones de todo el entorno de control de la empresa con respecto a I&T.		
5. Alinear el uso ético y el procesamiento de la información y su impacto en la sociedad, el entorno natural y los intereses de los interesados internos y externos con la dirección, las metas y los objetivos de la empresa.	3	
6. Articular los principios que guiarán el diseño del gobierno y la toma de decisiones de I&T.		
7. Determinar el modelo óptimo de toma de decisiones para I&T.		
8. Determinar los niveles adecuados de delegación de autoridad, incluidas las reglas de limitaciones, para las decisiones de I&T.		

A. Componente: Proceso (cont.)		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		GE.AG Apply Governance System; GE.MG Monitor Governance System
ISO/IEC 38500:2015(E)		5.2 Principle 1: Responsibility (Evaluate)
ITIL V3, 2011		Service Strategy, 2.3 Governance and management systems
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018		3.1 Preparation (Tasks 2, 3, 4, 5)
Práctica de gobierno		Métricas modelo
EDM01.02 Dirigir el sistema de gobierno. Informar a los líderes sobre los principios de gobierno de I&T y obtener su apoyo, aprobación y compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de I&T en línea con los principios de gobierno, los modelos de toma de decisiones y los niveles de autoridad acordados. Definir la información requerida para la toma de decisiones informada.		a. Grado en el cual los principios de gobierno de I&T acordados son evidentes en procesos y prácticas (porcentaje de procesos y prácticas que se atribuyen a los principios) b. Frecuencia de presentación de informes del gobierno de I&T al comité ejecutivo y el consejo de administración c. Número de roles, responsabilidades y autoridades para el gobierno de I&T que son definidos, asignados y aceptados por los directivos de negocio e I&T correspondientes.
Actividades		Nivel de capacidad
1. Comunicar el gobierno de los principios de I&T y acordar con la administración ejecutiva la forma de establecer un liderazgo informado y comprometido.		2
2. Establecer o delegar el establecimiento de estructuras, procesos y prácticas de gobierno en línea con los principios de diseño acordados.		
3. Establecer un consejo de administración de gobierno de I&T (o equivalente) a nivel del consejo de administración. Este consejo de administración debería garantizar que el gobierno de la información y la tecnología, como parte del gobierno de la empresa, se aborda de forma adecuada; aconsejar sobre la dirección estratégica a seguir; y determinar la priorización de los programas de inversión habilitados por I&T en línea con la estrategia y prioridades del negocio de la empresa.		
4. Asignar la responsabilidad, autoridad y rendición de cuentas por las decisiones de I&T en línea con los principios de diseño de gobierno, de los modelos de toma de decisiones y de delegación acordados.		3
5. Asegurar que los mecanismos de comunicación y presentación de informes proporcionan la información adecuada a los responsables de la supervisión y toma de decisiones.		
6. Direccionar al personal para que siga las directrices relevantes en cuanto al comportamiento ético y profesional y asegurar que se conozcan y se apliquen las consecuencias del incumplimiento.		
7. Direccionar el establecimiento de un sistema de recompensas para fomentar el cambio cultural deseado.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		GE.DG Direct Governance System
ISF, The Standard of Good Practice for Information Security 2016		SG1.1 Security Governance Framework
ISO/IEC 38500:2015(E)		5.2 Principle 1: Responsibility (Direct)
ISO/IEC 38502:2017(E)		Governance of IT - Framework and model (all chapters)
King IV Report on Corporate Governance for South Africa, 2016		Part 5.4: Governance functional areas - Principle 12
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.14 Planning (PL-2, PL-10)
Práctica de gobierno		Métricas modelo
EDM01.03 Monitorizar el sistema de gobierno Monitorizar la eficacia y el rendimiento del gobierno de I&T de la empresa. Evaluar si el sistema de gobierno y los mecanismos implementados (incluyendo las estructuras, los principios y los procesos) están operando de forma efectiva y ofrecen una supervisión apropiada de I&T para permitir la creación de valor.		a. Ciclo de vida real vs. objetivo para decisiones clave b. Frecuencia de revisiones independientes del gobierno de I&T c. Nivel de satisfacción de la parte interesada (medido a partir de encuestas) d. Número de problemas de gobierno de I&T comunicados

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Evaluar la eficacia y el rendimiento de aquellas partes interesadas a las que se le ha delegado la responsabilidad y autoridad para el gobierno empresarial de I&T.	3
2. Evaluar de forma periódica si los mecanismos de I&T que se han acordado (estructuras, principios, procesos, etc.) se han establecido y operan de forma eficiente.	4
3. Evaluar la eficacia del diseño de gobierno e identificar acciones para rectificar cualquier desviación que se encuentre.	
4. Mantener la supervisión de hasta qué punto la I&T satisface las obligaciones (regulación, legislación, leyes comunes, contractuales), políticas internas, estándares y guías profesionales.	
5. Proporcionar la supervisión de la eficacia del sistema de control de la empresa y el cumplimiento con el mismo.	
6. Monitorizar los mecanismos regulares y rutinarios para garantizar que el uso de I&T cumpla con las obligaciones (regulación, legislación, leyes comunes, contractuales), estándares y guías.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
ISO/IEC 38500:2015(E)	5.2 Principle 1: Responsibility (Monitor)
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.14 Planning (PL-11)

B. Componente: Estructuras organizativas					
Práctica clave de gobierno					
EDM01.01 Evaluar el sistema de gobierno.	A	R	R	R	R
EDM01.02 Dirigir el sistema de gobierno.	A	R			R
EDM01.03 Monitorizar el sistema de gobierno.	A	R	R	R	R
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica				
COSO Enterprise Risk Management, junio de 2017	6. Governance and Culture—Principle 2				
ISO/IEC 38502:2017(E)	5.1 Responsibilities of the governing body				
King IV Report on Corporate Governance for South Africa, 2016	Part 2: Fundamental concepts—Definition of corporate governance; Part 5.3: Governing structures and delegation—Principle 6 & 7				

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gobierno	Entradas		Salidas	
EDM01.01 Evaluar el sistema de gobierno	De	Descripción	Descripción	A
	MEA03.02	Comunicaciones de requisito de cambios en el cumplimiento	Principios rectores del gobierno empresarial	Todos los EDM; APO01.01; APO01.03 APO01.04
	Fuera de COBIT	<ul style="list-style-type: none">• Constitución/ reglamentos/estatutos de la organización• Modelo de gobierno/toma de decisiones• Leyes/regulaciones• Tendencias del entorno empresarial	<div>Modelo de toma de decisiones</div> <div>Niveles de autoridad</div>	<div>Todos los EDM; APO01.04</div> <div>Todos los EDM; APO01.05</div>
EDM01.02 Dirigir el sistema de gobierno.			Comunicación del gobierno de la empresa	Todos los EDM; APO01.02
			Método de sistema de recompensa	APO07.03; APO07.04
EDM01.03 Monitorizar el sistema de gobierno.	MEA01.04	Informes de desempeño	Retroalimentación sobre el rendimiento y la eficacia del gobierno	Todos los EDM; APO01.11
	MEA01.05	Estado y resultados de las acciones		
	MEA02.01	<ul style="list-style-type: none">• Resultados de la supervisión y revisión del control interno• Resultados del benchmarking y otras evaluaciones		
	MEA02.03	Resultados de las revisiones de las autoevaluaciones		
	MEA03.03	Confirmaciones de cumplimiento		
	MEA03.04	<ul style="list-style-type: none">• Informes de aseguramiento del cumplimiento• Informes de los problemas y causa raíz del incumplimiento		
	MEA04.02	Planes de aseguramiento		
	Fuera de COBIT	<ul style="list-style-type: none">• Informes de auditoría• Obligaciones		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
National Institute of Standards and Technology Special Publication 800-37, Revisión 2, septiembre de 2017		3.1 Preparation (Task 2, 3, 4, 5): Inputs and Outputs		

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gobierno de SI	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.9. IS Governance
Gobierno de TI	Skills Framework for the Information Age V6, 2015	GOVN

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de Delegación de Autoridad	Especifica la autoridad que el consejo de administración estrictamente conserva para sí. Enumera los principios generales de la delegación de autoridad y la planificación de la delegación (incluidos límites claros). Define las estructuras organizativas a las cuales el consejo de administración delega la autoridad.	(1) ISO/IEC 38500:2015(E); (2) ISO/IEC 38502:2017(E); (3) King IV Report on Corporate Governance for South Africa, 2016	(1) 5.2 Principle 1: Responsibility; (2) 5.3 Delegation; (3) Part 5.3: Governing structures and delegation Principle—8 and 10
Política de gobierno	Proporciona los principios rectores de gobierno (p. ej., el gobierno de I&T es crítico para el éxito empresarial; I&T y el negocio se alinean estratégicamente; los requisitos y beneficios empresariales determinan las prioridades; la aplicación debe ser equitativa, oportuna y consistente; las mejores prácticas, marcos de referencia y estándares de la industria deben evaluarse e implementarse como corresponda). Incluye imperativos de gobierno, como construir confianza y alianzas, para tener éxito. Enfatiza que el gobierno de I&T refleja un proceso de mejora continua y debe personalizarse, mantenerse y actualizarse para asegurar su relevancia.	National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.14 Planning (PL-1)

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Identificar y comunicar la cultura de toma de decisiones, la ética organizativa y comportamientos individuales que encarnan los valores de la empresa. Demostrar el liderazgo ético y marcar la actitud de la alta gerencia.	(1) National Institute of Standards and Technology Special Publication 800-53, Revisión 5, agosto de 2017; (2) ISO/IEC 38500:2015(E); (3) King IV Report on Corporate Governance for South Africa, 2016	(1) 3.14 Planning (PL-4); (2) 4.1 Principles; (3) Part 5.1: Leadership, ethics and corporate citizenship - Principle 2

G. Componente: Servicios, infraestructura y aplicaciones
<ul style="list-style-type: none"> • COBIT y productos/herramientas relacionados • Marcos y estándares equivalentes

Página dejada en blanco intencionadamente

Dominio: Evaluar, Dirigir y Monitorizar Objetivo de gobierno: EDM02 – Asegurar la obtención de beneficios		Área prioritaria: Modelo Core de COBIT
Descripción		
Optimizar el valor al negocio de las inversiones en procesos empresariales, servicios de I&T y activos de I&T.		
Propósito		
Asegurar un valor óptimo de las iniciativas, servicios y activos habilitados para I&T; la entrega rentable de soluciones y servicios; y una imagen confiable y precisa de los costes y beneficios probables para que las necesidades empresariales se satisfagan de forma eficaz y eficiente.		
El objetivo de gobierno respalda el logro de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales <ul style="list-style-type: none"> • EG08 Optimización de la funcionalidad de procesos internos del negocio • EG12 Gestión de programas de transformación digital 		Metas de alineamiento <ul style="list-style-type: none"> • AG03 Beneficios obtenidos del portafolio de inversiones y servicios habilitados por I&T
Métricas modelo para metas empresariales EG08 <ul style="list-style-type: none"> a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarial b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores externos con las capacidades de la cadena de suministro EG12 <ul style="list-style-type: none"> a. Número de programas ejecutados a tiempo y dentro del presupuesto b. Porcentaje de partes interesadas satisfechas con la ejecución del programa c. Porcentaje de programas de transformación del negocio suspendidos d. Porcentaje de programas de transformación del negocio con actualizaciones del estado notificado regularmente 		Métricas modelo para metas de alineamiento AG03 <ul style="list-style-type: none"> a. Porcentaje de inversiones posibilitadas por I&T en las que los beneficios previstos en el caso de negocio se cumplen o exceden b. Porcentaje de servicios de I&T para los que se han logrado los beneficios esperados (indicados en los acuerdos de nivel de servicio)

A. Componente: Proceso		
Práctica de gobierno	Métricas modelo	
EDM02.01 Establecer el objetivo de la mezcla de inversión. Revisar y asegurarse que las estrategias y los servicios actuales de la empresa y de I&T sean claros. Definir una mezcla de inversión apropiada basada en el coste, la alineación con la estrategia, el tipo de beneficio de los programas en el portafolio, el grado de riesgo y las medidas financieras como el coste y el retorno de la inversión (ROI) esperado durante todo el ciclo de vida económico. Ajustar las estrategias empresariales y de I&T cuando sea necesario.	a. Porcentaje de inversiones de I&T que se atribuyen a la estrategia empresarial b. Porcentaje de inversiones de I&T basadas en el coste, la alineación con la estrategia, y las medidas financieras (p. ej., el coste y el ROI durante todo el ciclo de vida económico), el grado de riesgo y el tipo de beneficio para los programas del portafolio.	
Actividades		Nivel de capacidad
1. Crear y mantener portafolios de programas de inversión habilitados por I&T, servicios y activos de TI, que forman la base para el presupuesto actual de TI y respaldan los planes tácticos y estratégicos de I&T.		2
2. Obtiene un conocimiento común entre TI y otras funciones empresariales sobre las posibles oportunidades para que TI habilite y contribuya a la estrategia empresarial.		
3. Identificar las categorías generales de sistemas de información, aplicaciones, datos, servicios de TI, infraestructura, activos de I&T, recursos, habilidades, prácticas, controles y relaciones de TI necesarias para respaldar la estrategia empresarial.		
4. Acordar las metas de I&T, tener en cuenta las interrelaciones entre la estrategia de la empresa y los servicios de I&T, activos y otros recursos.. Identificar y aprovechar las sinergias que pueden lograrse.		
5. Definir una mezcla de inversión que logre el equilibrio adecuado entre distintas dimensiones, incluido un equilibrio adecuado de resultados a corto y largo plazo, beneficios financieros y no financieros e inversiones de alto y bajo riesgo.		3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
King IV Report on Corporate Governance for South Africa, 2016	Parte 5.5: Stakeholder relationships—Principle 17	
The Open Group IT4IT Reference Architecture, Versión 2.0	3.2 IT Value Chain and IT4IT Reference Architecture	

A. Componente: Proceso (cont.)		
Práctica de gobierno		Métricas modelo
EDM02.02 Evaluar la optimización del valor. Evaluar continuamente el portafolio de inversiones, servicios y activos de I&T con el fin de determinar la probabilidad de alcanzar los objetivos de la empresa y proporcionar un valor. Identificar y evaluar cualquier cambio en la dirección que debe ofrecerse a la gerencia para optimizar la creación de valor.		a. Desviación entre la mezcla de inversión objetivo y real b. Porcentaje de portafolio de inversiones habilitadas por I&T con el fin de determinar la probabilidad de alcanzar los objetivos de la empresa y proporcionar un valor a un coste razonable.
Actividades		Nivel de capacidad
1. Conocer los requisitos de las partes interesadas; los problemas estratégicos de I&T; así como la dependencia en I&T; y la percepción y capacidades de tecnología con respecto a la importancia real y potencial de I&T para la estrategia empresarial.		2
2. Conocer los elementos clave de gobierno para ofrecer de forma confiable, segura y económica un valor óptimo procedente del uso de servicios, activos y recursos de I&T actuales y nuevos.		3
3. Entender y discutir regularmente las oportunidades que podrían surgir para la empresa derivadas de los cambios habilitados por las tecnologías actuales, nuevas o emergentes, y optimizar el valor creado a partir de esas oportunidades.		
4. Conocer lo que constituye valor para la empresa y considerar lo bien que se comunica, conoce y aplica en todos los procesos de la empresa.		
5. Evaluar la eficacia con la que las estrategias empresariales y de I&T se han integrado y alineado dentro de la empresa y con los objetivos de la empresa para entregar valor.		4
6. Conocer y considerar la eficacia de los roles, responsabilidades, rendición de cuentas y órganos de toma de decisiones actuales a la hora de asegurar la creación de valor a partir de las inversiones, servicios y activos de I&T.		
7. Considere lo bien que está alineada la gestión de las inversiones, servicios y activos de I&T con la gestión de valor empresarial y las prácticas de gestión financiera.		
8. Evaluar el portafolio de inversiones, servicios y activos para su alineación con los objetivos estratégicos de la empresa; el valor de la empresa, tanto financiera como no financiera; el riesgo, tanto el riesgo de entrega como el riesgo de beneficios; el alineamiento del proceso de negocio; la eficacia en términos de usabilidad, disponibilidad y capacidad de respuesta; y la eficiencia en cuanto a costes, redundancia y salud técnica.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
COSO Enterprise Risk Management, junio de 2017		7. Strategy and Objective-Setting—Principle 8
ISF, The Standard of Good Practice for Information Security 2016		SG2.2 Stakeholder Value Delivery
ISO/IEC 38500:2015(E)		5.3 Principle 2: Strategy (Evaluate)
King IV Report on Corporate Governance for South Africa, 2016		Part 5.2: Strategy, performance and reporting—Principle 4
The Open Group IT4IT Reference Architecture, Versión 2.0		5. Strategy to Portfolio (S2P) Value Stream
Práctica de gobierno		Métricas modelo
EDM02.03 Dirigir la optimización del valor. Dirigir los principios y las prácticas de gestión de valor para permitir la obtención óptima de valor de las inversiones de I&T durante todo su ciclo de vida económico.		a. Porcentaje de iniciativas de I&T en el portafolio general donde el valor se administra durante todo el ciclo de vida b. Porcentaje de iniciativas de I&T que usan principios y prácticas de gestión de valor
Actividades		Nivel de capacidad
1. Definir y comunicar los tipos, categorías, criterios y peso relativo al criterio de portafolio e inversiones que permitan puntajes de valor relativo total.		2
2. Definir los requisitos para los cambios de fase (stage-gate) y otras revisiones para ver el peso de la inversión para la empresa y el riesgo asociado, las planificaciones del programa, los planes de financiación y la entrega de capacidades y beneficios y contribución continua al valor.		3
3. Dirigir a la gestión para que considere los potenciales usos innovadores de I&T que permiten a la empresa responder a nuevas oportunidades y retos, emprender nuevos negocios, aumentar la competitividad o mejorar los procesos.		
4. Dirigir cualquier cambio requerido en la asignación de rendición de cuentas y responsabilidades para ejecutar el portafolio de inversiones y entrega de valor por parte de los procesos y servicios empresariales.		
5. Dirigir cualquier cambio requerido al portafolio de inversiones y servicios para realinearse con los objetivos y/o limitaciones empresariales actuales y esperadas.		4
6. Recomendar la consideración de innovaciones, cambios organizativos o mejoras operativas posibles que podrían generar un mayor valor para la empresa a partir de iniciativas de I&T.		
7. Definir y comunicar las metas y medidas de resultados de la entrega de valor a nivel de empresa para permitir una supervisión eficaz.		

A. Componente: Proceso (cont.)	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
ISO/IEC 38500:2015(E)	5.3 Principle 2: Strategy (Direct)
Práctica de gobierno	Métricas modelo
EDM02.04 Monitorizar la optimización del valor. Supervisar las metas y métricas clave para determinar si el negocio está recibiendo el valor y los beneficios esperados para el negocio a través de las inversiones y los servicios de I&T. Identificar los problemas significativos y considerar acciones correctivas	a. Número de nuevas oportunidades empresariales logradas como resultado directo de los desarrollos de I&T b. Porcentaje de objetivos empresariales estratégicos obtenidos como resultado de iniciativas estratégicas de I&T c. Nivel de satisfacción de la dirección ejecutiva con el coste y la entrega de valor de I&T d. Nivel de satisfacción de las partes interesadas con el avance hacia las metas identificadas (entrega de valor basada en encuestas). e. Nivel de satisfacción de las partes interesadas con la capacidad de la empresa para obtener valor de las iniciativas habilitadas por I&T f. Número de incidentes que tienen lugar debido a la evasión actual o intentada de los principios y prácticas de gestión de valor establecidos g. Porcentaje logrado del valor esperado
Actividades	Nivel de capacidad
1. Definir un conjunto equilibrado de objetivos, métricas, metas y benchmarks. Las métricas deberían cubrir mediciones de actividad y resultados, incluyendo indicadores de avance y de retraso, así como un equilibrio adecuado entre mediciones financieras y no financieras. Revisar y acordar con TI y otras funciones de la empresa, así como con otras partes interesadas relevantes.	4
2. Recopilar datos relevantes, oportunos, completos, creíbles y precisos para informar sobre el progreso a la hora de la entrega de valor en comparación con los objetivos. Obtener una vista resumen general de 360° del rendimiento del portafolio, programa y de I&T (capacidades técnicas y operativas) que respalden la toma de decisiones. Asegurar el logro de los resultados esperados.	
3. Obtener informes regulares y relevantes de rendimiento del portafolio, programa y de I&T (tecnológicos y funcionales). Revisar el progreso de la empresa a la hora de identificar metas y el grado de realización de los objetivos planificados, los entregables obtenidos, los objetivos de desempeño alcanzados y el riesgo mitigado.	
4. Una vez revisados los informes, asegurar que se ha iniciado y controlado acciones correctivas al área de gestión pertinente.	5
5. Una vez revisados los informes, llevar a cabo la acción de gestión adecuada para asegurar la optimización del valor.	
Documentación relacionada (Estándares Marcos, Requisitos de cumplimiento)	Referencia específica
ISO/IEC 38500:2015(E)	5.3 Principle 2: Strategy (Monitor)

B. Componente: Estructuras organizativas									
Práctica clave de gobierno	Consejo de Administración	Comité Ejecutivo	Director general ejecutivo	Director general financiero	Director de operaciones	Director de TI	Consejo de gobierno de I&T	Gestor de Portafolio	
EDM02.01 Establecer el objetivo de la mezcla de inversión.	A	R	R	R	R	R	R	R	
EDM02.02 Evaluar la optimización del valor.	A	R	R	R	R	R	R	R	
EDM02.03 Dirigir la optimización del valor.	A	R	R	R	R	R	R	R	
EDM02.04 Monitorizar la optimización del valor.	A	R	R	R	R	R	R	R	R
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica								
King IV Report on Corporate Governance for South Africa, 2016	Part 2: Fundamental concepts—Definition of corporate governance								

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gobierno	Entradas		Salidas	
EDM02.01 Establecer el objetivo de la mezcla de inversión.	De	Descripción	Descripción	A
	AP002.05	<ul style="list-style-type: none">Definición de iniciativas estratégicasIniciativas de evaluación de riesgosHoja de ruta estratégica	Retroalimentación sobre estrategia y metas	AP002.05
	AP009.01	Definiciones de servicios estándar	Recursos y capacidades identificados requeridos para respaldar la estrategia	Interna
	BAI03.11	Definiciones de servicios	Mezcla de inversión definida	Interna EDM02.03
	EDM02.03	Tipos y criterios de inversión		
EDM02.02 Evaluar la optimización del valor.	AP002.05	Hoja de ruta estratégica	Evaluación del alineamiento estratégico	AP002.04; AP005.02
	AP005.01	Expectativas acerca del retorno de la inversión	Evaluación de los portafolios de inversiones y servicios	AP005.02; AP005.03; AP006.02
	AP005.02	Programas seleccionados con objetivos de retorno de inversión (ROI)		
	AP005.05	Resultados de beneficios y comunicaciones relacionadas		
	BAI01.06	Resultados de la revisión por etapas		
EDM02.03 Dirigir la optimización del valor.	AP005.03	Informes de rendimiento del portafolio de inversiones	Requisitos de las revisiones de cambio de fases	BAI01.01; BAI11.01
	EDM02.01	Mezcla de inversión definida	Tipos y criterios de inversión	EDM02.01; AP005.02
EDM02.04 Monitorizar la optimización del valor.	AP005.03	Informes de rendimiento del portafolio de inversiones	Acciones para mejorar la entrega de valor	AP005.03; AP006.02; BAI01.01; BAI11.01; EDM05.01
			Retroalimentación sobre el rendimiento del portafolio y los programas	AP005.03; AP006.05; BAI01.06
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Benefits management	Skills Framework for the Information Age V6, 2015	BENM

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de elaboración y ejecución de presupuestos	Establece las directrices para identificar las necesidades y requisitos de las inversiones, monitorizar su cumplimiento y asegurar el máximo beneficio. Abordar la formulación de solicitudes presupuestarias. Supervisar la ejecución del rendimiento presupuestario y técnico conforme a lo estimado. Recomendar la reasignación o reprogramación justificadas. Abordar la supervisión del rendimiento en relación a los acuerdos de nivel de servicio y otras métricas basadas en el rendimiento.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
El valor que I&T proporciona depende del grado de alineamiento de I&T con el negocio y del cumplimiento de sus expectativas. Optimizar el valor de I&T estableciendo una cultura en la que los servicios de I&T se proporcionen a tiempo y dentro del presupuesto, con la calidad adecuada.		

G. Componente: Servicios, infraestructura y aplicaciones	
<ul style="list-style-type: none"> • Sistema de contabilidad de costes • Herramienta de gestión de programas 	

Página dejada en blanco intencionadamente

Dominio: Evaluar, Dirigir y Monitorizar Objetivo de gobierno: EDM03 – Asegurar la optimización del riesgo		Área prioritaria: Modelo Core de COBIT
Descripción		
Asegurar que el apetito y la tolerancia al riesgo de la empresa se entiendan, articulen y comuniquen, y que se identifique y gestione el riesgo para el valor de negocio relacionado con el uso de I&T.		
Propósito		
Asegurarse de que el riesgo de negocio relacionado con la I&T no exceda el apetito y tolerancia al riesgo de la empresa, que se identifique y gestione el impacto del riesgo de I&T para el valor de negocio y que se minimicen los posibles fallos de cumplimiento.		
El objetivo de gobierno respalda la realización de un conjunto de metas empresariales y de alineamiento primarias:		
Metas empresariales <ul style="list-style-type: none"> • EG02 Gestión de riesgo de negocio • EG06 Continuidad y disponibilidad del servicio del negocio 	➔	Metas de alineamiento <ul style="list-style-type: none"> • AG02 Gestión de riesgo relacionado con I&T • AG07 Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad
Métricas modelo para metas empresariales EG02 <ul style="list-style-type: none"> a. Porcentaje de objetivos y servicios empresariales críticos cubiertos por la evaluación de riesgos b. Número de incidentes significativos que no se identificaron en la evaluación de riesgos frente al total de incidentes c. Frecuencia de actualización del perfil de riesgo EG06 <ul style="list-style-type: none"> a. Número de interrupciones del servicio al cliente o procesos empresariales que han causado incidentes significativos b. Coste empresarial de los incidentes c. Número de horas de procesamiento perdidas en el negocio debido a interrupciones inesperadas del servicio d. Porcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados 		Métricas modelo para metas de alineamiento AG02 <ul style="list-style-type: none"> a. Frecuencia de actualización del perfil de riesgo b. Porcentaje de las evaluaciones de riesgo empresarial, incluido el riesgo relacionado con I&T c. Número de incidentes significativos relacionados con I&T que no se identificaron en la evaluación de riesgos AG07 <ul style="list-style-type: none"> a. Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o descrédito público b. Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o descrédito público c. Número de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o descrédito público

A. Componente: Proceso		
Práctica de gobierno	Métricas modelo	
EDM03.01 Evaluar la gestión de riesgos. Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las I&T en la empresa. Considerar si el apetito al riesgo de la empresa es apropiada, y que se identifique y gestione el riesgo para el valor de la empresa relacionado con el uso de I&T.	a. Nivel de impacto empresarial inesperado b. Porcentaje de riesgo de I&T que excede la tolerancia al riesgo de la empresa c. Frecuencia de actualización de la evaluación del factor de riesgo	
Actividades	Nivel de capacidad	
1. Conocer la organización y su contexto en relación al riesgo de I&T.	2	
2. Determinar el apetito al riesgo de la organización, es decir, el nivel de riesgo relacionado con I&T que la empresa está dispuesta a tomar en la búsqueda de sus objetivos empresariales.		
3. Determinar los niveles de tolerancia al riesgo frente al apetito al riesgo, es decir, las desviaciones aceptables temporalmente del apetito al riesgo.		
4. Determinar el grado de alineamiento de la estrategia de riesgos en I&T de la empresa con la estrategia de riesgos de la empresa en su conjunto y garantizar que el apetito al riesgo se sitúe por debajo de la capacidad de riesgo de la organización.		
5. Evaluar los factores de riesgo de I&T de forma proactiva antes de tomar decisiones estratégicas a nivel de empresa y garantizar que las consideraciones del riesgo formen parte del proceso de decisión estratégico de la empresa.	3	
6. Evaluar las actividades de gestión de riesgos para asegurar que se alineen con la capacidad de la empresa para las pérdidas relacionadas con I&T y la tolerancia correspondiente por parte de la dirección.		
7. Atraer y conservar las habilidades y el personal necesarios para la gestión de riesgos de las I&T		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
COSO Enterprise Risk Management, junio de 2017	Strategy and Objective-Setting—Principles 6 and 7; 9. Review and Revision—Principle 16	

A. Componente: Proceso (cont.)		
Práctica de gobierno		Métricas modelo
EDM03.02 Dirigir la gestión de riesgos. Dirigir el establecimiento de prácticas de gestión de riesgos para ofrecer una seguridad razonable de que las prácticas de gestión de riesgos de I&T son apropiadas y que el riesgo de I&T actual no sobrepasa al apetito al riesgo del consejo de administración.		a. Nivel de alineamiento entre el riesgo de I&T y el riesgo empresarial b. Porcentaje de proyectos de la empresa que consideran el riesgo de I&T.
Actividades		Nivel de capacidad
1. Dirigir la traducción e integración de la estrategia de riesgo de I&T en las prácticas de gestión de riesgos y las actividades operativas.		2
2. Dirigir el desarrollo de planes de comunicación de riesgos (que se extiendan a todos los niveles de la empresa).		
3. Dirigir la implementación de los mecanismos adecuados para responder de forma rápida al cambio de riesgos e informar inmediatamente a los cargos de dirección correspondientes, siguiendo los principios de escalamiento (qué comunicar, cuándo, dónde y cómo).		
4. Ordenar que el riesgo, oportunidades, problemas o preocupaciones puedan identificarse y comunicarse por cualquier persona a la parte correspondiente en cualquier momento. El riesgo debe gestionarse conforme a las políticas y procedimientos publicados y comunicados a los responsables de la toma de decisiones.		
5. Identificar las metas y métricas claves de los procesos de gobierno y gestión de riesgos que deben monitorizarse, y aprobar las estrategias, métodos, técnicas y procesos para capturar y comunicar la información de las mediciones.		3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		RS.AS Apply Risk Management Strategy; BC.RO Determine Strategic Risk Objectives
ISF, The Standard of Good Practice for Information Security 2016		IR1.1 Information Risk Assessment—Management Approach
King IV Report on Corporate Governance for South Africa, 2016		Part 5.4: Governance functional areas—Principle 11
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018		3.5 Assessment (Task 2)
Práctica de gobierno		Métricas modelo
EDM03.03 Monitorizar la gestión de riesgos. Monitorizar r las metas y las métricas clave de los procesos de gestión de riesgos. Establecer cómo las desviaciones o los problemas se identificarán, se les dará seguimiento y se comunicarán para su solución.		a. Número de áreas potenciales de riesgo de I&T identificadas y gestionadas b. Porcentaje de riesgo crítico que ha sido mitigado efectivamente c. Porcentaje de planes de acción de riesgo de I&T ejecutados a tiempo
Actividades		Nivel de capacidad
1. Comunicar cualquier problema de gestión de riesgos al consejo de administración o comité ejecutivo.		2
2. Supervise hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de tolerancia y apetito de riesgo de la empresa.		3
3. Monitorizarr las metas y métricas de los procesos de gobierno y gestión de riesgos contra los objetivos, analizar la causa de las posibles desviaciones, y poner en marcha las acciones remediales s para solucionar las causas subyacentes.		4
4. Facilitar la revisión por parte de las partes interesadas clave del progreso de la empresa con respecto a las metas identificadas.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
COSO Enterprise Risk Management, junio de 2017		9. Review and Revision—Principle 17
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018		3.1 Preparation (Task 7); 3.5 Assessment (Task 1); 3.6 Authorization (Task 1)
The Open Group IT4IT Reference Architecture, Versión 2.0		6. Requirement to Deploy (R2D) Value Stream; 7. Request to Fulfill (R2F) Value Stream

B. Componente: Estructuras organizativas									
Práctica clave de gobierno								Consejo de Administración	Comité Ejecutivo
EDM03.01 Evaluar la gestión de riesgos.								A	R
EDM03.02 Dirigir la gestión de riesgos.								A	R
EDM03.03 Monitorizar la gestión de riesgos.								A	R
Documentación relacionada (Estándares Marcos, Requisitos de cumplimiento)					Referencia específica				
COSO Enterprise Risk Management, junio de 2017					6. Governance and Culture—Principle				
King IV Report on Corporate Governance for South Africa, 2016					Part 2: Fundamental concepts—Definition of corporate governance				

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gobierno	Entradas		Salidas	
EDM03.01 Evaluar la gestión de riesgos.	De	Descripción	Descripción	A
	AP012.01	Problemas y factores de riesgo emergentes	Guía de apetito al riesgo	AP004.01; AP012.03
	Fuera de COBIT	Principios de gestión de riesgos empresariales (ERM)	Evaluación de actividades de gestión de riesgos	AP012.01
			Niveles aprobados de tolerancia al riesgo	AP012.03
EDM03.02 Dirigir la gestión de riesgos.	AP012.03	Perfil de riesgo agregado, incluido el estado de las acciones de gestión de riesgos	Proceso aprobado para la medición de la gestión de riesgos	AP012.01
	Fuera de COBIT	Planes de mitigación y perfiles para la gestión de riesgos empresariales (ERM)	Objetivos clave a monitorizar para la gestión de riesgos	AP012.01
			Políticas de gestión de riesgos	AP012.01
EDM03.03 Monitorizar la gestión de riesgos.	AP012.02	Resultados del análisis de riesgos	Acciones remediales para solucionar las desviaciones de gestión de riesgos	AP012.06
	AP012.04	<ul style="list-style-type: none"> Análisis de riesgos e informes del perfil de riesgo para las partes interesadas Resultados de evaluaciones de riesgos de terceros Oportunidades para la aceptación de un riesgo mayor 	Problemas de gestión de riesgos para el consejo de administración	EDM05.01
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
National Institute of Standards and Technology Special Publication 800-37, Revisión 2, septiembre de 2017		3.1 Preparation (Task 7): Inputs and Outputs; 3.5 Assessment (Tasks 1, 2): Inputs 2, and Outputs; 3.6 Authorization (Task 1): Inputs and Outputs		

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión de riesgo del negocio	Skills Framework for the Information Age V6, 2015	BURM
Gestión de riesgos	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.3. Risk Management

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de riesgos empresariales	Define el gobierno y gestión del riesgo empresarial a nivel estratégico, táctico y operativo, en búsqueda de satisfacer los objetivos de negocio. Traduce el gobierno de la empresa en política y principios de gobierno del riesgo y elabora actividades de gestión de riesgos.	National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.17 Risk assessment (RA-1)

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Promover una cultura consciente de los riesgos de I&T en todos los niveles de la organización y facultar proactivamente a la empresa para que identifique, comunique y escale el riesgo, oportunidad y posibles impactos del negocio en I&T. La dirección senior establece el rumbo y muestra un apoyo visible y genuino a las prácticas de riesgo. Además, la dirección debe definir claramente el apetito al riesgo y garantizar un nivel de debate adecuado como parte de las actividades diarias. Entre los comportamientos deseables se encuentran fomentar que los empleados informen sobre problemas o resultados negativos y muestren transparencia con respecto al riesgo de I&T. Los Dueños de la empresa deben aceptar el riesgo de I&T cuando corresponda y demostrar un compromiso genuino con la gestión de riesgos en I&T, proporcionando los niveles de recursos adecuados.	COSO Enterprise Risk Management, junio de 2017	6. Governance and Culture—Principles 3 and 4

G. Componente: Servicios, infraestructura y aplicaciones	
Sistema de gestión de riesgos	

Dominio: Evaluar, Dirigir y Monitorizar Objetivo de gobierno: EDM04 – Asegurar la optimización de los recursos		Área prioritaria: Modelo Core de COBIT
Descripción		
Asegurar que se dispone de recursos adecuados y suficientes relacionadas con I&T (personas, procesos y tecnología) y con el negocio para apoyar eficazmente los objetivos empresariales, a un coste óptimo.		
Propósito		
Asegurarse de que las necesidades de recursos de la empresa se satisfagan de manera óptima, que los costes de I&T se optimicen, y que exista una mayor probabilidad de obtener beneficios y disponibilidad para cambios futuros.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales		Metas de alineamiento
<ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG08 Optimización de la funcionalidad de procesos internos del negocio • EG12 Gestión de programas de transformación digital 		AG09 Ejecución de programas dentro del plazo, sin exceder el presupuesto, y que cumplen con los requisitos y estándares de calidad
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 <ul style="list-style-type: none"> a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios 		AG09 <ul style="list-style-type: none"> a. Número de programas/proyectos ejecutados a tiempo y dentro del presupuesto b. Número de programas que necesitan una revisión significativa debido a defectos de calidad c. Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto
EG08 <ul style="list-style-type: none"> a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarial b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores externos con las capacidades de la cadena de suministro 		
EG12 <ul style="list-style-type: none"> a. Número de programas ejecutados a tiempo y dentro del presupuesto b. Porcentaje de partes interesadas satisfechas con la ejecución del programa c. Porcentaje de programas de transformación del negocio suspendidos d. Porcentaje de programas de transformación del negocio con actualizaciones del estado notificadas regularmente 		

A. Componente: Proceso		
Práctica de gobierno		Métricas modelo
EDM04.01 Evaluar la gestión de recursos. Examinar y analizar continuamente la necesidad actual y futura de recursos empresariales y de I&T (financieros y humanos), las opciones de recursos (incluyendo estrategias de abastecimiento), y principios de asignación y gestión para satisfacer las necesidades de la empresa de manera óptima.		a. Número de desviaciones del plan de recursos b. Porcentaje de estrategias del plan de recursos y arquitectura empresarial que proporciona valor y mitiga el riesgo con recursos asignados
Actividades		Nivel de capacidad
1. Partiendo de las estrategias actuales y futuras, examinar las posibles opciones para proporcionar recursos relacionados con I&T (recursos tecnológicos, financieros y humanos), y desarrollar capacidades para hacer frente a las necesidades actuales y futuras (incluidas opciones de abastecimiento).		2
2. Definir los principios fundamentales de la asignación y gestión de recursos y capacidades, de forma que I&T puede satisfacer las necesidades de la empresa conforme a las prioridades acordadas y los límites presupuestarios. Por ejemplo, definir opciones preferidas de abastecimiento definidas para determinados servicios y los límites presupuestarios por opción de abastecimiento.		
3. Revisar y aprobar las estrategias del plan de recursos y de la arquitectura empresarial para proporcionar valor y mitigar el riesgo con los recursos asignados.		
4. Entender los requisitos para el alineamiento de la gestión de recursos de I&T con la planificación de recursos humanos (RR. HH.) y financieros de la empresa.		
5. Definir los principios para la gestión y el control de la arquitectura empresarial		3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		GR.DR Direct Resource Management Needs
ISO/IEC 38500:2015(E)		5.4 Principle 3: Acquisition (Evaluate)

A. Componente: Proceso (cont.)		
Práctica de gobierno		Métricas modelo
EDM04.02 Dirigir la gestión de recursos. Asegurar la adopción de principios de gestión de recursos para permitir un uso óptimo de los recursos empresariales y de I&T durante todo su ciclo de vida económico.		a. Número de desviaciones de, y excepciones con respecto a los principios de gestión de recursos b. Porcentaje de reutilización de componentes de la arquitectura
Actividades		Nivel de capacidad
1. Asignar responsabilidades para la ejecución de la gestión de recursos.		2
2. Establecer los principios relacionados con la protección de los recursos.		
3. Comunicar y dirigir la adopción de estrategias de gestión de recursos, principios y del plan de recursos y arquitectura empresarial acordados.		3
4. Alinear la gestión de recursos con la planificación financiera y de RR. HH. de la empresa.		
5. Definir las metas, mediciones y métricas clave para la gestión de recursos.		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		GR.ER Evaluate Resource Management Needs
COSO Enterprise Risk Management, junio de 2017		6. Governance and Culture—Principle 5
ISO/IEC 38500:2015(E)		5.4 Principle 3: Acquisition (Direct)
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.14 Planning (PL-4)
Práctica de gobierno		Métricas modelo
EDM04.03 Monitorizar la gestión de recursos. Monitorizar las metas y las métricas clave de los procesos de gestión de recursos. Establecer cómo las desviaciones o los problemas se identificarán, se hará seguimiento y se comunicarán para su solución.		a. Nivel de retroalimentación de las partes interesadas sobre la optimización de recursos b. Número de beneficios (como ahorro de costes) logrados a través de la utilización óptima de los recursos c. Número de objetivos de rendimiento en gestión de recursos logrados d. Porcentaje de proyectos y programas con un estatus de medio o alto riesgo debido a problemas de gestión de recursos e. Porcentaje de proyectos con asignaciones de recursos adecuadas
Actividades		Nivel de capacidad
1. Supervisar la asignación y optimización de recursos conforme a los objetivos y prioridades de la empresa usando metas y métricas acordadas.		4
2. Supervisar las estrategias de abastecimiento de I&T, las estrategias de arquitectura empresarial y las capacidades y recursos empresariales y de TI para garantizar que se puedan satisfacer las necesidades y objetivos actuales y futuros de la empresa.		
3. Monitorizar el rendimiento de los recursos en relación a los objetivos, analizar la causa de las posibles desviaciones, y poner en marcha las acciones remediales para solucionar las causas subyacentes.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		GR.MR Monitor Resource Management Needs
ISO/IEC 38500:2015(E)		5.4 Principle 3: Acquisition (Evaluate)

B. Componente: Estructuras organizativas						
Práctica clave de gobierno						
EDM04.01 Evaluar la gestión de recursos.	A	R	R	R	R	R
EDM04.02 Dirigir la gestión de recursos.	A	R	R	R	R	R
EDM04.03 Monitorizar la gestión de recursos.	A	R	R	R	R	R
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)			Referencia específica			
King IV Report on Corporate Governance for South Africa, 2016			Part 2: Fundamental concepts—Definition of corporate governance			

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gobierno	Entradas		Salidas	
EDM04.01 Evaluar la gestión de recursos.	De	Descripción	Descripción	A
	AP002.04	Brechas y cambios requeridos para lograr la capacidad del objetivo	Principios directrices para la asignación de recursos y capacidades	AP002.01; AP007.01; BAI03.11
	AP007.03	Planes de desarrollo de competencias	Plan de recursos aprobado	AP002.05; AP007.01; AP009.02
	AP010.02	Resultados de las decisiones de las evaluaciones de proveedores	Principios directrices para la arquitectura empresarial	AP003.01
EDM04.02 Dirigir la gestión de recursos.			Principios para la protección de recursos	AP001.02
			Responsabilidades asignadas para la gestión de recursos	AP001.05; DSS06.03
			Comunicación de estrategias de gestión de recursos	AP002.06; AP007.05; AP009.02
EDM04.03 Monitorizar la gestión de recursos.			Acciones remediales para solucionar las desviaciones de gestión de recursos	AP002.05; AP007.01; AP007.03; AP009.04
			Retroalimentación sobre la asignación y eficiencia de recursos y capacidades	EDM05.01; AP002.02; AP007.05; AP009.05
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin Documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión del portafolio	Skills Framework for the Information Age V6, 2015	POMG
Gestión de recursos	Skills Framework for the Information Age V6, 2015	RESC

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de medición del desempeño	Identifica la necesidad de poseer un sistema de medición del desempeño más allá de la rendición de cuentas convencional. Este sistema incluye la medición de las relaciones y los activos de conocimiento necesarios para competir en la era de la información, incluyendo centrarse en el cliente, la eficiencia de los procesos y la habilidad para aprender y crecer (cuadro de mando integral). El cuadro de mando integral traduce la estrategia en acción para lograr las metas empresariales, teniendo en cuenta intangibles como la satisfacción del cliente, armonizando las funciones internas, la creación de eficiencias operativas y el desarrollo de habilidades del personal. Esta visión holística de las operaciones ayuda a vincular los objetivos estratégicos a largo plazo con las acciones a corto plazo.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Establecer una cultura en la que se valoren los recursos, y la inversión, el uso y la asignación de recursos (ya sean personas, información, aplicaciones, tecnología o instalaciones) se alineen con las necesidades de la organización. Ilustrar estos valores garantizando que existan métodos apropiados y competencias adecuadas en la organización; por ejemplo, asegurar que los beneficios de la prestación de servicios sean reales y alcanzables, e implementar sistemas de medición del desempeño sólidos (como el cuadro de mando integral).		

G. Componente: Servicios, infraestructura y aplicaciones
Sistema de medición del desempeño (p. ej., cuadro de mando integral, herramienta de gestión de competencias)

Dominio: Evaluar, Dirigir y Monitorizar		Área prioritaria: Modelo Core de COBIT	
Objetivo de gobierno: EDM05 – Asegurar el compromiso de las partes interesadas			
Descripción			
Asegurar que se identifica e involucra a las partes interesadas en el sistema de gobierno de I&T y que la medición y comunicación sobre el rendimiento y conformidad de I&T de la empresa sean transparentes, con las partes interesadas aprobando las metas y métricas y las acciones remediales necesarias.			
Propósito			
Asegurarse de que las partes interesadas apoyen la estrategia y la hoja de ruta de I&T, que la comunicación con las partes interesadas sea eficaz y oportuna, y que se establezcan las bases para los informes con el fin de aumentar el rendimiento. Identificar las áreas de mejora y confirmar que los objetivos y estrategias relacionados con I&T se ajusten a la estrategia de la empresa.			
El objetivo de gobierno respalda que se alcancen una serie de metas empresariales y de alineamiento primarias:			
Metas empresariales		➡	Metas de alineamiento
• EG04 Calidad de la información financiera • EG07 Calidad de la información sobre gestión			AG10 Calidad de la información sobre gestión de I&T
Métricas modelo para metas empresariales			Métricas modelo para metas de alineamiento
EG04	a. Encuesta de satisfacción de las partes interesadas clave con respecto al nivel de transparencia, comprensión y precisión de la información financiera de la empresa b. Coste de incumplimiento con respecto a regulaciones financieras		AG10 a. Nivel de satisfacción del usuario con la calidad, oportunidad y disponibilidad de la información de gestión relacionada con I&T, tras considerar los recursos disponibles b. Relación y extensión de las decisiones de negocio erróneas en las que la información errónea o no disponible relacionada con I&T fue un factor clave c. Porcentaje de información que satisface los criterios de calidad
EG07	a. Grado de satisfacción del consejo de administración y la dirección ejecutiva con la información para la toma de decisiones b. Número de incidentes causados por decisiones erróneas de negocio basadas en información imprecisa c. Tiempo que se tarda en proporcionar la información que respalde la toma de decisiones empresariales eficaces d. Periodicidad de la información sobre gestión		

A. Componente: Proceso		
Práctica de gobierno		Métricas modelo
EDM05.01 Evaluar el compromiso y los requisitos de reportes de las partes interesadas Examinar y evaluar continuamente los requisitos actuales y futuros de compromiso y presentación de informes a las partes interesadas (incluyendo informes obligatorios por requisito regulatorios), y comunicaciones a otras partes interesadas. Establecer principios para el compromiso y comunicación con las partes interesadas.		a. Fecha de la última revisión de los requisitos de informes b. Porcentaje de partes interesadas incluidas en los requisitos de informes
Actividades		Nivel de capacidad
1. Identificar todas las partes interesadas de I&T relevantes dentro y fuera de la empresa. Agrupar a las partes interesadas en categorías de partes interesadas con requisitos similares.		2
2. Examinar y juzgar los requisitos de informes obligatorios actuales y futuros relacionados con el uso de I&T dentro de la empresa (regulación, legislación, leyes comunes, contractuales), incluidos su alcance y frecuencia.		
3. Examinar y juzgar los requisitos de comunicación e informes actuales y futuros para otras partes interesadas relacionados con el uso de I&T dentro de la empresa, incluidos el nivel requerido de participación/consulta y el alcance de la comunicación/nivel de detalle y condiciones.		
4. Mantener los principios para la comunicación con partes interesadas externas e internas, incluidos formatos y canales de comunicación, así como la aceptación y firma de informes de las partes interesadas.		3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		SR.DR Direct Stakeholder Communication and Reporting

A. Componente: Proceso (cont.)	
Práctica de gobierno	Métricas modelo
EDM05.02 Dirigir el compromiso, la comunicación y reporte de las partes interesadas. Asegurar el establecimiento de participación, comunicación y reportes efectivos para las partes interesadas, incluyendo mecanismos para asegurar la calidad y la integridad de la información, la monitorización de los informes obligatorios, y la creación de una estrategia de comunicación hacia las partes interesadas.	a. Número de brechas de los requisitos de informes obligatorios b. Satisfacción de las partes interesadas con la comunicación y elaboración de informes
Actividades	Nivel de capacidad
1. Dirigir el establecimiento de la estrategia de consulta y comunicación para las partes interesadas externas e internas.	2
2. Dirigir la implementación de mecanismos para asegurar que la información cumple con todos los criterios de los requisitos de elaboración de informes obligatorios de I&T para la empresa.	
3. Establecer mecanismos para la validación y aprobación de la elaboración de informes obligatorios.	
4. Establecer los mecanismos de escalamiento de los informes.	3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Cybermaturity Platform, 2018	SR.AR Apply Stakeholder Reporting Requirements
King IV Report on Corporate Governance for South Africa, 2016	Part 5.5: Stakeholder relationships—Principle 16
King IV Report on Corporate Governance for South Africa, 2016	Part 5.2: Strategy, performance and reporting—Principle 5
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity V1.1, abril de 2018	3.3 Communicating Cybersecurity Requirements with Stakeholders
Práctica de gobierno	Métricas modelo
EDM05.03 Monitorizar el compromiso de las partes interesadas. Monitorizar los niveles de participación de las partes interesadas y la efectividad de la comunicación con las partes interesadas. Evaluar los mecanismos para asegurar la precisión, confiabilidad y efectividad, y evaluar si se están cumpliendo los requisitos de las diferentes partes interesadas en cuanto a la elaboración de informes y la comunicación.	a. Nivel de participación de las partes interesadas en I&T de la empresa b. Porcentaje de informes que contienen imprecisiones c. Porcentaje de informes entregados a tiempo
Actividades	Nivel de capacidad
1. Evaluar periódicamente la eficiencia de los mecanismos para garantizar la precisión y confiabilidad de informes obligatorios.	4
2. Evaluar de forma periódica la efectividad de los mecanismos para, y los resultados de, la participación y comunicación con partes interesadas internas y externas.	
3. Determinar si se cumplen con los requisitos de las distintas partes interesadas y evaluar los niveles de participación de las partes interesadas.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Cybermaturity Platform, 2018	SR.MC Monitor Stakeholder Communication

B. Componente: Estructuras organizativas					
Práctica clave de gobierno	Consejo de Administración	Comité Ejecutivo	Director general ejecutivo	Director de riesgos	Director de TI
EDM05.01 Evaluar el compromiso y los requisitos de reportes de las partes interesadas.	A	R	R	R	R
EDM05.02 Dirigir el compromiso, comunicación y reporte de las partes interesadas.	A	R	R	R	R
EDM05.03 Monitorizar el compromiso de las partes interesadas.	A	R	R	R	R
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica				
King IV Report on Corporate Governance for South Africa, 2016	Part 2: Fundamental concepts—Definition of corporate governance				

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gobierno	Entradas		Salidas	
EDM05.01 Evaluar el compromiso y los requisitos de reportes de las partes interesadas.	De	Descripción	Descripción	A
	EDM02.04	Acciones para mejorar la entrega de valor	Principios de reporte y comunicación	MEA01.01
	EDM03.03	Problemas de gestión de riesgos para el consejo de administración	Evaluación de requisitos de reporte de la empresa	MEA01.01
	EDM04.03	Retroalimentación sobre la asignación y eficiencia de recursos and capacidades		
EDM05.02 Dirigir el compromiso, comunicación y reporte de las partes interesadas.	APO12.04	Análisis de riesgos y reporte del perfil de riesgo para las partes interesadas	Reglas para la validación y aprobación de informes obligatorios	MEA01.01; MEA03.04
			Directrices de escalamiento	MEA01.05
EDM05.03 Monitorizar el compromiso de las partes interesadas.	MEA04.08	<ul style="list-style-type: none">Resultados de la revisión de aseguramientoInformes de revisión de aseguramiento	Evaluación de la eficacia de la elaboración de informes	MEA01.01; MEA03.04
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin Documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión de relaciones	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.4. Relationship Management

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de transparencia	Aborda la importancia de la comunicación abierta y frecuente con todas las partes interesadas para garantizar que entienden la importancia estratégica de I&T para el éxito empresarial. Garantiza que la transparencia respalde la mitigación adecuada del riesgo, vinculando la transparencia y la gestión de riesgos eficiente al valor de I&T y al crecimiento empresarial.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Crear una cultura en la que se proporciona una comunicación abierta y estructurada a las partes interesadas, en línea con sus requisitos.		

G. Componente: Servicios, infraestructura y aplicaciones	
<ul style="list-style-type: none"> Herramientas y canales de comunicación Creación de tableros de control de TI Herramientas de encuestas de las partes interesadas 	

Página dejada en blanco intencionadamente

4.2 ALINEAR, PLANIFICAR Y ORGANIZAR (APO)

- 01 Gestionar el marco de gestión de I&T
- 02 Gestionar la estrategia.
- 03 Gestionar la arquitectura empresarial.
- 04 Gestionar la innovación.
- 05 Gestionar el portafolio.
- 06 Gestionar el presupuesto y los costes.
- 07 Gestionar los recursos humanos.
- 08 Gestionar las relaciones.
- 09 Gestionar los acuerdos de servicio
- 10 Gestionar los proveedores
- 11 Gestionar la calidad.
- 12 Gestionar el riesgo
- 13 Gestionar la seguridad
- 14 Gestionar los datos

Página dejada en blanco intencionadamente

Dominio: Alinear, Planificar y Organizar		Área prioritaria: Modelo Core de COBIT
Objetivo de gestión: APO01 – Gestionar el marco de gestión de I&T		
Descripción		
Diseñar el sistema de gestión para la I&T de la empresa basándose en las metas empresariales y otros factores de diseño. En base a este diseño, implementar todos los componentes necesarios del sistema de gestión.		
Propósito		
Implementar un enfoque de gestión consistente para permitir que se alcancen los requisitos de gobierno empresarial, con cobertura de componentes de gobierno, como los procesos de gestión, las estructuras organizativas, los roles y las responsabilidades, las actividades confiables y repetibles, los elementos de información, las políticas y procedimientos, las habilidades y las competencias, la cultura y el comportamiento, y los servicios, infraestructura y aplicaciones.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales		Metas de alineamiento
<ul style="list-style-type: none"> • EG03 Cumplimiento de leyes y regulaciones externas • EG08 Optimización de la funcionalidad de procesos del negocio internos • EG11 Cumplimiento de las políticas internas • EG12 Gestión de programas de transformación digital 	➔	<ul style="list-style-type: none"> • AG03 Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T • AG11 Cumplimiento de I&T con las políticas internas
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
<p>EG03</p> <ul style="list-style-type: none"> a. Coste de incumplimiento regulatorio, incluidos acuerdos y multas b. Número de problemas de incumplimiento regulatorio que causan comentarios públicos o publicidad negativa c. Número de problemas de incumplimiento señalados por los reguladores d. Número de problemas de incumplimiento regulatorio relacionados con acuerdos contractuales con socios de negocio 		<p>AG03</p> <ul style="list-style-type: none"> a. Porcentaje de inversiones posibilitadas por las I&T en las que los beneficios previstos se cumplen o exceden b. Porcentaje de servicios de I&T para los que se han logrado los beneficios esperados (indicados en los acuerdos de nivel de servicio)
<p>EG08</p> <ul style="list-style-type: none"> a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarial b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro 		<p>AG11</p> <ul style="list-style-type: none"> a. Número de incidentes relacionados con el incumplimiento de las políticas relacionadas con I&T. b. Número de excepciones a las políticas internas c. Frecuencia de revisión y actualización de la política
<p>EG11</p> <ul style="list-style-type: none"> a. Número de incidentes relacionados con el incumplimiento de la política b. Porcentaje de las partes interesadas que entienden las políticas c. Porcentaje de políticas respaldadas por estándares y prácticas de trabajo eficaces 		
<p>EG12</p> <ul style="list-style-type: none"> a. Número de programas ejecutados a tiempo y dentro del presupuesto b. Porcentaje de partes interesadas satisfechas con la ejecución del programa c. Porcentaje de programas de transformación del negocio suspendidos d. Porcentaje de programas de transformación del negocio con actualizaciones del estado notificadas regularmente 		

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
AP001.01 Diseñar el sistema de gestión para la I&T de la empresa Diseñar un sistema de gestión adaptado a las necesidades de la empresa. Las necesidades de gestión de la empresa se definen a través del uso de la cascada de metas y por la aplicación de factores de diseño. Asegurar que los componentes de gobierno están integrados y alineados con el gobierno, la filosofía de gestión y estilo operativo de la empresa.		a. Número de aprobaciones formales por estructuras de gobierno aplicable de los objetivos prioritarios para el sistema de gestión de I&T b. Porcentaje de los componentes de gobierno integrados y alineados con el gobierno, filosofía de gestión y estilo operativo de la empresa
Actividades		Nivel de capacidad
1. Adquirir el conocimiento de la visión, dirección y estrategia empresarial, así como el contexto empresarial actual y sus desafíos.		2
2. Considerar el entorno interno de la empresa, incluyendo la cultura y filosofía de gestión, la tolerancia al riesgo, la política de seguridad y privacidad, los valores éticos, el código de conducta, la rendición de cuentas y los requisitos para la integridad de la gestión.		
3. Aplicar la cascada de metas y los factores de diseño de COBIT a la estrategia y el contexto empresarial para decidir cuáles son las prioridades para el sistema de gestión y, por ende, la implementación de los objetivos de gestión prioritarios.		
4. Validar las prioridades seleccionadas para la implementación de objetivos de gestión con buenas prácticas o requisitos propios de la industria (p. ej.: regulaciones específicas de la industria) y con estructuras de gobierno adecuadas.		3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
COSO Enterprise Risk Management, junio de 2017		7. Strategy and Objective-Setting—Principle 9
ISO/IEC 27001:2013/Cor.2:2015(E)		International standard for establishing, implementing and maintaining a management system (all chapters)
ITIL V3, 2011		Service Strategy, 2.3 Governance and management systems
Práctica de gestión		Métricas modelo
AP001.02 Gestionar la comunicación de objetivos, dirección y decisiones tomadas. Concienciar y fomentar el entendimiento de los objetivos de alineamiento de I&T a las partes interesadas en toda la empresa. Comunicar regularmente decisiones importantes relacionadas con I&T y su impacto para la organización.		a. Frecuencia de comunicación de los objetivos y dirección de gestión para I&T b. Asignación de responsabilidad para el envío de comunicaciones regulares
Actividades		Nivel de capacidad
1. Proporcionar los recursos capacitados suficientes para respaldar el proceso de comunicación.		2
2. Definir las reglas básicas de comunicación, identificando las necesidades de comunicación e implementando planes basados en dichas necesidades, considerando la comunicación ascendente, descendente y horizontal.		3
3. Comunicar continuamente los objetivos y la dirección de las I&T. Asegurar que las comunicaciones vengan respaldadas por las acciones y las palabras de la dirección ejecutiva, usando todos los canales disponibles.		
4. Asegurar que la información comunicada incluya una clara misión articulada, objetivos de servicio, controles internos, calidad, código ético/conducta, políticas y procedimientos, roles y responsabilidades, etc. Comunicar la información con el nivel de detalle adecuado a las audiencias respectivas dentro de la empresa.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para este componente.		

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
AP001.03 Gestionar la implementación de procesos (para respaldar la consecución de objetivos de gobierno y gestión). Definir los niveles de capacidad del proceso objetivos y la implementación prioritaria basándose en el diseño del sistema de gestión.		a. Número de procesos prioritarios que deben implementarse o mejorarse para cumplir con el nivel de capacidad objetivo b. Número de métricas definidas para el seguimiento de la implementación satisfactoria del proceso
Actividades		Nivel de capacidad
1. Desarrollar el modelo de procesos objetivo de gobierno de I&T específico para la organización, basándose en la selección de los objetivos de gestión prioritarios (salido del ejercicio de cascada de metas y factores de diseño).		2
2. Analizar la brecha entre el modelo de proceso objetivo para la organización y las prácticas y actividades actuales.		3
3. Hacer el borrador de una hoja de ruta para la implementación de prácticas y actividades de proceso faltante. Usar métricas de práctica para hacer el seguimiento de una implementación satisfactoria		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
AP001.04 Definir e implementar las estructuras organizativas. Establecer las estructuras organizativas (como los comités) internas y externas requeridas por el diseño del sistema de gestión, permitiendo una toma de decisiones efectiva y eficaz. Asegurar que la tecnología y conocimiento de la información requeridos se incluyan en la composición de las estructuras de gestión.		a. Nivel de satisfacción ejecutiva con la toma de decisiones de gestión b. Número de decisiones que no se pudieron resolver dentro de las estructuras de gestión y fueron escaladas a estructuras de gobierno
Actividades		Nivel de capacidad
1. Identificar las decisiones requeridas para la consecución de resultados empresariales y la estrategia de I&T y para la gestión y ejecución de los servicios de I&T.		2
2. Involucrar a las partes interesadas críticas con la toma de decisiones (quien rinde cuentas, responsable, consultado o informado).		
3. Definir el alcance, foco, mandato y responsabilidades de cada función dentro de la organización de I&T, en línea con la dirección de gobierno.		
4. Definir el alcance de las funciones internas y externas, los roles internos y externos, y las capacidades y derechos de decisión requeridas para cubrir todas las prácticas, incluidas aquellas ejecutadas por terceros.		3
5. Alinear la organización relacionada con I&T con los modelos organizativos de arquitectura de la empresa.		
6. Establecer un comité de dirección de I&T (o equivalente) compuesto por directores ejecutivos, de negocio y de I&T para hacer un seguimiento del estado de los proyectos, resolver los conflictos de recursos y monitorizar los niveles y mejoras del servicio.		
7. Proporcionar las directrices para cada estructura de gestión (incluidas el mandato, objetivos, asistentes a reuniones, plazos, seguimiento, supervisión y control), así como los insumos requeridos y los resultados esperados de las reuniones.		4
8. Comprobar de forma regular la adecuación y eficacia de las estructuras organizativas.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
APO01.05 Establecer roles y responsabilidades. Definir y comunicar roles y responsabilidades para I&T de la empresa, incluidos los niveles de autoridad, responsabilidad y rendición de cuentas.		a. Número de roles de I&T asignados a individuos b. Número de descripciones de roles completos
Actividades		Nivel de capacidad
1. Establecer, acordar y comunicar los roles y responsabilidades relacionadas con I&T a todo el personal de la empresa, de acuerdo con las necesidades y objetivos de la empresa. Delinear claramente las responsabilidades y la rendición de cuentas, especialmente para la toma de decisiones y aprobaciones.		2
2. Considerar los requisitos para la continuidad del negocio y del servicio de I&T al definir los roles, incluyendo los requisitos de personal de respaldo y entrenamiento cruzado.		
3. Proporcionar información al proceso de continuidad de servicios de I&T, manteniendo la información de contacto y las descripciones de roles de la empresa actualizados.		
4. Incluir requisitos específicos en las descripciones de roles y responsabilidades relativos al cumplimiento de las políticas y procedimientos de gestión, el código ético y las prácticas profesionales.		
5. Asegurar que se defina la rendición de cuentas a través de roles y responsabilidades.		
6. Estructurar roles y responsabilidades para reducir la posibilidad de que un único rol comprometa un proceso crítico.		
7. Implementar las prácticas de supervisión adecuadas para asegurar que los roles y responsabilidades se ejerzan adecuadamente, para asegurar que todo el personal tiene la autoridad y recursos suficientes para ejecutar sus roles y responsabilidades, y de forma general, para revisar el rendimiento. El nivel de supervisión debe alinearse con la sensibilidad del puesto y la extensión de las responsabilidades asignadas.		3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
APO01.06 Optimizar la ubicación de la función de TI. Colocar las capacidades de TI en la estructura organizativa general para reflejar la importancia estratégica y la dependencia operativa de las TI dentro de la empresa. La línea de reporte del CIO y la representación de TI dentro de la alta dirección debe ser proporcional a la importancia de I&T dentro de la empresa.		a. Número de partes interesadas claves que han aprobado el establecimiento de la función de TI b. Porcentaje de partes interesadas con una opinión favorable del establecimiento de la función de TI
Actividades		Nivel de capacidad
1. Entender el contexto del establecimiento de la función de TI, incluida la evaluación de la estrategia empresarial y el modelo operativo (centralizado, federado, descentralizado, híbrido), la importancia de las I&T y la situación y opciones de abastecimiento.		3
2. Identificar, evaluar y priorizar las opciones para los modelos de ubicación, abastecimiento y operaciones de la organización.		
3. Definir el establecimiento de la función de TI y lograr un acuerdo.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISO/IEC 27002:2013/Cor.2:2015(E)		8.2 Information classification
Práctica de gestión		Métricas modelo
APO01.07 Definir la propiedad de la información (datos) y del sistema de información. Definir y mantener las responsabilidades de propiedad de información (datos) y sistemas de información. Asegurar que los Dueños clasifiquen la información y los sistemas y los protejan conforme a su clasificación.		a. Porcentaje de activos de datos con Dueños claramente definidos b. Porcentaje de sistemas de información con Dueños claramente definidos c. Porcentaje de elementos de información clasificados conforme a los niveles de clasificación acordados
Actividades		Nivel de capacidad
1. Proporcionar las directrices para garantizar la clasificación adecuada y consistente de los elementos de información en toda la empresa.		3
2. Crear y mantener un inventario de información (sistemas y datos) que incluyan una lista de Dueños, custodios y clasificaciones. Incluir sistemas que sean externalizados y aquellos cuya propiedad debería estar dentro de la empresa.		
3. Evaluar y distinguir entre datos, información y sistemas críticos (de alto valor) y no críticos. Asegurar la protección adecuada para cada categoría.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
AP001.08 Definir las habilidades y competencias objetivo. Definir las habilidades y competencias requeridas para lograr los objetivos de gestión relevantes.		a. Número de personas que han asistido a sesiones de formación o concienciación para habilidades seleccionadas, competencias y comportamientos deseados b. Porcentaje de personas con las habilidades y competencias requeridas alineados con objetivos de gestión específicos
Actividades		Nivel de capacidad
1. Identificar las habilidades y competencias requeridas para lograr objetivos de gestión específicos.		2
2. Analizar la brecha entre las habilidades y capacidades objetivas de la empresa y las habilidades actuales del personal. Consulte AP007– Gestionar los recursos humanos para el desarrollo de habilidades y las prácticas de gestión.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
AP001.09 Definir y comunicar políticas y procedimientos. Implementar procedimientos para mantener el cumplimiento y medir el rendimiento de las políticas y otros componentes del marco de control, y hacer cumplir las consecuencias del incumplimiento o rendimiento inadecuado. Dar seguimiento a las tendencias y el rendimiento y considerarlos en el futuro diseño y mejora del marco de control.		a. Porcentaje de políticas y procedimientos activos , que están documentados y actualizados b. Número de miembros del personal conocedores y capaces de demostrar su competencia con respecto a políticas y procedimientos
Actividades		Nivel de capacidad
1. Crear una serie de políticas para mejorar las expectativas de control de IT en temas clave relevantes, como la calidad, la seguridad, la privacidad, los controles internos, el uso de activos de I&T, la ética y los derechos de propiedad intelectual.		3
2. El despliegue y refuerzo de las políticas de I&T de forma uniforme para todo el personal relevante para que se construyan dentro de las operaciones empresariales y acaben siendo parte integrante de estas.		
3. Evaluar y actualizar las políticas, como mínimo anualmente, para encajar en entornos empresariales u operativos cambiantes.		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
AP001.10 Definir e implementar la infraestructura, servicios y aplicaciones para respaldar el sistema de gobierno y gestión. Definir e implementar infraestructura, servicios y aplicaciones para respaldar el sistema de gobierno y gestión (p. ej.: los repositorios de arquitectura, el sistema de gestión de riesgos, las herramientas de gestión de proyectos, las herramientas de seguimiento de costes y las herramientas de monitorización de incidentes).		a. Número de herramientas seleccionadas para respaldar procesos prioritarios b. Adecuación/coertura de las herramientas de procesos de I&T claves c. Satisfacción de los destinatarios con la precisión, integridad y puntualidad de la información d. Porcentaje de satisfacción de las partes interesadas con las herramientas seleccionadas para respaldar sus necesidades
Actividades		Nivel de capacidad
1. Identificar objetivos de gestión prioritarios que podrían lograrse mediante la automatización de servicios, aplicaciones o infraestructura.		2
2. Seleccionar e implementar las herramientas más adecuadas comunicarlo a las partes interesadas.		
3. Proporcionar formación en herramientas específicas, conforme se requiera.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		

A. Componente: Proceso (cont.)

Práctica de gestión	Métricas modelo
AP001.11 Gestionar la mejora continua del sistema de gestión de I&T. Mejorar continuamente los procesos y otros componentes del sistema de gestión para asegurar que pueden cumplir con los objetivos de gobierno y gestión. Considerar la guía de implementación de COBIT, los estándares emergentes, los requisitos de cumplimiento, las oportunidades de automatización, y la retroalimentación de las partes interesadas.	a. Fecha de las últimas actualizaciones al marco y a los componentes b. Número de exposiciones a pérdidas relacionadas con las I&T debidas a insuficiencias en el diseño del entorno de control
Actividades	Nivel de capacidad
1. Evaluar de forma regular el rendimiento de los componentes del marco y llevar a cabo las acciones correspondientes.	4
2. Identificar los procesos críticos para el negocio basado en los motivadores de rendimiento y conformidad y el riesgo relacionado. Evaluar la capacidad e identificar los objetivos de mejora. Analizar las brechas de capacidad y control. Identificar opciones para mejorar o rediseñar el proceso.	
3. Priorizar iniciativas para mejoras basadas en los posibles beneficios y costes. Implementar las mejoras acordadas, actuar conforme a la práctica normal del negocio, y establecer metas y métricas de rendimiento que permitan monitorizar las mejoras.	5
4. Considerar la manera de mejorar la eficiencia y la eficacia (p. ej.: a través de la formación, documentación, estandarización y/o automatización de procesos).	
5. Aplicar prácticas de gestión de la calidad para actualizar el proceso.	
6. Eliminar componentes de gobierno desactualizados (procesos, elemento de información, políticas, etc.).	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
ITIL V3, 2011	Continual Service Improvement, 4.1 The 7-Step Improvement Process

B. Componente: Estructuras organizativas

Práctica clave de gestión	Comité Ejecutivo	Director de riesgos	Director de TI	Director de tecnología	Director de tecnologías digitales	Consejo de gobierno de I&T	Consejo de arquitectura	Comité de riesgos empresariales	Director de seguridad de la información	Dueños del proceso de negocio	Función de gestión de datos	Director de Recursos Humanos	Gestor de relaciones	Jefe de arquitectura	Jefe de desarrollo	Jefe de operaciones de TI	Jefe de administración de TI	Gestor de Servicios	Gestor de seguridad de la información	Gestor de continuidad del negocio	Director de privacidad
AP001.01 Diseñar el sistema de gestión para la I&T de la empresa.	A		R	R	R	R															
AP001.02 Gestionar la comunicación de objetivos, dirección y decisiones tomadas.	A	R	R	R	R	R			R				R								
AP001.03 Gestionar la implementación de procesos (para respaldar la consecución de objetivos de gobierno y gestión).	A	R	R	R	R	R			R												
AP001.04 Definir e implementar las estructuras organizativas.	A		R	R	R	R						R									
AP001.05 Establecer roles y responsabilidades.	A		R	R	R	R															
AP001.06 Optimizar la ubicación de la función de TI.	A		R	R	R	R		R													
AP001.07 Definir la propiedad de la información (datos) y sistemas de información.	A		R	R	R	R		R		R	R			R							
AP001.08 Definir las habilidades y competencias objetivo.	A		R	R	R	R								R	R	R	R				
AP001.09 Definir y comunicar políticas y procedimientos.	A		R	R	R	R	R	R		R	R	R		R	R	R	R	R	R	R	R
AP001.10 Definir e implementar la infraestructura, servicios y aplicaciones para respaldar el sistema de gobierno y gestión.	A		R	R	R	R				R				R	R	R	R	R	R	R	R
AP001.11 Gestionar la mejora continua del sistema de gestión de I&T.	A		R	R	R	R				R	R			R	R	R	R	R	R	R	R

B. Componente: Estructuras organizativas (cont.)	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
COSO Enterprise Risk Management, junio de 2017	6. Governance and Culture—Principle 2
ISO/IEC 27001:2013/Cor.2:2015(E)	5.3. Roles, responsabilidades y autoridades organizativas

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
AP001.01 Diseñar el sistema de gestión para la I&T de la empresa	AP002.05	Hoja de ruta estratégica	Objetivos prioritarios de gobierno y gestión	Todos los APO; todos los BAI; todos los DSS; todos los MEA
	AP012.01	Problemas y factores de riesgo emergentes	Diseño del sistema de gestión	Todos los APO; todos los BAI; todos los DSS; todos los MEA
	AP012.02	Resultados del análisis de riesgos		
	EDM01.01	<ul style="list-style-type: none"> Principios rectores del gobierno empresarial Modelo de toma de decisiones 		
AP001.02 Gestionar la comunicación de objetivos, dirección y decisiones tomadas.	AP012.06	Comunicación del impacto del riesgo	Reglas básicas de comunicación	Todos los APO; todos los BAI; todos los DSS; todos los MEA
	DSS04.01	Política y objetivos para la continuidad del negocio	Comunicación de los objetivos de I&T	Todos los APO; todos los BAI; todos los DSS; todos los MEA
	DSS05.01	Política de prevención de software malicioso		
	DSS05.02	Política de seguridad de la conectividad		
	DSS05.03	Políticas de seguridad para los dispositivos Endpoint		
	EDM01.02	Comunicación del gobierno de la empresa		
	EDM04.02	Principios para la protección de recursos		
AP001.03 Gestionar la implementación de procesos (para respaldar la consecución de objetivos de gobierno y gestión).	AP002.04	Brechas y cambios requeridos para lograr la capacidad objetivo	Análisis de brecha del modelo objetivo	Todos los APO; todos los BAI; todos los DSS; todos los MEA
	EDM01.01	Principios rectores del gobierno empresarial	Niveles de capacidad del proceso	AP001.11
AP001.04 Definir e implementar las estructuras organizativas.	AP003.02	Modelo de arquitectura de procesos	Directrices operativas de la empresa	AP003.02
	EDM01.01	Principios rectores del gobierno empresarial	Definición de estructura organizativa y funciones	AP003.02

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
APO01.05 Establecer roles y responsabilidades.	De	Descripción	Descripción	A
	AP007.03	<ul style="list-style-type: none"> Matriz de habilidades y competencias Planes de desarrollo de competencias 	Definición de prácticas supervisoras	AP007.01
	AP011.01	Roles, responsabilidad y derechos de decisión del sistema de gestión de la calidad (QMS)	Definición de roles y responsabilidades relacionadas con I&T	DSS05.04
	AP013.01	Declaración del alcance del sistema de gestión de seguridad de la información (SGSI)		
	DSS06.03	<ul style="list-style-type: none"> Roles y responsabilidades asignadas Niveles de autoridad asignados 		
	EDM01.01	Niveles de autoridad		
	EDM04.02	Responsabilidades asignadas para la gestión de recursos		
APO01.06 Optimizar la ubicación de la función de TI.	Fuera de COBIT	<ul style="list-style-type: none"> Estrategia empresarial Modelo operativo empresarial 	Ubicación operativa definida de la función de TI	AP003.02
			Evaluación de opciones para la organización de TI	AP003.02
APO01.07 Definir la propiedad de la información (datos) y sistemas de información.			Directrices de la clasificación de datos	AP003.02; AP014.01; BAI02.01; DSS05.02; DSS06.01
			Directrices de la seguridad y control de los datos	AP014.04; AP014.10; BAI02.01
			Procedimientos de integridad de los datos	AP014.04; BAI02.01; DSS06.01
APO01.08 Definir las habilidades y competencias objetivo.			Matriz de habilidades y competencias	AP007.03
APO01.09 Definir y comunicar políticas y procedimientos.	DSS01.04	Políticas ambientales.	Acciones remediales para el incumplimiento	MEA01.05
	MEA03.02	Políticas, principios, procedimientos y Estándares actualizados		
APO01.10 Definir e implementar la infraestructura, servicios y aplicaciones para respaldar el sistema de gobierno y gestión.	AP009.01	Brechas identificadas en los servicios de I&T para la empresa	Planificar la dimensión adecuada del entorno de I&T incluidas las capacidades, servicios y aplicaciones de I&T faltantes	AP002.02; AP002.03
	Fuera de COBIT	Evaluación de escenario de I&T, incluidos servicios, aplicaciones e infraestructura		

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
APO01.11 Gestionar la mejora continua del sistema de gestión de I&T.	De	Descripción	Descripción	A
	APO01.03	Niveles de capacidad del proceso	Oportunidades de mejora del proceso	Todos los APO; todos los BAI; todos los DSS; todos los MEA
	EDM01.03	Retroalimentación sobre la eficacia y rendimiento del gobierno	Metas y métricas de rendimiento para el seguimiento de mejoras de procesos	MEA01.02
	MEA03.02	Políticas, principios, procedimientos y Estándares actualizados	Evaluaciones de la capacidad del proceso	MEA01.03
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin Documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gobierno de TI	Skills Framework for the Information Age V6, 2015	GOVN
Gestión de TI	Skills Framework for the Information Age V6, 2015	ITMG

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Marco de gestión de I&T	Establece el sistema de gestión para la I&T de la empresa basándose en las metas empresariales y otros factores de diseño. Considera políticas y principios detallados para la gestión de I&T en todos los componentes.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Definir una cultura interna de alineamiento entre la empresa y las TI, estableciendo los objetivos, estructuras, procesos y roles y responsabilidades necesarios que permitan la toma de decisiones y la creación de valor de la forma más eficaz y eficiente.		

G. Componente: Servicios, infraestructuras y aplicaciones	
<ul style="list-style-type: none"> • COBIT y productos/herramientas relacionados • Marcos y estándares equivalentes 	

Página dejada en blanco intencionadamente

Dominio: Alinear, Planificar y Organizar Objetivo de gestión: APO02 – Gestionar la estrategia		Área prioritaria: Modelo Core de COBIT
Descripción		
Proporcionar una visión holística del entorno empresarial y de I&T actual, la dirección futura y las iniciativas necesarias para migrar al entorno futuro deseado. Garantizar que el nivel de digitalización deseado sea integral en la dirección y la estrategia de I&T futuras. Evaluar la madurez digital actual de la organización y desarrollar una hoja de ruta para reducir las brechas. Repensar, con la empresa, las operaciones internas así como las actividades de cara al cliente. Garantizar el alcance en la ruta de transformación a través de toda la empresa. Aprovechar los bloques de construcción de la arquitectura empresarial, los componentes del gobierno y el ecosistema de la organización, incluyendo servicios y capacidades relacionadas que se proporcionan externamente, para permitir una respuesta confiable, y también ágil y eficiente a los objetivos estratégicos.		
Propósito		
Apoyar la estrategia de transformación digital de la organización y proporcionar el valor deseado a través de una hoja de ruta con cambios incrementales. Usar un enfoque holístico en cuanto a I&T, asegurando que cada iniciativa esté claramente conectada con una estrategia global. Habilitar el cambio en todos los diversos aspectos de la organización, desde los canales y procesos a los datos, cultura, habilidades, modelo operativo e incentivos.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:		
Metas empresariales	➔	Metas de alineamiento
<ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG05 Cultura de servicio orientada al cliente • EG08 Optimización de la funcionalidad de procesos internos del negocio • EG12 Gestión de programas de transformación digital 		AG08 Habilitar y dar soporte a procesos de negocio mediante la integración de aplicaciones y tecnología
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios		AG08 a. Plazo para la ejecución de servicios o procesos empresariales b. Número de programas empresariales habilitados por I&T retrasados o que incurren en costes adicionales debido a problemas de integración tecnológica c. Número de cambios en los procesos de negocio que se deben aplazar o revisar debido a problemas de integración tecnológica d. Número de aplicaciones o infraestructuras críticas que operan en silos y no están integradas
EG05 a. Número de interrupciones del servicio al cliente b. Porcentaje de partes interesadas del negocio satisfechas con que la prestación de servicios al cliente cumpla con los niveles de servicio acordados c. Número de quejas del servicio al cliente d. Tendencia de los resultados de la encuesta de satisfacción al cliente		
EG08 a. Niveles de satisfacción de la junta directiva y la dirección ejecutiva con las capacidades del proceso empresarial b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro		
EG12 a. Número de programas ejecutados a tiempo y dentro del presupuesto b. Porcentaje de partes interesadas satisfechas con la ejecución del programa c. Porcentaje de programas de transformación del negocio d. Porcentaje de programas de transformación del negocio con actualizaciones del estado notificado regularmente		

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
AP002.01 Comprender el contexto y la dirección de la empresa. Entender el contexto de la empresa (impulsores de la industria, la regulación relevante, la base para la competencia), su forma actual de funcionar y su nivel de ambición en cuanto a la digitalización.		a. Nivel de conocimiento dentro de la dirección de I&T de la organización y contexto empresariales actuales b. Nivel of conocimiento dentro de la dirección de I&T de las metas y dirección empresariales c. Nivel de conocimiento de las partes interesadas claves sobre I&T y sus requisitos específicos
Actividades		Nivel de capacidad
1. Desarrollar y mantener un conocimiento del entorno externo de la empresa.		2
2. Desarrollar y mantener un conocimiento de la forma actual de trabajo, incluido el entorno en el que opera, la arquitectura empresarial (dominios del negocio, la información, los datos, las aplicaciones y la tecnología), la cultura de la empresa y los retos actuales.		
3. Desarrollar y mantener un conocimiento de la dirección futura de la empresa, incluidas la estrategia, metas y objetivos empresariales. Conocer el nivel de ambición de la empresa en términos de digitalización, lo cual puede incluir aspirar a alcanzar una serie de metas , desde recorte de gastos, aumento a centrarse en el cliente, o una comercialización más rápida mediante la digitalización de las operaciones internas, para crear nuevos flujos de ingresos procedentes de nuevos modelos de negocio (como el negocio de plataformas).		
4. Identificar a partes interesadas clave y obtener información sobre sus requisitos.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
COSO Enterprise Risk Management, junio de 2017		7. Strategy and Objective-Setting—Principle 6
Práctica de gestión		Métricas modelo
AP002.02 Evaluar las capacidades, rendimiento y madurez digital actual de la empresa. Evaluar el rendimiento de los servicios de I&T actuales, y desarrollar una comprensión de las capacidades de la empresa y de I&T actuales (tanto internas como externas). Evaluar la madurez digital actual de la empresa y su apetito de cambio.		a. Porcentaje de personal satisfecho con sus capacidades actuales b. Porcentaje de satisfacción del Dueño de negocio con la inversión y la utilización de la base de activos interna y externa para cumplir con factores críticos de éxito
Actividades		Nivel de capacidad
1. Desarrollar una línea base de las capacidades y servicios empresariales y de I&T actuales. Incluir la evaluación de servicios externalizados, el gobierno de I&T y las habilidades y competencias de I&T de toda la empresa.		2
2. Evaluar la madurez digital en distintas dimensiones (p. ej., la capacidad de liderazgo para aprovechar la tecnología, el nivel de riesgo tecnológico aceptado, la estrategia de innovación, la cultura y el nivel de conocimiento de los usuarios). Evaluar el apetito por el cambio.		3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
COSO Enterprise Risk Management, junio de 2017		7. Strategy and Objective-Setting—Principle 6; 9. Review and Revision—Principle 15
Práctica de gestión		Métricas modelo
AP002.03 Definir las capacidades digitales objetivo. A partir del conocimiento del contexto y dirección de la empresa, definir los productos y servicios objetivo de I&T y las capacidades requeridas. Considerar los estándares de referencia, las mejores prácticas y las tecnologías emergentes validadas.		a. Porcentaje de objetivos empresariales considerados en las metas/objetivos de I&T b. Porcentaje de objetivos de I&T que apoyan la estrategia empresarial
Actividades		Nivel de capacidad
1. Resumir el contexto y la dirección de la empresa e identificar aspectos de I&T específicos de la estrategia empresarial (como procesos de digitalización, implementación de nueva tecnología, soporte de la arquitectura legacy, aplicación de nuevos modelos de negocio digital, desarrollo de portafolio de producto digitales, etc.).		2
2. Definir objetivos y metas de I&T de alto nivel y especificar su contribución a los objetivos empresariales.		
3. Detallar los servicios y productos de I&T requeridos para lograr los objetivos empresariales. Considerar ideas sobre tecnologías emergentes o innovación validadas, estándares de referencia, capacidades empresariales y de I&T de los competidores, benchmarks comparativos de buenas prácticas y provisión de servicios de I&T emergentes.		3
4. Determinar las estrategias en cuanto a capacidades, metodologías y enfoques organizativos de I&T requeridas para lograr el portafolio definido de productos y servicios de I&T. Considerar distintas metodologías de desarrollo (Agile, Scrum, Waterfall, Bimodal IT), dependiendo de los requisitos del negocio. Considerar como cada uno de ellos puede contribuir a lograr los objetivos de I&T.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		

A. Componente: Proceso (cont.)			
Práctica de gestión		Métricas modelo	
APO02.04 Llevar a cabo un análisis de brecha Identificar las brechas entre los entornos actual y objetivo y describir los cambios de alto nivel en la arquitectura empresarial.		a. Número de cambios de gran impacto requeridos en los distintos dominios de la arquitectura empresarial b. Número de brechas significativas entre el entorno actual y las buenas prácticas	
Actividades			Nivel de capacidad
1. Identificar todas las brechas y cambios requeridos para lograr el entorno objetivo.			3
2. Describir los cambios de alto nivel en la arquitectura empresarial (dominios del negocio, la información, los datos, las aplicaciones y la tecnología).			
3. Considerar las implicaciones de alto nivel de todas las brechas. Evaluar el impacto de los posibles cambios en los modelos operativos de I&T y empresarial, las capacidades de investigación y desarrollo de I&T y los programas de inversión en I&T.			
4. Considerar el valor de los posibles cambios en las capacidades de I&T y del negocio, los servicios y la arquitectura empresarial de TI y las implicaciones de no lograr ningún cambio.			4
5. Perfeccionar la definición del entorno objetivo y preparar una declaración de valor que destaque los beneficios del entorno objetivo.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin Documentación relacionada para esta práctica de gestión			
Práctica de gestión		Métricas modelo	
APO02.05 Definir el plan estratégico y el mapa de ruta. Desarrollar una estrategia digital holística, en cooperación con las partes interesadas relevantes, y detallar una hoja de ruta que defina los pasos incrementales a seguir requeridos para lograr las metas y objetivos. Asegurar el foco en la ruta de transformación, mediante el nombramiento de una persona que ayude a liderar la transformación digital e impulse el alineamiento entre I&T y la empresa.		a. Nivel de apoyo de las partes interesadas al plan de transformación digital b. Porcentaje de iniciativas en la estrategia de I&T que se autofinancian (con beneficios financieros que exceden los costes) c. Grado de correspondencia entre la estrategia empresarial y la estrategia y objetivos de I&T	
Actividades			Nivel de capacidad
1. Definir las iniciativas requeridas para eliminar las brechas entre los entornos actual y el objetivo. Integrar las iniciativas en una estrategia de I&T coherente que alinee a la I&T con todas las facetas empresariales.			3
2. Detallar una hoja de ruta que defina los pasos incrementales requeridos para lograr las metas y objetivos de la estrategia de I&T. Garantizar que se incluyan acciones para formar al personal en nuevas habilidades, apoyar la adopción de nueva tecnología, mantener el cambio en toda la organización, etc.			
3. Considerar el ecosistema externo (socios empresariales, proveedores, startups, etc.) para que contribuya a apoyar la ejecución de la hoja de ruta			
4. Agrupar las acciones en programas y/o proyectos con una meta o entregable claros. Identificar para cada proyecto los requisitos de recursos de alto nivel, la programación de actividades, el presupuesto para la inversión/operativo, el riesgo, el impacto del cambio, etc.			
5. Determinar las dependencias, solapamientos, sinergias e impactos entre proyectos, y priorizar.			
6. Finalizar la hoja de ruta, indicando una programación relativa de actividades y las interdependencias entre proyectos.			
7. Garantizar el foco en la ruta de transformación. Designar a un campeón de transformación y alineamiento digital entre la empresa y la I&T (el director de tecnologías digitales (CDO) u otro rol tradicional directivo).			
8. Obtener el apoyo y aprobación formal del plan de las partes interesadas.			4
9. Trasladar los objetivos a resultados medibles representados por métricas (qué) y objetivos (cuánto). Asegurar que los resultados y medidas se correspondan con los beneficios empresariales.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
ISF, The Standard of Good Practice for Information Security 2016		SG2.1 Information Security Strategy	
ITIL V3, 2011		Service Strategy, 4.1 Strategy management for IT services	

A. Componente: Proceso (cont.)	
Práctica de gestión	Métricas modelo
AP002.06 Comunicar la dirección y estrategia de I&T. Crear concienciación y comprensión de los objetivos y la dirección del negocio y de I&T, tal como se registró en la estrategia de I&T, mediante la comunicación a las partes interesadas y los usuarios apropiados en toda la empresa.	a. Frecuencia de actualizaciones del plan de comunicación de la estrategia de I&T b. Porcentaje de partes interesadas conocedoras de la dirección y estrategia de I&T
Actividades	Nivel de capacidad
1. Desarrollar un plan de comunicación que cubra los mensajes, el público objetivo, los mecanismos/canales de comunicación y la programación de actividades requeridas.	3
2. Preparar un paquete de comunicación que presente el plan de forma eficaz usando los medios de comunicación y tecnologías disponibles.	
3. Desarrollar y mantener una red para promocionar, apoyar e impulsar la estrategia de I&T.	
4. Obtener retroalimentación y actualizar el plan de comunicación y su presentación como corresponda.	4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin Documentación relacionada para esta práctica de gestión	

B. Componente: Estructuras organizativas																	
Práctica clave de gestión	Director general ejecutivo	Director de TI	Director de tecnología	Director de tecnologías digitales	Consejo de gobierno de I&T	Dueños del proceso de negocio	Oficina de gestión de proyectos	Función de gestión de datos	Gestor de relaciones	Jefe de arquitectura	Jefe de desarrollo	Jefe de operaciones de TI	Jefe de administración de TI	Gestor de Servicios	Gestor de seguridad de la información	Gestor de continuidad del negocio	Director de privacidad
AP002.01 Comprender el contexto y la dirección de la empresa.		A	R	R				R	R	R	R	R	R	R	R	R	R
AP002.02 Evaluar las capacidades, rendimiento y madurez digital actual de la empresa.		A	R	R				R		R	R	R	R	R	R	R	R
AP002.03 Definir las capacidades digitales objetivo.			R	R	A		R		R	R	R	R	R	R	R	R	R
AP002.04 Llevar a cabo un análisis de brecha			R	R	R	A	R		R		R	R	R	R	R	R	R
AP002.05 Definir el plan estratégico y el mapa de ruta.			R	R	R	A	R	R	R		R	R	R	R	R	R	R
AP002.06 Comunicar la dirección y estrategia de I&T.	R	R	R	R	A												
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica																
ISO/IEC 38502:2017(E)	5.4 Responsibilities of managers																

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
AP002.01 Comprender el contexto y la dirección de la empresa.	AP004.02	Oportunidades de innovación relacionadas con los motivadores empresariales	Fuentes y prioridades del cambio	Interna
	EDM04.01	Principios rectores para la asignación de recursos y capacidades		
	Fuera de COBIT	Estrategia empresarial y análisis de fortalezas, oportunidades, debilidades y amenazas(FODA)		

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
AP002.02 Evaluar las capacidades, rendimiento y madurez digital actual de la empresa.	AP006.05	Oportunidades de optimización de costes	Brechas y riesgos relacionados con las capacidades actuales	AP012.01
	AP008.05	Definición de posibles proyectos de mejora	Análisis FODA de capacidades	Interna
	AP009.01	Brechas identificadas en servicios de TI para la empresa	Línea base de capacidades actuales	Interna
	AP009.04	Planes de acción de mejora y remediaciones		
	AP012.01	Problemas y factores de riesgo emergentes		
	AP012.02	Resultados del análisis de riesgos		
	AP012.03	Perfil de riesgo agregado, incluido el estado de las acciones de gestión de riesgos		
	AP012.05	Propuestas de proyecto para reducir el riesgo		
	BAI04.03	• Priorizar las mejoras • Planes de rendimiento y capacidad		
	BAI04.05	Acciones correctivas		
	BAI09.01	Resultados de revisiones adecuadas para el propósito		
	BAI09.04	• Resultados de las revisiones de optimización de costes • Oportunidades para reducir los costes o aumentar el valor de los activos		
	EDM04.03	Retroalimentación sobre la asignación y eficiencia de recursos and capacidades		
AP002.03 Definir las capacidades digitales objetivo.	AP004.05	• Resultados y recomendación de iniciativas de valoraciones de concepto • Análisis de iniciativas rechazadas	Cambios propuestos a la arquitectura empresarial	AP003.03
			Capacidades empresariales y de TI requeridas	Interna
			Metas de alto nivel relacionadas con I&T	Interna
AP002.04 Llevar a cabo un análisis de brecha	AP004.06	Evaluaciones del uso de enfoques innovadores	Brechas y cambios requeridos para lograr la capacidad objetivo	AP001.03; AP013.02; BAI03.11; EDM04.01
	AP005.01	Expectativas de retorno de inversión	Declaración del beneficio de valor del entorno objetivo	BAI03.11
	BAI01.05	Resultados de la monitorización de la consecución de metas del programa		
	BAI01.06	Resultados de la revisión de los cambios de fases (stage-gate)		
	BAI11.09	Resultados de la revisión posterior a la implementación		
	EDM02.02	Evaluación del alineamiento estratégico		

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
APO02.05 Definir el plan estratégico y el mapa de ruta.	De	Descripción	Descripción	A
	APO03.01	<ul style="list-style-type: none">Alcance definido para la arquitecturaCaso de negocio y propuesta de valor del concepto de arquitectura	Estrategia y objetivos de I&T	Todos los APO; todos los BAI; todos los DSS; todos los MEA
	APO03.02	Modelo de la arquitectura de información	Hoja de ruta estratégica	APO01.01; APO03.01; APO08.01; EDM02.01; EDM02.02
	APO03.03	Arquitectura de transición	Definición de iniciativas estratégicas	EDM02.01
	APO05.01	Opciones de financiación	Iniciativas de evaluación de riesgos	EDM02.01, APO12.01
	APO06.02	Asignaciones de presupuesto		
	APO06.03	Presupuestos de I&T		
	BAI09.05	Plan de acción para ajustar el número de licencias y asignaciones		
	DSS04.02	Opciones estratégicas aprobadas		
	EDM02.01	Retroalimentación sobre estrategia y metas		
	EDM04.01	Plan de recursos aprobado		
EDM04.03	Acciones remediales para solucionar las desviaciones de gestión de recursos			
APO02.06 Comunicar la dirección y estrategia de I&T.	EDM04.02	Comunicación de estrategias de gestión de recursos	Paquete de comunicación	Todos los APO; todos los BAI; todos los DSS; todos los MEA
			Plan de comunicación	Interna
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
ITIL V3, 2011		Service strategy, 3.9 Service strategy inputs and outputs		

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Desarrollo del plan de negocio	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.3. Business Plan Development
Supervisión de tecnologías emergentes	Skills Framework for the Information Age V6, 2015	EMRG
Estrategia y planificación de I&T	Skills Framework for the Information Age V6, 2015	ITSP
Alineamiento estratégico	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.1. IS and Business Strategy Alignment

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Principios de la estrategia de servicio de I&T	Para obtener más información, consulte la Documentación relacionada.	ITIL V3, 2011	Service Strategy, 3. Service strategy principles
Política y principios estratégicos de I&T	Proporcionar una visión holística del entorno empresarial y de I&T actual, la dirección futura y las iniciativas necesarias para migrar al entorno futuro deseado. Garantizar que la estrategia empresarial y de I&T refleje el nivel de digitalización objetivo.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
<p>Establecer una cultura y valores subyacentes que encajen con la estrategia global de la empresa (es decir, orientada al cliente, impulsada por la innovación basada en los productos). Encontrar formas de acelerar los procesos e introducir una cultura y comportamiento que lo apoye, que permitan moverse a mayor velocidad. Se podría empezar con el cambio de hábitos básicos como tener más reuniones frecuentes de liderazgo de estrategia o automatizando ciertas actividades.</p> <p>En el contexto actual de modelos de negocio, ecosistemas y disrupción digitales, es fundamental para muchas organizaciones priorizar la transformación digital en su estrategia. Crear una cultura que desafíe el status quo y explore nuevos métodos de trabajo (como invertir en automatización para responder rápidamente a los clientes, desarrollar sistemas de elaboración de informes y analíticas sofisticadas para interpretar las necesidades de los clientes, crear interfaces innovadoras para recopilar los datos del cliente, crear mecanismos para ofrecer contenido y ofertas en todos los canales relevantes).</p>	El Scaled Agile Framework for Lean Enterprises (SAFe®)	Un marco de trabajo configurable que ayuda a las organizaciones a ofrecer nuevos productos y soluciones en un plazo de tiempo sostenible más corto posible (todos los capítulos)

G. Componente: Servicios, infraestructura y aplicaciones
<ul style="list-style-type: none"> • Análisis de clientes • Benchmarks de la industria • Sistema de medición del desempeño (p. ej., cuadro de mando integral, herramienta de gestión de competencias) • Servicios y herramientas de vigilancia tecnológica

Página dejada en blanco intencionadamente

Dominio: Alinear, Planificar y Organizar Objetivo de gestión: APO03 – Gestionar la Arquitectura Empresarial		Área prioritaria: Modelo Core de COBIT
Descripción Establecer una arquitectura común que consiste en capas de arquitectura de procesos de negocio, información, datos, aplicaciones y tecnología. Crear modelos y prácticas claves que describen las arquitecturas base y objetivo, en línea con la estrategia de I&T de la empresa. Definir los requisitos de taxonomía, estándares, directrices, procedimientos, plantillas y herramientas, y proporcionar un vínculo para estos componentes. Mejorar el alineamiento, aumentar la agilidad, mejorar la calidad de la información y generar ahorros potenciales de costes mediante iniciativas como la reutilización de componentes de bloques de construcción.		
Propósito Representar los diferentes bloques de construcción que conforman la empresa y sus interrelaciones, así como los principios que guían su diseño y evolución a lo largo del tiempo, para posibilitar una prestación estándar, responsable y eficiente de los objetivos operativos y estratégicos.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:		
Metas empresariales <ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG05 Cultura de servicio orientada al cliente • EG08 Optimización de la funcionalidad de procesos internos del negocio • EG12 Gestión de programas de transformación digital 	➔	Metas de alineamiento <ul style="list-style-type: none"> • AG06 Agilidad para convertir los requisitos del negocio en soluciones operativas AG08 Habilitar y dar soporte a procesos de negocio mediante la integración de aplicaciones y tecnología
Métricas modelo para metas empresariales EG01 <ol style="list-style-type: none"> Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente Porcentaje de productos y servicios que proporcionan una ventaja competitiva Plazo de comercialización para nuevos productos y servicios 		Métricas modelo para metas de alineamiento AG06 <ol style="list-style-type: none"> Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de I&T a los nuevos requisitos Plazo de comercialización promedio para servicios y aplicaciones nuevos relacionados con las I&T Tiempo promedio para convertir los objetivos estratégicos de I&T en iniciativas acordadas y aprobadas Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas
EG05 <ol style="list-style-type: none"> Número de interrupciones del servicio al cliente Porcentaje de partes interesadas del negocio satisfechas con que la prestación de servicios al cliente cumpla con los niveles de servicio acordados Número de quejas de los clientes Tendencia de los resultados de la encuesta de satisfacción al cliente 		AG08 <ol style="list-style-type: none"> Plazo para la ejecución de servicios y procesos empresariales Número de programas empresariales facilitados por I&T retrasados o que incurren en costes adicionales debido a problemas de integración tecnológica Número de cambios en los procesos de negocio que se deben aplazar o revisar debido a problemas de integración tecnológica Número de aplicaciones o infraestructuras críticas que operan en silos y no están integradas
EG08 <ol style="list-style-type: none"> Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarial Niveles de satisfacción de los clientes con las capacidades de prestación de servicios Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro 		
EG12 <ol style="list-style-type: none"> Número de programas ejecutados a tiempo y dentro del presupuesto Porcentaje de partes interesadas satisfechas con la ejecución del programa Porcentaje de programas de transformación del negocio suspendidos Porcentaje de programas de transformación del negocio con actualizaciones del estado notificadas regularmente 		

A. Componente: Proceso	
Práctica de gestión APO03.01 Desarrollar la visión de la arquitectura empresarial. La visión de la arquitectura ofrece una temprana descripción de alto nivel de la línea base y la arquitectura objetivo, cubriendo los dominios del negocio, la información, los datos, la aplicación y la tecnología. La visión de la arquitectura ofrece al patrocinador una herramienta clave para promover los beneficios de las capacidades propuestas a las partes interesadas de la empresa. La visión de la arquitectura describe cómo las nuevas capacidades (en línea con la estrategia y objetivos de I&T) cumplirán con las metas y los objetivos empresariales estratégicos, y abordará las preocupaciones de las partes interesadas cuando se implemente.	Métricas modelo <ol style="list-style-type: none"> Nivel de retroalimentación de los clientes sobre la arquitectura Grado en el que las arquitecturas base y objetivo cubren los dominios del negocio, la información, los datos, la aplicación y la tecnología.

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Identificar a las partes interesadas clave y sus preocupaciones/objetivos. Definir los requisitos clave de la empresa que deben abordarse, así como las visualizaciones de la arquitectura que deben desarrollarse para satisfacer los requisitos de las partes interesadas.	2
2. Identificar las metas y motivadores estratégicos de la empresa. Definir las limitaciones que deben abordarse, incluidas las limitaciones de la empresa en su conjunto y las específicas de los proyectos (como plazos, programación de actividades, recursos, etc.).	
3. Alinear los objetivos de la arquitectura con las prioridades del programa estratégico.	
4. Entender las capacidades y metas empresariales, e identificar a continuación opciones para conseguir dichas metas.	
5. Evaluar la preparación de la empresa para el cambio.	
6. Definir el alcance de la arquitectura de referencia y la arquitectura objetiva. Enumerar elementos que están dentro del alcance y aquellos que no lo están. (La arquitectura de referencia y objetiva no debe describirse con el mismo nivel de detalle.)	
7. Entender las metas y objetivos estratégicos empresariales actuales. Trabajar con el proceso de planificación estratégico para garantizar que se aprovechen las oportunidades de la arquitectura empresarial de I&T para el desarrollo del plan estratégico.	
8. Basándose en las preocupaciones de las partes interesadas, los requisitos de las capacidades empresariales, el alcance, restricciones y principios crear la visión de la arquitectura (es decir, la vista de alto nivel de las arquitecturas de referencia y objetiva).	
9. Confirmar y elaborar los principios de arquitectura, incluyendo los principios empresariales. Asegurar que todas las definiciones existentes estén actualizadas. Aclarar cualquier aspecto ambiguo.	3
10. Identificar el riesgo al cambio empresarial asociado con la visión de la arquitectura. Evaluar el nivel inicial de riesgo (como crítico, marginal o insignificante). Desarrollar una estrategia de mitigación para cada riesgo significativo.	
11. Desarrollar un caso de negocio de concepto de arquitectura empresarial y diseñar planes y la declaración del trabajo de la arquitectura. Asegurar la aprobación para iniciar un proyecto alineado e integrado con la estrategia empresarial.	
12. Definir las propuestas de valor, metas y métricas de la arquitectura objetivo.	4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.15 Program management (PM-7)
The Open Group Standard TOGAF version 9.2, 2018	6. Phase A: Architecture Vision
Práctica de gestión	Métricas modelo
AP003.02: Definir la arquitectura de referencia. La arquitectura de referencia describe las arquitecturas actuales y objetivo para los dominios de negocio, información, datos, aplicación y tecnología.	a. Fecha de la última actualización de las arquitecturas de dominio y/o federadas b. Número de excepciones a los estándares y referencias de la arquitectura solicitadas y concedidas
Actividades	Nivel de capacidad
1. Mantener un repositorio de arquitectura, que contiene estándares, componentes reutilizables, los artefactos de modelado, las relaciones, las dependencias y las visualizaciones, para permitir la uniformidad de la organización y mantenimiento de la arquitectura.	3
2. Seleccionar puntos de vista de referencia del repositorio de la arquitectura que permite al arquitecto demostrar cómo se abordan las preocupaciones de las partes interesadas en la arquitectura.	
3. Seleccionar modelos necesarios para respaldar la vista específica requerida, para cada punto de vista. Usar las herramientas y métodos seleccionados y el nivel de descomposición adecuado.	
4. Desarrollar las descripciones de dominio arquitectónico de referencia, usando el alcance y nivel de detalle necesario para respaldar la arquitectura objetivo y, hasta donde sea posible, identificando los bloques de construcción relevantes de la arquitectura del repositorio de arquitectura.	
5. Mantener un modelo de arquitectura de procesos, como parte de las descripciones de dominios de referencia y objetivo. Normalizar las descripciones y documentación de procesos. Definir los roles y responsabilidades de los responsables de la toma de decisiones del proceso, el Dueño del proceso, los usuarios del proceso, el equipo del proceso y otras partes interesadas del proceso que deberían involucrarse.	
6. Mantener un modelo de arquitectura de la información como parte de las descripciones de los dominios de referencia y objetivo, consistente con la estrategia empresarial para adquirir, almacenar y usar los datos de forma óptima para respaldar la toma de decisiones.	
7. Comprobar la consistencia y precisión interna de los modelos de arquitectura. Realizar un análisis de brecha entre la referencia y el objetivo. Priorizar las brechas y definir componentes nuevos o modificados que deben desarrollarse para la arquitectura objetivo. Resolver incompatibilidades, inconsistencias o conflictos dentro de la arquitectura objetivo.	
8. Conducir una revisión formal de las partes interesadas, comparando la arquitectura propuesta con la intención original del proyecto de la arquitectura y la declaración del trabajo de arquitectura.	
9. Finalizar las arquitecturas de los dominios del negocio, la información, los datos, las aplicaciones y la tecnología. Crear un documento de definición de la arquitectura.	

A. Componente: Proceso (cont.)		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Data Management Maturity Model, 2014		Platform and Architecture—Architectural Approach; Platform and Architecture—Data Integration
ITIL V3, 2011		Service Strategy, 5.4 IT service strategy and enterprise architecture
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018		3.1 Preparation (Task 9)
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.5 Configuration management (CM-8)
The Open Group Standard TOGAF versión 9.2, 2018		7. Phase B: Business Architecture; 8. Phase C: Information Systems Architectures; 9. Phase C: Information Systems Architectures Data Architecture; 10. Phase C: Information Systems Architectures Application Architecture; 11. Phase D: Technology Architecture
Práctica de gestión		Métricas modelo
AP003.03 Seleccionar oportunidades y soluciones. Racionalizar las brechas entre las arquitecturas de referencia y la objetivo, tomando tanto las perspectivas de negocio como técnicas, y agruparlas lógicamente en paquetes de trabajo del proyecto. Integrar el proyecto con todos los programas de inversión habilitados por I&T para asegurarse de que las iniciativas de la arquitectura estén alineadas y permitan estas iniciativas como parte de un cambio empresarial general. Hacer de este un esfuerzo colaborativo con las partes interesadas clave del negocio y de TI para evaluar la disposición de transformación de la empresa, e identificar oportunidades, soluciones y todas las restricciones de implementación.		a. Número de brechas identificadas en los modelos empresariales de los dominios de arquitectura del negocio, la información, los datos, la aplicación y la tecnología b. Porcentaje de partes interesadas clave del negocio y de TI para evaluar la disposición de transformación de la empresa, e identificar oportunidades, soluciones y todas las restricciones de implementación
Actividades		Nivel de capacidad
1. Determinar y confirmar atributos de cambios empresariales clave. Considerar la cultura de la empresa, el impacto potencial de la cultura en la implementación de la arquitectura y las capacidades de transición de la empresa.		3
2. Identificar cualquier factor empresarial que limitaría la secuencia de implementación. Incluir una revisión empresarial y de línea estratégica de negocio de la empresa y de los planes de negocio, . Considerar la madurez de la arquitectura empresarial actual.		
3. Revisar y consolidar los resultados del análisis de recha entre las arquitecturas de referencia y la objetivo. Evaluar las implicaciones con respecto a posibles soluciones, oportunidades, interdependencias y alineamiento con los programas actuales habilitados por I&T.		
4. Evaluar los requisitos, brechas, soluciones y otros factores para identificar un conjunto mínimo de requisitos funcionales cuya integración en paquetes de trabajo llevarían a una implementación más eficaz y eficiente de la arquitectura objetivo.		
5. Conciliar los requisitos consolidados con posibles soluciones.		
6. Perfeccionar las dependencias iniciales e identificar las restricciones de los planes de implementación y migración. Compilar un informe de análisis de dependencias.		
7. Confirmar la disposición de la empresa a la transformación empresarial y el riesgo asociado a ella.		
8. Formular una estrategia de alto nivel para la implementación y la migración. Implementar la arquitectura objetivo (e implementar cualquier arquitectura de transición) conforme a la estrategia, objetivos y plazos de la empresa en su conjunto.		
9. Identificar y agrupar paquetes de trabajo importantes en un conjunto coherente de programas y proyectos, relacionados con la dirección y el enfoque de la implementación estratégica empresarial.		
10. Desarrolla arquitecturas de transición en las que el alcance del cambio requerido por la arquitectura necesita un enfoque incremental.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Data Management Maturity Model, 2014		Platform and Architecture—Architectural Approach; Platform and Architecture—Data Integration
The Open Group Standard TOGAF versión 9.2, 2018		12. Phase E: Opportunities and Solutions

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
AP003.04 Definir la implementación de la arquitectura. Crear una aplicación viable y un plan de migración en alineación con los portafolios de programas y proyectos. Asegurarse que el plan esté estrechamente coordinado para garantizar que se brinde valor y que los recursos necesarios estén disponibles para completar el trabajo necesario.		a. Definición clara de los requisitos de gobierno para la implementación de la arquitectura b. Porcentaje de partes interesadas conocedoras de la implementación y migración de la arquitectura
Actividades		Nivel de capacidad
1. Establecer los elementos requeridos para el plan de implementación y migración como parte de la planificación de programas y proyectos. Asegurar que el plan está alineado con los requisitos de los responsables de toma de decisiones relevantes.		3
2. Confirmar los incrementos y las fases de la arquitectura de transición. Actualizar el documento de definición de la arquitectura		
3. Definir y completar la implementación de la arquitectura y el plan de migración, incluidos los requisitos de gobierno relevantes. Integrar el plan, actividades y dependencias en el programa y la planificación del proyecto.		
4. Comunicar la hoja de ruta de la arquitectura definida a las partes interesadas relevantes. Informar a las partes interesadas acerca de la definición de la arquitectura objetivo, las directrices y principios de arquitectura, el portafolio de servicios, etc.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Data Management Maturity Model, 2014		Platform and Architecture—Architectural Approach; Platform and Architecture—Data Integration
The Open Group Standard TOGAF versión 9.2, 2018		13. Phase F: Migration Planning
Práctica de gestión		Métricas modelo
AP003.05 Proporcionar servicios de arquitectura empresarial. Proporcionar servicios de arquitectura empresarial dentro de la empresa que incluyen guía y supervisión de proyectos de implementación, formalización de maneras de trabajar a través de contratos de arquitectura, y medición y comunicación del valor agregado y supervisión del cumplimiento.		a. Nivel de retroalimentación del cliente sobre los servicios de arquitectura b. Porcentaje de proyectos que utilizan el marco y la metodología para reutilizar componentes definidos c. Porcentaje de proyectos que utilizan servicios de arquitectura empresarial d. Los beneficios del proyecto obtenidos que pueden atribuirse a la participación de la arquitectura (p. ej., reducción de costes mediante la reutilización)
Actividades		Nivel de capacidad
1. Confirmar el alcance y las prioridades y proporcionar directrices para desarrollar e implementar soluciones (p. ej., usando la arquitectura orientada a los servicios).		3
2. Gestionar los requisitos de la arquitectura empresarial y respaldar el negocio y TI con consejos e información experta sobre principios, modelos y bloques de construcción. Garantizar que las nuevas implementaciones (como cambios a la arquitectura actual) están alineadas con los principios y requisitos de la arquitectura empresarial.		
3. Gestionar el portafolio de servicios de la arquitectura empresarial y garantizar el alineamiento con los objetivos estratégicos y el desarrollo de soluciones.		
4. Identificar las prioridades de la arquitectura empresarial. Alinear las prioridades con los factores que proporcionan valor. Definir y recopilar métricas de valor y medir y comunicar el valor de la arquitectura empresarial.		4
5. Establecer un foro de tecnología para proporcionar directrices de arquitectura, asesorar proyectos y guiar la selección de tecnología. Medir el cumplimiento con los estándares y directrices, incluido el cumplimiento con los requisitos externos y con la relevancia empresarial interna.		5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Data Management Maturity Model, 2014		Platform and Architecture—Architectural Standards
ITIL V3, 2011		Service Design, 3.9 Service Oriented Architecture
The Open Group Standard TOGAF versión 9.2, 2018		14. Phase G: Implementation Governance; 15. Phase H: Architecture Change Management

B. Componente: Estructuras organizativas									
							Director de operaciones	Director de TI	Director de tecnología
							Director de tecnologías digitales	Consejo de gobierno de I&T	Consejo de arquitectura
							Función de gestión de datos		Jefe de arquitectura
Práctica clave de gestión									
APO03.01 Desarrollar la visión de arquitectura empresarial.								R	R
APO03.02 Definir la arquitectura de referencia.								R	R
APO03.03 Seleccionar oportunidades y soluciones.								R	R
APO03.04 Definir la implementación de la arquitectura.							R	R	R
APO03.05 Proporcionar servicios de arquitectura empresarial.							R	R	R
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)							Referencia específica		
The Open Group Standard TOGAF versión 9.2, 2018							41. Architecture Board		

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
APO03.01 Desarrollar la visión de arquitectura empresarial.	APO02.05	Hoja de ruta estratégica	Alcance definido para la arquitectura	APO02.05
	EDM04.01	Principios directrices para la arquitectura empresarial	Caso de negocio y propuesta de valor del concepto de arquitectura	APO02.05; APO05.02
	Fuera de COBIT	Estrategia empresarial	Principios de arquitectura	BAI02.01; BAI03.01; BAI03.02
APO03.02 Definir la arquitectura de referencia.	APO01.04	• Definición de la estructura organizativa y sus funciones • Directrices operativas de la empresa	Modelo de arquitectura de procesos	APO01.04
	APO01.06	• Evaluación de opciones para la organización de TI • Ubicación operativa de la función de TI definida	Modelo de arquitectura de la información	APO02.05; APO14.03; BAI02.01; BAI03.02; DSS05.03; DSS05.04; DSS05.06

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
AP003.02 Definir la arquitectura de referencia. (cont.)	De	Descripción	Descripción	A
	AP001.07	Directrices de clasificación de datos	Descripciones de dominios de referencia y definición de arquitectura	AP013.02; BAI02.01; BAI03.01; BAI03.02; BAI03.12
	AP014.01	Estrategia de gestión de datos		
	AP014.03	Documentación de metadatos		
	Fuera de COBIT	Estrategia empresarial		
AP003.03 Seleccionar oportunidades y soluciones.	AP002.03	Cambios propuestos a la arquitectura empresarial	Arquitectura de transición	AP002.05
	Fuera de COBIT	<ul style="list-style-type: none"> • Motivadores empresariales • Estrategias empresariales 		
AP003.04 Definir la implementación de la arquitectura.			Descripciones de la fase de implementación	BAI01.01; BAI01.02; BAI11.01
			Requisitos del gobierno de arquitectura	BAI01.01; BAI11.01
			Requisitos de recursos	BAI01.02
AP003.05 Proporcionar servicios de arquitectura empresarial.			Directrices para el desarrollo de soluciones	BAI02.01; BAI02.02; BAI03.02; BAI03.12
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
National Institute of Standards and Technology Special Publication 800-37, Revisión 2, septiembre de 2017		3.1 Preparation (Task 9): Inputs and Outputs		
The Open Group Standard TOGAF version 9.2, 2018		6. Phase A: Architecture Vision: Inputs and Outputs; 7. Phase B: Business Architecture: Inputs and Outputs; 9. Phase C: Information Systems Architectures Data Architecture: Inputs and Outputs; 10. Information Systems Architectures Application Architecture: Inputs and Outputs; 11. Phase D: Technology Architecture: Inputs and Outputs; 12. Phase E: Opportunities and Solutions: Inputs and Outputs; 13. Phase F: Migration Planning: Inputs and Outputs; 14. Phase G: Implementation Governance: Inputs and Outputs; 15. Phase H: Architecture Change Management: Inputs and Outputs		

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Diseño de arquitectura	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.5. Architecture Design
Análisis de datos	Skills Framework for the Information Age V6, 2015	DTAN
Arquitectura empresarial y del negocio	Skills Framework for the Information Age V6, 2015	STPL
Planificación de productos/servicios	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.4. Product/Service Planning
Arquitectura solución	Skills Framework for the Information Age V6, 2015	ARCH

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Principios de arquitectura	Define los principios generales para informar reglas y 20. Directrices de los principios de arquitectura para procesos, procedimientos, capas de arquitectura y uso e interconexión general de los recursos y activos de I&T. Señala los principios de la arquitectura para mejorar la toma de decisiones. Asegura un alineamiento de la arquitectura actual y objetivo con los objetivos y estrategia empresarial.	The Open Group Standard TOGAF versión 9.2, 2018	20. Architecture Principles

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Crear un entorno que el que la dirección entienda las necesidades de la arquitectura con respecto a las metas y objetivos del negocio. Impulsar una práctica eficaz de la arquitectura empresarial en toda la organización (no solo para los arquitectos de la empresa). Garantizar un enfoque holístico que vincule los componentes perfectamente (por ej. dejar de contar con equipos dedicados de especialistas en aplicaciones).		

G. Componente: Servicios, infraestructura y aplicaciones	
Repositorio de arquitectura	

Página dejada en blanco intencionadamente

Dominio: Alinear, Planificar y Organizar		Área prioritaria: Modelo Core de COBIT	
Objetivo de gestión: APO04 – Gestionar la innovación			
Descripción			
Mantener una concienciación de I&T y tendencias de servicio relacionadas y monitorizar las tendencias tecnológicas emergentes. Identificar de forma proactiva oportunidades de innovación y planificar cómo beneficiarse de la innovación en relación con las necesidades empresariales y la estrategia de I&T. Analizar qué oportunidades de mejora o innovación empresarial pueden crearse mediante tecnologías emergentes, servicios o innovación empresarial habilitada por I&T, así como a través de tecnologías ya establecidas y por la innovación de procesos empresariales y de TI. Influir en la planificación estratégica y las decisiones de arquitectura empresarial.			
Propósito			
Lograr ventajas competitivas, innovación empresarial, una mejor experiencia del cliente y una mayor eficacia y eficiencia operativa con el aprovechamiento de los desarrollos de I&T y tecnologías emergentes.			
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:			
Metas empresariales		➔	Metas de alineamiento
• EG01 Portafolio de productos y servicios competitivos • EG13 Innovación de producto y del negocio			• AG06 Agilidad para convertir los requisitos del negocio en soluciones operativas • AG13 Conocimiento, habilidad e iniciativas para la innovación empresarial
Métricas modelo para metas empresariales			Métricas modelo para metas de alineamiento
EG01 a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios			AG06 a. Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de I&T a los nuevos requisitos b. Tiempo promedio de comercialización para nuevos servicios y aplicaciones relacionados con I&T c. Tiempo promedio para convertir los objetivos estratégicos de I&T en iniciativas acordadas y aprobadas d. Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas
EG13 a. Nivel de conocimiento y comprensión de las oportunidades de innovación del negocio b. Satisfacción de las partes interesadas con los niveles de habilidades e ideas sobre innovación y productos c. Número de iniciativas de productos y servicios aprobadas como resultado de ideas innovadoras			AG13 a. Nivel de conocimiento y comprensión de los ejecutivos del negocio sobre las posibilidades de innovación de las I&T b. Número de iniciativas aprobadas como resultado de ideas innovadoras de I&T c. Número de campeones en innovación reconocidos/premiados
A. Componente: Proceso			
Práctica de gestión		Métricas modelo	
APO04.01 Crear un entorno favorable que conduzca a la innovación. Crear un entorno que propicie la innovación, considerando métodos como la cultura, las recompensas, la colaboración, los foros de tecnología y los mecanismos para promover y capturar las ideas de los empleados.		a. Percepciones y retroalimentación de las partes interesadas de la empresa respecto a la innovación en I&T b. Inclusión de objetivos relacionados con la innovación o tecnología emergente en los objetivos de rendimiento para el personal relevante	
Actividades			Nivel de capacidad
1. Crear un plan de innovación que incluya el apetito al riesgo, un presupuesto propuesto para iniciativas de innovación y objetivos de innovación.			2
2. Proporcionar una infraestructura que pueda ser un componente de gobierno para la innovación (como herramientas de colaboración para mejorar el trabajo entre sitios geográficos y/o divisiones).			
3. Mantener un personal que gracias a programas presente ideas innovadoras y cree una estructura de toma de decisiones adecuada para evaluar las ideas y sacarlas adelante.			3
4. Fomentar las ideas innovadoras de los clientes, proveedores y socios empresariales.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin Documentación relacionada para esta práctica de gestión			

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
AP004.02 Mantener un entendimiento del entorno de la empresa. Trabajar con las partes interesadas pertinentes para entender sus desafíos. Mantener una comprensión adecuada de la estrategia de la empresa y del entorno competitivo y de otras restricciones, de forma que se puedan identificar las oportunidades habilitadas por las nuevas tecnologías.		a. Porcentaje de iniciativas implementadas con un claro vínculo a un objetivo empresarial b. Porcentaje de oportunidades habilitadas por nuevas tecnologías identificadas
Actividades		Nivel de capacidad
1. Mantener un conocimiento de los motivadores empresariales y de industria, la estrategia empresarial y de I&T y las operaciones empresariales y retos actuales. Aplicar el entendimiento para identificar posibles tecnologías de valor agregado e innovar en I&T		2
2. Conducir reuniones regulares con unidades de negocio, divisiones y/u otras partes interesadas para entender los problemas empresariales actuales, los cuellos de botella de los procesos y otras limitaciones, cuando las tecnologías emergentes o la innovación de I&T pueden crear oportunidades.		3
3. Entender los parámetros de inversión empresariales para la innovación y nuevas tecnologías con el fin de desarrollar tecnologías adecuadas.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
AP004.03 Monitorizar explorar el entorno tecnológico. Implementar una vigilancia tecnológica para monitorizar y explorar sistemáticamente el entorno externo de la empresa para identificar las tecnologías emergentes que tengan el potencial de crear valor (p. ej., lograr la estrategia empresarial, optimizar costes, evitar la obsolescencia y habilitar de mejor manera los procesos empresariales y de I&T). Monitorizar el mercado, el entorno competitivo, los sectores de la industria y las tendencias legales y regulatorias para poder analizar las tecnologías emergentes o las ideas de innovación en el contexto empresarial.		a. Frecuencia de la investigación y exploración del entorno realizadas para identificar ideas y tendencias innovadoras b. Porcentaje de partes interesadas satisfechas con los esfuerzos para monitorizar el mercado, el entorno competitivo, los sectores de la industria y las tendencias legales y regulatorias para poder analizar las tecnologías emergentes o las ideas de innovación en el contexto empresarial.
Actividades		Nivel de capacidad
1. Entender el apetito y potencial de la empresa en cuanto a innovación tecnológica. Centrar los esfuerzos de concienciación en las innovaciones tecnológicas más oportunas.		2
2. Establecer un proceso de vigilancia tecnológica e investigar y explorar el entorno externo, incluidos sitios webs, revistas y conferencias adecuadas, para identificar las tecnologías emergentes y su valor potencial para la empresa.		
3. Consultar a terceros expertos conforme sea necesario para confirmar la investigación o suministrar información sobre tecnologías emergentes.		
4. Captar las ideas innovadoras del personal de I&T y revisar su posible implementación.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
AP004.04 Evaluar el potencial de las tecnologías emergentes y las ideas de innovación. Analizar las tecnologías emergentes identificadas y/u otras sugerencias de innovación en I&T para comprender su potencial empresarial. Trabajar con las partes interesadas para validar las suposiciones sobre el potencial de nuevas tecnologías e innovación.		a. Porcentaje de iniciativas implementadas que logran los beneficios previstos b. Porcentaje de iniciativas de pruebas de concepto exitosas para poner a prueba tecnologías emergentes u otras ideas de innovación
Actividades		Nivel de capacidad
1. Evaluar las tecnologías identificadas, considerando aspectos como el tiempo para alcanzar la madurez, el riesgo inherente (incluidas las posibles implicaciones legales), su encaje con la arquitectura empresarial y el potencial de valor, en línea con la estrategia empresarial y de I&T.		2
2. Identificar asuntos que pudieran ser resueltos o validado a través de una iniciativa de prueba de concepto.		3
3. Alcance de la iniciativa de prueba de concepto, incluidos los resultados deseados, el presupuesto requerido, los plazos y las responsabilidades.		
4. Obtener la aprobación para la iniciativa de prueba de concepto.		
5. Conducir iniciativas de prueba de concepto para poner a prueba tecnologías emergentes u otras ideas de innovación. Identificar problemas y determinar si la implementación o despliegue debería considerarse basada en la factibilidad y el ROI potencial.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
AP004.05 Recomendar iniciativas adicionales apropiadas . Evaluar y monitorizar los resultados de las iniciativas de prueba de concepto y, si son favorables, generar recomendaciones para más iniciativas. Obtener el apoyo de las partes interesadas.		a. Número de iniciativas de prueba de concepto evaluadas y aprobadas para su posterior implementación b. Número de iniciativas de prueba de concepto que han sido apalancadas con la inversión real.
Actividades		Nivel de capacidad
1. Documentar los resultados de la prueba de concepto, incluidas directrices y recomendaciones de tendencias y programas de innovación		3
2. Comunicar oportunidades de innovación viables en la estrategia de I&T y los procesos de arquitectura empresarial.		
3. Analizar y comunicar las razones de iniciativas de pruebas de concepto rechazadas.		
4. Hacer un seguimiento de las iniciativas de prueba de concepto para medir la inversión real.		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
AP004.06 Supervisar la implementación y el uso de la innovación. Supervisar la implementación y el uso de las tecnologías emergentes y las innovaciones durante la adopción, integración, y todo el ciclo de vida económico para garantizar que se obtengan los beneficios prometidos y para identificar las lecciones aprendidas.		a. Aumentar la cuota de mercado o competitividad debido a innovaciones b. Número de lecciones aprendidas y oportunidades de mejora captadas para su uso futuro
Actividades		Nivel de capacidad
1. Captar las lecciones aprendidas y las oportunidades de mejora.		3
2. Garantizar que las iniciativas de innovación estén alineadas con la estrategia empresarial y de I&T. Monitorizar continuamente el alineamiento. Ajustar el plan de innovación, si fuera necesario.		
3. Evaluar nueva tecnología o innovaciones de I&T implementadas como parte de la estrategia de I&T y el desarrollo de la arquitectura empresarial. Evaluar el nivel de adopción durante la gestión de iniciativas del programa.		4
4. Identificar y evaluar el valor potencial de la innovación.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		

B. Componente: Estructuras organizativas													
	Comité Ejecutivo	Director de TI	Director de tecnología	Director de tecnologías digitales	Dueños del proceso de negocio	Función de gestión de datos	Director de Recursos Humanos	Gestor de relaciones	Jefe de arquitectura	Jefe de desarrollo	Jefe de operaciones de TI	Gestor de Servicios	Gestor de seguridad de la información
Práctica clave de gestión													
AP004.01 Crear un entorno favorable que conduzca a la innovación.	A	R	R	R	R	R	R		R	R	R	R	R
AP004.02 Mantener un entendimiento del entorno de la empresa.	A	R	R	R	R	R		R	R	R	R	R	R
AP004.03 Monitorizar y explorar el entorno tecnológico.	A	R	R	R	R	R			R	R	R	R	R
AP004.04 Evaluar el potencial de las tecnologías emergentes y las ideas de innovación.	A	R	R	R	R	R			R	R	R	R	R
AP004.05 Recomendar iniciativas adicionales apropiadas .	A	R	R	R	R	R			R	R	R	R	R
AP004.06 Supervisar la implementación y el uso de la innovación.	A	R	R	R	R	R			R	R	R	R	R
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica												
Sin Documentación relacionada para este componente.													

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
APO04.01 Crear un entorno favorable que conduzca a la innovación.	De	Descripción	Descripción	A
	EDM03.01	Guía del apetito de riesgo	Programa de reconocimiento y recompensas	AP007.04
			Plan de innovación	Interna
APO04.02 Mantener un entendimiento del entorno de la empresa.	Fuera de COBIT	Estrategia empresarial y análisis análisis de fortalezas, oportunidades, debilidades, amenazas (FODA)	Oportunidades de innovación relacionadas con los motivadores empresariales	AP002.01
APO04.03 Monitorizar y explorar el entorno tecnológico.	Fuera de COBIT	Tecnologías emergentes	Análisis de investigación de las posibilidades de innovación	BAI03.01
APO04.04 Evaluar el potencial de las tecnologías emergentes y las ideas de innovación.			Alcance de la prueba de conceptos y descripción del caso de negocio	AP005.02; AP006.02
			Evaluación de las iniciativas de innovación	BAI03.01
			Comprobar resultados de iniciativas de prueba de concepto	Interna
APO04.05 Recomendar iniciativas adicionales apropiadas .			Análisis de iniciativas rechazadas	AP002.03; BAI03.08
			Resultados y recomendación de iniciativas de prueba de concepto	AP002.03; BAI03.09
APO04.06 Supervisar la implementación y el uso de la innovación.			Evaluaciones del uso de estrategias innovadoras	AP002.04; BAI03.02
			Evaluación de los beneficios de innovación	AP005.03
			Ajuste de los planes de innovación	Interna
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin Documentación relacionada para este componente.				


D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Desarrollo de plan de negocio	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.3. Plan de negocio Desarrollo
Monitorización de tecnologías emergentes	Skills Framework for the Information Age V6, 2015	EMRG
Innovación	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.9. Innovación
Innovation	Skills Framework for the Information Age V6, 2015	INOV
Investigación	Skills Framework for the Information Age V6, 2015	RSCH
Monitorización de tendencias tecnológicas	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.7. Tendencias tecnológicas Supervisión

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Principios de innovación	Define principios generales garantizando que las ideas nuevas/innovadoras se evalúan de forma exhaustiva a la hora de definir nuevas metas y decisiones estratégicas.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Crear un entorno propicio para la innovación, al mantener las iniciativas relevantes de RR. HH., como el reconocimiento por la innovación y los programas de recompensas, la rotación adecuada de puestos de trabajo, y el tiempo opcional para la experimentación. Asegurar una colaboración y coordinación estrechas de las iniciativas en toda la organización.		

G. Componente: Servicios, infraestructuras y aplicaciones	
<ul style="list-style-type: none"> • Plataformas de colaboración • Benchmarks de la industria • Servicios y herramientas de vigilancia tecnológica 	

Página dejada en blanco intencionadamente

Dominio: Alinear, Planificar y Organizar Objetivo de gestión: APO05 – Gestionar el portafolio		Área prioritaria: Modelo Core de COBIT	
Descripción			
Ejecutar la dirección estratégica establecida para las inversiones, en línea con la visión de la arquitectura empresarial y la hoja de ruta de I&T. Considerar las diferentes categorías de inversiones y las limitaciones de recursos y financiación. Evaluar, priorizar y equilibrar los programas y servicios, gestionando la demanda dentro de las limitaciones de recursos y financiamiento, basándose en su alineación con los objetivos estratégicos, el valor y el riesgo de la empresa. Mover los programas seleccionados al portafolio de productos o servicios activa para su ejecución. Supervisar el rendimiento del portafolio general de productos y servicios, y programas, proponiendo ajustes según sea necesario en respuesta al rendimiento del programa, producto o servicio, o cambiando las prioridades de la empresa.			
Propósito			
Optimizar el rendimiento del portafolio general de programas en respuesta al rendimiento individual de programas, productos y servicios y a las cambiantes prioridades y demandas de la empresa.			
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:			
Metas empresariales			Metas de alineamiento
<ul style="list-style-type: none">• EG01 Portafolio de productos y servicios competitivos• EG08 Optimización de la funcionalidad de procesos internos del negocio• EG12 Gestión de programas de transformación digital			<ul style="list-style-type: none">• AG03 Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T• AG05 Prestación de servicios de I&T conforme a los requisitos del negocio
Métricas modelo para metas empresariales			Métricas modelo para metas de alineamiento
EG01 <ul style="list-style-type: none">a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercadob. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del clientec. Porcentaje de productos y servicios que proporcionan una ventaja competitivad. Plazo de comercialización para nuevos productos y servicios			AG03 <ul style="list-style-type: none">a. Porcentaje de inversiones posibilitadas por I&T en las que los beneficios previstos se cumplen o excedenb. Porcentaje de servicios de I&T para los que se han logrado los beneficios esperados (indicados en los acuerdos de nivel de servicio)
EG08 <ul style="list-style-type: none">a. Niveles de satisfacción de la junta directiva y la dirección ejecutiva con las capacidades del proceso del negociob. Niveles de satisfacción de los clientes con las capacidades de prestación de serviciosc. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro			AG05 <ul style="list-style-type: none">a. Porcentaje de partes interesadas del negocio satisfechas con que la prestación de servicios de I&T cumpla con los niveles de servicio acordadosb. Número de interrupciones del negocio debido a incidentes de servicios de I&Tc. Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de I&T
EG12 <ul style="list-style-type: none">a. Número de programas ejecutados a tiempo y dentro del presupuestob. Porcentaje de partes interesadas satisfechas con la ejecución del programac. Porcentaje de programas de transformación del negocio suspendidosd. Porcentaje de programas de transformación del negocio con actualizaciones del estado notificadas regularmente			

A. Componente: Proceso			
Práctica de gestión		Métricas modelo	
APO05.01 Determinar la disponibilidad y las fuentes de fondos. Determinar posibles fuentes de fondos, diferentes opciones de financiamiento y las implicaciones de las fuentes de financiamiento en las expectativas de retorno de inversión.		a. Proporción entre los fondos asignados y los fondos utilizados b. Proporción entre los ingresos retenidos y los fondos asignados	
Actividades			Nivel de capacidad
1. Entender la disponibilidad y el compromiso actual de fondos, el gasto real aprobado y el gasto real hasta la fecha.			2
2. Identificar opciones de financiación adicional para inversiones facilitadas por I&T, considerando fuentes internas y externas.			
3. Determinar las implicaciones de las fuentes de financiación en las expectativas de retorno de inversión.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin Documentación relacionada para esta práctica de gestión			

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
APO05.02 Evaluar y seleccionar programas para financiar. Basándose en los requisitos generales de la mezcla general del portafolio de inversión y el plan estratégico y la hoja de ruta de I&T, evaluar y establecer prioridades de los casos de negocio del programa y tomar decisiones sobre las propuestas de inversión. Asignar fondos e iniciar los programas.		a. Porcentaje de proyectos en el portafolio de proyectos de I&T que pueden atribuirse directamente a la estrategia de I&T b. Porcentaje de unidades de negocio involucradas en el proceso de evaluación y priorización
Actividades		Nivel de capacidad
1. Identificar y clasificar las oportunidades de inversión en línea con las categorías del portafolio de inversiones. Concretar el/los resultado(s) empresariales esperados, las iniciativas requeridas para lograr el/los resultado(s) esperados, los costes de alto nivel, las dependencias y el riesgo. Concretar la metodología para medir los resultados, el coste y el riesgo.		2
2. Realizar una evaluación detallada de todos los casos de negocio del programa. Evaluar el alineamiento estratégico, el beneficio empresarial, el riesgo y la disponibilidad de recursos.		3
3. Evaluar el impacto de añadir posibles programas al conjunto del portafolio de inversiones, incluidos cambios que pudieran ser requeridos por otros programas.		
4. Decidir qué programas candidatos deberían trasladarse al portafolio de inversiones activas. Decidir si los programas rechazados deberían conservarse para su consideración futura o dotarse de financiación inicial para determinar si el caso de negocio puede mejorarse o descartarse.		
5. Determinar los hitos requeridos para cada ciclo de vida económico completo del programa seleccionado. Asignar y reservar la financiación total de programa total por hito. Trasladar el programa al portafolio activo de inversión.		
6. Establecer procedimientos para comunicar el coste, el beneficio y aspectos de portafolios relacionados con los riesgos, para su consideración en la priorización del presupuesto, la gestión de costes y los procesos de gestión de beneficios.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
PMBOK Guide Sixth Edition, 2017		Part 1: 1.2.3 Relationship of project, program, portfolio and operations management
Práctica de gestión		Métricas modelo
APO05.03 Monitorizar, optimizar e informar sobre el rendimiento del portafolio de inversión. Monitorizar y optimizar de forma periódica el rendimiento del portafolio de inversión y los programas individuales durante todo el ciclo de vida de las inversiones. Garantizar un seguimiento continuo al alineamiento del portafolio con la estrategia de I&T.		a. Tendencias en ROI de las iniciativas incluidas en la estrategia de I&T b. Nivel de satisfacción con los informes de monitorización del portafolio c. Porcentaje de programas alineados con los requisitos de negocio de la empresa
Actividades		Nivel de capacidad
1. Revisar regularmente el portafolio para identificar y explotar sinergias, eliminar la duplicación entre programas, e identificar y mitigar el riesgo.		3
2. Cuando se producen los cambios, reevaluar y repriorizar el portafolio para garantizar el alineamiento con la estrategia empresarial y de I&T. Mantener la combinación de inversiones objetivo para que el portafolio optimice el valor total. Los programas podrían cambiar, postergarse o retirarse, y nuevos programas podrían iniciarse, para reequilibrar y optimizar el portafolio.		
3. Ajustar los objetivos de la empresa, las estimaciones, los presupuesto y, de ser necesario, el grado de monitorización para reflejar los gastos y beneficios empresariales atribuibles a programas del portafolio de inversiones activas. Cargar los gastos del programa. Establecer procesos presupuestarios flexibles para que proyectos prometedores consigan los recursos para escalar rápidamente.		
4. Desarrollar métricas para medir la contribución de I&T a la empresa. Establecer objetivos de rendimiento adecuado que reflejen los objetivos requeridos de capacidad empresarial y de I&T. Usar los consejos de expertos externos y realizar benchmark de datos para desarrollar métricas.		4
5. Proporcionar una vista exacta del rendimiento del portafolio de inversión a todas las partes interesadas.		
6. Proporcionar informes para revisión de los altos directivos sobre el progreso de la empresa hacia los objetivos identificados, que incluyan que debe aún gastarse y lograr en los plazos dados.		
7. En la monitorización regular del rendimiento , incluir información sobre el grado de consecución de los objetivos planificados, el riesgo mitigado, las capacidades creadas, los entregables obtenidos y los objetivos de desempeño alcanzados.		
8. Identificar desviaciones del presupuesto vs. gasto real y ROI esperado de inversiones.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		

A. Componente: Proceso (cont.)			
Práctica de gestión		Métricas modelo	
APO05.04 Mantener los portafolios. Mantener los portafolios de los programas y proyectos de inversión, productos y servicios de I&T y los activos de I&T.		a. Números de programas y proyectos finalizados b. Tiempo transcurrido desde la última actualización del portafolio de servicios	
Actividades			Nivel de capacidad
1. Crear y mantener portafolios de programas de inversión habilitados por I&T, servicios prestados por I&T y activos de I&T, que forman la base para el presupuesto de I&T actual y respaldan los planes tácticos y estratégicos de I&T.			3
2. Trabajar con gestores de servicios para conservar el portafolio de servicios. Trabajar con gestores de operaciones, gestores de producto y arquitectos para conservar los portafolios de activos. Priorizar los portafolios para respaldar las decisiones de inversión.			
3. Retirar un programa del portafolio de inversiones activas cuando los beneficios empresariales deseados se han alcanzado o cuando está claro que los beneficios no se alcanzarán dentro de los criterios de valor establecidos para el programa.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
ITIL V3, 2011		Service Strategy, 4.2 Service portfolio management	
Práctica de gestión		Métricas modelo	
APO05.05 Gestionar el logro de beneficios. Monitorizar los beneficios de ofrecer y mantener productos de I&T apropiados, basándose en el caso de negocio acordado y vigente.		a. Porcentaje de cambios del programa de inversiones reflejados en los portafolios relevantes de I&T b. Porcentaje de partes interesadas satisfechas con los esfuerzos para monitorizar los beneficios de ofrecer y mantener productos de I&T apropiados, basándose en el caso de negocio acordado y vigente.	
Actividades			Nivel de capacidad
1. Usar las métricas acordadas y hacer un seguimiento de cómo se alcanzan los beneficios, cómo evolucionan a lo largo del ciclo de vida de programas y proyectos, cómo se obtienen de productos y servicios de I&T, y cómo se comparan con benchmarks internos y de la industria. Comunicar resultados a las partes interesadas			4
2. Implementar la acción correctiva cuando los beneficios logrados se desvían significativamente de los beneficios esperados. Actualizar el caso de negocio para nuevas iniciativas e implementar procesos de negocio y mejoras de servicio, conforme sean necesarias.			5
3. Considerar la obtención de ayuda de expertos externos, líderes de la industria y datos de benchmarking comparativos para poner a prueba y mejorar las métricas y objetivos.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin Documentación relacionada para esta práctica de gestión			

B. Componente: Estructuras organizativas											
Práctica clave de gestión	Director general financiero	Director de TI	Director de tecnología	Director de tecnologías digitales	Consejo de gobierno de I&T	Dueños del proceso de negocio	Gestor de portafolio	Gestor de programas	Oficina de gestión de proyectos		
	AP005.01 Determinar la disponibilidad y las fuentes de fondos.	R	R			A		R			
	AP005.02 Evaluar y seleccionar programas para financiar.	R	R	R	R	A		R	R		
	AP005.03 Monitorizar, optimizar e informar sobre el rendimiento del portafolio de inversión.		R	R	R	A		R	R		
	AP005.04 Mantener los portafolios.		R	R	R	A		R	R	R	
	AP005.05 Gestionar el logro de beneficios.	R	R	R	R	A	R	R	R		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica									
Sin Documentación relacionada para este componente.											

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
AP005.01 Determinar la disponibilidad y las fuentes de fondos.	De	Descripción	Descripción	A
			Expectativas de retorno de inversión	AP002.04; AP006.02; BAI01.06; EDM02.02
			Opciones de financiación	AP002.05

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
APO05.02 Evaluar y seleccionar programas para financiar.	De	Descripción	Descripción	A
	APO03.01	Caso de negocio y propuesta de valor del concepto de arquitectura	Caso de negocio del programa	APO06.02; BAI01.02
	APO04.04	Alcance de la prueba de conceptos y descripción del caso de negocio	Evaluaciones de casos de negocio	APO06.02; BAI01.06
	APO06.02	• Asignaciones de presupuesto • Priorización y clasificación de las iniciativas de I&T	Programas seleccionados con hitos de retorno de inversión (ROI)	BAI01.04; EDM02.02
	APO06.03	• Presupuesto de TI • Comunicaciones del presupuesto		
	APO09.01	Brechas identificadas en servicios de TI prestados a la empresa		
	APO09.03	Acuerdos de nivel de servicio (SLA)		
	APO13.02	Casos de negocio de seguridad de la información		
	BAI01.02	• Plan de obtención de beneficios del programa • Caso de negocio del concepto del programa • Mandato e resumen del programa		
	EDM02.02	• Evaluación del alineamiento estratégico • Evaluación de los portafolios de inversiones y servicios		
	EDM02.03	Tipos y criterios de inversión		
	APO05.03 Monitorizar, optimizar e informar sobre el rendimiento del portafolio de inversión.	APO04.06	Evaluación de los beneficios de innovación	Informes de rendimiento del portafolio de inversiones
BAI01.06		Resultados de la revisión por fases		
EDM02.02		Evaluación de los portafolios de inversiones y servicios		
EDM02.04		• Retroalimentación sobre el rendimiento del portafolio y los programas • Acciones para mejorar la entrega de valor		
APO05.04 Mantener los portafolios.	BAI01.09	Comunicación de la retirada de programas y rendición de cuentas futuras	Portafolios actualizados de programas, servicios y activos	APO09.02; BAI01.01
	BAI03.11	Portafolio de servicios actualizada		
APO05.05 Gestionar el logro de beneficios.	BAI01.04	Registro del presupuesto y los beneficios del programa	Acciones correctivas para mejorar la obtención de beneficios	APO09.04; BAI01.06
	BAI01.05	Resultados de la monitorización de la obtención de beneficios	Resultados de beneficios y comunicaciones relacionadas	APO09.04; BAI01.06; EDM02.02
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin Documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión de beneficios	Skills Framework for the Information Age V6, 2015	BENM
Gestión del portafolio	Skills Framework for the Information Age V6, 2015	POMG
Planificación de productos/servicios	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.4. Planificación de productos/servicios

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Principios del portafolio	Define los principios generales que garantizan la selección correcta y diversa de programas y proyectos para lograr la estrategia de I&T; considerar el alineamiento con la estrategia empresarial, una combinación de inversión adecuada, etc.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Fomentar la gestión sistemática de inversiones de I&T; medir y evaluar escenarios de inversión objetivamente.		
Apoyar la velocidad y agilidad, asegurar que los líderes evalúan el portafolio de inversiones activa de forma decisiva. Si un prototipo no funciona, el liderazgo debe acabar con el proyecto de forma decisiva, incorporando las lecciones aprendidas y siguiendo hacia delante. Dedicar rápidamente recursos adicionales a proyectos de éxito para escalarlos de forma adecuada.		

G. Componente: Servicios, infraestructura y aplicaciones
Herramientas de gestión del portafolio/inversión

Dominio: Alinear, Planificar y Organizar Objetivo de gestión: APO06 – Gestionar el presupuesto y los costes		Área prioritaria: Modelo Core de COBIT
Descripción		
Gestionar las actividades financieras relacionadas con I&T en las funciones empresariales y de TI, cubriendo el presupuesto, la gestión de costes y beneficios, y la priorización de gastos mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de asignación de costes a la empresa. Consultar a las partes interesadas para identificar y controlar los costes y beneficios totales dentro del contexto de los planes estratégicos y tácticos de I&T. Iniciar la acción correctiva cuando sea necesario.		
Propósito		
Fomentar la asociación entre las partes interesadas de la empresa y de TI para permitir el uso eficaz y eficiente de los recursos relacionados con I&T, y proporcionar transparencia y rendición de cuentas sobre el coste y el valor para el negocio de soluciones y servicios. Habilitar a la empresa para que tome decisiones informadas sobre el uso de soluciones y servicios de I&T.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales		Metas de alineamiento
<ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG04 Calidad de la información financiera • EG07 Calidad de la información sobre gestión • EG08 Optimización de la funcionalidad de procesos internos del negocio • EG09 Optimización de costes de los procesos del negocio • EG12 Gestión de programas de transformación digital 	➔	<ul style="list-style-type: none"> • AG04 Calidad de la información financiera relacionada con la tecnología • AG09 Ejecución de programas dentro del plazo, sin exceder el presupuesto, y que cumplen con los requisitos y estándares de calidad
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios		AG04 a. Satisfacción de partes interesadas clave con respecto al nivel de transparencia, comprensión y precisión de la información financiera de I&T b. Porcentaje de servicios de I&T con costes operativos claramente definidos y aprobados, y beneficios esperados
EG04 a. Encuesta de satisfacción de las partes interesadas clave con respecto al nivel de transparencia, comprensión y precisión de la información financiera de la empresa b. Coste de incumplimiento con respecto a regulaciones financieras		AG09 a. Número de programas/proyectos ejecutados a tiempo y dentro del presupuesto b. Número de programas que necesitan una revisión significativa debido a defectos de calidad c. Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto
EG07 a. Grado de satisfacción del consejo de administración y la dirección ejecutiva con la información para la toma de decisiones b. Número de incidentes causados por decisiones erróneas de negocio basadas en información imprecisa c. Tiempo que se tarda en proporcionar la información que respalde la toma de decisiones empresariales eficaces d. Periodicidad de la información sobre gestión		
EG08 a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarial b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro		
EG09 a. Relación entre el coste y los niveles de servicio conseguidos b. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarial		
EG12 a. Número de programas ejecutados a tiempo y dentro del presupuesto b. Porcentaje de partes interesadas satisfechas con la ejecución del programa c. Porcentaje de programas de transformación del negocio suspendidos d. Porcentaje de programas de transformación del negocio con actualizaciones del estado notificadas regularmente		

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
AP006.01 Gestión financiera y contable. Establecer y mantener un método para gestionar y contabilizar todos los costes y la depreciación relacionados con I&T como una parte integral de los sistemas y contabilidad financiera de la empresa. Elaborar un informe con los sistemas de medición financiera de la empresa.		a. Número de desviaciones entre las categorías presupuestarias esperadas y reales b. Utilidad de la información financiera como información para casos de negocio para nuevas inversiones en activos y servicios de I&T
Actividades		Nivel de capacidad
1. Definir procesos, entradas, salidas y responsabilidades para la gestión y contabilidad financiera de I&T en línea con el presupuesto y las políticas y estrategia de contabilidad de costes de la empresa. Definir cómo analizar e informar (a quién y cómo) sobre el proceso de control presupuestario de I&T.		2
2. Definir un esquema de clasificación para identificar todos los elementos de costes relacionados con la I&T (gastos de capital [capex] vs. gastos operativos [opex], hardware, software, personas, etc.). Identificar cómo se captan.		
3. Utilidad de la información financiera a fin de proporcionar información en casos de negocio para nuevas inversiones en activos y servicios de I&T.		3
4. Garantizar que los costes se mantengan en los portafolios de activos y servicios de I&T.		
5. Establecer y mantener prácticas para la planificación financiera y la optimización de costes operativos recurrentes a fin de obtener el máximo valor para la empresa con el mínimo gasto.		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ITIL V3, 2011		Service Strategy, 4.3 Financial management for IT services
Práctica de gestión		Métricas modelo
AP006.02 Establecer prioridades para la asignación de recursos. Implementar un proceso de toma de decisiones para establecer prioridades sobre la asignación de recursos y establecer reglas para las inversiones discrecionales por unidades individuales de negocio. Incluir el posible uso de proveedores de servicios externos y considerar las opciones de compra, desarrollo y alquiler.		a. Número de problemas de asignación de recursos escalados b. Porcentaje de alineamiento de recursos de I&T con iniciativas de alta prioridad
Actividades		Nivel de capacidad
1. Clasificar todas las iniciativas y solicitudes de presupuesto de I&T con base en los casos de negocio y las prioridades estratégicas y tácticas. Establecer procedimientos para determinar la asignación de presupuesto y los puntos de corte.		2
2. Asignar recursos empresariales y de TI (incluidos proveedores de servicios externos) dentro de las asignaciones presupuestarias de alto nivel para programas, servicios y activos relacionados con I&T. Considerar las opciones para la compra o desarrollo de activos y servicios capitalizados frente a activos y servicios utilizados externamente con base en el pago por uso.		
3. Establecer un procedimiento para comunicar las decisiones presupuestarias y revisarlas con los responsables de presupuesto de las unidades de negocio.		
4. Identificar, comunicar y resolver los impactos significativos de las decisiones presupuestarias en los casos de negocio, portafolios y planes estratégicos. (Por ejemplo, esto podría incluir las situaciones donde los presupuestos deben revisarse debido al cambio de las circunstancias empresariales o cuando éstas no son suficientes para respaldar los objetivos estratégicos u objetivos del caso de negocio).		
5. Obtener la ratificación del comité ejecutivo para las implicaciones presupuestarias de I&T que tengan un impacto negativo en los planes estratégicos o tácticos de la entidad. Sugerir acciones para resolver estos impactos.		3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
AP006.03 Crear y mantener presupuestos. Preparar un presupuesto que refleje las prioridades de inversión con base en el portafolio de programas habilitados por I&T y los servicios de I&T.		a. Número de cambios presupuestarios debido a omisiones y errores b. Utilidad del presupuesto de I&T a la hora de identificar todos los costes de I&T esperados de los programas, servicios y activos habilitados por I&T.

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Implementar un presupuesto de I&T formal, incluidos todos los costes de I&T esperados de los programas, servicios y activos habilitados por I&T.	2
2. A la hora de crear el presupuesto, considerar los componentes siguientes: alineamiento con el negocio; alineamiento con la estrategia de abastecimiento; fuentes de financiación autorizadas; costes de recursos internos, incluido el personal, activos de información y garantías; costes de terceros, incluidos los contratos de externalización, consultores y proveedores de servicios; gastos de capital y operativos; y elementos de coste que dependen de la carga de trabajo.	
3. Documentar las razones que justifican las contingencias y revisarlas de forma regular.	
4. Instruir a los dueños del proceso, servicio y programa, así como a los gestores de proyecto y activos, para planificar los presupuestos.	
5. Revisar los planes presupuestarios y tomar decisiones sobre las asignaciones de presupuesto. Recopilar y ajustar el presupuesto con base en los cambios de las necesidades de la empresa y consideraciones financieras.	3
6. Registrar, mantener y comunicar el presupuesto de I&T actual, incluidos los gastos comprometidos y los gastos actuales, mediante la consideración de los proyectos de I&T registrados en los portafolios de inversión habilitados por I&T y el funcionamiento y mantenimiento de los portafolios de activos y servicios.	
7. Monitorizar la efectividad de los distintos aspectos del presupuesto.	4
8. Usar los resultados monitorizados para implementar mejoras y asegurar que los presupuestos futuros sean más precisos, confiables y rentables.	5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
ISO/IEC 20000-1:2011(E)	6.4 Budgeting and accounting for services
PMBOK Guide Sixth Edition, 2017	Part 1: 7. Project cost management
Práctica de gestión	Métricas modelo
AP006.04 Modelar y asignar los costes. Establecer y usar un modelo basado en los costes de I&T, por ejemplo, en la definición de los servicios. Este enfoque garantiza que la asignación de costes para servicios sea identificable, medible y predecible, y fomenta el uso responsable de los recursos, incluidos aquellos proporcionados por proveedores de servicios. Revisar y comparar regularmente el modelo de coste/devoluciones para conservar su relevancia y adecuación a las cambiantes actividades empresariales y de TI.	a. Porcentaje de costes generales de I&T que se asignan de acuerdo con los modelos de costes acordados b. Número de revisiones y benchmarks del modelo de costes/devoluciones y su adecuación para las cambiantes actividades empresariales y de I&T
Actividades	Nivel de capacidad
1. Decidir un modelo de asignación de costes que permita una asignación justa, transparente, repetible y comparable de costes relacionados con I&T a los usuarios. Un ejemplo de modelo de asignación básico es la asignación uniforme de costes compartidos relacionados con I&T. Se trata de un sencillísimo modelo de asignación que es fácil de aplicar; sin embargo, según el contexto de la empresa, se suele considerar injusto y que no fomenta el uso responsable de los recursos. Un esquema de costes basado en actividades, en aquel en el que los costes se asignan a servicios de TI y se cargan a los usuarios de estos servicios, permite una asignación de costes más transparente y comparable.	3
2. Inspeccionar los catálogos de definiciones de servicios para identificar aquellos sujetos a devolución a los usuarios y aquellos que son servicios compartidos.	
3. Diseñar el modelo de costes de manera que sea lo bastante transparente como para permitir a los usuarios identificar el uso y cargo actual, con categorías y factores de costes que tengan sentido para el usuario (como, coste por llamada a Help Desk, costo por licencia de software) y para permitir una mejor predictibilidad de costes de I&T y utilización eficaz y eficiente de los recursos de I&T. Analizar los factores de coste (tiempo dedicado por actividad, gastos, proporción de costes fijos frente a variables, etc.). Decidir una diferenciación adecuada (p. ej. distintas categorías de usuarios con distinto peso) y usar aproximaciones o medias de coste cuando los costes reales tienen una naturaleza muy variable.	
4. Explicar los principios y el resultado del modelo de costes a las partes interesadas clave. Obtener su retroalimentación para perfeccionarlo con vistas a lograr un modelo transparente y exhaustivo.	
5. Obtener la aprobación de las partes interesadas clave para comunicar el modelo de costes de I&T a la dirección de los departamentos de usuario.	
6. Comunicar cambios importantes en los principios del modelo de coste/repercusión a las partes interesadas y directivos clave de los departamentos de usuario.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin Documentación relacionada para esta práctica de gestión	

A. Componente: Proceso (cont.)	
Práctica de gestión	Métricas modelo
AP006.05 Gestionar los costes. Implementar un proceso de gestión de costes que compare los costes actuales contra el presupuesto. Es necesario monitorizar e informar sobre los costes. Las desviaciones presupuestarias deben identificarse de forma oportuna, así como su impacto sobre los procesos empresariales y los servicios evaluados.	a. Porcentaje de variación entre presupuestos, previsiones y costes reales b. Puntualidad de la monitorización e información en caso de desviaciones, así como su impacto sobre los procesos empresariales y los servicios evaluados.
Actividades	Nivel de capacidad
1. Obtener la aprobación de las partes interesadas clave para comunicar el modelo de costes de I&T a la dirección de los departamentos de usuario.	2
2. Establecer escalas de tiempo para la ejecución del proceso de gestión de costes en línea con los requisitos y el plazo del presupuesto y la contabilidad.	
3. Definir un método para recopilar los datos relevantes para identificar desviaciones del presupuesto frente a los gastos reales, el ROI de la inversión, las tendencias de los costes de servicios, etc.	
4. Definir cómo se consolidan los costes para los niveles adecuados en la empresa (TI central frente al presupuesto de TI dentro de los departamentos de la empresa) y cómo se presentarán a las partes interesadas. El informe proporciona información de los costes por categoría de costes, estado del presupuesto frente a los gastos actuales, mayores gastos, etc., para permitir la identificación oportuna de las acciones correctivas requeridas.	3
5. Instruir a aquellos responsables de la gestión de costes a captar, recoger y consolidar los datos y presentar e informar de los datos a los responsables de presupuesto correspondientes. Los analistas y responsables del presupuesto analizan conjuntamente las desviaciones y comparan el rendimiento con benchmarks internos y de la industria. Estos deberían establecer y mantener el método de asignación de superávits. El resultado del análisis proporciona una explicación de las desviaciones significativas y las acciones correctivas sugeridas.	
6. Garantizar que los niveles directivos adecuados revisen los resultados del análisis y aprueben las acciones correctivas sugeridas.	
7. Garantizar que se identifiquen los cambios en estructuras de costes y necesidades empresariales, y que se revisen los presupuestos y previsiones, conforme sea necesario.	4
8. En intervalos regulares, y sobre todo cuando hay recortes de presupuesto debido a limitaciones financieras, identificar la forma de optimizar los costes e introducir eficiencias sin poner en peligro los servicios.	5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin Documentación relacionada para esta práctica de gestión	

B. Componente: Estructuras organizativas						
	Director general financiero	Director de TI	Director de tecnología	Director de tecnologías digitales	Gestor de portafolio	Jefe de administración de TI
Práctica clave de gestión						
AP006.01 Gestión financiera y contable.	A				R	R
AP006.02 Establecer prioridades para la asignación de recursos.	R	A	R	R	R	R
AP006.03 Crear y mantener presupuestos.	R	A	R	R		R
AP006.04 Modelar y asignar los costes.	R	A				R
AP006.05 Gestionar los costes.	R	A	R	R		R
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica					
Sin Documentación relacionada para este componente.						

C. Componente: Flujos y elementos de gestión (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
APO06.01 Gestión financiera y contable.	De	Descripción	Descripción	A
	BAI09.01	Registro de activos	Prácticas de planificación financiera	Interna
			Esquema de clasificación de costes de I&T	Interna
			Procesos contables	Interna
APO06.02 Establecer prioridades para la asignación de recursos.	APO04.04	Alcance de prueba de concepto y descripción del caso de negocio	Asignaciones de presupuesto	APO02.05; APO05.02; APO07.05; BAI03.11
	APO05.01	Expectativas de retorno de inversión	Priorización y clasificación de las iniciativas de I&T	APO05.02
	APO05.02	• Caso de negocio del programa • Evaluaciones del caso de negocio		
	EDM02.02	Evaluación de los portafolios de inversiones y servicios		
	EDM02.04	Acciones para mejorar la entrega de valor		
APO06.03 Crear y mantener presupuestos.			Presupuestos de I&T	APO02.05; APO05.02; APO07.01; BAI03.11
			Comunicaciones del presupuesto	APO05.02; APO07.01; BAI03.11
APO06.04 Modelar y asignar los costes.			Procedimientos operativos	Interna
			Comunicaciones de asignación de costes	Interna
			Modelo de asignación de costes	Interna
			Costes de I&T categorizados	Interna
APO06.05 Gestionar los costes.	BAI01.02	Plan de obtención de beneficios del programa	Oportunidades de optimización de costes	APO02.02
	BAI01.04	Registro del presupuesto y los beneficios del programa	Método de consolidación de costes	Interna
	BAI01.05	Resultados de monitorización de obtención de beneficios	Método de recolección de datos de costes	Interna
	EDM02.04	Observaciones sobre el rendimiento del portafolio y los programas		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
PMBOK Guide Sixth Edition, 2017		Part 1: 7. Project cost management: Inputs and Outputs		

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión financiera	Skills Framework for the Information Age V6, 2015	FMIT

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política presupuestaria	Se encarga de la preparación y plazos del presupuesto anual y la predicción de la posición financiera anual. Señala los procesos de elaboración de informes requeridos por la dirección. Establece la rendición de cuentas y la responsabilidad del plan presupuestario y otros documentos financieros.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
La gestión efectiva y eficaz de I&T viene apoyada por una cultura de transparencia del presupuesto, costes y beneficios en toda la organización. La Dirección debería habilitar una cultura basada en la toma de decisiones soportada en hechos a través de, por ejemplo, estimaciones comparables de los costes y beneficios empresariales y de TI como insumo a la gestión de portafolio la asignación justa de costes de activos y recursos de TI y la elaboración de presupuestos repetidos de TI.		

G. Componente: Servicios, infraestructura y aplicaciones	
Sistema de contabilidad de costes	

Dominio: Alinear, planificar y organizar Objetivo de gestión: APO07–Gestionar los recursos humanos		Área prioritaria: Modelo Core de COBIT
Descripción		
Proporcionar un enfoque estructurado para asegurar una contratación/adquisición, planificación, evaluación y desarrollo de recursos humanos óptimos (tanto interna como externamente).		
Propósito		
Optimizar las capacidades de recursos humanos para satisfacer los objetivos de la empresa.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales	➔	Metas de alineamiento
<ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG10 Habilidades, motivación y productividad del personal • EG13 Innovación de productos y del negocio 		<ul style="list-style-type: none"> • AG12 Personal competente y motivado con un entendimiento mutuo de la tecnología y el negocio • AG13 Conocimiento, experiencia e iniciativas para la innovación empresarial
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 <ul style="list-style-type: none"> a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios 		AG12 <ul style="list-style-type: none"> a. Porcentaje de empresarios con comprensión en I&T (es decir, aquellos que tienen los conocimientos y el entendimiento de I&T requeridos para guiar, dirigir, innovar y ver las oportunidades de I&T en su área de especialización empresarial) b. Porcentaje de empresarios con comprensión en I&T (es decir, aquellos que tienen los conocimientos y el entendimiento de los dominios empresariales relevantes para guiar, dirigir, innovar y ver las oportunidades de I&T para su dominio empresarial) c. Número o porcentaje de empresarios con experiencia en gestión de tecnología
EG10 <ul style="list-style-type: none"> a. Productividad del personal comparada con benchmarks b. Nivel de satisfacción de las partes interesadas con los niveles de conocimientos y habilidades del personal c. Porcentaje de personal cuyas habilidades son insuficientes con respecto a la competencia en su rol d. Porcentaje de personal satisfecho 		AG13 <ul style="list-style-type: none"> a. Nivel de conocimiento y comprensión de los ejecutivos del negocio sobre las posibilidades de innovación de las I&T b. Número de iniciativas aprobadas como resultado de ideas innovadoras de I&T c. Número de líderes en innovación reconocidos/premiados
EG13 <ul style="list-style-type: none"> a. Nivel de conocimiento y comprensión de las posibilidades de innovación del negocio b. Satisfacción de las partes interesadas con los niveles de conocimientos e ideas sobre innovación y productos c. Número de iniciativas de productos y servicios aprobadas como resultado de ideas innovadoras 		

A. Componente: Proceso		
Práctica de gestión	Métricas modelo	
APO07.01 Adquirir y mantener una dotación de personal suficiente y adecuada. Establecer y mantener un método para gestionar y contabilizar todos los costes, inversiones y depreciación relacionados con I&T como una parte integral de los sistemas y contabilidad financiera de la empresa. Elaborar un informe con los sistemas de medición financiera de la empresa.	a. Duración promedio de las vacantes b. Porcentaje de puestos de TI vacantes c. Porcentaje de rotación de personal	
Actividades	Nivel de capacidad	
1. Evaluar los requisitos de personal de forma periódica o ante cambios mayores Asegurar que tanto la empresa como la función de TI tengan los suficientes recursos para apoyar las metas y los objetivos empresariales, procesos y controles empresariales y las iniciativas habilitadas por I&T de forma adecuada y apropiada.	2	
2. Mantener los procesos de contratación y retención de personal empresarial y de TI en línea con todas las políticas y procedimientos de personal de la empresa.		
3. Establecer una estructura de recursos flexible, como el uso de transferencias, contratistas externos y acuerdos de servicio con terceros, para apoyar el cambio en las necesidades empresariales.		
4. Incluir verificaciones de antecedentes en el proceso de contratación de TI para empleados, contratistas y terceros. El alcance y frecuencia de estas verificaciones debe depender de la sensibilidad y/o criticidad de la función.	3	

A. Componente: Proceso (cont.)		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
COSO Enterprise Risk Management, junio de 2017		6. Governance and Culture—Principle 5
Skills Framework for the Information Age V6, 2015		SFIA and skills management—Acquire
Práctica de gestión		Métricas modelo
APO07.02 Identificar al personal clave de TI. Identificar al personal clave de TI. Usar la captura de conocimientos (documentación), intercambio de conocimientos, planificación de sucesión y personal de respaldo para minimizar la dependencia en un único individuo que realice un trabajo crítico.		a. Porcentaje de trabajos críticos en los que la empresa depende de un único individuo b. Número de planes de respaldo de personal realizados
Actividades		Nivel de capacidad
1. Como precaución de seguridad, proporcionar directrices sobre un tiempo mínimo de vacaciones anuales que tomarán las personas clave.		2
2. Tomar las acciones pertinentes relativas a cambios laborales, en especial terminación de contratos.		
3. Usar la captura de conocimientos (documentación), intercambio de conocimientos, planificación de sucesión y personal de respaldo para minimizar la dependencia en un único individuo que realice un trabajo crítico.		
4. Comprobar regularmente los planes de respaldo de personal		3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		RI.RR Identification of Roles and Responsibilities
Skills Framework for the Information Age V6, 2015		SFIA and skills management—Acquire
Práctica de gestión		Métricas modelo
APO07.03 Mantener las habilidades y competencias del personal. Definir y administrar las habilidades y competencias que necesita el personal. Verificar periódicamente que el personal cuente con las competencias necesarias para realizar sus funciones conforme a su educación, capacitación y/o experiencia. Verificar que estas competencias se mantengan con programas de aptitud y certificación cuando sea apropiado. Dar a los empleados oportunidades de aprendizaje continuas para mantener sus conocimientos, habilidades y competencias al nivel requerido para alcanzar las metas empresariales.		a. Identificar habilidades y competencias clave que no se encuentren en la matriz de recursos b. Número de brechas identificadas entre las habilidades requeridas y las disponibles c. Número de programas de capacitación proporcionados
Actividades		Nivel de capacidad
1. Identificar las habilidades y competencias disponibles actuales, tanto de recursos internos como externos.		2
2. Identificar las brechas entre las habilidades requeridas y las disponibles Desarrollar planes de acción, como capacitación (habilidades técnicas y de conducta), contratación, reasignación y cambio de las estrategias de abastecimiento, para resolver las brechas desde el punto de vista individual y colectivo.		
3. Revisar los materiales y programas de capacitación de forma regular. Garantizar su idoneidad con respecto a los requisitos en constante evolución de la empresa y su impacto sobre el conocimiento, capacidades y habilidades necesarias.		3
4. Proporcionar acceso a los repositorios de conocimiento para respaldar el desarrollo de habilidades y competencias.		
5. Desarrollar y ofrecer programas de capacitación conforme a los requisitos del proceso y organizativos, incluidos los requisitos para el conocimiento empresarial, control interno, conducta ética, seguridad y privacidad.		
6. Realizar evaluaciones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos y externos. Evaluar la planificación de los reemplazos.		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISF, The Standard of Good Practice for Information Security 2016		PM2.3 Security Education/Training
ISO/IEC 27001:2013/Cor.2:2015(E)		7.2 Competence
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity V1.1, abril de 2018		PR.AT Awareness and Training
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.2 Awareness and training (AT-3, AT-4)
Skills Framework for the Information Age V6, 2015		SFIA and skills management—Deploy
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016		CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
APO07.04 Evaluar y reconocer/recompensar el rendimiento laboral de los empleados. Realizar evaluaciones regulares y oportunas del rendimiento contra los objetivos individuos derivados de las metas empresariales, estándares establecidos, responsabilidades específicas de los cargos, y marco de habilidades y competencias. Implementar un proceso de remuneración/reconocimiento que reconozca el logro de las metas de desempeño.		a. Número de momentos de retroalimentación oficial y evaluaciones de 360 grados realizadas b. Número y valor de las recompensas otorgadas al personal
Actividades		Nivel de capacidad
1. Considerar las metas empresariales/funcionales como el contexto para establecer metas individuales		2
2. Establecer metas individuales alineadas con las metas empresariales y de I&T relevantes. Basar las metas en objetivos específicos, medibles, alcanzables, relevantes y en tiempo (SMART) que reflejen las competencias principales, los valores empresariales y las habilidades requeridas para los roles.		
3. Proporcionar retroalimentación oportuna acerca del rendimiento comparado con las metas individuales.		
4. Proporcionar instrucciones específicas para el uso y el almacenamiento de la información personal en el proceso de evaluación, en cumplimiento de la legislación vigente sobre datos personales y laboral vigente.		
5. Recopilar resultados de evaluación de rendimiento de 360 grados.		3
6. Proporcionar planes formales de planificación y de desarrollo profesional conforme a los resultados del proceso de evaluación para fomentar el desarrollo de competencias y las oportunidades para el avance personal y para reducir la dependencia de individuos clave. Proporcionar coaching a los empleados sobre el rendimiento y la conducta cuando sea apropiado.		
7. Implementar un proceso de remuneración/reconocimiento que premie el compromiso adecuado, desarrollo de competencias y logro de las metas de desempeño. Asegurar que el proceso se aplique de forma consistente y en línea con las políticas organizativas.		
8. Implementar y comunicar un proceso disciplinario.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Skills Framework for the Information Age V6, 2015		SFIA and skills management—Develop
Práctica de gestión		Métricas modelo
APO07.05 Planificar y hacer seguimiento del uso de los recursos humanos del negocio y de TI. Comprender y hacer un seguimiento de la demanda actual y futura de recursos humanos del negocio y de TI con responsabilidades en las I&T empresariales. Identificar las carencias y proporcionar recomendaciones sobre los planes de abastecimiento, procesos de contratación de la empresa y de TI, y procesos de contratación de negocio y de TI.		a. Número de carencias identificadas y habilidades ausentes a la hora de planificar el personal b. Tiempo utilizado por cada empleado a tiempo completo (FTE) en trabajos y proyectos
Actividades		Nivel de capacidad
1. Crear y mantener un inventario de recursos humanos empresariales y de TI.		2
2. Entender la demanda actual y futura de recursos humanos para contribuir a lograr los objetivos de I&T y ofrecer servicios y soluciones conforme al portafolio de iniciativas relacionadas con I&T, al portafolio de inversión futura y necesidades operativas diarias.		3
3. Identificar las carencias y proporcionar recomendaciones sobre los planes de abastecimiento, así como de los procesos de contratación de personal empresarial y de TI. Crear y revisar la planificación de personal, mediante un seguimiento de su uso real.		
4. Mantener una información adecuada sobre el tiempo dedicado a las distintas tareas, trabajos, servicios o proyectos.		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Skills Framework for the Information Age V6, 2015		SFIA and skills management—Assess; Reward
Práctica de gestión		Métricas modelo
APO07.06 Gestionar al personal contratado. Asegurarse de que los consultores y el personal por contrato, que dan soporte a la empresa con habilidades de I&T, conozcan y cumplan las políticas de la organización y los requisitos contractuales acordados.		a. Porcentaje de contratistas que firman el marco de control empresarial b. Frecuencia de las revisiones periódicas llevadas a cabo para garantizar la exactitud y el cumplimiento con la ley, del personal del contratista.

A. Componente: Proceso (cont.)

Actividades	Nivel de capacidad
1. Implementar las políticas y procedimientos del personal contratado	2
2. Al inicio del contrato, obtener el acuerdo formal de los contratistas de que deben cumplir con el marco de control de I&T empresarial, así como con las políticas y verificaciones de seguridad, control del acceso físico y lógicos, uso de las instalaciones, requisitos de confidencialidad de la información y acuerdos de no revelación	
3. Avisar a los contratistas de que los directivos se reservan el derecho a supervisar e inspeccionar todo el uso de los recursos de TI, incluido el correo electrónico, comunicaciones de voz y todos los programas y archivos de datos.	
4. Como parte de sus contratos, proporcionar a los contratistas una definición clara de sus roles y responsabilidades, incluidos los requisitos explícitos para documentar su trabajo conforme a los estándares y formatos acordados.	
5. Revisar el trabajo de contratistas y basar la aprobación de los pagos en los resultados.	
6. En contratos formales y no ambiguos, definir todo el trabajo realizado por personal externo.	3
7. Realizar revisiones periódicas para garantizar que el personal contratado haya firmado y aceptado todos los acuerdos necesarios.	4
8. Realizar revisiones periódicas para garantizar que los roles de los contratistas y los derechos de acceso sean adecuados y conforme a los contratos.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Skills Framework for the Information Age V6, 2015	SFIA and skills management—Deploy

B. Componente: Estructuras organizativas

Componente Estándares organizativos																

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
APO07.01 Adquirir y mantener una dotación de personal suficiente y adecuada.	AP001.05	Definición de prácticas de supervisión	Descripciones de puestos y planes de contratación de personal	Interna
	AP006.03	• Presupuesto de TI • Comunicaciones de presupuesto	Evaluaciones de requisitos de contratación	Interna
	EDM04.01	• Principios rectores para la asignación de recursos y capacidades • Plan de recursos aprobado	Planes de desarrollo de competencias y de carrera	Interna; APO07.02
	EDM04.03	Acciones remediales para solucionar las desviaciones de gestión de recursos		
	Fuera de COBIT	• Políticas y procedimientos de RR. HH. de la empresa • Metas y objetivos empresariales		
APO07.02 Identificar al personal clave de TI.	AP007.01	Planes de desarrollo de competencias y de carrera	Planes de terminación de empleo	Interna
			Directrices sobre vacaciones mínimas	Interna
APO07.03 Mantener las habilidades y las competencias del personal.	AP001.08	Matriz de habilidades y competencias	Matriz de habilidades y competencias	AP001.05; AP014.01 BAI01.02; BAI01.04; BAI03.12
	BAI08.02	Repositorios de conocimientos publicados	Planes de desarrollo de competencias	AP001.05; EDM04.01
	BAI08.03	Conocimiento y esquemas de concienciación y capacitación	Informes de revisión	Interna
	DSS04.06	• Requisitos de capacitación • Monitorización de resultados de habilidades y competencias.		
	EDM01.02	Enfoque del sistema de recompensa		
	EDM04.03	Acciones remediales para solucionar las desviaciones de gestión de recursos		
	Fuera de COBIT	Metas y objetivos empresariales		

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
AP007.04 Evaluar y reconocer/recompensar el rendimiento laboral de los empleados.	AP004.01	Programa de reconocimiento y recompensas	Planes de mejora	Interna
	BAI05.04	Objetivos de rendimiento de RR. HH alineados	Evaluaciones del rendimiento	Interna
	BAI05.06	Resultados de revisión del rendimiento de RR. HH.	Metas de personal	Interna
	DSS06.03	Derechos de acceso asignados		
	EDM01.02	Método del sistema de recompensa		
	Fuera de COBIT	Metas y objetivos empresariales		
AP007.05 Planificar y hacer seguimiento del uso de los recursos humanos del negocio y TI.	AP006.02	Asignaciones de presupuesto	Inventario de recursos humanos del negocio y de TI	BAI01.04
	BAI01.04	Requisitos de recursos y roles	Registros de utilización de recursos	BAI01.06
	BAI11.08	Requisitos de recursos para proyectos	Análisis de déficit de recursos	BAI01.06
	EDM04.02	Comunicación de estrategias de gestión de recursos		
	EDM04.03	Retroalimentación sobre la asignación y eficiencia de recursos y capacidades		
	Organización empresarial	Portafolios actuales y futuros		
	Fuera de COBIT	Estructura de la organización empresarial		
AP007.06 Gestionar al personal contratado.	BAI01.04	Requisitos de recursos y roles	Revisiones de acuerdos contractuales	Interna
	BAI01.09	Comunicación de la retirada de programas y rendición de cuentas en curso	Acuerdos contractuales	Interna
	BAI11.08	Requisitos de recursos para proyectos	Políticas de contratación de persona	Interna
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
PMBOK Guide Sixth Edition, 2017		Part 1: 9. Gestión de recursos para proyectos: Inputs and Outputs		

D. Componente: Personas, habilidades y competencias		
Habilidad	Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Provisión de educación y capacitación	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	D. Enable—D.3. Provisión de educación y capacitación
Gestión del aprendizaje y desarrollo	Skills Framework for the Information Age V6, 2015	ETMG
Gestión de rendimiento	Skills Framework for the Information Age V6, 2015	PEMT
Desarrollo del personal	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework, 2016	D. Enable—D.9. Desarrollo del personal
Desarrollo profesional	Skills Framework for the Information Age V6, 2015	PDSV
Dotación de recursos	Skills Framework for the Information Age V6, 2015	RESC

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Guía correspondiente	Referencia específica
Política de contratación de personal	Enumera los criterios para aumentar el personal con consultores de terceros y/o contratistas conforme a la política de contratación de TI empresarial y el marco de control de I&T. Especifica qué tipo de trabajo pueden realizar o aumentar los terceros, bajo qué condiciones y cuándo.	National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.16 Personnel security (PS-1)
Políticas de recursos humanos (RH)	Señala expectativas mutuas de la empresa y sus empleados. Enumera comportamientos aceptables e inaceptables de los empleados en un código de conducta para ayudar a gestionar el riesgo relacionado con el comportamiento humano.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Guía correspondiente	Referencia específica
Describir los roles y responsabilidades de los usuarios hacia la información, uso de medios y red, seguridad y privacidad. Fomentar y comunicar una cultura común que prescriba los comportamientos esperados en todos los individuos de la empresa y que establezca cero tolerancia respecto a los comportamientos poco éticos.	National Institute of Standards and Technology Special Publication 800-53, Revisión 5, agosto de 2017	3.14 Planning (PL-4)

G. Componente: Servicios, infraestructura y aplicaciones
<ul style="list-style-type: none"> • Sistema de gestión de recursos humanos • Sistema de medición del rendimiento (p. ej., cuadro de mando integral, herramientas de gestión de competencias) • Herramientas de planificación de recursos

Página dejada en blanco intencionadamente

Dominio: Alinear, planificar y organizar Objetivo de gestión: APO08—Gestionar las relaciones		Área prioritaria: Modelo Core de COBIT
Descripción		
Gestionar las relaciones con las partes interesadas de una manera formal y transparente que asegure una confianza mutua y un enfoque combinado en lograr las metas estratégicas dentro de las limitaciones de los presupuestos y la tolerancia al riesgo. Basar las relaciones de la comunicación abierta y transparente, un lenguaje común, así como la voluntad de responsabilizarse y rendir cuentas por las decisiones clave por ambas partes. La empresa y TI deben trabajar juntos para generar resultados empresariales exitosos que respalden los objetivos empresariales.		
Propósito		
Facilitar el conocimiento, habilidades y comportamientos correctos para generar mejores resultados, aumentar la confianza, credibilidad mutua y uso eficaz de los recursos para estimular una relación productiva con las partes interesadas de la empresa.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales		Metas de alineamiento
<ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG08 Optimización de la funcionalidad interna de los procesos del negocio • EG10 Habilidades, motivación y productividad del personal • EG13 Innovación de productos y negocio 	➔	<ul style="list-style-type: none"> • AG05 Prestación de servicios de T&I en línea con los requisitos del negocio • AG06 Agilidad para convertir los requisitos del negocio en soluciones operativas • AG12 Personal competente y motivado con un entendimiento mutuo de la tecnología y el negocio • AG13 Conocimiento, habilidad e iniciativas para la innovación empresarial
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 <ul style="list-style-type: none"> a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios 		AG05 <ul style="list-style-type: none"> a. Porcentaje de partes interesadas del negocio satisfechas con que la prestación de servicios de I&T cumple con los niveles de servicio acordados b. Número de interrupciones del negocio debido a incidentes de servicios de I&T c. Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de I&T
EG08 <ul style="list-style-type: none"> a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarial b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores externos con las capacidades de la cadena de suministro 		AG06 <ul style="list-style-type: none"> a. Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de I&T a los nuevos requisitos b. Plazo de comercialización promedio para nuevos servicios y aplicaciones relacionadas con I&T c. Tiempo promedio para convertir los objetivos estratégicos de I&T en iniciativas acordadas y aprobadas d. Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas
EG10 <ul style="list-style-type: none"> a. Productividad del personal comparada con benchmarks b. Nivel de satisfacción de las partes interesadas con los niveles de conocimientos y habilidades del personal c. Porcentaje de personal cuyas habilidades son insuficientes con respecto a la competencia en su rol d. Porcentaje de personal satisfecho 		AG12 <ul style="list-style-type: none"> a. Porcentaje de empresarios con comprensión de I&T (es decir, aquellos que tienen el conocimiento y entendimiento de I&T requeridos para guiar, dirigir, innovar y ver las oportunidades de I&T en su área de especialización empresarial) b. Porcentaje de empresarios con comprensión de I&T (es decir, aquellos que tienen los conocimientos y entendimiento de los dominios empresariales relevantes para guiar, dirigir, innovar y ver las oportunidades de I&T para su dominio empresarial) c. Número o porcentaje de empresarios con experiencia en gestión de tecnología
EG13 <ul style="list-style-type: none"> a. Nivel de conocimiento y comprensión de las posibilidades de innovación del negocio b. Satisfacción de las partes interesadas con los niveles de conocimientos e ideas sobre innovación y productos c. Número de iniciativas de productos y servicios aprobadas como resultado de ideas innovadoras 		AG13 <ul style="list-style-type: none"> a. Nivel de conocimiento y comprensión de los ejecutivos del negocio sobre las posibilidades de innovación de las I&T b. Número de iniciativas aprobadas como resultado de ideas innovadoras de I&T c. Número de campeones en innovación reconocidos/premiados

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
APO08.01 Entender las expectativas del negocio. Entender los problemas, objetivos y expectativas actuales del negocio sobre I&T. Asegurar que se comprendan, gestionen y comuniquen los requisitos, y que su estado se acepte y apruebe.		a. Número de problemas empresariales actuales identificados b. Números de requisitos empresariales definidos para servicios habilitados por I&T
Actividades		Nivel de capacidad
1. Identificar a las partes interesadas del negocio, sus intereses y áreas de responsabilidad.		2
2. Revisar la dirección, problemas, objetivos estratégicos actuales de la empresa y su alineamiento con la arquitectura empresarial.		
3. Entender el entorno de negocio, limitaciones o problemas actuales de los procesos, expansión o contracción geográfica y factores de la industria/regulatorios.		
4. Mantener un conocimiento de los procesos empresariales y actividades asociadas. Entender los patrones de la demanda que se relacionan con los volúmenes y uso del servicio.		
5. Gestionar expectativas garantizando que las unidades de negocio entiendan las prioridades, dependencias, limitaciones financieras y la necesidad de programar solicitudes.		3
6. Clarificar las expectativas empresariales para los servicios y soluciones habilitados por I&T. Asegurar que los requisitos vengan definidos con criterios y métricas de aceptación empresarial.		4
7. Confirmar que existe un acuerdo entre TI y todos los departamentos de la empresa acerca de las expectativas y cómo se medirán. Asegurar que este acuerdo sea confirmado por todas las partes interesadas.		
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin guía correspondiente para esta práctica de gestión		
Práctica de gestión		Métricas modelo
APO08.02: Alinear la estrategia de I&T con las expectativas empresariales e identificar oportunidades para que TI mejore el negocio. Alinear las estrategias de I&T con los objetivos y expectativas empresariales actuales para permitir que TI sea un socio que agregue valor para el negocio y sea un componente de gobierno para mejorar el rendimiento empresarial.		a. Tasa de inclusión de las oportunidades tecnológicas en las propuestas de inversión b. Encuesta sobre el nivel de conocimiento tecnológico de las partes interesadas del negocio
Actividades		Nivel de capacidad
1. Posicionar TI como un socio del negocio Jugar un papel proactivo a la hora de identificar y comunicarse con partes interesadas clave acerca de oportunidades, riesgo y limitaciones. Entre ellos se incluyen tecnologías emergentes, servicios y modelos de procesos empresariales actuales.		3
2. Colaborar en las principales iniciativas nuevas con gestión del portafolio, programas y proyectos. Garantizar la participación de la organización de TI desde el inicio de una nueva iniciativa mediante consejos y recomendaciones que añadan valor (p. ej. desarrollo de casos de negocio, definición de requisitos, diseño de soluciones) y responsabilizándose de los flujos de trabajo de I&T.		
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ITIL V3, 2011		Service Strategy, 4.4 Demand management
Práctica de gestión		Métricas modelo
APO08.03 Gestionar la relación con el negocio. Gestionar la relación entre la organización de servicio de TI y sus socios empresariales. Asegurar que los roles y responsabilidades de las relaciones se definan y asignen, y que se facilite la comunicación.		a. Calificaciones de encuestas de satisfacción de usuarios y personal de TI b. Porcentaje de roles y responsabilidades en las relaciones definidos, asignados y comunicados
Actividades		Nivel de capacidad
1. Asignar un gestor de relaciones como un único punto de contacto para cada unidad de negocio significativa. Asegurar que se identifique una única contraparte en la organización de la empresa y que la contraparte entienda el negocio, conozca suficientemente la tecnología y tenga el nivel de autoridad adecuado.		3
2. Gestionar la relación de una manera formal y transparente que asegure un enfoque en el logro de una meta común y compartida de resultados empresariales exitosos, en apoyo de las metas estratégicas y dentro de las limitaciones de los presupuestos y la tolerancia al riesgo.		
3. Definir y comunicar las reclamaciones y el procedimiento de escalamiento para resolver cualquier problema de relaciones.		
4. Asegurar que las partes interesadas responsables relevantes. acuerden y aprueben las decisiones claves		
5. Planificar interacciones y calendarios específicos basados en objetivos acordados y un lenguaje común (reunión de revisión del servicio y el rendimiento, revisión de nuevas estrategias o planes, etc.).		4

A. Componente: Proceso (cont.)	
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
ISO/IEC 20000-1:2011(E)	7.1 Business relationship management
ITIL V3, 2011	Service Strategy, 4.5 Business relationship management
Práctica de gestión	Métricas modelo
AP008.04 Coordinar y comunicar. Trabajar con todas las partes interesadas relevantes y coordinar la prestación íntegra de los servicios y soluciones de I&T que se ofrecen a la empresa.	a. Tiempo transcurrido desde la última actualización del plan de comunicación para toda la empresa b. Porcentaje de satisfacción del dueño de negocio con la coordinación de la prestación íntegra de servicios y soluciones de I&T
Actividades	Nivel de capacidad
1. Coordinar y comunicar los cambios y actividades de transición como planes de cambios o proyectos, calendarios, políticas de liberación, errores conocidos en la liberación y capacitación de sensibilización.	2
2. Coordinar y comunicar actividades operativas, roles y responsabilidades, incluida la definición de los tipos de peticiones, escalamiento jerárquico, interrupciones mayores (planificadas y no planificadas) y contenido y frecuencia de los informes de servicio.	
3. Hacerse responsable de la respuesta al negocio en el caso de eventos importantes que podrían influir en la relación con el negocio. Proporcionar un soporte directo, si fuera necesario.	
4. Mantener un plan completo de comunicación que defina el contenido, frecuencia y destinatarios de la información de la prestación del servicio, incluido el estado del valor ofrecido y cualquier riesgo identificado.	3
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin guía correspondiente para esta práctica de gestión	
Práctica de gestión	Métricas modelo
AP008.05 Proporcionar aportes para la mejora continua de los servicios. Mejorar y evolucionar continuamente los servicios habilitados por I&T, y la entrega de servicios para que la empresa se alinee con los objetivos empresariales y de tecnología en constante evolución.	a. Porcentaje de servicios de I&T alineados con los requisitos de negocio de la empresa b. Porcentaje de las causas raíz identificadas y resueltas para todos los problemas
Actividades	Nivel de capacidad
1. Realizar análisis de satisfacción para clientes y proveedores. Asegurar que se resuelvan los problemas; informar de los resultados y el estado.	4
2. Trabajar juntos para identificar, comunicar e implementar iniciativas de mejora.	5
3. Trabajar con la dirección del servicio y los dueños del proceso para asegurar que los servicios y los procesos de gestión de servicios habilitados por I&T se mejoren de forma continua y que las causas raíz de todos los problemas se identifiquen y resuelvan.	
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin guía correspondiente para esta práctica de gestión	

B. Componente: Estructuras organizativas

Práctica clave de gestión	Director general ejecutivo	Director general financiero	Director de operaciones	Director de TI	Director de tecnología	Director de tecnologías digitales	Consejo de gobierno de I&T	Dueños del proceso de negocio	Gestor de relaciones	Jefe de arquitectura	Jefe de desarrollo	Jefe de operaciones de TI	Gestor de servicios	Gestor de seguridad de la información	Gestor de continuidad del negocio	Director de privacidad
AP008.01 Entender las expectativas del negocio.				A	R	R		R	R		R	R	R	R	R	R
AP008.02: Alinear la estrategia de I&T con las expectativas empresariales e identificar oportunidades para que TI mejore el negocio.				A	R	R	R	R	R	R	R	R	R			
AP008.03 Gestionar la relación con el negocio.	R	R	R	A	R	R		R	R		R	R	R			
AP008.04 Coordinar y comunicar.	R	R	R	A	R	R		R	R		R	R	R			
AP008.05 Proporcionar aportes para la mejora continua de los servicios.				A	R	R		R	R		R	R	R			
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica														
Sin guía correspondiente para este componente.																

C. Componente: Flujos y elementos de información (ver también la sección 3.6)

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
AP008.01 Entender las expectativas del negocio.	AP002.05	Hoja de ruta estratégica	Expectativas del negocio explicados y acordados	Interna
AP008.02: Alinear la estrategia de I&T con las expectativas empresariales e identificar oportunidades para que TI mejore el negocio.	AP009.01	Brechas identificadas en servicios de TI para la empresa	Próximos pasos y planes de acción acordados	Interna
	AP009.04	<ul style="list-style-type: none"> • Informes de rendimiento del nivel de servicio • Planes de acción de mejora y remediaciones 		
	AP011.03	Causas raíz de la falla al ofrecer calidad		
AP008.03 Gestionar la relación con el negocio.	DSS02.02	Peticiones de servicio e incidentes clasificados y priorizados	Estado de reclamaciones y escalamiento	Interna
	DSS02.06	<ul style="list-style-type: none"> • Cerrar las peticiones e incidentes de servicio. • Confirmación del usuario del cumplimiento o resolución satisfactoria 	Decisiones clave acordadas	Interna
	DSS02.07	<ul style="list-style-type: none"> • Estado de incidentes e informe de tendencias • Estado de cumplimiento de peticiones e informe de tendencias 		

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
APO08.04 Coordinar y comunicar.	De	Descripción	Descripción	A
	AP009.03	Acuerdos de nivel de servicio (SLA)	Respuestas del cliente	Interna
	AP012.06	Comunicación de impacto del riesgo	Paquetes de comunicación	Interna
	BAI05.05	Plan de uso y operación	Plan de comunicación	Interna
	BAI07.07	Plan de soporte suplementario		
	BAI09.02	Comunicaciones de tiempos de suspensión del servicio por mantenimientos planificados		
	DSS03.04	Comunicación de conocimientos adquiridos		
APO08.05 Proporcionar aportes para la mejora continua de los servicios.	AP009.02	Catálogos de servicios	Definición de posibles proyectos de mejora	APO02.02; BAI03.11
	AP011.02	• Requisitos del cliente para la gestión de la calidad • Resultado de la calidad del servicio, incluida la retroalimentación de los clientes	Análisis de satisfacción	APO09.04
	AP011.03	Resultados de la monitorización de la calidad para la prestación de servicios y soluciones		
	AP011.04	Resultados de las revisiones y auditorías de calidad		
	BAI03.10	Plan de mantenimiento		
	BAI05.05	Mediciones y resultados del éxito		
	BAI07.07	Plan de apoyo complementario		
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin guía correspondiente para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión de relaciones	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.4. Relationship Management
Gestión de relaciones	Skills Framework for the Information Age V6, 2015	RLMT

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Guía correspondiente	Referencia específica
Política de gestión de relaciones empresa—TI	Proporciona las directrices para establecer y mantener las relaciones entre la empresa y TI. Fomenta la transparencia, una confianza mutua y un enfoque compartido en lograr las metas estratégicas dentro del contexto presupuestario y la tolerancia al riesgo.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Guía correspondiente	Referencia específica
Establecer una cultura basada en la confianza mutua, comunicación transparente, términos abiertos y comprensibles, lenguaje común, propiedad y rendición de cuentas. Deben existir buenas relaciones entre la empresa y las TI dentro de la empresa para lograr un objetivo común.		

G. Componente: Servicios, infraestructura y aplicaciones		
<ul style="list-style-type: none">• Plataformas de colaboración• Servicios internos de capacitación y concienciación		

Dominio: Alinear, planificar y organizar Objetivo de gestión: APO09 – Gestionar los acuerdos de servicio		Área prioritaria: Modelo Core de COBIT
Descripción		
Alinear los productos y servicios habilitados por I&T y los niveles de servicio con las necesidades y expectativas de la empresa, incluidos la identificación, especificación, diseño, publicación, acuerdo y monitorización de los productos y servicios de I&T, niveles de servicio e indicadores de rendimiento.		
Propósito		
Asegurarse que los productos, servicios y niveles de servicio de I&T satisfagan las necesidades actuales y futuras de la empresa.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales	➔	Metas de alineamiento
<ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG08 Optimización de la funcionalidad interna de procesos del negocio 		AG05 Prestación de servicios de I&T conforme a los requisitos del negocio
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 <ul style="list-style-type: none"> a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios 		AG05 <ul style="list-style-type: none"> a. Porcentaje de partes interesadas del negocio satisfechas con que la prestación de servicios de I&T cumpla con los niveles de servicio acordados b. Número de interrupciones del negocio debido a incidentes de servicios de I&T c. Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de I&T
EG08 <ul style="list-style-type: none"> a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso de negocio b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores externos con las capacidades de la cadena de suministro 		

A. Componente: Proceso		
Práctica de gestión	Métricas modelo	
APO09.01 Identificar los servicios de I&T. Analizar los requisitos del negocio y hasta qué punto los servicios habilitados por I&T y los niveles de servicio apoyan los procesos del negocio. Analizar y acordar los servicios y niveles de servicio potenciales con el negocio. Comparar los niveles de servicio potenciales con el portafolio actual de servicios; identificar opciones nuevas o modificadas de servicios o de nivel de servicio.	a. Número de actividades empresariales que no reciben el apoyo de ningún servicio de I&T b. Número de servicios obsoletos identificados	
Actividades	Nivel de capacidad	
1. Evaluar los servicios y niveles de servicios de I&T actuales para identificar las brechas entre los servicios actuales y las actividades empresariales que apoyan. Identificar áreas de mejora de los servicios existentes y opciones de nivel de servicio.	2	
2. Analizar, estudiar y estimar la demanda futura y confirmar la capacidad de servicios actuales habilitados por I&T.		
3. Analizar actividades del proceso empresarial para identificar la necesidad de servicios de I&T nuevos o rediseñados.	3	
4. Comparar los requisitos identificados con los componentes de servicio vigentes del portafolio. Si fuera posible, incluir los componentes de servicio vigentes (servicios de I&T, opciones de nivel de servicio y paquetes de servicio) en nuevos paquetes de servicio para satisfacer los requisitos del negocio identificados.		
5. Revisar regularmente el portafolio de servicios de I&T con la gestión del portafolio y la gestión de relaciones con el negocio para identificar servicios obsoletos. Acordar su retirada y proponer cambios.		
6. Cuando sea posible, hacer corresponder las demandas con los paquetes de servicio y crear servicios estandarizados para lograr eficiencias globales.	4	
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
ITIL V3, 2011	Service Strategy, 4.4 Demand management	

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
APO09.02 Catalogar los servicios habilitados por I&T. Definir y mantener uno o más catálogos de servicios para grupos objetivo relevantes. Publicar y mantener servicios activos habilitados por I&T en los catálogos de servicios.		a. Porcentaje de servicios activos habilitados por I&T y paquetes de servicio ofrecidos en comparación con el portafolio b. Tiempo transcurrido desde la última actualización del portafolio de servicios
Actividades		Nivel de capacidad
1. Publicar en catálogos los servicios activos importantes , paquetes de servicios y opciones de nivel de servicio habilitados por TI desde el portafolio.		2
2. Asegurar de forma continua que los componentes de servicio en el portafolio y los catálogos de servicios relacionados estén completos y actualizados.		3
3. Informar a la dirección de gestión de relaciones empresariales acerca de todas las actualizaciones de los catálogos de servicios.		
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ITIL V3, 2011		Service Design, 4.2 Service Catalogue Management
Práctica de gestión		Métricas modelo
APO09.03 Definir y preparar acuerdos de servicio. Definir y preparar acuerdos de servicio basados en las opciones de los catálogos de servicio. Incluir acuerdos operativos internos.		a. Número de procesos de negocio con acuerdos de servicio no definidos b. Porcentaje de servicios de TI activos cubiertos por acuerdos de servicio
Actividades		Nivel de capacidad
1. Analizar los requisitos para acuerdos de servicio nuevos o modificados recibidos de la gestión de relaciones con el negocio a fin de asegurar que puedan satisfacerse. Considerar aspectos como los tiempos de servicio, disponibilidad, rendimiento, capacidad, seguridad, privacidad, continuidad, problemas de cumplimiento y regulatorios, usabilidad, limitaciones de la demanda y calidad de los datos.		2
2. Redactar borradores de acuerdos de servicio al cliente basados en los servicios, paquetes de servicios y opciones de nivel de servicio en los catálogos de servicios relevantes.		
3. Finalizar los acuerdos de servicio al cliente con la gestión de relaciones con el negocio.		
4. Determinar, acordar y documentar acuerdos operativos internos que sustenten los acuerdos de servicio al cliente, si corresponde.		3
5. Relacionarse con la gestión de proveedores externos para garantizar que los adecuados contratos comerciales con proveedores de servicios externos sustenten los acuerdos de servicio al cliente, si corresponde.		
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISF, The Standard of Good Practice for Information Security 2016		SY2.1 Service Level Agreements
ISO/IEC 20000-1:2011(E)		4.5 Establish and improve the SMS; 6.1 Service level management
ITIL V3, 2011		Service Design, 4.3 Service Level Management
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.18 System and services acquisition (SA-9)
Práctica de gestión		Métricas modelo
APO09.04 Monitorizar y reportar los niveles de servicio. Monitorizar los niveles de servicio, informar sobre los logros e identificar tendencias. Ofrecer información gerencial apropiada para ayudar a la gestión del rendimiento.		a. Número y severidad de las brechas de servicio b. Porcentaje de clientes satisfechos con que la prestación de servicios cumple con los niveles acordados c. Porcentaje de objetivos de servicio alcanzados d. Porcentaje de servicios monitorizados contra los niveles de servicio
Actividades		Nivel de capacidad
1. Establecer y mantener medidas para monitorizar y recopilar datos de nivel de servicio.		4
2. Evaluar el rendimiento y proporcionar reportes sobre el rendimiento de los acuerdos de servicio regular y formalmente, incluidas las desviaciones de los valores acordados. Distribuir este informe a la gestión de relaciones con el negocio.		
3. Realizar revisiones regulares para pronosticar e identificar las tendencias del rendimiento de nivel de servicio. Incorporar prácticas de gestión de calidad en la monitorización de servicios.		
4. Ofrecer la información de gestión apropiada para contribuir a la gestión del rendimiento.		
5. Acordar planes de acción y remediaciones para cualquier problema de rendimiento o tendencias negativas.		
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
HITRUST CSF versión 9, septiembre de 2017		09.02 Control Third Party Service Delivery
ISO/IEC 20000-1:2011(E)		6.2 Service reporting

A. Componente: Proceso (cont.)	
Práctica de gestión	Métricas modelo
AP009.05 Revisar los acuerdos y los contratos de servicio. Realizar revisiones periódicas de los acuerdos de servicio y revisarlos cuando sea necesario.	a. Número de revisiones de los acuerdos de servicio realizadas b. Porcentaje de objetivos de servicio alcanzados c. Porcentaje de partes interesadas satisfechas con la calidad de los acuerdos de servicio d. Número de acuerdos de servicio revisados, conforme sea necesario
Actividades	Nivel de capacidad
1. Revisar de forma regular los acuerdos de servicio conforme a los términos acordados para garantizar que sean efectivos y estén actualizados. Cuando corresponda, tener en cuenta cambios en requisitos, servicios habilitados por I&T, paquetes de servicio y opciones de nivel de servicio.	3
2. Cuando sea necesario, revisar el acuerdo de servicio vigentes con el proveedor de servicios. Acordar y actualizar los acuerdos operativos internos.	4
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin guía correspondiente para esta práctica de gestión	

B. Componente: Estructuras organizativas											
Práctica clave de gestión	Director de operaciones	Director de TI	Director de tecnología	Comité de riesgos empresariales	Dueños del proceso de negocio	Jefe de operaciones de TI	Jefe de administración de TI	Gestor de Servicios	Gestor de seguridad de la información	Director de privacidad	Asesor legal
AP009.01 Identificar los servicios de I&T.	R	R	A		R			R			
AP009.02 Catalogar los servicios habilitados por I&T.		R	A	R				R			
AP009.03 Definir y preparar acuerdos de servicio.		R	A			R	R	R	R	R	R
AP009.04 Monitorizar y reportar los niveles de servicio.		R	A		R			R			R
AP009.05 Revisar los acuerdos y los contratos de servicio.	R	A	R			R	R	R			
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica										
ISO/IEC 20000-1:2011(E)	4.1.1 Management commitment										

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
AP009.01 Identificar los servicios de I&T.	De	Descripción	Descripción	A
			Brechas identificadas en los servicios de I&T prestados a la empresa	AP001.10; AP002.02; AP005.02; AP008.02
			Definiciones de servicios estándar	EDM02.01
AP009.02 Catalogar los servicios habilitados por I&T.	AP005.04	Portafolios actualizados con programas, servicios y activos	Catálogos de servicios	AP008.05
	EDM04.01	Plan de recursos aprobado		
	EDM04.02	Comunicación de estrategias de gestión de recursos		
AP009.03 Definir y preparar acuerdos de servicio.	AP011.02	Requisitos del cliente para la gestión de la calidad	Acuerdos de nivel de servicio (SLA)	AP005.02; AP008.04; DSS01.02; DSS02.01; DSS02.02; DSS04.01; DSS05.02; DSS05.03
	AP014.07	Requisitos de calidad de los datos	Acuerdos de nivel operativo (OLAs)	DSS01.02; DSS02.07; DSS04.03; DSS05.03
AP009.04 Monitorizar y reportar los niveles de servicio.	AP005.03	Informes de rendimiento del portafolio de inversiones	Planes de acción de mejora y remediaciones	AP002.02; AP008.02
	AP005.05	<ul style="list-style-type: none"> Resultados de beneficios y comunicaciones relacionadas Acciones correctivas para mejorar la obtención de beneficios 	Informes de rendimiento del nivel de servicio	AP008.02; MEA01.03
	AP008.05	Análisis de satisfacción		
	AP011.03	<ul style="list-style-type: none"> Resultados de la monitorización de la calidad para la prestación de servicios y soluciones Causas raíz de los fallos de entrega de calidad 		
	AP011.04	Resultados de las revisiones y auditorías de calidad		
	DSS02.02	Peticiones de servicio e incidentes clasificados y priorizados		
	DSS02.06	Cierre de peticiones de servicio e incidentes		
	DSS02.07	<ul style="list-style-type: none"> Estado de incidentes e informe de tendencias Estado de cumplimiento de peticiones e informe de tendencias 		
	EDM04.03	Acciones remediales para solucionar las desviaciones de gestión de recursos		

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
AP009.05 Revisar los acuerdos y los contratos de servicio.	De	Descripción	Descripción	A
	AP011.02	Resultados de la calidad del servicio, incluidas la retroalimentación de los clientes	SLA actualizados	Interna
	AP011.04	Resultados de las revisiones y auditorías de calidad		
	BAI04.01	Evaluaciones con respecto a los SLA		
	EDM04.03	Retroalimentación sobre la asignación y eficiencia de recursos y capacidades		
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
PMBOK Guide, 6.ª edición, 2017		Part 1: 12. Gestión de proyectos de adquisición: Entradas y salidas		

D. Componente: Personas, habilidades y competencias		
Habilidad	Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión del nivel de servicio	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.2. Service Level Management
Gestión del nivel de servicio	Skills Framework for the Information Age V6, 2015	SLMO

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Guía correspondiente	Referencia específica
Política de acuerdo de nivel de servicio (SLA)	Describe los estándares y criterios generales para informar sobre los requisitos específicos y los plazos de entrega de los servicios, ya sea entre entidades de la empresa o entre la empresa y un tercero.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Guía correspondiente	Referencia específica
Establecer un contrato entre un proveedor de servicios (interno o externo) y el usuario final que define el nivel de servicio esperado. Asegurar que este nivel de servicio se base en la entrega, mediante una definición específica de lo que el cliente recibirá en objetivos SMART (específico, medible, alcanzable, realista y acotado en el tiempo). Establecer una cultura en la que se respeten los niveles de servicio. Disuadir del incumplimiento a través de un sistema de penalización.		

G. Componente: Servicios, infraestructura y aplicaciones	
<ul style="list-style-type: none"> • Sistema de gestión de contratos • Herramientas de monitorización del nivel de servicio 	

Página dejada en blanco intencionadamente

Dominio: Alinear, planificar y organizar Objetivo de gestión: APO10 – Gestionar los proveedores		Área prioritaria: Modelo Core de COBIT
Descripción		
Gestionar los productos y servicios relacionados con I&T proporcionados por todo tipo de proveedores para que satisfagan los requisitos de la empresa. Esto incluye la búsqueda y selección de proveedores, gestión de relaciones, gestión de contratos y revisión y monitorización del rendimiento de proveedores y el ecosistema de proveedores (incluida la cadena ascendente de suministro) para que sea efectiva y cumpla con la legislación.		
Propósito		
Optimizar las capacidades de I&T disponibles para apoyar la estrategia y la hoja de ruta de I&T, minimizar el riesgo asociado con proveedores que no rinden o cumplen con los requisitos y asegurar precios competitivos.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales	➔	Metas de alineamiento
<ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG08 Optimización de la funcionalidad interna de procesos de negocio 		AG05 Prestación de servicios de I&T conforme a los requisitos del negocio
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 <ul style="list-style-type: none"> a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios 		AG05 <ul style="list-style-type: none"> a. Porcentaje de partes interesadas del negocio satisfechas con que la prestación de servicios de I&T cumpla con los niveles de servicio acordados b. Número de interrupciones del negocio debido a incidentes de servicios de I&T c. Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de I&T
EG08 <ul style="list-style-type: none"> a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarial b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores externos con las capacidades de la cadena de suministro 		

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
APO10.01 Identificar y evaluar los contratos y las relaciones con los proveedores. Buscar e identificar continuamente proveedores y clasificarlos en tipo, importancia y criticidad. Establecer criterios de evaluación del proveedor y de los contratos. Evaluar el portafolio general de proveedores y contratos vigentes y alternativos.		a. Porcentaje de criterios de evaluación definidos logrados para los proveedores externos y contratos vigentes b. Porcentaje de proveedores externos alternativos que proporcionan servicios equivalentes a contratos de proveedores externos vigentes
Actividades		Nivel de capacidad
1. Evaluar continuamente el entorno empresarial en búsqueda de nuevos socios y proveedores que puedan proporcionar capacidades complementarias y ayudar a ejecutar la estrategia de I&T, la hoja de ruta y los objetivos empresariales.		3
2. Establecer y mantener los criterios relacionados con el tipo, importancia y criticidad de proveedores y contratos de proveedores, para permitir enfocarse en los proveedores preferidos e importantes.		
3. Identificar, registrar y clasificar los proveedores y los contratos vigentes según los criterios definidos para mantener un registro detallado de proveedores preferidos que se deban gestionar cuidadosamente.		
4. Establecer y mantener un criterio de evaluación de proveedores y contratos para permitir una revisión y comparación general del rendimiento de los proveedores de forma consistente.		4
5. Evaluar y comparar de forma periódica el rendimiento de proveedores vigentes y alternativos para identificar oportunidades o una necesidad apremiante de reconsideración de los contratos de los proveedores actuales.		5
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin guía correspondiente para esta práctica de gestión		

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
AP010.02 Seleccionar proveedores. Seleccionar proveedores externos de acuerdo con una práctica justa y formal para garantizar la mejor selección basado en los requisitos especificados. Los requisitos deben optimizarse con la participación de los proveedores externos potenciales.		a. Número de brechas identificadas entre las ofertas del proveedor seleccionado y las necesidades señaladas en la solicitud de propuesta (RFP) b. Porcentaje de partes interesadas satisfechas con los proveedores
Actividades		Nivel de capacidad
1. Revisar todas las solicitudes de información (RFI) y solicitudes de propuestas (RFP) para asegurar que definan claramente los requisitos (p. ej., los requisitos de la empresa en cuanto a seguridad y privacidad de la información, requisitos de los procesos operativos empresariales y de I&T, prioridades para la prestación del servicio) e incluir un procedimiento para aclarar los requisitos. Las RFI y RFP deben proporcionar a los proveedores el tiempo suficiente para preparar sus propuestas y deben definir claramente los criterios de adjudicación y el proceso de decisión.		2
2. Evaluar las RFI y RFP conforme al proceso/criterios de evaluación aprobados y mantener las pruebas documentales de las evaluaciones. Comprobar las referencias de los proveedores candidatos.		
3. Seleccionar el proveedor que mejor encaje con la RFP. Documentar y comunicar la decisión y firmar el contrato.		
4. En el caso específico de la adquisición de software, incluir y reforzar los derechos y obligaciones de todas las partes en los términos contractuales. Estos derechos y obligaciones podrían incluir la titularidad y licencias de Propiedad Intelectual (PI); mantenimiento; garantías; procedimientos de arbitraje; términos de las actualizaciones; e idoneidad, además de la seguridad, privacidad, escrow (depósito en fideicomiso) y derechos de acceso.		3
5. En el caso específico de la adquisición de recursos para desarrollo, incluir y reforzar los derechos y obligaciones de todas las partes en los términos contractuales. Estos derechos y obligaciones podrían incluir la titularidad y licencias de PI; idoneidad, incluidas las metodologías de desarrollo; pruebas; procesos de gestión de la calidad, incluyendo los criterios de rendimiento requeridos y revisiones de rendimiento; condiciones para el pago; garantías; procedimientos de arbitraje; gestión de los recursos humanos; y cumplimiento con las políticas de la empresa.		
6. Obtener asesoría jurídica sobre los acuerdos de adquisiciones de desarrollo relacionados con la titularidad y licencias de PI.		
7. En el caso específico de la adquisición de infraestructura, instalaciones y servicios relacionados, incluir y reforzar los derechos y obligaciones de todas las partes en los términos contractuales. Estos derechos y obligaciones podrían incluir los niveles de servicio, procedimientos de mantenimiento, controles de acceso, seguridad, privacidad, revisión del rendimiento, condiciones para el pago y procedimientos de arbitraje.		
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin guía correspondiente para esta práctica de gestión		
Práctica de gestión		Métricas modelo
AP010.03 Gestionar los contratos y las relaciones con los proveedores. Formalizar y gestionar la relación con el proveedor para cada uno de los proveedores. Gestionar, mantener y monitorizar los contratos y la prestación de servicios. Asegurar que los contratos nuevos o modificados cumplan con los estándares de la empresa y con los requisitos legales y regulatorios. Tratar las disputas contractuales.		a. Porcentaje de terceros proveedores que tienen contratos que definen los requisitos de control b. Número de disputas formales con proveedores c. Número de reuniones de revisión con los proveedores d. Porcentaje de disputas resueltas amistosamente en un plazo razonable
Actividades		Nivel de capacidad
1. Asignar dueños de relaciones para todos los proveedores y hacerles que rindan cuentas de la calidad del servicio(s) proporcionado(s).		3
2. Especificar una comunicación formal y un proceso de revisión, incluidos las interacciones y calendarios de los proveedores.		
3. Acordar, gestionar, mantener y renovar formalmente los contratos con el proveedor. Asegurar que los contratos cumplan con los estándares de la empresa y con los requisitos legales y regulatorios.		
4. Incluir disposiciones en los contratos con los proveedores de servicio clave para la revisión de las instalaciones del proveedor y de las prácticas internas y de los controles por parte de la dirección o terceros independientes. Acordar una auditoría y controles de aseguramiento independientes de los entornos operativos de proveedores que proporcionen servicios externalizados para confirmar que se han atendido de forma adecuada los requisitos acordados.		
5. Usar procedimientos establecidos para tratar las disputas contractuales. Siempre que sea posible, usar primero relaciones y comunicaciones eficaces para solventar los problemas del servicio.		
6. Definir y formalizar los roles y responsabilidades de cada proveedor de servicio. Cuando se combinen varios proveedores para proporcionar un servicio, considerar asignar un rol de contratista líder a uno de los proveedores para que se haga responsable del contrato general.		
7. Evaluar la eficacia de la relación e identificar las mejoras necesarias.		4
8. Definir, comunicar y acordar la forma de implementar las mejoras requeridas a la relación.		5
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISO/IEC 20000-1:2011(E)		7.2 Supplier management
ITIL V3, 2011		Service Design, 4.8 Supplier Management

A. Componente: Proceso (cont.)		
Práctica de gestión	Métricas modelo	
AP010.04 Gestionar los riesgos de los proveedores. Identificar y gestionar el riesgo relacionado con los proveedores para proporcionar continuamente una prestación de servicios segura, eficiente y eficaz. Esto también incluye a los subcontratistas o proveedores de nivel superior que son relevantes para la prestación del servicio del proveedor directo.	a. Frecuencia de las sesiones de gestión de riesgos con el proveedor b. Número de eventos relacionados con riesgos que conducen a incidentes de servicio c. Porcentaje de incidentes relacionados con el riesgo resueltos de manera aceptable (en tiempo y coste)	
Actividades		Nivel de capacidad
1. Cuando se prepara el contrato, es necesario considerar el posible riesgo de servicio mediante una definición clara de los requisitos de servicio, incluido los acuerdos de depósito en fideicomiso (escrow) de software, acuerdos standby o con proveedores alternativos, para mitigar los posibles fallos del proveedor; seguridad y protección de Propiedad intelectual (PI); privacidad; y cualquier requisito legal o regulatorio.		3
2. Identificar, monitorizar y, donde sea adecuado, gestionar el riesgo relacionado con la habilidad del proveedor para proporcionar el servicio de forma eficaz, eficiente, segura, confidencial, confiable y continua. Integrar los procesos internos críticos de gestión de TI con aquellos de los proveedores de servicios externalizados, para cubrir, por ejemplo, la planificación de rendimiento y capacidad, gestión del cambio y gestión de la configuración.		4
3. Evaluar el ecosistema más amplio del proveedor e identificar, monitorizar y, cuando corresponda, gestionar el riesgo relacionado con los subcontratistas y los proveedores en sentido ascendente que incluyen en la capacidad del proveedor para proporcionar el servicio de forma eficaz, eficiente, segura, confidencial, fiable y continua.		
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
CMMI Cybermaturity Platform, 2018	RM.MP Manage External Participation	
ISF, The Standard of Good Practice for Information Security 2016	SC1.1 External Supplier Management Process	
ISO/IEC 27002:2013/Cor.2:2015(E)	15. Supplier relationships	
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, abril de 2018	D.SC Supply Chain Risk Management	
Práctica de gestión	Métricas modelo	
AP010.05 Supervisar el rendimiento y el cumplimiento del proveedor. Revisar periódicamente el rendimiento general de los proveedores, el cumplimiento con los requisitos contractuales y la ejecución del valor del contrato. Abordar los problemas identificados.	a. Número de incumplimientos en los servicios relacionados con I&T causados por los proveedores b. Porcentaje de proveedores que cumplen con los requisitos acordados	
Actividades		Nivel de capacidad
1. Solicitar revisiones independientes de las prácticas y controles internos del proveedor, si es necesario.		3
2. Definir y documentar los criterios para supervisar el rendimiento de los proveedores alineado con los acuerdos de nivel de servicio. Asegurar que el proveedor informe de forma regular y transparente sobre los criterios acordados.		4
3. Supervisar y revisar la prestación de servicios para garantizar que el proveedor proporcione una calidad del servicio aceptable, cumpla con los requisitos y se adhiera a las condiciones del contrato.		
4. Revisar el rendimiento de los proveedores y la ejecución del valor del contrato. Asegurar que el proveedor sea confiable y competitivo, comparado con los proveedores alternativos y las condiciones del mercado.		
5. Monitorizar y evaluar la información disponible externamente sobre el proveedor y la cadena de suministro del proveedor.		
6. Registrar y evaluar los resultados de la revisión periódicamente y discutirlos con el proveedor para identificar las necesidades y las oportunidades de mejora.		5
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
Sin guía correspondiente para esta práctica de gestión		

B. Componente: Estructuras organizativas

Práctica clave de gestión					Director de riesgos	Director de TI	Director de tecnología	Director de tecnologías digitales	Consejo de gobierno de I&T	Comité de riesgos empresariales	Jefe de desarrollo	Jefe de operaciones de TI	Jefe de administración de TI	Gestor de Servicios	Gestor de seguridad de la información	Director de privacidad	Asesor legal
APO10.01 Identificar y evaluar los contratos y las relaciones con los proveedores.						R	R	R	A				R				R
APO10.02 Seleccionar proveedores.						R	R	R	A		R	R	R	R	R	R	
APO10.03 Gestionar los contratos y las relaciones con los proveedores.						R	R	R	A		R	R	R	R			R
APO10.04 Gestionar los riesgos de los proveedores.					R	R	R	R	A	R	R	R	R	R	R	R	
APO10.05 Supervisar el rendimiento y el cumplimiento del proveedor.					R	R	R	R	A	R	R	R	R	R			R
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)										Referencia específica							
Sin guía correspondiente para este componente.																	

C. Componente: Flujos y elementos de información (ver también la sección 3.6)

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
AP010.01 Identificar y evaluar los contratos y relaciones con los proveedores.	Fuera de COBIT	Contratos de proveedores	Catálogo de proveedores	BAI02.02
			Revisiones posibles a los contratos de los proveedores	Interna
			Importancia del proveedor y criterios de evaluación	Interna
AP010.02 Seleccionar proveedores.	BAI02.02	Plan de desarrollo/adquisiciones de alto nivel	RFI y RFP de proveedores	BAI02.01; BAI02.02
			Evaluaciones de RFI y RFP	BAI02.02
			Resultados de las decisiones de las evaluaciones de proveedores	evaluaciones de proveedores BAI02.02; EDM04.01
AP010.03 Gestionar los contratos y las relaciones con los proveedores.	BAI03.04	Plan de adquisición aprobado	Resultados y mejoras sugeridas	Interna
			Proceso de comunicación y revisión	Interna
			Roles y responsabilidades de los proveedores	Interna
AP010.04 Gestionar los riesgos de los proveedores.	AP012.04	<ul style="list-style-type: none"> Análisis de riesgos e informes del perfil de riesgo para las partes interesadas Resultados de evaluaciones de riesgos de terceros 	Riesgo identificado de prestaciones de los proveedores	AP012.01; AP012.03; BAI01.01; BAI11.01
			Requisitos del contrato identificados para minimizar el riesgo	Interna
AP010.05 Supervisar el rendimiento y el cumplimiento del proveedor.			Criterios de supervisión del cumplimiento de proveedores	Interna
			Resultados de revisión de supervisión del cumplimiento de proveedores	MEA01.03

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)	
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin guía correspondiente para este componente.	

D. Componente: Personas, habilidades y competencias		
Habilidad	Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión de contratos	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework, 2016	D. Enable—D.8. Contract Management
Gestión de contratos	Skills Framework for the Information Age V6, 2015	ITCM
Compras	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	D. Enable—D.4. Purchasing
Abastecimiento	Skills Framework for the Information Age V6, 2015	SORC

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Guía correspondiente	Referencia específica
Política de adquisiciones de TI	Señala los principios y procedimientos para la adquisición de hardware, software y soluciones de hosting de TI. Detalla los estándares de los sistemas operativos, redes de computadores, especificaciones de hardware, etc. Proporciona directrices para la gestión de contratos (p. ej., términos y condiciones, supervisión de contratos).		
Política de gestión de prestación de servicios de terceros de TI.	Establece las directrices para gestionar el riesgo relacionado con los servicios de terceros. Establece el marco de expectativas de comportamientos y enumera las precauciones de seguridad requeridas para los proveedores de servicio externalizados a la hora de gestionar el riesgo relacionado con los servicios proporcionados.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Guía correspondiente	Referencia específica
Crear y gestionar un ecosistema de proveedores que puedan ayudar a la organización con su transformación e innovación digital. Evaluar continuamente el entorno en busca de nuevos socios efectivos.		
La dirección establece el ambiente y ejemplifica los comportamientos correctos cuando se comunica con los proveedores para acordar e implementar las mejoras necesarias. Asegurar que los contratos cumplan con los estándares de la empresa y con los requisitos legales y regulatorios.		

G. Componente: Servicios, infraestructura y aplicaciones	
<ul style="list-style-type: none"> • Sistema de gestión de contratos • Servicios de aseguramiento de terceros 	

Página dejada en blanco intencionadamente

Dominio: Alinear, planificar y organizar Objetivo de gestión: APO11 – Gestionar la calidad		Área prioritaria: Modelo Core de COBIT
Descripción		
Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados empresariales relacionados. Habilitar los controles, monitorización continua y uso de prácticas y estándares probados en esfuerzos de mejora y eficiencia continuos.		
Propósito		
Asegurar la prestación consistente de soluciones y servicios tecnológicos para satisfacer los requisitos de calidad de la empresa y las necesidades de las partes interesadas.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales		Metas de alineamiento
<ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG04 Calidad de la información financiera • EG07 Calidad de la información sobre gestión • EG08 Optimización de la funcionalidad de procesos internos del negocio • EG12 Gestión de programas de transformación digital 	➔	<ul style="list-style-type: none"> • AG09 Ejecución de programas dentro del plazo, sin exceder el presupuesto, y que cumplan con los requisitos y estándares de calidad • AG10 Calidad de la información sobre gestión de I&T
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 <ul style="list-style-type: none"> a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios 		AG09 <ul style="list-style-type: none"> a. Número de programas/proyectos ejecutados a tiempo y dentro del presupuesto b. Número de programas que necesitan una revisión significativa debido a defectos de calidad c. Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto
EG04 <ul style="list-style-type: none"> a. Encuesta de satisfacción de las partes interesadas clave con respecto al nivel de transparencia, comprensión y precisión de la información financiera de la empresa b. Coste de incumplimiento con respecto a regulaciones financieras 		AG10 <ul style="list-style-type: none"> a. Nivel de satisfacción del usuario con la calidad, puntualidad y disponibilidad de la información de gestión relacionada con I&T, tras considerar los recursos disponibles b. Relación y extensión de las decisiones de negocio erróneas en las que la información errónea o no disponible relacionada con I&T fue un factor clave c. Porcentaje de información que satisface los criterios de calidad
EG07 <ul style="list-style-type: none"> a. Grado de satisfacción del consejo de administración y la dirección ejecutiva con la información para la toma de decisiones b. Número de incidentes causados por decisiones erróneas de negocio basadas en información imprecisa c. Tiempo que se tarda en proporcionar la información que respalde la toma de decisiones empresariales eficaces d. Periodicidad de la información sobre gestión 		
EG08 <ul style="list-style-type: none"> a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarial b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro 		
EG12 <ul style="list-style-type: none"> a. Número de programas ejecutados a tiempo y dentro del presupuesto b. Porcentaje de partes interesadas satisfechas con la ejecución del programa c. Porcentaje de programas de transformación del negocio detenidos d. Porcentaje de programas de transformación del negocio con actualizaciones del estado notificadas regularmente 		

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
AP011.01 Establecer un sistema de gestión de calidad (SGC). Establecer y mantener un sistema de gestión de calidad (SGC) que proporciona un enfoque estándar, formal y continuo para la gestión de calidad de la información. El SGC debería habilitar la tecnología y los procesos del negocio que están alineados con los requisitos del negocio y la gestión de la calidad empresarial.		a. Porcentaje de la eficacia de las revisiones de gestión de la calidad b. Porcentaje de satisfacción de partes interesadas clave con el programa de revisión de gestión de la calidad
Actividades		Nivel de capacidad
1. Asegurar que el marco de control de I&T y los procesos empresariales y de TI, incluyen una estrategia estándar, formal y continua con respecto a la gestión de la calidad que está alineada con los requisitos de la empresa. Dentro del marco de control de I&T y los procesos empresariales y de TI, identificar los requisitos y criterios de calidad (p. ej. conforme con los requisitos legales y los requisitos de los clientes).		3
2. Definir roles, tareas y derechos de decisión y responsabilidades para la gestión de la calidad en la estructura organizativa.		
3. Obtener insumos de la dirección y las partes interesadas externas e internas sobre la definición de los requisitos de calidad y los criterios de gestión de la calidad.		
4. Gestionar y revisar regularmente el SGC frente a los criterios de aceptación acordados. Incluir retroalimentación de los clientes, usuarios y dirección.		4
5. Responder a las discrepancias de los resultados de la revisión para mejorar continuamente el SGC.		5
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
PMBOK Guide, 6.ª edición, 2017		Part 1: 8.1 Plan quality management
Práctica de gestión		Métricas modelo
AP011.02: Enfocar la gestión de la calidad en los clientes. Enfocar la gestión de la calidad en los clientes para determinar sus requisitos y asegurar su integración en las prácticas de gestión de la calidad.		a. Porcentaje de satisfacción del cliente b. Porcentaje de requisitos y expectativas del cliente comunicadas a la empresa y la organización de TI
Actividades		Nivel de capacidad
1. Enfocar la gestión de la calidad en los clientes para determinar los requisitos del cliente interno y externo y asegurar el alineamiento de los estándares y las prácticas de I&T. Definir y comunicar los roles y responsabilidades relacionados con la resolución de conflictos entre el usuario/cliente y la organización de TI.		3
2. Gestionar las necesidades y expectativas empresariales para cada proceso de negocio y servicio operativo y nuevas soluciones de TI. Mantener sus criterios de aceptación de calidad.		
3. Comunicar los requisitos y expectativas del cliente al negocio y la organización de TI		
4. Obtener las opiniones de clientes de forma periódica sobre los procesos de negocio y la prestación de servicios y entrega de soluciones de TI. Determinar el impacto de los estándares y prácticas de I&T y garantizar que se satisfagan y pongan en práctica las expectativas del cliente.		4
5. Capturar los criterios de aceptación de calidad para su inclusión en los SLA.		
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin guía correspondiente para esta práctica de gestión		
Práctica de gestión		Métricas modelo
AP011.03 Gestionar los estándares, prácticas y procedimientos de calidad e integrar la gestión de la calidad en los procesos y soluciones clave. Identificar y mantener los requisitos, estándares, procedimientos y prácticas para los procesos clave con el fin de guiar a la empresa hacia el logro de los estándares de gestión de la calidad (SGC) acordados. Esta actividad debería alinearse con los requisitos del marco de control de I&T. Considerar la certificación de procesos clave, unidades organizativas, productos o servicios.		a. Número de procesos con requisitos de calidad definidos b. Número de defectos descubiertos antes del paso a producción c. Número de servicios con un plan formal de gestión de la calidad d. Número de SLAs que incluyen criterios de aceptación de la calidad

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Definir los estándares, prácticas y procedimientos de gestión de la calidad en línea con los requisitos del marco de control de I&T y los criterios y políticas de gestión de la calidad empresariales.	2
2. Integrar las prácticas de gestión de la calidad requeridas en procesos y soluciones clave en toda la organización.	3
3. Cuantificar los beneficios y costes de las certificaciones de calidad.	
4. Comunicar de forma eficaz el enfoque de gestión de la calidad (p. ej., a través de programas de capacitación de calidad formales y regulares).	
5. Registrar y monitorizar los datos de calidad. Usar buenas prácticas de la industria como referencia a la hora de mejorar y personalizar las prácticas de calidad de la empresa.	4
6. Revisar regularmente la relevancia, eficiencia y eficacia continua de los procesos específicos de gestión de calidad. Monitorizar el logro de los objetivos de calidad.	
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
PMBOK Guide, 6.ª edición, 2017	Part 1: 8.2 Manage quality
Práctica de gestión	Métricas modelo
AP011.04 Llevar a cabo la monitorización, control y revisiones de calidad. Monitorizar la calidad de los procesos y los servicios de forma continua, en línea con los estándares de gestión de la calidad. Definir, planificar e implementar medidas para monitorizar la satisfacción del cliente con la calidad, así como con el valor proporcionado por el sistema de gestión de la calidad (SGC). El Dueño del proceso debería utilizar la información recopilada para mejorar la calidad.	a. Porcentaje de soluciones y servicios entregados con certificación formal b. Calificación promedio de satisfacción de las partes interesadas con las soluciones y los servicios c. Número de procesos con un reporte formal de evaluación de la calidad d. Porcentaje de proyectos revisados que cumplen con las metas y los objetivos de calidad esperados e. Número, robustez y plazo de los análisis de riesgo
Actividades	Nivel de capacidad
1. Preparar y realizar las revisiones de calidad para procesos y soluciones organizativas clave.	3
2. Para estos procesos y soluciones organizativas clave, monitorizar las métricas de calidad basadas en metas alineadas con los objetivos generales en cuanto a calidad.	4
3. Asegurar que la dirección y los responsables de los procesos revisen regularmente el rendimiento de la gestión de la calidad en comparación con las métricas de calidad definidas.	
4. Analizar los resultados generales del rendimiento de gestión de la calidad.	
5. Informar sobre los resultados de revisión de rendimiento y gestión de la calidad e iniciar las mejoras necesarias.	5
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
PMBOK Guide, 6.ª edición, 2017	Part 1: 8.3 Control quality
Práctica de gestión	Métricas modelo
AP011.05 Mantener la mejora continua. Mantener y comunicar periódicamente un plan de calidad general que promueva la mejora continua. El plan debería definir la necesidad y los beneficios de la mejora continua. Obtener y analizar datos sobre el sistema de gestión de la calidad (SGC) y mejorar su efectividad. Corregir las no conformidades para evitar la recurrencia.	a. Número de análisis de causa raíz completados b. Porcentaje de servicios y productos completados dentro del plazo
Actividades	Nivel de capacidad
1. Establecer una plataforma para compartir buenas prácticas y captar información sobre los defectos y errores para permitir el aprendizaje a partir de ellos.	2
2. Identificar ejemplos de procesos de entrega de calidad excelente que puedan beneficiar a otros servicios o proyectos. Compartirlos con los equipos de ejecución de proyectos y servicios para fomentar la mejora.	3
3. Identificar ejemplos recurrentes de defectos de calidad. Determinar su causa raíz, evaluar su impacto y resultado y acordar acciones de mejora con los equipos de ejecución del servicio y/o proyecto.	
4. Proporcionar a los empleados formación en métodos y herramientas de mejora continua.	
5. Hacer un análisis comparativo de los resultados de benchmarks de calidad con los datos históricos internos, directrices de la industria, estándares y datos de tipos de empresas similares.	4
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, abril de 2018	DE.DP Detection Processes

B. Componente: Estructuras organizativas																																		
Práctica clave de gestión										Director de operaciones	Director de riesgos	Director de TI	Director de tecnología	Director de tecnologías digitales	Consejo de gobierno de I&T	Dueños del proceso de negocio	Gestor de Portafolio	Gestor de programas	Jefe de proyecto	Oficina de gestión de proyectos	Función de gestión de datos	Jefe de arquitectura	Jefe de desarrollo	Jefe de operaciones de TI	Jefe de administración de TI	Gestor de servicio	Gestor de seguridad de la información	Gestor de continuidad del negocio						
										A		R		R															R	R				
												A		R		R															R			
												A	R	R		R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	
											R	A		R	R	R																R		
												A				R	R	R	R	R		R	R	R	R	R	R	R	R	R	R	R	R	R
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)										Referencia específica																								
Sin guía correspondiente para este componente.																																		

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
AP011.01 Establecer un sistema de gestión de calidad (SGC).	Fuera de COBIT	Sistema de calidad empresarial	Roles, responsabilidades y derechos de decisión del sistema de gestión de calidad (SGC)	AP001.05; DSS06.03
			Planes de gestión de la calidad	AP014.04; AP014.06; BAI01.07; BAI11.05
			Resultados de las revisiones de eficiencia del SGC	BAI03.06
AP011.02: Enfocar la gestión de la calidad en los clientes.	Fuera de COBIT	Requisitos de calidad del negocio y los clientes	Requisitos del cliente para la gestión de la calidad	AP008.05; AP009.03; BAI01.07; BAI11.06
			Resultados de la calidad del servicio, incluida la retroalimentación de los clientes	AP008.05; AP009.05; BAI05.01; BAI07.07
			Criterios de aceptación	BAI02.01; BAI02.02

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
APO11.03 Gestionar los estándares, prácticas y procedimientos de calidad e integrar la gestión de la calidad en los procesos y soluciones clave.	De	Descripción	Descripción	A
	BAI02.04	Revisión de la calidad aprobada	Estándares de gestión de calidad	Todos los APO; todos los BAI; todos los DSS; todos los MEA
	Fuera de COBIT	• Certificaciones de calidad disponibles • Buenas prácticas de la industria	• Causas raíz de los fallos de entrega de calidad	AP008.02; AP009.04; BAI07.08; MEA02.04; MEA04.04
			Resultados de la monitorización de la calidad	AP008.05; AP009.04; BAI07.08
APO11.04 Llevar a cabo la monitorización, control y revisiones de calidad.	BAI03.06	• Plan de aseguramiento de calidad • Resultados, excepciones y correcciones de la revisión de calidad	Metas y métricas del proceso de calidad del servicio	Todos los APO; todos los BAI; Todos los DSS; todos los MEA
	DSS02.07	• Estado de incidentes e informe de tendencias • Estado de cumplimiento de peticiones e informe de tendencias	Resultados de las revisiones y auditorías de calidad	AP008.05; AP009.04; AP009.05; BAI07.08
APO11.05 Mantener la mejora continua.			Resultados del benchmark de revisión de calidad	Todos los APO; todos los BAI; Todos los DSS; todos los MEA
			Ejemplos de buenas prácticas a compartir	Todos los APO; todos los BAI; Todos los DSS; todos los MEA
			Comunicaciones sobre mejora continua y mejores prácticas	Todos los APO; todos los BAI; Todos los DSS; todos los MEA
Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
PMBOK Guide, 6.ª edición, 2017		Part 1: 8. Gestión de la calidad de proyectos: Entradas y salidas (inputs y outputs)		

D. Componente: Personas, habilidades y competencias		
Habilidad	Guía correspondiente (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Desarrollo de estrategias de calidad de la tecnología de la información y las telecomunicaciones (ICT)	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	D. Enable—D.2. ICT Quality Desarrollo de estrategia
Aseguramiento de calidad	Skills Framework for the Information Age V6, 2015	QUAS
Gestión de la calidad	Skills Framework for the Information Age V6, 2015	QUMG
Estándares de calidad	Skills Framework for the Information Age V6, 2015	QUST

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Guía correspondiente	Referencia específica
Política de gestión de la calidad	Captar la visión de la gestión de los objetivos de calidad de la empresa, nivel de calidad aceptable y labores de equipos y entidades específicas para garantizar la calidad.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Guía correspondiente	Referencia específica
Promover una cultura de calidad y mejora continua. Mantener y comunicar periódicamente la necesidad, y los beneficios, de la calidad y la mejora continua.		

G. Componente: Servicios, infraestructura y aplicaciones		
<ul style="list-style-type: none">• SGC• Servicios de aseguramiento de calidad de terceros		

Dominio: Alinear, Planificar y Organizar Objetivo de gestión: APO12–Gestionar el riesgo		Área prioritaria: Modelo Core de COBIT
Descripción		
Identificar, evaluar y reducir continuamente los riesgos relacionados con I&T dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la empresa.		
Propósito		
Integrar la gestión del riesgo empresarial relacionado con la I&T con la gestión del riesgo empresarial global (ERM), y equilibrar los costes y beneficios de la gestión del riesgo empresarial relacionado con las I&T.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales <ul style="list-style-type: none"> • EG02 Gestión de riesgo de negocio • EG06 Continuidad y disponibilidad del servicio de negocio 	➔	Metas de alineamiento <ul style="list-style-type: none"> • AG02 Gestión de riesgo relacionado con I&T • AG07 Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad
Métricas modelo para metas empresariales EG02 a. Porcentaje de objetivos y servicios críticos del negocio, cubiertos por la evaluación de riesgos b. Proporción de incidentes significativos que no se identificaron en la evaluación de riesgos frente al total de incidentes c. Frecuencia de actualización del perfil de riesgo EG06 a. Número de interrupciones del servicio al cliente o procesos empresariales que han causado incidentes significativos b. Coste de incidentes para el negocio c. Número de horas de procesamiento de negocio perdidas debido a interrupciones del servicio no planificadas d. Porcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados		Métricas modelo para metas de alineamiento AG02 a. Frecuencia de actualización del perfil de riesgo b. Porcentaje de las evaluaciones de riesgo en la empresa que incluyen el riesgo relacionado con la I&T c. Número de incidentes significativos relacionados con I&T que no se identificaron en la evaluación de riesgos AG07 a. Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o descrédito público b. Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o descrédito público c. Número de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o descrédito público

A. Componente: Proceso		
Práctica de gestión	Métricas modelo	
APO12.01 Recopilar datos. Identificar y recopilar datos relevantes para habilitar una efectiva identificación, análisis y reporte de los riesgos relacionados con I&T.	a. Número de eventos de pérdida con características clave capturados en repositorios b. Porcentaje de auditorías, eventos y tendencias capturados en repositorios c. Porcentaje de sistemas críticos con problemas conocidos	
Actividades	Nivel de capacidad	
1. Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con el riesgo de I&T.	2	
2. Registrar datos relevantes y significativos relacionados con los riesgos de I&T en el entorno operativo interno y externo de la empresa.		
3. Adoptar o definir una taxonomía de riesgo para las definiciones consistentes de escenarios de riesgo y categorías de impacto y probabilidad.	3	
4. Registrar datos de eventos de riesgo que han causado o podrían causar impacto en el negocio conforme a las categorías de impacto definidas en la taxonomía de riesgo. Capturar datos relevantes de cuestiones, incidentes, problemas e investigaciones.		
5. Estudiar y analizar los datos históricos de riesgo de I&T y de pérdidas experimentadas a partir de datos y tendencias externos disponibles, homólogos de la industria a través de logs de eventos de la industria, bases de datos, y acuerdos de la industria, para la publicación común de eventos.	4	
6. Para clases de eventos similares, organizar los datos recopilados y resaltar los factores causantes. Determinar los factores causantes comunes en múltiples eventos.		
7. Determinar las condiciones específicas que existieron o estuvieron ausentes cuando tuvieron lugar los eventos de riesgo y la forma en que las condiciones afectaron a la frecuencia del evento y la magnitud de la pérdida.		
8. Realizar un análisis periódico de eventos y factores de riesgo para identificar riesgos nuevos o emergentes y para mejorar el entendimiento de los factores de riesgo internos y externos asociados.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
CMMI Data Management Maturity Model, 2014	Supporting Processes - Risk Management	
COSO Enterprise Risk Management, junio de 2017	8. Performance—Principle 10	
ISO/IEC 27005:2011(E)	8.2 Risk identification; 12. Information security risk monitoring and review	
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018	3.1 Preparation (Task 7)	

A. Componente: Proceso (cont.)		
Práctica de gestión	Métricas modelo	
AP012.02 Analizar el riesgo. Desarrollar una visión fundamentada del riesgo de I&T vigente, que soporte las decisiones de riesgo.	a. Número de escenarios de riesgo de I&T identificados b. Tiempo transcurrido desde la última actualización de los escenarios de riesgos de I&T	
Actividades	Nivel de capacidad	
1. Definir el alcance adecuado de los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y/o la criticidad de los activos para el negocio.	3	
2. Crear y actualizar regularmente los escenarios de riesgo de I&T; las exposiciones a pérdidas relacionadas con I&T; y los escenarios relacionados con el riesgo reputacional, incluidos escenarios compuestos de tipos de amenazas y eventos en cascada y/o coincidentes. Desarrollar previsiones para actividades de control específicas y capacidades de detección.		
3. Estimar la frecuencia (o probabilidad) y la magnitud de la pérdida o ganancia asociada con escenarios de riesgos de I&T. Tener en cuenta todos los factores de riesgo aplicables y evaluar controles operativos conocidos.		
4. Comparar el riesgo actual (exposición a pérdidas de I&T) con el apetito al riesgo y la tolerancia de riesgo aceptable. Identificar el riesgo inaceptable o elevado.		
5. Proponer respuestas al riesgo para riesgos que excedan el apetito al riesgo y los niveles de tolerancia.		
6. Especificar los requisitos de alto nivel para los proyectos o programas que implementarán las respuestas a los riesgos seleccionadas. Identificar los requisitos y expectativas para los controles clave adecuados a fin de proporcionar respuestas de mitigación de riesgos.		
7. Validar el análisis de riesgo y los resultados del análisis de impacto del negocio (BIA) antes de usarlos en la toma de decisiones. Confirmar que el análisis se corresponde con los requisitos empresariales y comprobar que los sesgos de las estimaciones se calibraron y analizaron de forma adecuada.	4	
8. Analizar el coste/beneficio de las posibles opciones de respuesta al riesgo, como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/aprovechar. Confirmar la respuesta óptima al riesgo.	5	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
CMMI Data Management Maturity Model, 2014	Supporting Processes—Risk Management	
COSO Enterprise Risk Management, junio de 2017	8. Performance—Principle 11	
ISF, The Standard of Good Practice for Information Security 2016	IR2.1 Risk Assessment Scope; IR2.2 Business Impact Assessment	
ISO/IEC 27001:2013/Cor.2:2015(E)	8.2 Information security risk assessment	
ISO/IEC 27005:2011(E)	8.3 Risk analysis	
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, abril de 2018	ID.RA Risk Assessment	
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018	3.6 Authorization (Task 3)	
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.17 Risk assessment (RA-3)	
Práctica de gestión	Métricas modelo	
AP012.03 Mantener un perfil de riesgo. Mantener un inventario de los riesgos conocidos y los atributos de riesgo, incluidos la frecuencia esperada, impacto potencial y respuestas. Documentar los recursos, capacidades y actividades de control actuales relacionados con elementos de riesgo.	a. Complejidad de atributos y valores en el perfil de riesgo b. Porcentaje de procesos clave de negocio incluidos en el perfil de riesgo	
Actividades	Nivel de capacidad	
1. Hacer un inventario de los procesos de negocio y documentar su dependencia con los procesos de gestión de servicios de I&T y los recursos de infraestructura de TI. Identificar el personal de apoyo, aplicaciones, infraestructura, instalaciones, registros manuales críticos, contratistas, proveedores, y terceros.	2	
2. Determinar y acordar qué servicios de I&T y recursos de infraestructura de TI son esenciales para sostener el funcionamiento de los procesos de negocio. Analizar las dependencias e identificar los eslabones débiles.		
3. Agregar los escenarios de riesgos actuales por categoría, línea de negocio y área funcional.		
4. Capturar regularmente toda la información del perfil de riesgo y consolidarla en un perfil de riesgo agregado.	3	
5. Capturar información sobre el estado del plan de acción de riesgos para su inclusión en el perfil de riesgo de I&T de la empresa.		
6. Con base en todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan una identificación y monitorización rápida del riesgo actual y las tendencias de riesgo.	4	
7. Capturar información sobre eventos de riesgo de I&T que se han materializado para su inclusión en el perfil de riesgo de TI de la empresa.		

A. Componente: Proceso (cont.)	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Cybermaturity Platform, 2018	RS.DT Define Organizational Risk Tolerance
COSO Enterprise Risk Management, junio de 2017	8. Performance—Principle 12
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.17 Risk assessment (RA-7)
Práctica de gestión	Métricas modelo
AP012.04 Articular el riesgo. Comunicar de manera oportuna información sobre el estado actual de las exposiciones y oportunidades relacionadas con I&T a todas las partes interesadas requeridas para obtener una respuesta apropiada.	a. Nivel de satisfacción de las partes interesadas con los informes de riesgos proporcionados b. Completitud de los informes del perfil de riesgos (incluida información alineada con los requisitos de las partes interesadas) c. Uso de informes de riesgos en la toma de decisiones de gestión
Actividades	Nivel de capacidad
1. Informar sobre los resultados del análisis de riesgo a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones empresariales. Siempre que sea posible, incluir las probabilidades y rangos de pérdidas o ganancias, junto con los niveles de confianza, para permitir que la gerencia haga balance del retorno del riesgo.	3
2. Proporcionar a los responsables de la toma de decisiones la comprensión de los escenarios más probables y peores, exposiciones a pérdidas de I&T y consideraciones significativas de reputación, legales y regulatorias, o cualquier otra categoría de impacto conforme a la taxonomía de riesgos.	
3. Informar sobre el perfil de riesgo actual a todas las partes interesadas. Incluir información sobre la eficacia del proceso de gestión de riesgos, eficacia del control, brechas, inconsistencias, redundancias, estado de remediación y sus impactos en el perfil de riesgo.	
4. De forma periódica, en áreas con riesgos relativos y capacidades de riesgo similares, identificar oportunidades relacionadas con I&T que permitirían la aceptación de un riesgo mayor y un mayor crecimiento y retorno.	
5. Revisar los resultados de las evaluaciones objetivas de terceros y revisiones de auditoría interna y de aseguramiento de la calidad. Incluirlos en el perfil de riesgo. Revisar las brechas identificadas y las exposiciones de pérdidas relacionadas con I&T para determinar la necesidad de un análisis de riesgos adicional.	4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Cybermaturity Platform, 2018	RS.CR Determine Critical Infrastructure Requirements
COSO Enterprise Risk Management, junio de 2017	10. Information, Communication, and Reporting—Principle 19
ISO/IEC 27005:2011(E)	11. Comunicación y consulta de riesgos de seguridad de la información
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, abril de 2018	ID.RM Risk Management Strategy
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.15 Program management (PM-32)
Práctica de gestión	Métricas modelo
AP012.05 Definir un portafolio con acciones de gestión de riesgos. Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.	a. Número de incidentes significativos no identificados e incluidos en el portafolio de gestión de riesgos b. Porcentaje de propuestas de proyectos de gestión de riesgos rechazadas por falta de consideración de otros riesgos relacionados
Actividades	Nivel de capacidad
1. Mantener un inventario de las actividades de control que se han implantado para mitigar el riesgo y que permiten que se tomen riesgos alineados con el apetito y la tolerancia al riesgo. Clasificar las actividades de control y asignarlas a escenarios de riesgos de I&T específicos y escenarios de riesgos de I&T agregados.	2
2. Determinar si cada entidad organizativa monitoriza el riesgo y acepta la responsabilidad de actuar dentro de los niveles de tolerancia individuales y del portafolio.	3
3. Definir un conjunto de propuestas de proyectos equilibrada diseñada para reducir el riesgo y/o proyectos que permitan oportunidades empresariales estratégicas, con consideración de los costes, beneficios, efecto en el perfil de riesgo actual y en las regulaciones.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Data Management Maturity Model, 2014	Supporting Processes—Risk Management
COSO Enterprise Risk Management, junio de 2017	8. Performance—Principle 14
HITRUST CSF versión 9, septiembre de 2017	03.01 Risk Management Program

MARCO DE REFERENCIA COBIT® 2019: OBJETIVOS DE GOBIERNO Y GESTIÓN

A. Componente: Proceso (cont.)		
Práctica de gestión	Métricas modelo	
AP012.06 Responder al riesgo. Responder de manera oportuna a eventos de riesgo materializados con medidas eficaces para limitar la magnitud de las pérdidas.	a. Número de medidas que no reducen el riesgo residual b. Porcentaje de planes de acción de riesgo de I&T ejecutados según se diseñaron	
Actividades	Nivel de capacidad	
1. Preparar, mantener y probar planes que documenten los pasos específicos que deben darse cuando un evento de riesgo pudiera causar un incidente significativo de desarrollo u operativo con un impacto grave para el negocio. Asegurar que los planes incluyan vías de escalamiento en la empresa.	3	
2. Aplicar el plan de respuesta adecuado para minimizar el impacto cuando ocurren incidentes de riesgo.		
3. Clasificar los incidentes y comparar las exposiciones a pérdidas relacionadas con I&T con los umbrales de tolerancia al riesgo. Comunicar los impactos de negocio a los responsables de la toma de decisiones como parte del reporte y actualización del perfil de riesgo.	4	
4. Examinar eventos adversos/pérdidas y oportunidades del pasado no consideradas y determinar las causas raíz.		
5. Comunicar la causa raíz, requisitos adicionales de respuestas al riesgo y mejoras del proceso a los responsables de la toma de decisiones correspondientes. Asegurar que la causa, requisitos de respuesta y mejora del proceso se incluyan en los procesos de gobierno del riesgo.	5	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
COSO Enterprise Risk Management, junio de 2017	8. Performance—Principle 13	
ISF, The Standard of Good Practice for Information Security 2016	IR2.9 Risk Treatment	
ISO/IEC 27001:2013/Cor.2:2015(E)	6.1 Action to address risk and opportunities	
ISO/IEC 27005:2011(E)	9. Information security risk treatment	
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018	3.6 Authorization (Task 4)	
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.15 Program management (PM-9, PM-31)	

B. Componente: Estructuras organizativas																
Práctica clave de gestión	Director de riesgos	Director de TI	Director de tecnología	Director de tecnologías digitales	Comité de riesgos empresariales	Director de seguridad de la información	Dueños del proceso de negocio	Oficina de gestión de proyectos	Función de gestión de datos	Jefe de arquitectura	Jefe de desarrollo	Jefe de operaciones de TI	Jefe de administración de TI	Gestor de servicios	Gestor de seguridad de la información	Gestor de continuidad del negocio
AP012.01 Recopilar datos.	A	R	R	R		R	R	R	R	R	R	R	R	R	R	R
AP012.02 Analizar el riesgo.	A	R			R		R									
AP012.03 Mantener un perfil de riesgo.	A	R			R		R									
AP012.04 Articular el riesgo.	A	R			R		R									
AP012.05 Definir un portafolio con acciones de gestión de riesgos.	A	R			R		R									
AP012.06 Responder al riesgo.	R	A	R	R		R	R	R		R	R	R	R	R	R	R
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica															
National Institute of Standards and Technology Special Publication 800-37, Revisión 2, septiembre de 2017	3.1 Preparation (Task 1); Appendix A: Roles and Responsibilities															

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
AP012.01 Recopilar datos.	De	Descripción	Descripción	A
	AP002.02	Deficiencias y riesgos relacionados con las capacidades actuales	Problemas y factores de riesgo emergentes	AP001.01; AP002.02; EDM03.01
	AP002.05	Iniciativas de evaluación de riesgos	Datos sobre eventos de riesgo y factores causantes	Interna
	AP010.04	Riesgo identificado en prestaciones de los proveedores	Datos sobre el entorno operativo relacionados con el riesgo	Interna
	DSS02.07	Estado de incidentes e informe de tendencias		
	EDM03.01	Evaluación de actividades de gestión de riesgos		
	EDM03.02	<ul style="list-style-type: none"> Políticas de gestión de riesgos Objetivos clave a monitorizar para la gestión de riesgos Proceso aprobado para la medición de la gestión de riesgos 		
AP012.02 Analizar el riesgo.	DSS04.02	Análisis de impacto en el negocio (BIA)	Resultados del análisis de riesgos	AP001.01; AP002.02; EDM03.03; BAI01.08; BAI11.06
	DSS05.01	Evaluaciones de amenazas potenciales	Escenarios de riesgo de I&T	Interna
	Fuera de COBIT	Avisos de amenazas	Alcance del esfuerzo de análisis de riesgos	Interna
AP012.03 Mantener un perfil de riesgo.	AP010.04	Riesgo identificado en las prestaciones de los proveedores	Perfil de riesgo agregado, incluido el estado de las acciones de gestión de riesgos	AP002.02; EDM03.02
	DSS05.01	Evaluaciones de amenazas potenciales	Escenarios de riesgo documentados por línea de negocio y función	Interna
	EDM03.01	<ul style="list-style-type: none"> Guía del apetito de riesgo Niveles aprobados de tolerancia al riesgo 		
AP012.04 Articular el riesgo.			Análisis de riesgos e informes del perfil de riesgo para las partes interesadas	AP010.04; EDM03.03; EDM05.02; MEA04.05
			Resultados de evaluaciones de riesgos de terceros	AP010.04; EDM03.03; MEA02.01
			Oportunidades para la aceptación de un mayor riesgo	EDM03.03

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
APO12.05 Definir un portafolio con acciones de gestión de riesgos.	De	Descripción	Descripción	A
			Propuestas de proyecto para reducir el riesgo	AP002.02; AP013.02
APO12.06 Responder al riesgo.	EDM03.03	Acciones correctivas para solucionar las desviaciones de gestión de riesgos	Comunicación de impacto del riesgo	AP001.02; AP008.04; DSS04.02
			Causas raíz relacionadas con el riesgo	DSS02.03; DSS03.01; DSS03.02; DSS03.03; DSS03.05; DSS04.02; MEA02.04; MEA04.04; MEA04.06
			Plan de respuesta a incidentes relacionados con riesgos	DSS02.05
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
COSO Enterprise Risk Management, junio de 2017		10. Information, Communication, and Reporting—Principle 20		
SF, The Standard of Good Practice for Information Security 2016		IR1.3 Information Risk Assessment—Supporting Material		
National Institute of Standards and Technology Special Publication 800-37, Revisión 2, septiembre de 2017		3.1 Preparation (Task 7): Inputs and Outputs; 3.6 Authorization (Task 3, 4): Entradas y salidas (inputs y outputs)		
PMBOK Guide, 6.ª edición, 2017		Part 1: 11. Project risk management: Inputs and Outputs		

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión de riesgos de negocio	Skills Framework for the Information Age V6, 2015	BURM
Aseguramiento de la información	Skills Framework for the Information Age V6, 2015	INAS
Gestión de riesgos	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.3. Risk Management

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de riesgo empresarial	Define el gobierno y gestión del riesgo empresarial a nivel estratégico, táctico y operativo, en búsqueda de alcanzar los objetivos de negocio. Traduce el gobierno de la empresa en política y principios de gobierno del riesgo y elabora actividades de gestión de riesgos.	National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.17 Risk assessment (RA-1)
Política de riesgo de fraude	Informa sobre la protección de la marca, reputación y activos empresariales en caso de pérdida o daño derivados de fraude o mala conducta. Orienta a los empleados a la hora de informar sobre actividades sospechosas y manipulación de información sensible y la evidencia. Fomenta una cultura antifraude y cultiva una concienciación de los riesgos.	National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), August 2018	

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Con el objeto de respaldar una cultura del riesgo participativa y transparente, la alta dirección debería establecer el rumbo y mostrar un apoyo visible y genuino a la incorporación de las prácticas de riesgo en toda la empresa. La dirección debería fomentar una comunicación abierta y la propiedad empresarial sobre los riesgos de negocio relacionados con I&T. Los comportamientos deseables incluyen el alineamiento de políticas conforme al apetito al riesgo definido, comunicación de tendencias de riesgo a la alta dirección y organismos de gobierno de riesgos, recompensa a una gestión de riesgos eficaz y monitorización proactiva de riesgos y progreso con respecto al plan de acción sobre riesgos.	ISF, The Standard of Good Practice for Information Security 2016	IR1.2 Information Risk Assessment

G. Componente: Servicios, infraestructura y aplicaciones
<ul style="list-style-type: none"> • Servicios de gestión de crisis • Herramientas de gobierno, riesgo y cumplimiento (GRC) • Herramientas de análisis de riesgos • Servicios de inteligencia de riesgos

Página dejada en blanco intencionadamente

Dominio: Alinear, planificar y organizar Objetivo de gestión: APO13–Gestionar la seguridad		Área prioritaria: Modelo Core de COBIT
Descripción		
Definir, operar y monitorizar un sistema de gestión de seguridad de la información.		
Propósito		
Mantener el impacto y la ocurrencia de incidentes de seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales	➔	Metas de alineamiento
<ul style="list-style-type: none"> • EG02 Gestión de riesgo de negocio • EG06 Continuidad y disponibilidad del servicio del negocio 		AG07 Seguridad de la información, infraestructura y aplicaciones de procesamiento y privacidad
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG02 <ul style="list-style-type: none"> a. Porcentaje de objetivos de negocio y servicios críticos cubiertos por la evaluación de riesgos b. Proporción de incidentes significativos que no se identificaron en la evaluación de riesgos frente al total de incidentes c. Frecuencia de actualización del perfil de riesgo 		AG07 <ul style="list-style-type: none"> a. Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o descrédito público b. Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o descrédito público c. Número de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o descrédito público
EG06 <ul style="list-style-type: none"> a. Número de interrupciones del servicio al cliente o procesos de negocio que han causado incidentes significativos b. Coste de incidentes para el negocio c. Número de horas de procesamiento de negocio perdidas debido a interrupciones del servicio no planificadas d. Porcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados 		

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
APO13.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI). Establecer y mantener un sistema de gestión de seguridad de la información (SGSI) que proporcione un enfoque estándar, formal y continuo para la gestión de la seguridad de la información, mediante la habilitación de tecnología segura y procesos de negocio alineados con los requisitos del negocio.		a. Nivel de satisfacción de las partes interesadas con el plan de seguridad en toda la empresa
Actividades		Nivel de capacidad
1. Definir el alcance y los límites del sistema de gestión de seguridad de la información (SGSI) en términos de las características de la empresa, organización, ubicación, activos y tecnología. Incluir detalles y justificación de las exclusiones del alcance.		2
2. Definir un SGSI conforme a la política empresarial y el contexto en el que opera la empresa.		
3. Alinear el SGSI con el enfoque global de la empresa hacia la gestión de la seguridad.		
4. Obtener la autorización de la dirección para implementar y operar o cambiar el SGSI.		
5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.		
6. Definir y comunicar los roles y responsabilidades de la gestión de seguridad de la información.		
7. Comunicar la estrategia de SGSI.		

A. Componente: Proceso (cont.)		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
HITRUST CSF versión 9, septiembre de 2017		0.01 Information Security Management program
ISO/IEC 20000-1:2011(E)		6.6 Information security management
ITIL V3, 2011		Service Design, 4.7 Information Security Management
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018		3.3 Selection (Task 1); 3.4 Implementation (Task 1)
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.17 Risk assessment (RA-2)
Práctica de gestión		Métricas modelo
AP013.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad. Mantener un plan de seguridad de la información que describa cómo se debe manejar el riesgo de seguridad de la información y cómo se debe alinear con la estrategia y la arquitectura de la empresa. Asegurar que las recomendaciones para implementar mejoras a la seguridad se basen en casos de negocio aprobados, implementados como una parte integral del desarrollo de servicios y soluciones, y que operen como una parte integral de la operación del negocio.		a. Porcentaje de simulaciones de escenarios de riesgo de seguridad exitosas b. Número de empleados que han completado con éxito una formación de concienciación sobre seguridad de la información
Actividades		Nivel de capacidad
1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con objetivos estratégicos y la arquitectura empresarial. Asegurar que el plan identifique las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, responsabilidades y prioridades asociados para la gestión de los riesgos de seguridad de la información identificados.		3
2. Mantener, como parte de la arquitectura de la empresa, un inventario de los componentes de la solución establecida para gestionar los riesgos relacionados con la seguridad.		
3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad, apoyadas por casos de negocio apropiados que incluyan consideraciones de financiación y asignación de roles y responsabilidades.		
4. Proporcionar aportes para el diseño y desarrollo de prácticas y soluciones de gestión, seleccionadas en el plan de tratamiento de riesgos de seguridad de la información.		
5. Implementar programas de formación y concienciación sobre seguridad de la información y privacidad.		
6. Integrar la planificación, diseño, implementación y monitorización de procedimientos de seguridad de la información y privacidad y otros controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad.		4
7. Definir cómo medir la eficacia de las prácticas de gestión seleccionadas. Especificar cómo deben usarse estas medidas para evaluar la eficacia para producir resultados comparables y reproducibles.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
AP013.03 Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI). Mantener y comunicar periódicamente la necesidad y los beneficios de una mejora continua de seguridad de la información. Recopilar y analizar datos sobre el sistema de gestión de seguridad de la información (SGSI) y mejorar su efectividad. Corregir los incumplimientos para evitar la recurrencia.		a. Frecuencia de revisiones de seguridad programadas b. Número de hallazgos en revisiones de seguridad programadas regularmente c. Nivel de satisfacción de las partes interesadas con el plan de seguridad d. Número de incidentes relacionados con la seguridad causados por no adherirse adecuadamente al plan de seguridad

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Llevar a cabo revisiones regulares de la eficacia del SGSI. Incluir el cumplimiento de la política y los objetivos del SGSI y revisar las prácticas de seguridad y privacidad.	4
2. Realizar auditorías de SGSI a intervalos planificados.	
3. Realizar periódicamente una revisión de la gestión del SGSI para asegurar que el alcance sigue siendo adecuado y que se identifican mejoras en el proceso del SGSI.	
4. Registrar acciones y eventos que podrían tener un impacto en la eficacia o el rendimiento del SGSI.	
5. Hacer aportes para el mantenimiento de los planes de seguridad para tener en cuenta los hallazgos de las actividades de monitorización y revisión.	5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018	3.3 Selection (Task 3)

B. Componente: Estructuras organizativas												
Práctica clave de gestión	Director de TI	Director de tecnología	Comité de riesgos empresariales	Director de seguridad de la información	Dueños del proceso de negocio	Oficina de gestión de proyectos	Jefe de arquitectura	Jefe de desarrollo	Jefe de operaciones de TI	Jefe de administración de TI	Gestor de servicios	Gestor de seguridad de la información
AP013.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).	R		R	A						R		R
AP013.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad.	R		R	A						R		R
AP013.03 Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI).	R	R		A	R	R	R	R	R	R	R	R
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica											
ISF, The Standard of Good Practice for Information Security 2016	SG1.2 Security Direction											
ISO/IEC 27002:2013/Cor.2:2015(E)	6.1 Internal organization											

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
AP013.01 Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).	Fuera de COBIT	Estrategia de seguridad de la empresa	Declaración del alcance de la SGSI	AP001.05; DSS06.03
			Política de SGSI	Interna
AP013.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información.	AP002.04	Brechas y cambios requeridos para lograr la capacidad del objetivo	Plan de tratamiento del riesgo de seguridad de la información	Todos los APO; todos los BAI; Todos los DSS; todos los MEA; todos los EDM
	AP003.02	Descripciones de la línea base del dominio y definición de arquitectura	Casos de negocio de seguridad de la información	AP005.02
	AP012.05	Propuestas de proyecto para reducir el riesgo		

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
AP013.03 Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI).		Descripción	Descripción	A
	DSS02.02	Peticiones de servicio e incidentes clasificadas y priorizadas	Recomendaciones para la mejora del sistema de gestión de seguridad de la información (SGSI)	Interna
			Informes de auditoría del sistema de gestión de seguridad de la información (SGSI)	MEA02.01
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
National Institute of Standards and Technology Special Publication 800-37, Revisión 2, septiembre de 2017		3.3 Selection (Tasks 1, 3): Inputs and Outputs; 3.4 Implementation (Task 1): Inputs and Outputs		

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Seguridad de la información	Skills Framework for the Information Age V6, 2015	SCTY
Desarrollo de la estrategia de seguridad de la información	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework, 2016	D. Enable—D.1. Information Security Strategy Development

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de seguridad de la información y privacidad	Establecer las directrices de comportamiento para proteger la información, sistemas e infraestructura corporativa. Debido a que los requisitos del negocio en cuanto a seguridad y almacenamiento son más dinámicos que la gestión de riesgos y privacidad de I&T, su gobierno debería gestionarse aislado del riesgo y privacidad de I&T. Para alcanzar la eficiencia operativa, sincronizar la política de seguridad de la información con el riesgo y la política de privacidad de I&T.	(1) ISO/IEC 27001:2013/Cor.2:2015(E); (2) ISO/IEC 27002:2013/Cor.2:2015(E); (3) National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017; (4) HITRUST CSF version 9, September 2017; (5) ISF, The Standard of Good Practice for Information Security 2016	(1) 5.2 Policy; (2) 5. Information security policies; (3) 3.2 Awareness and training (AT-1); (4) 04.01 Information Security Policy; (5) SM1.1 Information Security Policy

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Establecer una cultura de concienciación de seguridad y privacidad que influya de forma positiva en el comportamiento deseado y la implementación real de la política de seguridad y privacidad en la práctica diaria. Proporcionar las suficientes directrices de seguridad y privacidad, indicar quiénes son los campeones en seguridad y privacidad (incluidos altos ejecutivos, líderes de RR. HH., profesionales de seguridad y/o privacidad) y apoyar y comunicar de forma proactiva los programas, innovaciones y desafíos de seguridad y privacidad.	(1) ISO/IEC 27001:2013/Cor.2:2015(E); (2) Creating a Culture of Security, ISACA, 2011	1) 7.3 Awareness; (2) Framework to achieve an intentional security aware culture (all chapters)

G. Componente: Servicios, infraestructura y aplicaciones	
<ul style="list-style-type: none"> Herramientas de gestión de la configuración Servicios de concienciación de seguridad y privacidad Servicios de evaluación de seguridad de terceros 	

Dominio: Alinear, planificar y organizar Objetivo de gestión: APO14 – Gestionar los datos		Área prioritaria: Modelo Core de COBIT
Descripción		
Lograr y mantener la gestión eficaz de los activos de datos de la empresa durante todo el ciclo de vida de los datos, desde la creación hasta su entrega, mantenimiento y archivo.		
Propósito		
Garantizar el uso eficaz de activos de datos críticos para lograr las metas y objetivos empresariales.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales	➔	Metas de alineamiento
<ul style="list-style-type: none"> • EG04 Calidad de la información financiera • EG07 Calidad de la información sobre gestión 		AG10 Calidad de la información sobre gestión de I&T
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG04 <ul style="list-style-type: none"> a. Encuesta de satisfacción de las partes interesadas clave con respecto al nivel de transparencia, comprensión y precisión de la información financiera de la empresa b. Coste de incumplimiento con respecto a regulaciones financieras 		AG10 <ul style="list-style-type: none"> a. Nivel de satisfacción del usuario con la calidad, puntualidad y disponibilidad de la información de gestión relacionada con I&T, tras considerar los recursos disponibles b. Proporción y extensión de las decisiones de negocio erróneas en las que la información errónea o no disponible relacionada con I&T fue un factor clave c. Porcentaje de información que satisface los criterios de calidad
EG07 <ul style="list-style-type: none"> a. Grado de satisfacción del consejo de administración y la dirección ejecutiva con la información para la toma de decisiones b. Número de incidentes causados por decisiones erróneas de negocio basadas en información imprecisa c. Tiempo que se tarda en proporcionar la información que respalde la toma de decisiones de negocio eficaces d. Puntualidad de la información sobre gestión 		

A. Componente: Proceso		
Práctica de gestión	Métricas modelo	
APO14.01 Definir y comunicar la estrategia y los roles y responsabilidades de la gestión de datos de la organización. Definir cómo gestionar y mejorar los activos de datos de la organización, en línea con la estrategia y objetivos de la empresa. Comunicar la estrategia de gestión de datos a todas las partes interesadas. Asignar roles y responsabilidades para garantizar que los datos corporativos se gestionen como activos críticos e implementar y mantener la estrategia de gestión de datos de forma eficaz y sostenible.	a. Número de violaciones de gestión de datos comparado con la estrategia definida b. Porcentaje de roles y responsabilidades identificadas para respaldar el gobierno de la gestión de datos y la interacción entre gobierno y la función de gestión de datos.	
Actividades		Nivel de capacidad
1. Establecer una función de gestión de los datos con responsabilidad de gestionar las actividades que respalden los objetivos de gestión de los datos.		2
2. Especificar roles y responsabilidades para respaldar la gestión de los datos y la interacción entre el gobierno y la función de gestión de datos.		
3. Asegurar que el negocio y la tecnología desarrollan de forma colaborativa la estrategia de gestión de datos de la organización. Asegurar que los objetivos, prioridades y alcance de la gestión de datos reflejen los objetivos empresariales, sean consistentes con las políticas y regulación de gestión de datos y cuenten con la aprobación de todas las partes interesadas.		3
4. Comunicar los objetivos, prioridades y alcance de la gestión de datos y ajustarlos conforme sea necesario, con base en la retroalimentación recibida.		
5. Usar métricas para evaluar y monitorizar la consecución de los objetivos de la gestión de datos.		4
6. Monitorizar el plan secuencial para la implementación de la estrategia de gestión de datos. Actualizarla como corresponda, con base en las revisiones de su progreso.		
7. Usar técnicas estadísticas y otras técnicas cuantitativas para evaluar la eficacia de los objetivos estratégicos de la gestión de datos a la hora de lograr los objetivos de negocio. Realizar las modificaciones necesarias, con base en las métricas.		
8. Asegurar que la organización investiga procesos innovadores de negocio y requisitos regulatorios emergentes para garantizar que el programa de gestión de datos sea compatible con futuras necesidades del negocio.		5
9. Realizar contribuciones a las mejores prácticas de la industria para el desarrollo e implementación de la estrategia de gestión de datos.		

A. Componente: Proceso (cont.)	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Data Management Maturity Model, 2014	Data Management Strategy - Data Management Strategy; Data Governance– Governance Management
ITIL V3, 2011	Service Design, 5.2 Management of Data and Information
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016	CSC 13: Data Protection
Práctica de gestión	Métricas modelo
AP014.02 Definir y mantener un glosario empresarial consistente. Crear, aprobar, actualizar y promover términos y definiciones de negocio consistentes para fomentar el uso compartido de datos en la organización.	a. Nivel de aceptación y frecuencia del uso de términos del glosario empresarial en toda la organización b. Número de sinónimos para la terminología del glosario de negocio definido que se usan en nuevos esfuerzos de desarrollo c. Nivel de granularidad de los términos definidos en el glosario empresarial
Actividades	Nivel de capacidad
1. Asegurar que los términos estándar de negocio estén disponibles y se comuniquen a las partes interesadas relevantes.	2
2. Asegurar que cada término de negocio añadido al glosario empresarial tenga un nombre y una definición únicos.	
3. Usar términos y definiciones de negocio estándar de la industria, como corresponda, en el glosario empresarial.	
4. Establecer, documentar y seguir un proceso para definir, gestionar, utilizar y mantener el glosario empresarial. Por ejemplo, las nuevas iniciativas deberían aplicar los términos estándar de negocio como parte del proceso de definición de requisitos de datos para garantizar la consistencia del lenguaje. Esto contribuye a lograr que el contenido se pueda comparar y facilitar el intercambio de datos en la organización.	3
5. Garantizar que el nuevo desarrollo, la integración de datos y trabajos de consolidación de datos aplican términos estándar de negocio como parte del proceso de definición de requisitos de datos.	
6. Integrar el glosario empresarial en el repositorio de metadatos de la organización, con permisos de acceso adecuados.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Data Management Maturity Model, 2014	Data Governance - Business Glossary
ISF, The Standard of Good Practice for Information Security 2016	IM1.1 Information Classification and Handling
Práctica de gestión	Métricas modelo
AP014.03 Establecer los procesos y la infraestructura para la gestión de metadatos. Establecer los procesos y la infraestructura para especificar y extender los metadatos sobre los activos de datos de la organización, para fomentar y respaldar el intercambio de datos, garantizar el cumplimiento del uso de datos, mejorar la respuesta de los cambios empresariales y reducir el riesgo relacionado con los datos.	a. Número de imprecisiones identificadas en los metadatos b. Porcentaje de metadatos que contienen medidas y métricas para evaluar la precisión y adopción de metadatos
Actividades	Nivel de capacidad
1. Establecer y seguir un proceso de gestión de metadatos.	2
2. Asegurar que la documentación de metadatos considera las interdependencias entre los datos.	
3. Establecer y seguir categorías, propiedades y estándares de metadatos.	
4. Desarrollar y usar los metadatos para realizar un análisis del impacto de los posibles cambios en los datos.	3
5. Poblar el repositorio de metadatos de la organización con categorías y clasificaciones adicionales de metadatos conforme a un plan de implementación por fases. Vincularlo con las capas de arquitectura.	
6. Validar los metadatos y cualquier cambio a los metadatos con la arquitectura actual.	
7. Asegurar que la organización haya desarrollado un metamodelo, integrado implementado en todas las plataformas.	
8. Asegurar que los tipos de metadatos y las definiciones de datos respaldan prácticas de importación, suscripción y consumo consistentes.	4
9. Usar medidas y métricas para evaluar la precisión y la adopción de los metadatos.	
10. Evaluar los cambios de datos planificados para generar un impacto en el repositorio de metadatos. Mejorar continuamente los procesos de captura, cambio y perfeccionamiento de los metadatos.	5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Data Management Maturity Model, 2014	Data Governance–Metadata Management
ISO/IEC 27002:2013/Cor.2:2015(E)	8.2 Information classification

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
AP014.04 Definir una estrategia de calidad de los datos. Definir una estrategia integrada en toda la organización para lograr y mantener el nivel de calidad de datos (como la complejidad, integridad, precisión, integridad, exactitud, completitud, validez, trazabilidad y oportunidad) requerido para respaldar las metas y objetivos empresariales.		a. Número de esfuerzos de mejora de la calidad de los datos identificados y registrados en un plan secuencial b. Porcentaje de partes interesadas satisfechas con la calidad de los datos
Actividades		Nivel de capacidad
1. Definir una estrategia de calidad de los datos en colaboración con las partes interesadas empresariales y tecnológicas, aprobada y gestionada por la dirección ejecutiva. La estrategia debería favorecer pasar del estado actual al objetivo. También debe alinearse de forma explícita con los objetivos empresariales y la estrategia de gestión de datos de la organización.		3
2. Asegurar que la estrategia de calidad de los datos se respete en toda la organización y venga acompañada de las políticas, procesos y directrices correspondientes.		
3. Afianzar las políticas, procesos y gobierno de la estrategia de calidad de los datos durante todo el ciclo de vida de los datos. Exigir los procesos correspondientes en la metodología del ciclo de vida de desarrollo del sistema.		
4. Desarrollar, monitorizar y mantener un plan secuencial para el esfuerzo de mejora de la calidad de los datos en toda la organización.		
5. Para evaluar el progreso, supervisar los planes a fin de cumplir las metas y objetivos de la estrategia de calidad de los datos.		4
6. Recopilar sistemáticamente los informes de las partes interesadas sobre problemas de calidad de los datos. Incluir sus expectativas para mejorar la calidad de los datos en la estrategia de calidad de los datos. Medirlos y monitorizarlos.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		DP.DR Safeguard Data at Rest; DP.DT Safeguard Data in Transit; DP.IP Integrity and Data Leak Prevention
CMMI Data Management Maturity Model, 2014		Data Quality - Data Quality Strategy
Práctica de gestión		Métricas modelo
AP014.05 Establecer las metodologías, procesos y herramientas para la creación de perfiles de datos. Implementar metodologías, procesos, prácticas, herramientas y plantillas para la creación de perfiles de datos estándares que puedan aplicarse en varios repositorios de datos y almacenes de datos.		a. Número de plantillas de datos definidas e implementadas y porcentaje de uso b. Número de conjuntos de datos compartidos con un perfil de datos definido
Actividades		Nivel de capacidad
1. Definir y estandarizar metodologías, procesos, prácticas, herramientas y plantillas de resultados de perfilado de datos. Asegurar que los procesos de creación de perfiles sean reutilizables y aprovechables en distintos almacenes de datos y repositorios de datos compartidos.		3
2. Asegurar que la gestión de datos identifique las series de datos principales compartidas que se monitorizan y perfilan regularmente		4
3. En trabajos de creación de perfiles de datos, incluir la evaluación de conformidad del contenido de los datos con sus metadatos y estándares aprobados.		
4. Durante una actividad de creación de perfiles de datos, comparar los problemas actuales con los problemas pronosticados estadísticamente, conforme a los resultados de creación de perfiles históricos.		
5. Garantizar que los resultados se almacenen de forma central y se analicen y monitoricen sistemáticamente con respecto a estadísticas y métricas. Proporcionar la información resultante para mejorar la calidad de los datos con el tiempo.		
6. Crear informes de perfiles en tiempo real o casi en tiempo real para todas las fuentes y repositorios de datos críticos.		5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Data Management Maturity Model, 2014		Data Quality—Data Profiling
National Institute of Standards and Technology Special Publication 800-53, Revisión 5, agosto de 2017		3.20 System and information integrity (SI-1)
Práctica de gestión		Métricas modelo
AP014.06 Asegurar un enfoque de evaluación de la calidad de los datos. Proporcionar un enfoque sistemático para medir y evaluar la calidad de los datos conforme a los procesos y técnicas y contra las reglas de calidad de los datos.		a. Número de problemas identificados en los resultados de evaluaciones de la calidad de los datos b. Número de resultados de evaluaciones de la calidad de los datos que incluyen recomendaciones para su remediación

A. Componente: Proceso (cont.)		
Actividades		Nivel de capacidad
1. Realizar de forma periódica evaluaciones de la calidad de los datos, conforme a una frecuencia aprobada por la política de evaluación de calidad de los datos. Asegurar que el gobierno de los datos determine la serie de atributos clave por área temática para las evaluaciones de calidad de los datos.		4
2. Incluir recomendaciones para su remediación , con explicaciones, en los resultados de evaluaciones de calidad de los datos.		
3. Evaluar la calidad de los datos, usar los umbrales y los objetivos establecidos para cada dimensión de calidad seleccionada.		
4. Generar informes de medición de la calidad de los datos de forma sistemática, basados en la criticidad de atributos y la volatilidad de los datos.		
5. Revisar y mejorar continuamente la evaluación de calidad de los datos y los procesos de generación de informes.		5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
CMMI Data Management Maturity Model, 2014	Data Quality—Data Quality Assessment	
Práctica de gestión	Métricas modelo	
AP014.07 Definir la estrategia de depuración de datos. Definir los mecanismos, reglas, procesos y métodos para validar y corregir los datos conforme a las reglas empresariales predefinidas.	a. Porcentaje de datos depurados correctamente b. Porcentaje de SLAs que incluyen criterios de calidad de datos y definen que quienes deben rendir cuentas sobre la depuración de los datos son los proveedores de datos	
Actividades		Nivel de capacidad
1. Establecer y mantener una política de depuración de datos.		2
2. Mantener un historial de cambio de datos a través de actividades de depuración.		3
3. Establecer métodos para corregir los datos y definir esos métodos dentro de un plan. Los métodos podrían incluir diversas comparaciones de repositorios, la verificación con relación a una fuente válida, comprobaciones lógicas, integridad referencial o rango de tolerancia.		4
4. En los acuerdos de nivel de servicio, incluir criterios de calidad de los datos que definan que quienes rinden cuentas sobre los datos depurados son los proveedores de datos.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
CMMI Data Management Maturity Model, 2014	Data Quality—Data Cleansing	
Práctica de gestión	Métricas modelo	
AP014.08 Gestionar el ciclo de vida de los activos de datos. Garantizar que la organización entienda, correlacione inventarios, y controle sus flujos de datos a través de los procesos empresariales durante todo el ciclo de vida de los datos, desde su creación o adquisición hasta su eliminación.	a. Número de requisitos de los consumidores de datos que no pueden correlacionarse con una fuente de datos b. Número de conjuntos de datos compartidos c. Tiempo transcurrido desde la última comprobación de cumplimiento con relación a la asignación de los procesos empresariales a los datos	
Actividades		Nivel de capacidad
1. Asignar y alinear los requisitos de los consumidores y productores de datos.		2
2. Definir las relaciones entre el proceso empresarial y los datos. Mantenerlas y revisarlas periódicamente para su cumplimiento.		3
3. Seguir un proceso definido para los acuerdos de colaboración con respecto a los datos compartidos y el uso de datos dentro de los procesos empresariales.		
4. Implementar flujos de datos y mapas completos de ciclo de vida íntegros entre datos y procesos para datos compartidos para los procesos empresariales importantes a nivel organizativo.		
5. Garantizar que los cambios a las series de datos compartidos o series de datos objetivo para un fin empresarial específico se gestionan por estructuras de gobierno de datos, con la participación de las partes interesadas relevantes.		
6. Usar métricas para ampliar la reutilización de los datos compartidos aprobados y eliminar la redundancia de procesos.		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
CMMI Data Management Maturity Model, 2014	Data Operations—Data Lifecycle Management	

A. Componente: Proceso (cont.)		
Práctica de gestión	Métricas modelo	
AP014.09 Soportar el archivo y retención de datos. Asegurar que el mantenimiento de datos satisfaga los requisitos organizativos y regulatorios para la disponibilidad de datos históricos. Asegurar que se cumplan los requisitos legales y regulatorios para el archivado y retención de datos.	a. Porcentaje de intentos no exitosos para transferir datos a su archivo b. Porcentaje de mantenimientos de datos que cumplen los requisitos organizativos y regulatorios para la disponibilidad de datos históricos y los requisitos legales y regulatorios para el archivado y retención de datos	
Actividades	Nivel de capacidad	
1. Asegurar que las políticas rijan la gestión de la historia de datos, incluidos los requisitos de retención, destrucción y pistas de auditoría	2	
2. Asegurar la existencia de un método definido que garantice el acceso a los datos históricos necesarios para respaldar las necesidades empresariales.		
3. Usar la política y los procesos para controlar el acceso, transmisión y modificaciones a datos históricos y archivados.		
4. Asegurar que la organización dispone de un repositorio de data warehouse que proporcione acceso a datos históricos para satisfacer las necesidades analíticas y respaldar los procesos empresariales.	3	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
CMMI Data Management Maturity Model, 2014	Platform and Architecture—Historical Data, Retention and Archiving	
Práctica de gestión	Métricas modelo	
AP014.10 Gestionar los acuerdos de toma de copia de seguridad y restauración de datos. Gestionar la disponibilidad de datos críticos para garantizar la continuidad operativa.	a. Porcentaje de intentos fallidos para hacer una copia de seguridad (backup) de datos b. Porcentaje de intentos satisfactorios para hacer una restauración de un backup de datos	
Actividades	Nivel de capacidad	
1. Definir una programación para garantizar una copia de seguridad (backup) correcta de todos los datos críticos.	2	
2. Definir requisitos para el almacenamiento en las instalaciones (on-site) y fuera de ellas (off-site) de copias de seguridad de datos, teniendo en cuenta el volumen, capacidad y periodo de retención, en línea con los requisitos empresariales.		
3. Establecer una programación para probar el backup de datos.. Asegurar que los datos puedan restaurarse de forma correcta sin un impacto drástico en el negocio.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016	CSC 10: Data Recovery Capability	

B. Componente: Estructuras organizativas								
Práctica clave de gestión	Director de riesgos	Director de TI	Director de tecnologías digitales	Comité de riesgos empresariales	Director de seguridad de la información	Función de gestión de datos	Asesor legal	
AP014.01 Definir y comunicar la estrategia y los roles y responsabilidades de la gestión de datos de la organización.	R	A	R		R	R		
AP014.02 Definir y mantener un glosario empresarial consistente.	R	A	R		R	R		
AP014.03 Establecer los procesos y la infraestructura para la gestión de metadatos.	R	A	R		R	R		
AP014.04 Definir una estrategia de calidad de los datos.	R	A	R		R	R		
AP014.05 Establecer las metodologías, procesos y herramientas para la creación de perfiles de datos.	R	A	R		R	R		
AP014.06 Asegurar un enfoque de evaluación de la calidad de los datos.	R	A	R		R	R		
AP014.07 Definir la estrategia de depuración de datos.	R	A	R		R	R		
AP014.08 Gestionar el ciclo de vida de los activos de datos.	R	A	R	R	R	R	R	
AP014.09 Soportar el archivado y retención de datos.	R	A	R	R	R	R	R	
AP014.10 Gestionar los acuerdos de toma de copias de seguridad y restauración de datos.	R	A	R		R	R	R	

B. Componente: Estructuras organizativas (cont.)	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin documentación relacionada para este componente.	

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
APO14.01 Definir y comunicar la estrategia y los roles y responsabilidades de la gestión de datos de la organización.	De	Descripción	Descripción	A
	APO01.06	Directrices de clasificación de datos	Estrategia de gestión de datos	APO03.02; APO14.10
	APO07.03	Matriz de habilidades y competencias	Roles y responsabilidades acordados para la gestión y el gobierno de datos	Interna
	Fuera de COBIT	• Estrategia empresarial • Políticas y regulación de gestión de datos	Publicaciones externas y presentaciones sobre las mejores prácticas en conferencias de la industria	Interna
Plan de implementación para la estrategia de gestión de datos			Interna	
APO14.02 Definir y mantener un glosario empresarial consistente.			Glosario empresarial	APO14.03; BAI02.01
APO14.03 Establecer los procesos y la infraestructura para la gestión de metadatos.	APO03.02	Modelo de arquitectura de la información	Documentación de metadatos	APO03.02
	APO14.02	Glosario empresarial		
APO14.04 Definir una estrategia de calidad de los datos.	APO01.06	Procedimientos de integridad de los datos	Estrategia de calidad de los datos	APO14.05; APO14.06; APO14.07
	APO01.07	Directrices de seguridad y control de los datos	Informes sobre problemas de calidad de los datos	Interna
	APO11.01	Planes de gestión de la calidad	Plan de mejora de la calidad de los datos	Interna
APO14.05 Establecer las metodologías, procesos y herramientas para la creación de perfiles de datos.	APO14.04	Estrategia de calidad de los datos	Metodologías, procesos, prácticas, herramientas y plantillas de resultados para el perfilado de datos.	Interna
APO14.06 Asegurar un enfoque de evaluación de la calidad de los datos.	APO11.01	Planes de gestión de la calidad	Resultados de la evaluación de la calidad de los datos	Interna
	APO14.04	Estrategia de calidad de los datos		
APO14.07 Definir la estrategia de depuración de datos.	APO14.04	Estrategia de calidad de los datos	Requisitos de calidad de los datos	APO09.03
APO14.08 Gestionar el ciclo de vida de los activos de datos.	APO01.07	Directrices de seguridad y control de los datos		
	DSS04.07	Copia de seguridad de los datos		
APO14.09 Soportar el archivo y retención de datos.	DSS06.05	Requisitos de retención	Archivado de datos	Interna
APO14.10 Gestionar los acuerdos de toma de copias de seguridad y restauración de datos.	APO01.07	Directrices de seguridad y control de los datos	Plan de prueba a las copias de seguridad	DSS04.07
	APO14.01	Estrategia de gestión de datos	Plan de copias de seguridad	DSS04.07
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Data analysis	Skills Framework for the Information Age V6, 2015	DTAN
Gestión de datos	Skills Framework for the Information Age V6, 2015	DATM
Aseguramiento de la información	Skills Framework for the Information Age V6, 2015	INAS
Gestión de la información	Skills Framework for the Information Age V6, 2015	IRMG

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de depuración de datos	Señalar el compromiso de la dirección con la depuración de los datos Prescribe la frecuencia, directrices y rendición de cuentas; documenta los métodos, soluciones y herramientas disponibles	CMMI Data Management Maturity Model, 2014	Data Cleansing
Política de gestión de datos	Describir el compromiso de la organización para gestionar los activos de datos durante todo el ciclo de vida de los mismos, desde su creación hasta su entrega, mantenimiento y archivado.		
Política de evaluación de la calidad de los datos	Describe la filosofía de evaluación del aseguramiento de la calidad de los datos de la organización para garantizar la integridad de los datos que se utilizan en la toma de decisiones que afectan a la organización. Asigna la frecuencia, directrices y rendición de cuentas de la evaluación de la calidad de los datos. Señala los métodos, soluciones y herramientas disponibles.	(1) CMMI Data Management Maturity Model, 2014; (2) National Institute of Standards and Technology Special Publication 800- 53, Revisión 5 (Borrador), agosto de 2017	(1) Data Quality Assessment; (2) 3.20 System and information integrity (SI-1)
Política de privacidad	Documenta la recogida, uso, revelación y gestión de los datos personales. Los datos personales pueden ser cualquier dato que pudiera utilizarse para identificar un individuo, incluidos pero no limitados a, nombre, dirección, fecha de nacimiento, estado civil, información de contacto, fecha de expedición y caducidad del ID, registros financieros, información de crédito, historial médico, destino de viaje e intención de adquirir bienes y servicios. La política de privacidad define cómo una empresa recopila, almacena y publica información personal; cómo y cuándo se informa al cliente de información específica que se recopila y si se mantiene confidencial, se comparte con socios o se vende a otras compañías o empresas. La política obliga el cumplimiento con la legislación relacionada con la protección de datos.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Crear una cultura de responsabilidad compartida para los activos de datos de la organización; reconocer el valor potencial de los activos de datos y garantizar que los roles y responsabilidades estén claros para el gobierno y gestión de activos de datos.	CMMI Data Management Maturity Model, 2014	Gobierno de datos
Crea concienciación alrededor de la integridad, exactitud, completitud y protección de los datos para establecer una cultura de calidad de datos. Relacionar la calidad de los datos con los valores principales de la empresa. Comunica de forma continua el impacto y los riesgos de la pérdida de datos. Asegura que los empleados entiendan el verdadero coste de no implementar una cultura de calidad de los datos.	CMMI Data Management Maturity Model, 2014	Calidad de los datos
G. Componente: Servicios, infraestructura y aplicaciones		
<ul style="list-style-type: none"> • Herramientas de modelado de datos • Repositorios de datos 		

4.3 CONSTRUIR, ADQUIRIR E IMPLEMENTAR (BAI)

- 01 Gestionar los programas
- 02 Gestionar la definición de requisitos
- 03 Gestionar la identificación y construcción de soluciones
- 04 Gestionar la disponibilidad y la capacidad
- 05 Gestionar el cambio organizativo
- 06 Gestionar los cambios de TI
- 07 Gestionar la aceptación y transición de los cambios de TI
- 08 Gestionar el conocimiento
- 09 Gestionar los activos
- 10 Gestionar la configuración
- 11 Gestionar los proyectos

Página dejada en blanco intencionadamente

Dominio: Construir, adquirir e implementar Objetivo de gestión: BAI01 – Gestionar los programas		Área prioritaria: Modelo Core de COBIT
Descripción		
Gestionar todos los programas del portafolio de inversión, de conformidad con la estrategia de la empresa y de forma coordinada, según un enfoque de gestión de programas estándar. Iniciar, planificar, controlar y ejecutar programas, y monitorizar el valor esperado del programa.		
Propósito		
Obtener el valor de negocio deseado y reducir el riesgo de retrasos, costes y erosión de valor inesperados. Para ello, mejorar las comunicaciones y la participación del negocio y usuarios finales, garantizar el valor y la calidad de los entregables del programa y realizar un seguimiento de los proyectos dentro de los programas, y maximizar la contribución del programa al portafolio de inversiones.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales	➔	Metas de alineamiento
<ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG08 Optimización de la funcionalidad de procesos internos del negocio • EG12 Gestión de programas de transformación digital 		<ul style="list-style-type: none"> • AG03 Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T • AG09 Ejecución de programas dentro de plazo, sin exceder el presupuesto, y que cumplan con los requisitos y estándares de calidad
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 <ul style="list-style-type: none"> a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios 		AG03 <ul style="list-style-type: none"> a. Porcentaje de inversiones posibilitadas por la I&T en las que los beneficios previstos se cumplen o exceden b. Porcentaje de servicios de I&T para los que se han logrado los beneficios esperados (indicados en los acuerdos de nivel de servicio)
EG08 <ul style="list-style-type: none"> a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarial b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro 		AG09 <ul style="list-style-type: none"> a. Número de programas/proyectos ejecutados a tiempo y dentro del presupuesto b. Número de programas que necesitan una revisión significativa debido a defectos de calidad c. Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto
EG12 <ul style="list-style-type: none"> a. Número de programas ejecutados a tiempo y dentro del presupuesto b. Porcentaje de partes interesadas satisfechas con la ejecución del programa c. Porcentaje de programas de transformación del negocio suspendidos d. Porcentaje de programas de transformación del negocio con actualizaciones de estado notificadas regularmente 		

A. Componente: Proceso		
Práctica de gestión	Métricas modelo	
BAI01.01 Mantener un enfoque estándar en la gestión de programas. Mantener un enfoque estándar para la gestión de programas que permita la revisión del gobierno y la gestión, la toma de decisiones y las actividades de gestión de la entrega. Estas actividades deben centrarse de consistentemente en el valor y los objetivos de la empresa (es decir, los requisitos, riesgo, costes, calendario y objetivos de calidad).	a. Porcentaje de programas exitosos conforme a la estrategia estándar definida b. Porcentaje de partes interesadas satisfechas con la gestión de programas	
Actividades	Nivel de capacidad	
1. Mantener y hacer cumplir una estrategia estándar de gestión de programas, alineada con el entorno específico de la empresa y con buenas prácticas, basadas en procesos definidos y al uso apropiado de la tecnología. Asegurar que la estrategia cubra todo el ciclo de vida y las disciplinas a seguir, incluida la gestión del alcance de , recursos, riesgo, coste, calidad, tiempo, comunicación, participación de las partes interesadas, adquisiciones, control de cambio, integración y obtención de beneficios.	2	
2. Establecer una oficina de programas o una oficina de gestión de proyectos (PMO) que mantenga una estrategia estándar para la gestión de programas y proyectos en toda la organización. La PMO respalda todos los programas y proyectos mediante la creación y el mantenimiento de plantillas de documentación de proyectos requeridos, formación y mejores prácticas para los gestores de programa/proyecto, seguimiento de las métricas sobre el uso de las mejores prácticas para la gestión de proyectos, etc. En algunos casos, la PMO podría también informar del progreso del programa/proyecto a la alta dirección y/o las partes interesadas, ayudar a priorizar proyectos y asegurar que todos los proyectos respaldan los objetivos globales de negocio de la empresa.	3	
3. Evaluar las lecciones aprendidas con base en el uso de la estrategia de gestión de programas y actualizar la estrategia, según sea necesario.	4	

A. Componente: Proceso (cont.)		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
BAI01.02 Iniciar un programa. Iniciar un programa para confirmar los beneficios esperados y obtener autorización para proceder. Esto incluye acordar el patrocinio, confirmar el mandato del programa mediante la aprobación del caso de negocio conceptual, asignar un equipo de dirección o un comité , cuyas tareas sean elaborar un resumen del programa, revisar y actualizar el caso de negocio, desarrollar un plan de consecución de beneficios y obtener la aprobación de los patrocinadores antes de proceder.		a. Porcentaje de iniciativas/proyectos de I&T promovidos por dueños del negocio b. Porcentaje de iniciativas estratégicas con rendición de cuentas asignada c. Porcentaje de programas emprendidos sin casos de negocio aprobados d. Porcentaje de partes interesadas que aprueban la necesidad empresarial, alcance, resultado planeado y nivel de riesgo del programa
Actividades		Nivel de capacidad
1. Acordar el patrocinio del programa. Nombrar un consejo de administración/comité de programas con los miembros que tienen un interés estratégico en el programa, responsabilidad en la toma de decisiones de inversión, que se verán impactados de forma significativa por el programa y que deberán facilitar que se produzca el cambio.		2
2. Nombrar a un gestor dedicado para el programa, con las competencias y habilidades adecuadas para gestionar el programa de forma eficaz y eficiente.		
3. Confirmar el mandato del programa con los patrocinadores y las partes interesadas. Articular los objetivos estratégicos para el programa, las posibles estrategias para la entregar, mejora y beneficios esperados, y cómo el programa encaja con otras iniciativas.		3
4. Desarrollar un caso de negocio detallado para un programa. Involucrar a todas las partes interesadas para desarrollar y documentar una comprensión completa de los resultados empresariales esperados, cómo se medirán, alcance global requerido de las iniciativas, riesgo involucrado e impacto en todos los aspectos de la empresa. Identificar y evaluar cursos de acción alternativos para lograr los resultados empresariales deseados.		
5. Desarrollar un plan de obtención de beneficios que se gestionarán a través del programa para asegurar que los beneficios planificados tengan siempre dueños y se logren, mantengan y optimicen.		
6. Preparar el caso de negocio del programa inicial (conceptual), proporcionar la información de toma de decisiones esencial relacionada con el propósito, contribución a los objetivos del negocio, valor esperado creado, intervalos de tiempo, etc. Presentarlo para su aprobación.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
BAI01.03 Gestionar el compromiso de las partes interesadas. Gestionar el compromiso de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna para todas las partes interesadas relevantes. Esto incluye planificar, identificar e involucrar a las partes interesadas y gestionar sus expectativas.		a. Nivel de satisfacción de las partes interesadas con su compromiso b. Porcentaje de partes interesadas involucradas de manera efectiva
Actividades		Nivel de capacidad
1. Planificar cómo las partes interesadas dentro y fuera de la empresa se identificarán, analizarán, comprometerán y gestionarán durante el ciclo de vida de los proyectos.		3
2. Identificar, comprometer y gestionar a las partes interesadas mediante el establecimiento y mantenimiento de los niveles de coordinación, comunicación y relación adecuadas para garantizar que estén comprometidos en el programa.		
3. Analizar los intereses y requisitos de las partes interesadas.		
4. Seguir un proceso definido para los acuerdos de colaboración con respecto a los datos compartidos y el uso de datos dentro de los procesos del negocio.		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
PMBOK Guide, 6.ª edición, 2017		Part 1: 10. Project communications management
Práctica de gestión		Métricas modelo
BAI01.04 Desarrollar y mantener el plan del programa. Formular un programa para sentar las bases iniciales. Posicionarlo para la ejecución exitosa mediante la formalización del alcance del trabajo y la identificación de los entregables que satisfarán las metas y producirán valor. Mantener y actualizar el plan del programa y el caso de negocio durante todo el ciclo de vida económico completo del mismo, para asegurar su alineación con los objetivos estratégicos, reflejar el estado actual y el conocimiento adquirido hasta la fecha.		a. Frecuencia de revisiones de estado del programa que no satisfacen los criterios de valor b. Porcentaje de programas activos llevados a cabo sin mapas de valor del programa válidas y actualizadas

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Especificar la financiación, coste, calendario e interdependencias de múltiples proyectos.	2
2. Definir y documentar el plan del programa que cubre todos los proyectos. Incluir lo necesario para introducir cambios en la empresa; su propósito, misión, valores, cultura, productos y servicios; procesos de negocio; habilidades y número de empleados; relaciones con las partes interesadas, clientes, proveedores y otros; necesidades tecnológicas y reestructuración organizativa requerida para lograr los resultados empresariales esperados del programa.	3
3. Asegurar que haya una comunicación efectiva de los planes de programa e informes de progresos entre todos los proyectos y con el programa en su conjunto. Asegurar que todos los cambios realizados a los planes individuales se reflejen en los otros planes de programa empresariales.	
4. Mantener el plan de programas para garantizar que esté actualizado y refleje el alineamiento con los objetivos estratégicos actuales, progreso actual y cambios materiales de los resultados, beneficios, costes y riesgo. Hacer que la empresa marque los objetivos y priorice todo el trabajo para asegurar que el programa, como se ha diseñado, cumpla con los requisitos de la empresa. Revisar el progreso de los proyectos individuales y ajustar los proyectos conforme sea necesario para cumplir con los hitos y las publicaciones programadas.	
5. Durante la vida económica del programa, actualizar y mantener el caso de negocio y un registro de beneficios para identificar y definir los beneficios clave que surgen de llevar a cabo el programa.	
6. Preparar un presupuesto para el programa que refleje los costes del ciclo de vida económico completo y los beneficios financieros y no financieros asociados.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin documentación relacionada para esta práctica de gestión	
Práctica de gestión	Métricas modelo
BAI01.05 Lanzar y ejecutar el programa. Poner en marcha el programa para adquirir y dirigir los recursos necesarios y así lograr las metas y beneficios del programa tal y como está definido en el plan. De acuerdo con los criterios de revisión de cambios de fase (stage-gate) o publicación, prepararse para la iteración de cambio de fase o revisiones de la publicación a fin de informar sobre el avance y tener el caso para financiar hasta la siguiente revisión de cambio de fase o publicación.	a. Porcentaje de firmas autorizadas de las partes interesadas para las revisiones de cambio de fase de los programas activos b. Número de análisis de causas raíz por desviaciones del plan y acciones remediales necesarias abordadas
Actividades	Nivel de capacidad
1. Planificar, distribuir y encargar los proyectos necesarios requeridos para lograr los resultados del programa, conforme a la revisión y aprobaciones de financiación en cada revisión de cambio de fase.	3
2. Gestionar cada programa o proyecto para asegurar que la toma de decisiones y las actividades generadas se centran en el valor mediante la obtención de beneficios para el negocio y la consecución de metas de forma consistente, abordando el riesgo y cumpliendo con los requisitos de las partes interesadas.	
3. Establecer las fases acordadas del proceso de desarrollo (puntos de comprobación del desarrollo). Al final de cada fase, facilitar debates formales de criterios aprobados con las partes interesadas. Después de la conclusión exitosa de la revisión de la funcionalidad, rendimiento y calidad, y antes de finalizar las actividades de la etapa, obtener una aprobación y aceptación formal de todas las partes interesadas y del dueño del proceso negocio/patrocinador.	
4. Llevar a cabo un proceso de obtención de beneficios durante el programa para asegurar que los beneficios planificados tengan siempre dueños y sea probable que se logren, mantengan y optimicen. Monitorizar la entrega de beneficios e informar de los objetivos de rendimiento en las revisiones de cambio de fase o iteración y publicación. Realizar análisis de las causas raíz de desviaciones del plan e identificar y abordar las acciones remediales necesarias.	4
5. Planificar auditorías, revisiones de calidad, revisiones de cambio de fase y revisiones de obtención de beneficios.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin documentación relacionada para esta práctica de gestión	

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
BAI01.06 Monitorizar, controlar y reportar sobre los resultados del programa. Monitorizar y controlar el rendimiento en comparación con el plan durante todo el ciclo de vida económico de la inversión, cubriendo la entrega de soluciones a nivel del programa y el valor/resultado a nivel de la empresa. Reportar el rendimiento al comité de dirección del programa y a los patrocinadores.		a. Porcentaje de beneficios de programas esperados y logrados b. Porcentaje de programas para los cuales se monitorizo el rendimiento y la acción remedial oportuna se llevó a cabo cuando fue necesario
Actividades		Nivel de capacidad
1. Actualizar los portafolios operativos de I&T para reflejar los cambios que resulten del programa en los portafolios de servicios, activos y recursos de I&T		3
2. Supervisar y controlar el rendimiento de todo el programa y los proyectos dentro del programa, incluidas las contribuciones del negocio y de TI a los proyectos. Informar de forma oportuna, completa y precisa. El reporte podría incluir calendario, financiación, funcionalidad, satisfacción del usuario, controles internos y aceptación de rendición de cuentas.		4
3. Monitorizar y controlar el rendimiento con relación a las estrategias y metas empresariales y de I&T. Reportar a la dirección sobre los cambios empresariales, implementados, beneficios obtenidos frente al plan de obtención de beneficios e idoneidad del proceso de obtención de beneficios.		
4. Monitorizar y controlar los servicios, activos y recursos de TI creados o modificados como resultado del programa. Tener en cuenta la implementación y las fechas en servicio. Informar a la dirección de los niveles de rendimiento, la prestación sostenida del servicio y la contribución al valor.		
5. Gestionar el rendimiento del programa con respeto a criterios clave (p. ej., alcance, calendario, calidad, obtención de beneficios, costes, riesgo, velocidad), identificar las desviaciones del plan y llevar a cabo las acciones correctivas oportunas cuando se precise.		
6. Monitorizar el rendimiento individual del proyecto en relación con la entrega de las capacidades, calendario, logro de beneficios, costes, riesgos u otras métricas esperadas. Identificar los impactos potenciales en el rendimiento del programa y tomar acciones remediales oportunas cuando se requieran.		
7. De acuerdo con los criterios de revisión de cambios de fase, publicación o iteración, llevar a cabo las revisiones para reportar sobre el avance del programa para que la dirección pueda decidir seguir adelante o no, o tomar decisiones de ajuste y aprobar más financiación hasta el siguiente cambio de fase, publicación o iteración.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
BAI01.07 Gestionar la calidad del programa. Preparar y ejecutar un plan de gestión de la calidad, procesos y prácticas, alineado con el sistema de gestión de calidad (SGC). Describe el enfoque de calidad hacia el programa y cómo se implementará. Todas las partes afectadas deberían revisar y aceptar formalmente el plan e incorporarlo al plan de programa integrado.		a. Porcentaje de paquetes de construcción sin errores b. Porcentaje de entregables del programa aprobados en cada revisión
Actividades		Nivel de capacidad
1. Identificar las tareas y prácticas de aseguramiento requeridas para respaldar la acreditación de sistemas nuevos o modificados durante la planificación del programa e incluirlos en los planes integrados. Asegurar que las tareas proporcionen aseguramiento de que los controles internos y las soluciones de seguridad/privacidad satisfacen los requisitos definidos.		3
2. Para proporcionar el aseguramiento de la calidad de los entregables del programa, identificar la propiedad y las responsabilidades, los procesos de revisión de la calidad, criterios de éxito y métricas de rendimiento.		4
3. Definir los requisitos para la validación y verificación independiente de la calidad de los entregables en el plan.		
4. Realizar actividades de aseguramiento y control de calidad conforme al plan de gestión de calidad y el SGC.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		

A. Componente: Proceso (cont.)			
Práctica de gestión		Métricas modelo	
BAI01.08 Gestionar el riesgo del programa. Eliminar o minimizar el riesgo específico asociado a los programas mediante un proceso sistemático de planificación, identificación, análisis, respuesta, monitorización y control de las áreas o eventos que, potencialmente, pueden ocasionar un cambio no deseado. Definir y registrar cualquier riesgo al que se enfrenta la gestión del programa.		a. Número de programas sin una evaluación de riesgos adecuada b. Porcentaje de programas alineados con el marco empresarial de gestión de riesgos	
Actividades			Nivel de capacidad
1. Establecer una estrategia de gestión de riesgos formal alineada con el marco de gestión de riesgos empresariales (ERM). Asegurar que la estrategia incluya la identificación, análisis, respuesta, mitigación, monitorización y control del riesgo.			3
2. Asignar a personal con habilidades adecuadas la responsabilidad de ejecutar el proceso de gestión de riesgos empresariales dentro de un programa y asegurar que esto se incorpore a las prácticas de desarrollo de soluciones. Considerar asignar este rol a un equipo independiente, sobre todo si se requiere un punto de vista objetivo o si un programa se considera crítico.			
3. Realizar la evaluación de riesgos para identificar y cuantificar el riesgo de forma continua en todo el programa. Gestionar y comunicar el riesgo de forma adecuada dentro de la estructura de gobierno del programa.			
4. Identificar a los dueños de las acciones para evitar, aceptar o mitigar el riesgo.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin documentación relacionada para esta práctica de gestión			
Práctica de gestión		Métricas modelo	
BAI01.09 Cerrar un programa. Retirar el programa del portafolio de inversiones activas cuando exista el acuerdo de que se ha alcanzado el valor deseado o cuando esté claro que no se alcanzará dentro de los criterios de valor establecidos para el programa.		a. Porcentaje de programas cerrados con éxito que lograron el valor deseado b. Tiempo entre el lanzamiento del programa y la detección de logro del valor	
Actividades			Nivel de capacidad
1. Cerrar el programa de forma ordenada, incluida la aprobación formal, disolución de la organización del programa y soporte de la función, validación de entregables y comunicación de la retirada.			3
2. Revisar y documentar las lecciones aprendidas. Cuando se ha retirado el programa, eliminarlo del portafolio de inversiones activas. Trasladar cualquier capacidad resultante a un portafolio de activos operativos para garantizar que sigue creándose y manteniéndose valor.			4
3. Establecer la rendición de cuentas y los procesos para garantizar que la empresa siga optimizando valor del servicio, activo o recursos. Puede que se requieran inversiones adicionales en algún momento para garantizar que esto ocurra.			5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, abril de 2018		RS.IM Improvements	

B. Componente: Estructuras organizativas											
	Director general ejecutivo	Director de riesgos	Director de TI	Consejo de gobierno de I&T	Dueños del proceso de negocio	Comité Estratégico (Programas/Proyectos)	Gestor de programas	Oficina de gestión de proyectos	Jefe de arquitectura	Jefe de desarrollo	Jefe de operaciones de TI
Práctica clave de gestión											
BAI01.01 Mantener un enfoque estándar en la gestión de programas.	A		R	R			R				
BAI01.02 Iniciar un programa.		R			R	A	R	R			
BAI01.03 Gestionar el compromiso de las partes interesadas.					R	A	R	R			
BAI01.04 Desarrollar y mantener el plan del programa.						A	R	R			
BAI01.05 Lanzar y ejecutar el programa.			R		R	A	R	R			
BAI01.06 Monitorizar, controlar y reportar sobre los resultados del programa.			R			A	R	R	R	R	R
BAI01.07 Gestionar la calidad del programa.					R	A	R	R			
BAI01.08 Gestionar el riesgo del programa.		R			R	A	R	R		R	
BAI01.09 Cerrar un programa.			R		R	A	R	R		R	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica										
Sin documentación relacionada para este componente.											

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
BAI01.01 Mantener un enfoque estándar en la gestión de programas.	AP003.04	• Descripciones de la fase de implementación • Requisitos de gobierno de la arquitectura	Enfoques de gestión de actualización de programas	Interna
	AP005.04	Portafolios actualizados de programas, servicios y activos		
	AP010.04	Riesgo identificado en las prestaciones de los proveedores		
	EDM02.03	Requisitos de las revisiones por fases		
	EDM02.04	Acciones para mejorar la entrega de valor		

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
BAI01.02 Iniciar un programa.	De	Descripción	Descripción	A
	AP003.04	• Requisitos de recursos • Descripciones de la fase de implementación	Mandato y resumen del programa	AP005.02
	AP005.02	Caso de negocio del programa	Caso de negocio del concepto del programa	AP005.02
	AP007.03	Matriz de habilidades y competencias	Plan de obtención de beneficios del programa	AP005.02; AP006.05
	BAI05.02	Visión y metas comunes		
BAI01.03 Gestionar el compromiso de las partes interesadas.			Resultados de las evaluaciones de eficacia para el compromiso de las partes interesadas	Interna
			Plan para el compromiso de las partes interesadas	Interna
BAI01.04 Desarrollar y mantener el plan del programa.	AP005.02	Programas seleccionados con hitos de retorno de inversión (ROI)	Registro del presupuesto y los beneficios del programa	AP005.05; AP006.05
	AP007.03	Matriz de habilidades y competencias	Requisitos de recursos y roles	AP007.05; AP007.06
	AP007.05	Inventario de recursos humanos de la empresa y de TI	Plan del programa	Interna
	BAI05.02	Equipo y roles para su implementación		
	BAI05.03	Plan de comunicación de la visión		
	BAI05.04	Ganancias rápidas identificadas.		
	BAI07.03	Plan de pruebas de aceptación aprobado		
	BAI07.05	Aceptación aprobada y preparación para pasar a producción		
BAI01.05 Lanzar y ejecutar el programa.	BAI05.03	Comunicaciones de la visión	Resultados de la monitorización de la consecución de metas del programa	AP002.04
			Resultados de la monitorización de la obtención de beneficios	AP005.05; AP006.05
			Planes de auditoría a los programas	MEA04.02

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
BAI01.06 Monitorizar, controlar y reportar sobre los resultados del programa.	De	Descripción	Descripción	A
	AP005.01	Expectativas de retorno de la inversión	Resultados de la revisión por fases	AP002.04; AP005.03; EDM02.02
	AP005.02	Evaluaciones de los casos de negocio	Resultados de las revisiones de rendimiento del programa	MEA01.03
	AP005.03	Informes sobre el rendimiento del Portafolio de inversiones		
	AP005.05	<ul style="list-style-type: none"> Resultados de beneficios y comunicaciones relacionadas Acciones correctivas para mejorar la obtención de beneficios 		
	AP007.05	<ul style="list-style-type: none"> Análisis de déficit de recursos Registro de la utilización de recursos 		
	BAI05.04	Comunicación de beneficios		
	BAI06.03	Informes de estado de peticiones de cambios		
	BAI07.05	Evaluación de los resultados de aceptación		
	EDM02.04	Retroalimentación sobre el rendimiento del Portafolio y los programas		
BAI01.07 Gestionar la calidad del programa.	AP011.01	Planes para la gestión de la calidad	Plan para la gestión de la calidad	BAI02.04; BAI03.06; BAI07.01
	AP011.02	Requisitos del cliente para la gestión de la calidad	Requisitos para la verificación independiente de los entregables	BAI07.03
BAI01.08 Gestionar el riesgo del programa.	AP012.02	Resultados del análisis de riesgos	Registro de riesgos del programa	Interna
	BAI02.03	<ul style="list-style-type: none"> Registro de riesgos de los requisitos Acciones para la mitigación de riesgos 	Resultados de la evaluación de riesgos del programa	Interna
	Fuera de COBIT	Marco para la gestión de riesgos empresariales (ERM)	Plan de gestión de riesgos del programa	Interna
BAI01.09 Cerrar un programa.	BAI07.08	<ul style="list-style-type: none"> Informe de la revisión post-implementación Plan de acciones remediales 	Comunicación de la retirada del programa y de la rendición de cuentas continua	AP005.04; AP007.06
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
PMBOK Guide, 6.ª edición, 2017		Part 1: 4. Project integration management: Inputs and Outputs; Part 1: 6. Project schedule management: Inputs and Outputs; Part 1: 10. Project communications management: Inputs and Outputs; Part 1: 11. Project risk management: Inputs and Outputs		

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión de beneficios	Skills Framework for the Information Age V6, 2015	BENM
Desarrollo de plan de negocio	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.3. Plan de negocio Desarrollo
Gestión de programas	Skills Framework for the Information Age V6, 2015	PGMG
Gestión de proyectos y Portafolio	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.2. Project and Portfolio Management

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de gestión de programas/proyectos	Orienta la gestión de los riesgos relacionados con programas y proyectos Detalla la postura y expectativa de la dirección con relación a la gestión de proyectos y programas Trata la rendición de cuentas, metas y objetivos relacionados con el rendimiento, presupuesto, análisis de riesgos, reporte y mitigación de eventos adversos durante la ejecución del programa/proyecto.	PMBOK Guide Sixth edition, 2017	Part 1: 2.3.1 Processes, policies and procedures

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Asegurar que la organización entiende y respalda el valor de la gestión del programa en toda la empresa. Establecer en toda la empresa una cultura que respalde la correcta implementación de la gestión del programa, considerando la estructura organizativa y el entorno empresarial. Asegurar que la oficina del programa tenga una visión central de todos los programas del portafolio empresarial.		

G. Componente: Servicios, infraestructura y aplicaciones	
Herramienta de gestión de programas	

Página dejada en blanco intencionadamente

Dominio: Construir, Adquirir e Implementar Objetivo de gestión: BAI02 – Gestionar la definición de requisitos		Área prioritaria: Modelo Core de COBIT
Descripción		
Identificar las soluciones y analizar los requisitos antes de su adquisición o construcción para asegurarse de que se ajustan a los requisitos estratégicos de la empresa cubriendo los procesos, aplicaciones, información/datos, infraestructura y servicios del negocio Coordinar la revisión de opciones viables con las partes interesadas afectadas, incluidos costes y beneficios relativos, análisis de riesgos y aprobación de los requisitos y soluciones propuestas.		
Propósito		
Crear soluciones óptimas que satisfagan las necesidades de la empresa mientras que se minimiza el riesgo.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales	➔	Metas de alineamiento
<ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG08 Optimización de la funcionalidad de los procesos internos del negocio • EG12 Gestión de programas de transformación digital 		<ul style="list-style-type: none"> • AG05 Prestación de servicios I&T alineados con los requisitos del negocio • AG06 Agilidad para convertir los requisitos del negocio en soluciones operativas • AG09 Ejecución de programas dentro del plazo, sin exceder el presupuesto y cumpliendo con los requisitos y estándares de calidad
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 <ul style="list-style-type: none"> a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios 		AG05 <ul style="list-style-type: none"> a. Porcentaje de partes interesadas del negocio satisfechas con que la prestación de servicios de I&T cumpla con los niveles de servicio acordados b. Número de interrupciones del negocio debido a incidentes de servicios de I&T c. Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de I&T
EG08 <ul style="list-style-type: none"> a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso del negocio b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro 		AG06 <ul style="list-style-type: none"> a. Nivel de satisfacción de los ejecutivos del negocio con la capacidad de respuesta de I&T a los nuevos requisitos b. Plazo de comercialización promedio para servicios y aplicaciones nuevos relacionados con las I&T c. Tiempo promedio para convertir los objetivos estratégicos de I&T en iniciativas acordadas y aprobadas d. Número de procesos de negocio críticos respaldados por infraestructura y aplicaciones actualizadas
EG12 <ul style="list-style-type: none"> a. Número de programas ejecutados a tiempo y dentro del presupuesto b. Porcentaje de partes interesadas satisfechas con la ejecución del programa c. Porcentaje de programas de transformación del negocio suspendidos d. Porcentaje de programas de transformación del negocio con actualizaciones del estado notificado regularmente 		AG09 <ul style="list-style-type: none"> a. Número de programas/proyectos ejecutados a tiempo y dentro del presupuesto b. Número de programas que necesitan una revisión significativa debido a defectos de calidad c. Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
BAI02.01 Definir y mantener los requisitos funcionales y técnicos del negocio. Con base en el caso de negocio, identificar, priorizar, especificar y acordar los requisitos de información, funcionales, técnicos y de control del negocio que cubran el alcance/compreensión de todas las iniciativas necesarias para lograr los resultados esperados de la solución empresarial propuesta habilitada por la I&T.		a. Porcentaje de requisitos reelaborados debido a la falta de alineación con las necesidades y expectativas de la empresa b. Porcentaje de los requisitos validados a través de enfoques como revisión realizada por colegas, validación del modelo o construcción de prototipos operativos
Actividades		Nivel de capacidad
1. Garantizar que todos los requisitos de las partes interesadas, incluidos los criterios de aceptación relevantes se consideren, capten, prioricen y registren de forma que sean comprensibles para todas las partes interesadas, reconociendo que los requisitos podrían cambiar y ser más detallados conforme se implementen.		2
2. Expresar los requisitos del negocio en términos de cómo debe abordarse la brecha entre las capacidades empresariales actuales y deseadas y cómo el usuario (empleado, cliente, et.) interactuará con la solución y la utilizará.		
3. Especificar y priorizar los requisitos de información, funcionales y técnicos, conforme al diseño de la experiencia de usuario y los requisitos confirmados de las partes interesadas		
4. Asegurar que los requisitos cumplan con las políticas y estándares empresariales, arquitectura empresarial, planes estratégicos y tácticos de I&T, procesos de negocios y de TI internos y externalizados, requisitos de seguridad, requisitos regulatorios, competencias del personal, estructura organizativa, caso de negocio y tecnología facilitadora.		3
5. Incluir requisitos de control de la información en los procesos del negocio, procesos automatizados y entornos de I&T para abordar el riesgo de la información y cumplir con la legislación, regulaciones y contratos comerciales.		
6. Confirmar la aceptación de aspectos clave de los requisitos, incluidos las reglas empresariales, experiencia de usuario, controles de información, continuidad del negocio, cumplimiento legal y regulatorio, auditoría, ergonomía, operatividad y usabilidad, seguridad, confidencialidad y documentación de soporte.		
7. Hacer un seguimiento y control del alcance, requisitos y los cambios durante todo el ciclo de vida de la solución, a medida que evoluciona la comprensión de la solución.		
8. Definir e implementar un procedimiento para la definición y el mantenimiento de los requisitos, así como un repositorio de requisitos que sean apropiados para el tamaño, complejidad, objetivos y riesgo de la iniciativa que la empresa considera llevar a cabo.		
9. Validar todos los requisitos a través de enfoques como la revisión realizada por colegas validación del modelo o construcción de prototipos operativos		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISF, The Standard of Good Practice for Information Security 2016		SD2.1 Specifications of Requirements
ISO/IEC 27002:2013/Cor.2:2015(E)		14.1 Security requirements of information systems
ITIL V3, 2011		Service Design, 5.1 Requirements engineering
PMBOK Guide, 6.ª edición, 2017		Part 1: 5. Project scope management
Práctica de gestión		Métricas modelo
BAI02.02 Realizar un estudio de factibilidad y formular soluciones alternativas. Realizar un estudio de factibilidad de las posibles soluciones alternativas, evaluar su viabilidad y seleccionar la opción preferida. Si es apropiado, implementar la opción seleccionada como un piloto para determinar posibles mejoras.		a. Porcentaje de objetivos del caso de negocio satisfechos por la solución propuesta b. Porcentaje de requisitos satisfechos por la solución propuesta
Actividades		Nivel de capacidad
1. Identificar las acciones requeridas para la adquisición o desarrollo de soluciones conforme a la arquitectura empresarial. Tener en cuenta las limitaciones de alcance y/o plazo y/o presupuesto.		2
2. Revisar las soluciones alternativas con todas las partes interesadas. Seleccionar la más apropiada con base en criterios de factibilidad, incluyendo el riesgo y el coste.		
3. Trasladar el curso de acción preferido a un plan de adquisición/desarrollo de alto nivel que identifique los recursos que se usarán y las etapas que requieran la decisión de seguir o no seguir adelante.		3
4. Definir y ejecutar un estudio de factibilidad, piloto o solución de trabajo básica que describa de forma clara y concisa las soluciones y medidas alternativas y cómo estas satisfarán los requisitos funcionales y del negocio. Incluir una evaluación de su factibilidad tecnológica y económica.		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
BAI02.03 Gestionar el riesgo de los requisitos. Identificar, documentar, priorizar y mitigar el riesgo funcional, técnico y de procesamiento de la información asociado con los requisitos empresariales, las hipótesis y la solución propuesta.		a. Porcentaje de riesgos de los requisitos no cubiertos por una adecuada respuesta al riesgo b. Nivel de detalle del riesgo de los requisitos documentado c. Qué tan completa es la probabilidad estimada y el impacto del riesgo de los requisitos y las respuestas al riesgo enumerados
Actividades		Nivel de capacidad
1. Identificar el riesgo de requisitos de calidad, funcionales y técnica (debido, por ejemplo, a la falta de participación del usuario, expectativas poco realistas, a los desarrolladores añadiendo una funcionalidad innecesaria, hipótesis poco realistas, etc.).		3
2. Determinar una respuesta apropiada al riesgo para el riesgo de los requisitos.		
3. Analizar el riesgo identificado estimando su probabilidad y su impacto en el presupuesto y en el calendario. Evaluar el impacto en el presupuesto de las adecuadas acciones de respuesta al riesgo.		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
BAI02.04 Obtener la aprobación de requisitos y soluciones. Coordinar la retroalimentación de las partes interesadas afectadas En etapas clave predeterminadas, obtener la aprobación y autorización del patrocinador del negocio o del dueño del producto para los requisitos funcionales y técnicos, estudios de factibilidad, análisis de riesgos y soluciones recomendadas.		a. Nivel de satisfacción de las partes interesadas con los requisitos b. Número de excepciones de la solución observadas durante la etapa de las revisiones. c. Porcentaje de partes interesadas que no aprueban la solución en relación con el caso de negocio
Actividades		Nivel de capacidad
1. Asegurar que el patrocinador del negocio o dueño del producto realice la elección final de la solución, estrategia de adquisición y diseño de alto nivel, de acuerdo con el caso de negocio. Obtener las aprobaciones necesarias de las partes interesadas afectadas (p. ej. dueño del proceso de negocio, arquitecto empresarial, director de operaciones, director de seguridad de la información, director de privacidad).		3
2. Obtener revisiones de calidad durante y al final de cada etapa, iteración o liberación clave del proyecto. Evaluar los resultados en comparación con los criterios de aceptación inicial. Contar con la aceptación de los patrocinadores del negocio y de otras partes interesadas en cada revisión de calidad satisfactoria.		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		

B. Componente: Estructuras organizativas												
Práctica clave de gestión	Director de riesgos	Director de TI										
	Dueños del proceso de negocio											
	Comité Estratégico (Programas/Proyectos)											
	Gestor de programas											
	Gestor de proyecto											
	Oficina de gestión de proyectos	Gestor de relaciones	Jefe de arquitectura	Jefe de desarrollo	Jefe de operaciones de TI	Gestor de seguridad de la información	Director de privacidad					
BAI02.01 Definir y mantener los requisitos funcionales y técnicos del negocio.			R	A	R	R	R	R	R		R	R
BAI02.02 Realizar un estudio de factibilidad y formular soluciones alternativas.			R	A	R	R	R			R		
BAI02.03 Gestionar el riesgo de los requisitos.	R	R	R	A	R	R	R			R	R	R
BAI02.04 Obtener la aprobación de requisitos y soluciones.			R	A	R	R	R					R
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica											
Sin documentación relacionada para este componente.												

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
BAI02.01 Definir y mantener los requisitos funcionales y técnicos del negocio.	De	Descripción	Descripción	A
	AP001.07	<ul style="list-style-type: none"> Directrices de clasificación de datos Directrices de la seguridad y control de los datos Procedimientos de integridad de los datos 	Repositorio de definiciones de requisitos	BAI03.01; BAI03.02; BAI03.12; BAI04.01; BAI05.01
	AP003.01	Principios de arquitectura	Criterios de aceptación confirmados por las partes interesadas	BAI03.01; BAI03.02; BAI03.12; BAI04.03; BAI05.01; BAI05.02
	AP003.02	<ul style="list-style-type: none"> Descripciones de dominios de referencia y definición de arquitectura Modelo de arquitectura de la información 	Registro de peticiones de cambio de requisitos	BAI03.09
	AP003.05	Guía para el desarrollo de soluciones		
	AP010.02	Solicitudes de información (RFI) y solicitudes de propuestas (RFP) para los proveedores		
	AP011.02	Criterios de aceptación		
	AP014.02	Glosario empresarial		
BAI02.02 Realizar un estudio de factibilidad y formular soluciones alternativas.	AP003.05	Guía de desarrollo de soluciones	Plan de desarrollo/adquisiciones de alto nivel	AP010.02; BAI03.01
	AP010.01	Catálogo de proveedores	Informe del estudio de factibilidad	BAI03.02; BAI03.03; BAI03.12
	AP010.02	<ul style="list-style-type: none"> Solicitudes de información (RFI) y solicitudes de propuestas (RFP) para los proveedores Evaluaciones de RFI y RFP Resultados de las decisiones de las evaluaciones de proveedores 		
	AP011.02	Criterios de aceptación		
BAI02.03 Gestionar el riesgo de los requisitos.			Registro de riesgos de los requisitos	BAI01.08; BAI03.02; BAI04.01; BAI05.01; BAI11.06
			Acciones para la mitigación de riesgos	BAI01.08; BAI03.02; BAI05.01
BAI02.04 Obtener la aprobación de requisitos y soluciones.	BAI01.07	Plan de gestión de la calidad	Revisiones de calidad aprobadas	AP011.03
	BAI11.05	Plan de gestión de la calidad del proyecto	Aprobaciones del patrocinador para los requisitos y las soluciones propuestas.	BAI03.02; BAI03.03; BAI03.04
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
PMBOK Guide, 6.ª edición, 2017		Part 1: 5. Project management scope: Inputs and Outputs		

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Diseño de aplicaciones	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	A. Plan—A.6. Application Design
Análisis del negocio	Skills Framework for the Information Age V6, 2015	BUAN
Mejora en el proceso del negocio	Skills Framework for the Information Age V6, 2015	BPRE
Identificación de necesidades	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	D. Enable—D.11. Needs Identification
Definición y gestión de requisitos	Skills Framework for the Information Age V6, 2015	REQM
Análisis de la experiencia del usuario	Skills Framework for the Information Age V6, 2015	UNAN

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de desarrollo de software	Estandarizar el desarrollo de software en la organización mediante un listado de todos los protocolos y estándares que se deben seguir.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Establecer una cultura que garantiza procesos coherentes y sólidos para definir los requisitos. Asegurar que los procesos alinean claramente los requisitos de desarrollo con los requisitos estratégicos empresariales.		

G. Componente: Servicios, infraestructura y aplicaciones	
Definición de requisitos y herramientas de documentación	

Página dejada en blanco intencionadamente

Dominio: Construir, adquirir e implementar Objetivo de gestión: BAI03 – Gestionar la identificación y construcción de soluciones		Área prioritaria: Modelo Core de COBIT
Descripción		
Establecer y mantener productos y servicios identificados (tecnología, procesos de negocio y flujos de trabajo) alineados con los requisitos de la empresa que cubran el diseño, desarrollo, adquisición/subcontratación y la asociación con proveedores. Gestionar la configuración, preparación de pruebas, pruebas, gestión de requisitos y mantenimiento de procesos de negocio, aplicaciones, información/datos, infraestructura y servicios.		
Propósito		
Garantizar una prestación ágil y escalable de productos y servicios digitales. Establecer soluciones oportunas y rentables (tecnología, procesos de negocio y flujos de trabajo) capaces de apoyar los objetivos estratégicos y operativos de la empresa.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales	➔	Metas de alineamiento
<ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG08 Optimización de la funcionalidad de procesos internos del negocio • EG12 Gestión de programas de transformación digital 		<ul style="list-style-type: none"> • AG05 Prestación de servicios de I&T en línea con los requisitos del negocio • AG06 Agilidad para convertir los requisitos del negocio en soluciones operativas • AG09 Ejecución de programas dentro del plazo, sin exceder el presupuesto, y que cumplan con los requisitos y estándares de calidad
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 <ul style="list-style-type: none"> a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios 		AG05 <ul style="list-style-type: none"> a. Porcentaje de partes interesadas del negocio satisfechas con que la prestación de servicios de I&T cumpla con los niveles de servicio acordados b. Número de interrupciones del negocio debido a incidentes de servicios de I&T c. Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de I&T
EG08 <ul style="list-style-type: none"> a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarial b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro 		AG06 <ul style="list-style-type: none"> a. Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de I&T a los nuevos requisitos b. Plazo de comercialización promedio para nuevos servicios y aplicaciones relacionados con la I&T c. Tiempo promedio para convertir los objetivos estratégicos de I&T en iniciativas acordadas y aprobadas d. Número de procesos críticos de negocio soportados por infraestructura y aplicaciones actualizadas
EG12 <ul style="list-style-type: none"> a. Número de programas ejecutados a tiempo y dentro del presupuesto b. Porcentaje de partes interesadas satisfechas con la ejecución del programa c. Porcentaje de programas de transformación del negocio suspendidos d. Porcentaje de programas de transformación del negocio con actualizaciones de estado notificadas regularmente. 		AG09 <ul style="list-style-type: none"> a. Número de programas/proyectos ejecutados a tiempo y dentro del presupuesto b. Número de programas que necesitan una revisión significativa debido a defectos de calidad c. Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto

A. Componente: Proceso	
Práctica de gestión	Métricas modelo
BAI03.01 Diseño de soluciones de alto nivel. Desarrollar y documentar diseños de alto nivel para la solución en términos de tecnología, procesos de negocio y flujos de trabajo. Usar técnicas de desarrollo por fases o Agile rápido acordadas y apropiadas. Asegurar la alineación con la estrategia de I&T y la arquitectura empresarial. Volver a evaluar y actualizar los diseños cuando se presenten problemas significativos durante las fases de diseño detallado o construcción, o según evolucione la solución. Aplicar un enfoque centrado en el usuario; asegurarse de que las partes interesadas participan activamente en el diseño y la aprobación de cada versión.	<ul style="list-style-type: none"> a. Número de deficiencias de la revisión del diseño b. Porcentaje de participación de las partes interesadas en el diseño y la aprobación de cada versión.

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Establecer una especificación de diseño de alto nivel que traslade la solución propuesta a un diseño de alto nivel para los procesos de negocio, los servicios que los soportan, flujos de trabajo, aplicaciones, infraestructura y repositorios de información capaces de satisfacer los requisitos del negocio y de la arquitectura empresarial.	2
2. Involucrar a diseñadores con experiencia con el usuario y especialistas de TI bien calificados y experimentados en el proceso de diseño para garantizar que el diseño proporcione una solución que use de forma óptima las capacidades propuestas de I&T para mejorar el proceso de negocio.	
3. Crear un diseño que cumpla con los estándares de diseño de la organización. Asegurar que mantiene un nivel de detalle adecuado para la solución y el método de desarrollo y consistente con las estrategias de negocio, empresariales y de I&T, arquitectura empresarial, plan de seguridad/privacidad y legislaciones, regulaciones y contratos aplicables.	
4. Después de la aprobación del aseguramiento de calidad, enviar el diseño de alto nivel final a las partes interesadas del proyecto y al patrocinador/dueño del proceso de negocio para su aprobación, conforme a los criterios acordados. Este diseño evolucionará a lo largo del proyecto a medida que aumente su comprensión.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
ISF, The Standard of Good Practice for Information Security 2016	SD2.2 System Design
Práctica de gestión	Métricas modelo
BAI03.02 Diseñar componentes detallados para la solución. Desarrollar, documentar y elaborar diseños detallados de forma progresiva. Usar técnicas de desarrollo Agile por fases o rápido acordadas y apropiadas, abordando todos los componentes (procesos de negocio y controles automatizados y manuales relacionados, aplicaciones soportadas por I&T, servicios de infraestructura y productos de tecnología, así como a los socios/proveedores). Asegurarse de que el diseño detallado incluya acuerdos de nivel de servicio (SLA) internos y externos, así como acuerdos de nivel operativo (OLA).	a. Número de deficiencias en la revisión del diseño b. Número de cambios de diseño en proceso
Actividades	Nivel de capacidad
1. Diseñar progresivamente las actividades del proceso de negocio y los flujos de trabajo que deben realizarse junto con el nuevo sistema de aplicación para satisfacer los objetivos empresariales, incluido el diseño de las actividades de control manual.	2
2. Diseñar los pasos del procesamiento de la aplicación. Estos pasos incluyen la especificación de los tipos de transacción y reglas de procesamiento del negocio, controles automatizados, definiciones de datos/objetos del negocio, casos de uso, interfaces externas, limitaciones del diseño y otros requisitos (p. ej. licenciamiento, legales, estándares e internacionalización/localización).	
3. Clasificar las entradas y salidas de datos conforme a los estándares de la arquitectura empresarial. Especificar el diseño de recopilación de datos fuente. Documentar las entradas de datos (independientemente de la fuente) y la validación de las transacciones del procesamiento, así como los métodos de validación. Diseñar las salidas identificadas, incluidas las fuentes de datos.	
4. Diseñar la interfaz del sistema/solución, incluido cualquier intercambio automático de datos.	
5. Diseñar el almacenamiento, ubicación, recuperación y mecanismos de recuperación de los datos.	
6. Diseñar la redundancia, recuperación y copias de seguridad adecuadas.	
7. Diseñar la interfaz entre el usuario y la aplicación del sistema para que sea fácil de usar y sea auto documentada.	3
8. Considerar el impacto de la necesidad de la solución en el rendimiento de la infraestructura, con sensibilidad respecto al número de activos de cómputo, intensidad del ancho de banda y sensibilidad temporal de la información.	
9. Evaluar proactivamente las debilidades del diseño (p. ej., inconsistencias, falta de claridad, posibles fallos) a lo largo del ciclo de vida. Identificar las mejoras cuando sea necesario.	
10. Proporcionar la capacidad para auditar transacciones e identificar las causas raíz de los errores de procesamiento.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
ISF, The Standard of Good Practice for Information Security 2016	SD2.2 System Design

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
BAI03.03: Desarrollar los componentes de la solución. Desarrollar progresivamente los componentes de la solución en un entorno independiente, de acuerdo con los diseños detallados siguiendo estándares y requisitos de desarrollo y documentación, de aseguramiento de la calidad (QA) y de aprobación. Asegurarse de que se abordan todos los requisitos de control en los procesos de negocio, las aplicaciones y los servicios de infraestructura soportadas por I&T, servicios y productos de tecnología, y los servicios de socios/proveedores.		a. Número de excepciones al diseño de la solución observadas durante la etapa de revisión. b. Número de diseños detallados para los procesos del negocio, servicios de soporte, aplicaciones e infraestructura y repositorios de información
Actividades		Nivel de capacidad
1. Dentro de un entorno separado, desarrollar el diseño detallado propuesto para los procesos de negocio, servicios de soporte, aplicaciones, infraestructura y repositorios de información.		2
2. Cuando los terceros están involucrados con el desarrollo de soluciones, garantizar que el mantenimiento, soporte, estándares de desarrollo y el licenciamiento se aborda y se cumple con las obligaciones contractuales.		
3. Hacer un seguimiento de las peticiones de cambio y de las revisiones de diseño, desempeño y calidad. Asegurar la participación activa de todas las partes interesadas afectadas.		
4. Documentar todos los componentes de la solución conforme a los estándares definidos. Mantener un control de versiones sobre todos los componentes desarrollados y la documentación asociada.		
5. Evaluar el impacto de la personalización y configuración de la solución en el rendimiento y la eficiencia de las soluciones adquiridas y en la interoperabilidad con las aplicaciones, sistemas operativos y otra infraestructura existente. Adaptar procesos de negocio cuando sea necesario para aprovechar la capacidad de la aplicación.		3
6. Garantizar que las responsabilidades de usar componentes de infraestructura de alta seguridad o de acceso restringido estén claramente definidas y sean comprendidas por aquellos que desarrollan e integran los componentes de infraestructura. Es necesario monitorizar e informar sobre su uso.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISF, The Standard of Good Practice for Information Security 2016		SD1.2 System Development Environments
ISO/IEC 27002:2013/Cor.2:2015(E)		14.2 Security in development and support processes
ITIL V3, 2011		Service Strategy, 5.5 IT service strategy and application development
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.18 System and services acquisition (SA-3)
Práctica de gestión		Métricas modelo
BAI03.04 Adquirir los componentes de la solución. Adquirir los componentes de la solución basados en el plan de adquisiciones, de acuerdo con los requisitos y diseños detallados, los principios y estándares de arquitectura, y los procedimientos generales de adquisición y contratos de la compañía, requisitos de QA y estándares de aprobación. Asegurarse de que el proveedor identifica y aborda todos los requisitos legales y contractuales.		a. Porcentaje de proveedores certificados b. Porcentaje de proveedores involucrados en el diseño colaborativo
Actividades		Nivel de capacidad
1. Crear y mantener un plan para la adquisición de componentes de la solución. Considerar su flexibilidad futura para las nuevas incorporaciones de capacidad, los costes de transición, el riesgo y las actualizaciones durante la vida del proyecto.		3
2. Revisar y aprobar todos los planes de adquisiciones. Considerar el riesgo, costes, beneficios y conformidad técnica con los estándares de arquitectura empresarial.		
3. Evaluar y documentar hasta qué punto las soluciones adquiridas necesitan adaptarse al proceso de negocio para obtener los beneficios de la solución adquirida.		
4. Seguir las aprobaciones requeridas en momentos clave de toma de decisiones durante los procesos de adquisición.		
5. Registrar en un inventario de activos la recepción de todas las adquisiciones de infraestructura y software.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISF, The Standard of Good Practice for Information Security 2016		SD2.3 Software Acquisition
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, abril de 2018		3.4 Buying Decisions
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.18 System and services acquisition (SA-4)

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
BAI03.05 Construir soluciones. Instalar y configurar soluciones e integrarlas con las actividades del proceso de negocio. Durante la configuración e integración del hardware y el software de infraestructura, implementar medidas de control, seguridad, privacidad y auditabilidad para proteger los recursos y asegurar la disponibilidad y la integridad de los datos. Actualizar el catálogo de productos o servicios para reflejar las nuevas soluciones.		a. Brecha entre el esfuerzo de desarrollo estimado frente al esfuerzo de desarrollo final b. Número de problemas de software comunicados c. Número de errores revisados
Actividades		Nivel de capacidad
1. Integrar y configurar los componentes de negocio y de la solución de TI y los repositorios de la información de acuerdo con las especificaciones detalladas y los requisitos de calidad. Considerar el rol de los usuarios, partes interesadas de la empresa y dueño del proceso en la configuración de los procesos del negocio.		2
2. Completar y actualizar los manuales del proceso de negocio y los manuales operativos, cuando sea necesario, para incluir la personalización o condiciones especiales únicas para la implementación.		
3. Considerar todos los requisitos de control de la información relevante en la integración y configuración de los componentes de la solución. Incluir la implementación de controles de negocio, donde corresponda, en los controles automáticos de aplicación, para que el procesamiento sea preciso, completo, oportuno, autorizado y auditable.		
4. Implementar pistas de auditoría durante la configuración y durante la integración del hardware y el software de infraestructura, para proteger los recursos y asegurar su disponibilidad e integridad.		3
5. Considerar cuando el efecto de las personalizaciones y configuraciones acumuladas (incluidos los cambios menores que no estaban sujetos a especificaciones formales del diseño) requiere una reevaluación de alto nivel de la solución y la funcionalidad asociada.		
6. Configurar el software de la aplicación adquirido para satisfacer los requisitos de procesamiento del negocio.		
7. Definir los catálogos de productos y servicios para grupos objetivos internos y externos relevantes, conforme a los requisitos del negocio.		
8. Garantizar la interoperabilidad de los componentes de la solución con pruebas de soporte, preferiblemente automáticas.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
HITRUST CSF versión 9, septiembre de 2017		10.05 Security in Development & Support Processes
ISF, The Standard of Good Practice for Information Security 2016		SD2.4 System Build
Práctica de gestión		Métricas modelo
BAI03.06 Realizar el aseguramiento de calidad (QA). Desarrollar, aprovisionar y ejecutar un plan de aseguramiento de la calidad (QA) que esté alineado con el sistema de gestión de la calidad (QMS) para obtener la calidad especificada en la definición de los requisitos y en las políticas y procedimientos de calidad de la empresa.		a. Número de diseños de soluciones reelaboradas debido a la falta de alineación con los requisitos b. Número y solidez de las actividades documentadas de supervisión realizadas
Actividades		Nivel de capacidad
1. Definir un plan de aseguramiento de la calidad, incluidos, por ejemplo, la especificación de los criterios de calidad, procesos de validación y verificación, definición sobre cómo se revisará la calidad, cualificaciones necesarias de los revisores de la calidad, y roles y responsabilidades para lograr la calidad.		3
2. Supervisar frecuentemente la calidad de la solución conforme a los requisitos del proyecto, políticas empresariales, cumplimiento de las metodologías de desarrollo, procedimientos de gestión de calidad y criterios de aceptación.		4
3. Emplear, como corresponda, la inspección de código, prácticas de desarrollo a base de pruebas, pruebas automáticas, integración continua, pruebas de recorrido y pruebas de las aplicaciones. Informar sobre los resultados del proceso de supervisión y las pruebas al equipo de desarrollo de software de aplicación y la dirección de TI.		
4. Supervisar todas las excepciones de calidad y abordar todas las acciones correctivas. Mantener un registro de todas las revisiones, resultados, excepciones y correcciones. Repetir revisiones de calidad, cuando sea necesario, basadas en la cantidad de trabajo que debe volverse a realizar y las acciones correctivas.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISF, The Standard of Good Practice for Information Security 2016		SD1.3 Quality Assurance

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
BAI03.07 Preparar las pruebas de la solución. Establecer un plan de pruebas y los entornos/ambientes necesarios para probar los componentes individuales e integrados de la solución. Incluir los procesos de negocio y los servicios de soporte, aplicaciones e infraestructura.		a. Número de usuarios del negocio involucrados en la construcción de un plan de pruebas b. Número y solidez de los casos de uso creados para las pruebas
Actividades		Nivel de capacidad
1. Crear un plan integrado de prácticas y pruebas que se corresponda con el entorno empresarial y los planes estratégicos de tecnología. Asegurar que el plan integrado de prácticas y pruebas permita la construcción de entornos de pruebas y simulación adecuados para ayudar a comprobar que la solución funcione correctamente en el entorno real y entregue los resultados deseados, y que los controles sean adecuados.		2
2. Crear un entorno de pruebas que apoye todo el alcance de la solución. Asegurar que el entorno de pruebas refleje, lo más fielmente posible, las condiciones del mundo real, incluidos los procesos y procedimientos del negocio, la totalidad de usuarios, tipos de transacciones y condiciones para el despliegue.		
3. Crear procedimientos de pruebas alineados con el plan y las prácticas y permitir la evaluación del funcionamiento de la solución en condiciones reales. Asegurar que los procedimientos de las pruebas evalúen la idoneidad de los controles, conforme a los estándares generales de la empresa que definen roles, responsabilidades y criterios de pruebas, y que sean aprobados por las partes interesadas del proyecto y el patrocinador/dueño del proceso de negocio.		3
4. Documentar y guardar los procedimientos de prueba, casos, controles y parámetros para las pruebas futuras de la aplicación.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		AD.DE Safeguard Development Environment
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.10 Maintenance (MA-2, MA-3)
Práctica de gestión		Métricas modelo
BAI03.08 Ejecutar las pruebas de la solución. Durante el desarrollo, ejecutar pruebas continuamente (incluidas pruebas de control), de acuerdo con el plan de pruebas definido y las prácticas de desarrollo en el entorno apropiado. Incluir a los dueños de los procesos de negocio y a los usuarios finales en el equipo de pruebas. Identificar, registrar y priorizar los errores y problemas que se identificaron durante las pruebas.		a. Número de errores encontrados durante la prueba b. Tiempo y esfuerzo para completar las pruebas
Actividades		Nivel de capacidad
1. Llevar a cabo las pruebas de soluciones y sus componentes, conforme al plan de pruebas. Incluir probadores independientes del equipo de la solución, con dueños del proceso de negocio y usuarios finales representativos. Asegurar que las pruebas se realicen solo dentro de los entornos de pruebas y desarrollo.		2
2. Usar instrucciones de pruebas claramente definidas, conforme a lo establecido en el plan de pruebas. Considerar el equilibrio adecuado entre las pruebas automatizadas y las pruebas interactivas del usuario.		
3. Llevar a cabo todas las pruebas conforme al plan y prácticas de prueba. Incluir la integración de los procesos de negocio y los componentes de la solución de TI y requisitos no funcionales (p. ej., seguridad, privacidad, interoperabilidad, usabilidad).		
4. Identificar, registrar y clasificar los errores (p. ej. menores, significativos, de misión crítica) durante las pruebas. Repetir las pruebas hasta que se hayan resuelto todos los errores significativos. Asegurar que se mantenga pistas de auditoría de los resultados de las pruebas.		
5. Registrar los resultados de las pruebas y comunicarlos a las partes interesadas conforme al plan de pruebas.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		
CMMI Cybermaturity Platform, 2018		AD.ST Secure Development Testing
ISF, The Standard of Good Practice for Information Security 2016		SD2.5 System Testing; SD2.6 Security Testing
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.18 System and services acquisition (SA-11)

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
BAI03.09 Gestionar los cambios a los requisitos. Hacer seguimiento al estado de requisitos individuales (incluidos todos los requisitos rechazados) durante el ciclo de vida del proyecto. Gestionar la aprobación de cambios a los requisitos.		a. Número de cambios a los que se les hizo seguimiento, y que fueron aprobados que generan nuevos errores b. Porcentaje de partes interesadas satisfechas con los procesos de gestión de cambios
Actividades		Nivel de capacidad
1. Evaluar el impacto de todas las peticiones de cambio durante el desarrollo de la solución, el caso de negocio original y el presupuesto. Clasificarlas y priorizarlas conforme sea necesario.		3
2. Hacer un seguimiento de los cambios a los requisitos, que permita a todas las partes interesadas supervisar, revisar y aprobar los cambios. Asegurar que los resultados del proceso de cambio sean entendidos y acordados en su totalidad por todas las partes interesadas y el patrocinador/dueño del proceso de negocio.		
3. Aplicar solicitudes de cambio, manteniendo la integridad de la combinación y configuración de los componentes de la solución. Evaluar el impacto de cualquier actualización mayor de la solución y clasificarla conforme a los criterios objetivos acordados (por ejemplo, requisitos de la empresa), según el resultado del análisis de riesgos (como el impacto en los sistemas y procesos actuales o la seguridad/privacidad), la justificación del coste-beneficio y otros requisitos.		
(Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISF, The Standard of Good Practice for Information Security 2016		SD2.9 Post-implementation Review
Práctica de gestión		Métricas modelo
BAI03.10 Mantener las soluciones. Desarrollar y ejecutar un plan para mantener los componentes de la solución y la infraestructura. Incluir revisiones periódicas frente a las necesidades del negocio y los requisitos operativos.		a. Número de demandas de mantenimiento no satisfechas b. Duración de las demandas de mantenimiento que se satisfacen y no se satisfacen
Actividades		Nivel de capacidad
1. Desarrollar y ejecutar un plan para mantener los componentes de la solución. Incluir revisiones periódicas frente a las necesidades del negocio y los requisitos operativos, como gestión de parches, estrategias de actualización, riesgo, privacidad, análisis de vulnerabilidades y requisitos de seguridad.		2
2. Evaluar la importancia de una actividad de mantenimiento propuesta sobre el diseño, funcionalidad y/o procesos de negocio de la solución actual. Considerar el riesgo, el impacto en el usuario y la disponibilidad de recursos. Asegurar que los dueños del proceso de negocio entiendan el efecto de los cambios designados como mantenimiento.		3
3. En el caso de cambios mayores a las soluciones actuales que deriven en un cambio significativo en los diseños y/o funcionalidad y/o procesos de negocio actuales, seguir el proceso de desarrollo utilizado para nuevos sistemas. En el caso de actualizaciones de mantenimiento, usar el proceso de gestión de cambios.		
4. Asegurar que el patrón y volumen de las actividades de mantenimiento se analice periódicamente para ver si hay tendencias anormales que indiquen problemas subyacentes en la calidad o rendimiento, en el coste/beneficio de actualizaciones mayores, o en la sustitución en lugar del mantenimiento.		4
(Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISO/IEC 27002:2013/Cor.2:2015(E)		14.3 Test data
Práctica de gestión		Métricas modelo
BAI03.11 Definir productos y servicios de TI y mantener el portafolio de servicios. Definir y acordar opciones nuevas o modificadas de productos o servicios de TI y del nivel de servicio. Documentar las definiciones de productos y servicios nuevas o modificadas y las opciones de nivel de servicio que se actualizarán en el portafolio de productos y servicios.		a. Porcentaje de partes interesadas que aprueban los nuevos servicios de I&T b. Porcentaje de definiciones y opciones de nivel de servicio nuevas o modificadas que están documentadas en el portafolio de servicios. c. Porcentaje de definiciones y opciones de nivel de servicio nuevas o modificadas que están actualizadas en el portafolio de servicios.

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Proponer definiciones de los productos y servicios de TI nuevos o modificados para asegurar que cumplan con su propósito. Documentar las definiciones propuestas que se desarrollarán en la lista del portafolio de productos y servicios.	3
2. Proponer opciones de nivel de servicio (tiempos de servicio, satisfacción del usuario, disponibilidad, rendimiento, capacidad, seguridad, privacidad, continuidad, cumplimiento y usabilidad) nuevas o modificadas para asegurar que los productos y servicios de TI sean adecuados. Documentar las opciones de servicio propuestas en el portafolio.	
3. Mediar con las direcciones de relaciones del negocio de gestión de portafolio para acordar las definiciones propuestas de productos y servicios y las opciones de nivel de servicio.	
4. Si los cambios en productos o servicios caen en el alcance de la autoridad de aprobación acordada, crear productos o servicios de TI u opciones de nivel de servicio nuevos o modificados. De no ser así, comunicar el cambio a la gestión de portafolio para que revise la inversión.	
Documentación relacionada(Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin Documentación relacionada para esta práctica de gestión	
Práctica de gestión	Métricas modelo
BAI03.12 Diseñar soluciones conforme a la metodología de desarrollo definida. Diseñar, desarrollar e implementar soluciones con la metodología de desarrollo adecuada (es decir, en cascada, Agile o bimodal I&T), conforme a la estrategia y requisitos globales.	a. Porcentaje de proyectos de desarrollo de soluciones que aplican las metodologías de desarrollo seleccionadas b. Porcentaje de procesos adaptados a la estrategia elegida
Actividades	Nivel de capacidad
1. Analizar y evaluar el impacto de elegir una metodología de desarrollo (es decir, en cascada, Agile, bimodal) sobre los recursos disponibles, los requisitos de la arquitectura, los ajustes de la configuración y la rigidez del sistema.	3
2. Establecer la metodología de desarrollo adecuada y la estrategia organizativa que lleve a cabo la solución propuesta de forma eficaz y eficiente y que sea capaz de satisfacer los requisitos de la empresa, arquitectura y sistema. Adaptar los procesos a la estrategia elegida como corresponda.	
3. Establecer los equipos de proyecto necesarios conforme a lo definido en la metodología de desarrollo elegida. Proporcionar la formación suficiente.	
4. Considerar la aplicación de un sistema dual, si fuera necesario, en el que grupos transversales (fábricas digitales) se centren en desarrollar un producto o proceso con una metodología tecnológica, operativa o gerencial distinta al resto de la compañía. Integrar estos grupos en las unidades de negocio tiene la ventaja de extender la nueva cultura del desarrollo ágil y hacer que esta fábrica digital se acerque cada vez más a la norma.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
ISF, The Standard of Good Practice for Information Security 2016	SD1.1 System Development Methodology

B. Componente: Estructuras organizativas																		
Práctica clave de gestión	Director de TI	Director de tecnología	Director de tecnologías digitales	Dueños del proceso de negocio	Gestor de Portafolio	Comité Estratégico (Programas/Proyectos)	Gestor de programas	Gestor de proyecto	Oficina de gestión de proyectos	Gestor de relaciones	Jefe de arquitectura	Jefe de desarrollo	Jefe de operaciones de TI	Jefe de administración de TI	Gestor de servicios	Gestor de seguridad de la información	Gestor de continuidad del negocio	Director de privacidad
BAI03.01 Diseño de soluciones de alto nivel.		R		R		A	R	R	R	R		R				R		
BAI03.02 Diseñar componentes detallados para la solución.		R		R		A	R	R	R			R						
BAI03.03: Desarrollar los componentes de la solución.		R		R		A	R	R	R			R						
BAI03.04 Adquirir los componentes de la solución.		R		R		A						R	R	R				
BAI03.05 Construir soluciones.		R		R		A	R	R	R			R				R		
BAI03.06 Realizar el aseguramiento de calidad (QA).		R		R		A	R	R	R			R						
BAI03.07 Preparar las pruebas de la solución.		R		R		A						R	R		R	R	R	R
BAI03.08 Ejecutar las pruebas de la solución.		R		R		A						R	R			R		R
BAI03.09 Gestionar los cambios a los requisitos.		R		R		A	R	R	R		R	R				R		R
BAI03.10: Mantener las soluciones.	A	R		R			R	R	R			R				R		R
BAI03.11 Definir productos y servicios de TI y mantener el portafolio de servicios.	A														R	R		R
BAI03.12 Diseñar soluciones conforme a la metodología de desarrollo definida.	A		R		R		R	R										
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)																		
Referencia específica																		
Sin Documentación relacionada para este componente.																		

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
BAI03.01 Diseño de soluciones de alto nivel.	AP003.01	Principios de arquitectura	Especificación de diseño de alto nivel aprobado	BAI04.03; BAI05.01
	AP003.02	Descripciones de dominios de referencia y definición de arquitectura		
	AP004.03	Análisis de investigación de las posibilidades de innovación		
	AP004.04	Evaluación de las iniciativas de innovación		
	BAI02.01	<ul style="list-style-type: none"> • Repositorio de definiciones de requisitos • Criterios de aceptación confirmados por las partes interesadas 		
	BAI02.02	Plan de adquisición/ desarrollo de alto nivel		
BAI03.02 Diseñar componentes detallados para la solución.	AP003.01	Principios de arquitectura	SLA internos y externos	BAI04.02
	AP003.02	<ul style="list-style-type: none"> • Descripciones de dominios de referencia y definición de arquitectura • Modelo de arquitectura de la información 	Especificación de diseño detallado aprobado	BAI04.03; BAI05.01
	AP003.05	Guía de desarrollo de soluciones		
	AP004.06	Evaluaciones de estrategias innovadoras		
	BAI02.01	<ul style="list-style-type: none"> • Repositorio de definiciones de requisitos • Criterios de aceptación confirmados por las partes interesadas 		
	BAI02.02	Informe del estudio de factibilidad		
	BAI02.03	<ul style="list-style-type: none"> • Registro de riesgos de los requisitos • Acciones para la mitigación de riesgos 		
	BAI02.04	Aprobación por parte del patrocinador de los requisitos y las soluciones propuestas		
BAI03.03: Desarrollar los componentes de la solución.	BAI02.02	Informe del estudio de factibilidad	Componentes de la solución documentados	BAI04.03; BAI05.05; BAI08.02; BAI08.03
	BAI02.04	Aprobación por parte del patrocinador de los requisitos y las soluciones propuestas		

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
BAI03.04 Adquirir los componentes de la solución.	BAI02.04	Aprobación por parte del patrocinador de los requisitos y las soluciones propuestas	Plan de adquisiciones aprobado	AP010.03
			Actualizaciones del inventario de activos	BAI09.01
BAI03.05 Construir soluciones.			Componentes de la solución integrados y configurados	BAI06.01
BAI03.06 Realizar el aseguramiento de calidad (QA).	AP011.01	Resultados de las revisiones de eficiencia del QMS	Resultados, excepciones y correcciones de la revisión de calidad	AP011.04
	BAI01.07	Plan de gestión de la calidad	Plan de aseguramiento de la calidad	AP011.04
	BAI11.05	Plan de gestión de la calidad del proyecto		
BAI03.07 Preparar las pruebas de la solución.			Procedimientos de prueba	BAI07.03
			Plan de pruebas	BAI07.03
BAI03.08 Ejecutar las pruebas de la solución.	AP004.05	Análisis de iniciativas rechazadas	Comunicación de los resultados de las pruebas	BAI07.03
			Logs de los resultados y pistas de auditoría de las pruebas	BAI07.03
BAI03.09 Gestionar los cambios a los requisitos.	AP004.05	Resultados y recomendaciones obtenidos a partir de iniciativas de pruebas de concepto	Registro de todas las peticiones de cambio aprobadas y aplicadas	BAI06.03
	BAI02.01	Registro de peticiones de cambio de requisitos		
BAI03.10 Mantener soluciones.			Plan de mantenimiento	AP008.05
			Componentes de la solución y su documentación relacionada actualizados	BAI05.05
BAI03.11 Definir productos y servicios de TI y mantener el portafolio de servicios.	AP002.04	<ul style="list-style-type: none"> Brechas y cambios necesarios para lograr la capacidad deseada Declaración del beneficio sobre el valor para el entorno objetivo 	Portafolio de servicios actualizado	AP005.04
	AP006.02	Asignaciones de presupuesto	Definiciones de servicio	EDM02.01; DSS01.03
	AP006.03	<ul style="list-style-type: none"> Presupuesto de I&T Comunicaciones del presupuesto 		
	AP008.05	Definición de posibles proyectos de mejora		
	BAI10.02	Configuración de referencia		
	BAI10.03	Cambios aprobados a la configuración de referencia		
	BAI10.04	Informes de estado de la configuración		
	EDM04.01	Principios rectores para la asignación de recursos y capacidades		

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
BAI03.12 Diseñar soluciones conforme a la metodología de desarrollo definida.	De	Descripción	Descripción	A
	AP003.02	Descripciones de dominios de referencia y definición de arquitectura		
	AP003.05	Guía de desarrollo de soluciones		
	AP007.03	Matriz de habilidades y competencias		
	BAI02.01	<ul style="list-style-type: none">• Criterios de aceptación confirmados por las partes interesadas• Repositorio de definiciones de requisitos		
	BAI02.02	Informe del estudio de factibilidad		
	BAI10.02	Configuración de referencia		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin documentación relacionada para este componente.				


D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Desarrollo de aplicaciones	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.1. Application Development
Pruebas de procesos de negocio	Skills Framework for the Information Age V6, 2015	BPTS
Integración de componentes	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.2. Component Integration
Diseño de la base de datos	Skills Framework for the Information Age V6, 2015	DBDS
Producción de documentación	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.5. Documentation Production
Diseño de hardware	Skills Framework for the Information Age V6, 2015	HWDE
Configuración de portabilidad/software	Skills Framework for the Information Age V6, 2015	PORT
Programación/desarrollo de software	Skills Framework for the Information Age V6, 2015	PROG
Liberación y despliegue	Skills Framework for the Information Age V6, 2015	RELM
Arquitectura de la solución	Skills Framework for the Information Age V6, 2015	ARCH
Despliegue de soluciones	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.4. Solution Deployment
Diseño de sistemas	Skills Framework for the Information Age V6, 2015	DESN
Gestión del desarrollo de sistemas	Skills Framework for the Information Age V6, 2015	DLMG
Ingeniería de sistemas	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.6. Systems Engineering

D. Componente: Personas, habilidades y competencias (cont.)		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Instalación/desmantelamiento de sistemas	Skills Framework for the Information Age V6, 2015	HSIN
Integración de sistemas	Skills Framework for the Information Age V6, 2015	SINT
Pruebas	Skills Framework for the Information Age V6, 2015	TEST
Pruebas	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.3. Testing
Diseño de experiencia de usuario	Skills Framework for the Information Age V6, 2015	HCEV

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de mantenimiento	Define el soporte adecuado de los componentes de software y hardware para asegurar una mayor vida de los activos, mejorar la productividad de los empleados y mantener una experiencia de usuario aceptable.	National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.10 Maintenance (MA-1)
Política de desarrollo de software	Estandarizar el desarrollo de software en la organización mediante una lista de todos los protocolos y estándares a seguir.		
Política de adquisición de sistemas y servicios	Proporciona procedimientos para evaluar, revisar y validar los requisitos para la adquisición de sistemas y servicios.	National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.18 System and services acquisition (SA-1)

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Asegurar una oferta ágil y escalable de servicios digitales; involucrar a un ecosistema de socios con los que la organización pueda trabajar o establecer una estructura bimodal IT con fábricas digitales, líderes y equipos ágiles, un flujo continuo y una mentalidad hacia la mejora.		
Establecer una cultura abierta y sin sesgos que evalúe las alternativas de forma justa y objetiva a la hora de investigar posibles soluciones nuevas (incluidas construcciones o compras).		

G. Componente: Servicios, infraestructura y aplicaciones	
<ul style="list-style-type: none"> • Servicios de fábrica digital, que separe las «TI rápidas» (la fábrica digital responsable del desarrollo de aplicaciones digitales) del core de TI heredado (legacy). • Evaluación de soluciones y selección de servicios • Herramientas y técnicas de pruebas 	

Dominio: Construir, adquirir e implementar		Área prioritaria: Modelo Core de COBIT		
Objetivo de gestión: BAI04 – Gestionar la disponibilidad y la capacidad				
Descripción				
Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con la prestación de servicios rentables. Incluir la evaluación de las capacidades actuales, previsión de las necesidades futuras basándose en los requisitos del negocio, el análisis de impactos en el negocio y la evaluación del riesgo para planificar e implementar acciones que satisfagan los requisitos identificados.				
Propósito				
Mantener la disponibilidad del servicio, la gestión eficiente de los recursos y la optimización del rendimiento del sistema a través de la predicción de los requisitos futuros de rendimiento y capacidad.				
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:				
Metas empresariales			Metas de alineamiento	
• EG01 Portafolio de productos y servicios competitivos • EG08 Optimización de la funcionalidad de procesos internos del negocio			AG05 Prestación de servicios de I&T conforme a los requisitos del negocio	
Métricas modelo para metas empresariales			Métricas modelo para metas de alineamiento	
EG01	a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios		AG05	a. Porcentaje de partes interesadas del negocio satisfechas con que la prestación de servicios de I&T cumpla con los niveles de servicio acordados b. Número de interrupciones del negocio debido a incidentes de servicios de I&T c. Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de I&T
EG08	a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso de negocio b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro			

A. Componente: Proceso			
Práctica de gestión		Métricas modelo	
BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actuales, y crear una línea de referencia. Evaluar la disponibilidad, rendimiento y capacidad de los servicios y recursos para asegurar que la capacidad y el rendimiento con un coste justificable están disponibles para apoyar las necesidades y entregables del negocio contra los acuerdos de nivel de servicio (SLA). Crear líneas de referencia de disponibilidad, rendimiento y capacidad para una comparación futura.		a. Porcentaje de uso real de la capacidad b. Porcentaje de disponibilidad real c. Porcentaje de rendimiento real	
Actividades			Nivel de capacidad
1. Considerar los elementos siguientes (actuales y estimados) en la evaluación de la disponibilidad, rendimiento y capacidad de servicios y recursos: requisitos del cliente, prioridades del negocio, objetivos empresariales, impacto presupuestario, utilización de recursos, capacidades de TI y tendencias de la industria.			2
2. Identificar y hacer un seguimiento de todos los incidentes causados por un rendimiento o capacidad inadecuados.			3
3. Monitorizar el uso real de la capacidad y el rendimiento frente a umbrales definidos y con el soporte, cuando sea necesario, de software automatizado.			4
4. Evaluar regularmente los niveles actuales de rendimiento para todos los niveles de procesamiento (demanda del negocio, capacidad de servicios y capacidad de recursos) comparándolos con las tendencias y los SLA. Tener en cuenta los cambios en el entorno.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
CMMI Cybermaturity Platform, 2018		DP.CP Capacity Planning	
ISF, The Standard of Good Practice for Information Security 2016		SY2.2 Performance and Capacity Management	
ISO/IEC 20000-1:2011(E)		6.5 Capacity management	
ITIL V3, 2011		Service Design, 4.4 Availability Management; 4.5 Capacity Management	
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.14 Planning (PL-10, PL-11)	

A. Componente: Proceso (cont.)		
Práctica de gestión	Métricas modelo	
BAI04.02 Evaluar el impacto en el negocio. Identificar servicios importantes para la empresa. Asignar servicios y recursos a los procesos de negocio e identificar sus dependencias de negocio. Asegurarse de que el impacto de los recursos no disponibles esté totalmente acordado y aceptado por el cliente. Para funciones vitales del negocio, asegurarse de que se pueden satisfacer los requisitos de disponibilidad definidos en los acuerdos de nivel de servicio (SLA).	a. Número de escenarios creados para evaluar situaciones de disponibilidad futuras b. Porcentaje de dueños de procesos de negocio que aprueban los resultados del análisis	
Actividades	Nivel de capacidad	
1. Identificar solo aquellas soluciones o servicios que sean críticos en el proceso de gestión de capacidad y disponibilidad.	2	
2. Asignar las soluciones y servicios seleccionados a la aplicación o aplicaciones y a la infraestructura (TI e instalaciones) de la que dependen para poder centrarse en recursos críticos para la planificación de la disponibilidad.	3	
3. Recopilar datos sobre patrones de disponibilidad a partir de los logs de fallos pasados y de monitorización del rendimiento. Usar herramientas de modelamiento que ayuden a predecir los fallos basándose en las tendencias pasadas de uso y las expectativas de la gerencia acerca de nuevas condiciones del entorno o de los usuarios.	4	
4. Con base en los datos recopilados, crear escenarios que describan situaciones de disponibilidad futuras que ilustren distintos niveles de capacidad posibles, necesarios para lograr el objetivo de rendimiento de la disponibilidad.		
5. Con base en los escenarios, determinar la probabilidad de que no se alcance el objetivo de rendimiento de la disponibilidad.		
6. Determinar el impacto de los escenarios en las medidas de rendimiento del negocio (p. ej., ingresos, beneficios, servicios al cliente). Involucrar a los líderes regionales, funcionales (sobre todo de finanzas) y de la línea del negocio para entender su evaluación del impacto.		
7. Asegurar que los dueños de los procesos de negocio entiendan y estén completamente de acuerdo con los resultados de este análisis. Obtener de los dueños del negocio una lista de escenarios de riesgos inaceptables que requieran una respuesta para reducir el riesgo a niveles aceptables.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
ISO/IEC 20000-1:2011(E)	6.3 Service continuity and availability management	
Práctica de gestión	Métricas modelo	
BAI04.03 Planificar los requisitos de los servicios nuevos o modificados. Planificar y priorizar las implicaciones de disponibilidad, rendimiento y capacidad de las necesidades del negocio cambiante y de los requisitos de servicio.	a. Número de actualizaciones no planificadas de capacidad, rendimiento o disponibilidad b. Porcentaje comparaciones realizadas por la dirección sobre la demanda actual de recursos contra la oferta y demanda estimadas	
Actividades	Nivel de capacidad	
1. Identificar las implicaciones en la disponibilidad y capacidad de las necesidades cambiantes del negocio y de las oportunidades de mejora. Usar técnicas de modelamiento para validar los planes de disponibilidad, rendimiento y capacidad.	3	
2. Revisar las implicaciones del análisis de tendencia de servicios sobre la disponibilidad y la capacidad.	4	
3. Garantizar que la dirección realice comparaciones de la demanda real de recursos contra la oferta y demanda estimadas para evaluar las técnicas de predicción actuales e implementar mejoras donde sea necesario.		
4. Priorizar las mejoras necesarias y crear planes de disponibilidad y capacidad que justifiquen el coste.	5	
5. Ajustar los planes de rendimiento y capacidad y los SLA con base en los cambios en los procesos de negocio, servicios de soporte, aplicaciones e infraestructura realistas, nuevos, propuestos y/o proyectados. Incluir también revisiones del uso real de la capacidad y del rendimiento, incluidos los niveles de carga de trabajo.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
ISO/IEC 20000-1:2011(E)	5. Design and transition of new changed services	
Práctica de gestión	Métricas modelo	
BAI04.04 Monitorizar y revisar la disponibilidad y la capacidad. Monitorizar, medir, analizar, reportar y revisar la disponibilidad, el rendimiento y la capacidad. Identificar las desviaciones de las líneas de referencia establecidas. Revisar los informes de análisis de tendencias, identificando problemas y variaciones significativas. Iniciar acciones cuando sea necesario y asegurar que se atiendan todos los problemas pendientes.	a. Número de eventos que exceden los límites de capacidad planificados b. Número de picos de transacciones que exceden el rendimiento objetivo	

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Proporcionar informes de capacidades a los procesos de presupuesto	2
2. Establecer un proceso de recopilación de datos para proporcionar a la dirección información de monitorización e informes sobre la disponibilidad, el rendimiento y la carga de trabajo de capacidad de todos los recursos relacionados con I&T.	3
3. Proporcionar en forma adecuada informes regulares sobre los resultados para revisión por TI y por la dirección de negocio y su comunicación a la dirección empresarial.	4
4. Integrar actividades de monitorización e informes en las actividades iterativas de gestión de la capacidad (monitorización, análisis, TUNING e implementaciones).	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin documentación relacionada para esta práctica de gestión	
Práctica de gestión	Métricas modelo
BAI04.05 Investigar y resolver los problemas de disponibilidad, rendimiento y capacidad. Abordar las desviaciones investigando y resolviendo los problemas identificados de disponibilidad, rendimiento y capacidad.	a. Número y porcentaje de incidencias de disponibilidad, rendimiento y capacidad sin resolver b. Número de incidentes de disponibilidad
Actividades	Nivel de capacidad
1. Obtener directrices de los manuales de producto de los proveedores para garantizar un nivel adecuado de disponibilidad de rendimiento durante los picos en las cargas de trabajo y procesamiento.	3
2. Definir un proceso de escalamiento para una resolución rápida de emergencias de capacidad y problemas de rendimiento.	
3. Identificar las brechas de rendimiento y capacidad con base en la monitorización del rendimiento actual y estimado. Usar especificaciones conocidas de disponibilidad, continuidad y recuperación para clasificar los recursos y permitir su priorización.	4
4. Definir acciones correctivas (p. ej., cambios en la carga de trabajo, priorizar tareas o añadir recursos cuando se identifiquen problemas de rendimiento y capacidad).	5
5. Integrar las acciones correctivas necesarias en los procesos apropiados de planificación y gestión del cambio.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin documentación relacionada para esta práctica de gestión	

B. Componente: Estructuras organizativas									
Práctica clave de gestión	Comité Ejecutivo	Director de TI	Director de tecnología	Dueños del proceso de negocio	Jefe de arquitectura	Jefe de operaciones de TI	Gestor de servicios	Gestor de continuidad del negocio	
		R	A	R		R	R		
	BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actuales y crear una línea de referencia.		R	A	R		R	R	
	BAI04.02 Evaluar el impacto en el negocio.	A			R		R	R	
	BAI04.03 Planificar los requisitos de los servicios nuevos o modificados.		R	A	R		R	R	
	BAI04.04 Monitorizar y revisar la disponibilidad y la capacidad.	A			R		R	R	
	BAI04.05 Investigar y resolver los problemas de disponibilidad, rendimiento y capacidad.		R	A	R	R	R	R	R
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica							
Sin Documentación relacionada para este componente.									

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actuales y crear una línea de referencia.	De	Descripción	Descripción	A
	BAI02.01	Repositorio de definición de requisitos	Evaluaciones con respecto a los SLA	AP009.05
	BAI02.03	Registro de riesgos de los requisitos	Línea base de disponibilidad, rendimiento y capacidad	Interna
BAI04.02 Evaluar el impacto en el negocio.	BAI03.02	Acuerdos de nivel de servicio internos y externos (SLA)	Evaluaciones de impacto al negocio de la disponibilidad, el rendimiento y la capacidad	Interna
			Escenarios de disponibilidad, rendimiento y capacidad	Interna
BAI04.03 Planificar los requisitos de los servicios nuevos o modificados.	BAI02.01	Criterios de aceptación confirmados por las partes interesadas	Planes de rendimiento y capacidad	AP002.02
	BAI03.01	Especificación aprobada de diseño de alto nivel	Priorización de mejoras	AP002.02
	BAI03.02	Especificación aprobada de diseño detallado		
	BAI03.03	Componentes documentados de la solución		
BAI04.04 Monitorizar y revisar la disponibilidad y la capacidad.			Informes de revisión de disponibilidad, rendimiento y capacidad	MEA01.03
BAI04.05 Investigar y resolver los problemas de disponibilidad, rendimiento y capacidad.			Acciones correctivas	AP002.02
			Procedimiento de escalamiento de emergencias	DSS02.02
			Brechas de rendimiento y capacidad	Interna
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin Documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión de disponibilidad	Skills Framework for the Information Age V6, 2015	AVMT
Gestión de capacidad	Skills Framework for the Information Age V6, 2015	CPMG

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de gestión de disponibilidad	Comunica la planificación de infraestructura en términos de disponibilidad, escalabilidad, confiabilidad y posible resiliencia. Incluye directrices para identificar el ancho de banda, capacidad y disponibilidad de los servicios (antes de su diseño y suministro), establece acuerdos de niveles de servicio (SLA) e implementa una monitorización continua de los circuitos, tráfico y tiempos de respuesta.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
<p>Para las empresas que dependen de la información, la gestión de la disponibilidad y la capacidad son críticas para el éxito de las operaciones. Establecer una cultura en la que se priorice la disponibilidad de productos y servicios y la capacidad (en línea con los requisitos del negocio), respaldada por procesos y comportamientos que no solo identifiquen la disponibilidad y capacidad requeridas antes del diseño, sino que también las consideren durante el suministro. Definir consistentemente los SLAs SMART; monitorizar continuamente los circuitos, el tráfico y los tiempos de respuesta; realizar pruebas regulares de continuidad del negocio y recuperación de infraestructura en caso de catástrofes.</p>		
G. Componente: Servicios, infraestructura y aplicaciones		
<ul style="list-style-type: none"> • Herramientas de planificación de capacidad • Servicios y herramientas de suministro • Herramientas de monitorización del nivel de servicio 		

Página dejada en blanco intencionadamente

Dominio: Construir, adquirir e implementar Objetivo de gestión: BAI05 – Gestionar el cambio organizativo		Área prioritaria: Modelo Core de COBIT
Descripción		
Maximizar la probabilidad de implementar con éxito un cambio organizativo sostenible en toda la empresa, de forma rápida y con un riesgo reducido. Cubrir el ciclo de vida completo del cambio y todas las partes interesadas en el negocio y en TI.		
Propósito		
Preparar y conseguir el compromiso de las partes interesadas para el cambio en el negocio y reducir el riesgo de fracaso.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales	➔	Metas de alineamiento
<ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG05 Cultura de servicio orientada al cliente • EG08 Optimización de la funcionalidad de procesos internos del negocio • EG12 Gestión de programas de transformación digital 		<ul style="list-style-type: none"> • AG03 Beneficios obtenidos del portafolio de inversiones y servicios habilitados por la I&T AG08 Habilitar y dar soporte a procesos de negocio mediante la integración de aplicaciones y tecnología • AG09 Ejecución de programas dentro del plazo, sin exceder el presupuesto y que cumplan con los requisitos y estándares de calidad
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios		AG03 a. Porcentaje de inversiones posibilitadas por la I&T en las que los beneficios previstos se cumplen o exceden b. Porcentaje de servicios de I&T para los que se han logrado los beneficios esperados (indicados en los acuerdos de nivel de servicio)
EG05 a. Número de interrupciones del servicio al cliente b. Porcentaje de partes interesadas del negocio satisfechas de que la prestación de servicios al cliente cumpla con los niveles de servicio acordados c. Número de quejas del servicio al cliente d. Tendencia de los resultados de la encuesta de satisfacción al cliente		AG08 a. Plazo para la ejecución de servicios y procesos del negocio b. Número de programas del negocio habilitados por I&T que se retrasan o que incurren en costes adicionales debido a problemas de integración tecnológica c. Número de cambios en los procesos de negocio que se deben aplazar o volver a realizar debido a problemas de integración tecnológica d. Número de aplicaciones o infraestructuras críticas que operan en silos y no están integradas
EG08 a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarial b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro		AG09 a. Número de programas/proyectos ejecutados a tiempo y dentro del presupuesto b. Número de programas que necesitan una revisión significativa debido a defectos de calidad c. Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto
EG12 a. Número de programas ejecutados a tiempo y dentro del presupuesto b. Porcentaje de partes interesadas satisfechas con la ejecución del programa c. Porcentaje de programas de transformación del negocio suspendidos d. Porcentaje de programas de transformación del negocio con actualizaciones de estado notificadas regularmente		

A. Componente: Proceso	
Práctica de gestión	Métricas modelo
BAI05.01 Establecer el deseo de cambiar. Comprender el alcance e impacto de los cambios deseados. Evaluar la preparación y voluntad de las partes interesadas para cambiar. Identificar acciones que motiven a las partes interesadas a aceptar y participar para que el cambio funcione con éxito.	a. Nivel de participación de la alta dirección b. Nivel de deseo de cambio de las partes interesadas

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Evaluar el alcance e impacto de los cambios visualizados, las partes interesadas afectadas, la naturaleza del impacto y la participación requerida de cada grupo de interés, además de la disposición y capacidad real para adoptar el cambio.	2
2. Para establecer el deseo de cambiar, identificar, aprovechar y comunicar los puntos de dolor actuales, eventos negativos, riesgo, insatisfacción de los clientes y problemas del negocio, así como los beneficios iniciales y futuras oportunidades y recompensas y ventajas competitivas.	
3. Emitir comunicaciones clave del comité ejecutivo o CEO que demuestren el compromiso con el cambio.	
4. Proporcionar un liderazgo visible de la alta dirección para establecer el rumbo y alinear, motivar e inspirar a las partes interesadas para que deseen el cambio.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
PROSCI® 3-Phase Change Management Process	Phase 1. Preparing for change—Define your change management strategy
Práctica de gestión	Métricas modelo
BAI05.02 Formar un equipo de implementación eficaz. Establecer un equipo de implementación eficaz con miembros apropiados, que genere confianza y establezca objetivos comunes y medidas de eficacia.	a. Número de habilidades identificadas o problemas de capacidad en el equipo de implementación b. Valoración de satisfacción de las partes interesadas con el equipo de implementación
Actividades	Nivel de capacidad
1. Identificar y conformar a un equipo eficaz de implementación principal que incluya a los miembros adecuados del negocio y TI con la capacidad para dedicar la cantidad de tiempo requerida y contribuir con su conocimiento y especialidad, experiencia, credibilidad y autoridad. Considerar la inclusión de personal externo, como consultores, para que proporcionen un punto de vista independiente y para abordar las brechas de habilidades. Identificar los posibles agentes de cambio dentro de las distintas partes de la empresa con las que el equipo principal puede trabajar para respaldar la visión y los cambios en cascada.	3
2. Crear confianza dentro del equipo de implementación principal a través de eventos planificados cuidadosamente con una comunicación eficaz y actividades conjuntas.	
3. Desarrollar una visión y metas comunes que respalden los objetivos de la empresa.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
PROSCI® 3-Phase Change Management Process	Phase 1. Preparing for change—Prepare your change management team
Práctica de gestión	Métricas modelo
BAI05.03 Comunicar la visión deseada. Comunicar la visión de cambio deseada en el lenguaje de los afectados por el mismo. La alta gerencia debe realizar la comunicación y debe incluir la justificación y beneficios del cambio, impactos de no hacer el cambio, así como la visión, hoja de ruta y participación requerida de las distintas partes interesadas.	a. Número de preguntas relacionadas con el cambio b. Retroalimentación de las partes interesadas sobre el nivel de comprensión del cambio
Actividades	Nivel de capacidad
1. Desarrollar un plan de comunicación de la visión para respaldar a los grupos de audiencia principales, sus perfiles de comportamiento y necesidades de información, canales de comunicación y principios.	3
2. Comunicar en los niveles adecuados de la empresa, conforme al plan.	
3. Reforzar la comunicación a través de múltiples foros y repeticiones.	
4. Hacer que todos los niveles de liderazgo rindan cuentas para demostrar la visión.	
5. Comprobar la comprensión de la visión deseada y responder a cualquier cuestión señalada por el personal.	4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin Documentación relacionada para esta práctica de gestión	

A. Componente: Proceso (cont.)	
Práctica de gestión	Métricas modelo
BAI05.04 Facultar a los roles participantes e identificar las ganancias a corto plazo. Facultar a los titulares de los roles de implementación mediante la asignación de la rendición de cuentas. Proporcionar formación y alinear las estructuras organizativas y los procesos de RR. HH. Identificar y comunicar las ganancias a corto plazo que son importantes desde una perspectiva de habilitación de cambio.	a. Nivel de satisfacción de los roles participantes con la operación, uso y mantenimiento del cambio b. Porcentaje de roles participantes capacitados c. Porcentaje de roles participantes con autoridad adecuada asignada d. Retroalimentación de los roles participantes sobre el nivel de empoderamiento e. Autoevaluación de los roles participantes sobre las capacidades relevantes
Actividades	Nivel de capacidad
1. Planificar las oportunidades de capacitación que necesitará el personal para desarrollar las habilidades y actitudes necesarias para sentirse empoderados.	2
2. Identificar, priorizar y ofrecer oportunidades de ganancias rápidas. Éstas podrían estar relacionadas con áreas conocidas de dificultad o factores externos reales que deben abordarse de forma urgente.	
3. Aprovechar las ganancias rápidas ofrecidas comunicando los beneficios a los afectados para mostrar que la visión va según lo previsto. Perfeccionar la visión, mantener a los líderes involucrados y construir el momentum (ganar impulso).	
4. Identificar las estructuras organizativas compatibles con la visión; de ser necesario, realizar cambios para asegurar el alineamiento.	3
5. Alinear los procesos de RR. HH. y los sistemas de medición (p. ej. evaluación del rendimiento, decisiones de compensación, decisiones de promoción, reclutamiento y contratación) para respaldar la visión.	
6. Identificar y gestionar a los líderes que siguen resistiéndose al cambio.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin documentación relacionada para esta práctica de gestión	
Práctica de gestión	Métricas modelo
BAI05.05 Habilitar la operación y el uso. Planificar e implementar todos los aspectos técnicos, operativos y de uso, de forma que todas las personas involucradas en el futuro estado del entorno puedan ejercer sus responsabilidades.	a. Porcentaje de usuarios empoderados adecuadamente para el cambio b. Porcentaje de planes desarrollados para la puesta en marcha y uso del cambio
Actividades	Nivel de capacidad
1. Desarrollar un plan para la operación y uso del cambio. El plan debería comunicar y construir a partir de las ganancias rápidas obtenidas, abordar, en términos globales, aspectos culturales y de comportamiento de la transición e incrementar el compromiso y la participación. Asegurar que el plan cubre una visión holística del cambio y que proporciona documentación (p. ej. procedimientos), asesoría, capacitación, tutoría, transferencia de conocimientos, soporte para el mejoramiento continuo inmediatamente después de su implantación.	3
2. Implementar el plan operativo y de uso. Definir y hacer seguimiento de las medidas de éxito, incluyendo medidas difíciles para el negocio y medidas de percepción que indiquen cómo se sienten las personas con un cambio. Implementar acciones correctivas si fuera necesario.	4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
PROSCI® 3-Phase Change Management Process	Phase 2. Managing change
Práctica de gestión	Métricas modelo
BAI05.06 Incorporar nuevos enfoques. Incorporar nuevos enfoques mediante seguimiento a los cambios implementados, a la evaluación de la efectividad del plan de operación y uso, y mantenimiento constante de concienciación a través de comunicación continua. Tomar las medidas correctivas que sean apropiadas (que pueden incluir la obligación de cumplimiento).	a. Nivel de satisfacción de los usuarios con la adopción del cambio b. Porcentaje de auditorías de cumplimiento que identificaron las causas raíz de la escasa adopción c. Número de auditorías de cumplimiento llevadas a cabo para identificar las causas raíz de la escasa adopción y acciones correctivas recomendadas
Actividades	Nivel de capacidad
1. Hacer que los dueños de los procesos rindan cuentas sobre las operaciones normales diarias.	2
2. Celebrar los éxitos e implementar programas de reconocimiento y recompensas para reforzar el cambio.	3
3. Proporcionar concienciación continua a través de la comunicación regular del cambio y su adopción.	
4. Usar sistemas de medición del rendimiento para identificar las causas raíz de la baja adopción. Empezar acciones correctivas	4
5. Llevar a cabo auditorías de cumplimiento para identificar las causas raíz de la baja adopción. Recomendar acciones correctoras.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
PROSCI® 3-Phase Change Management Process	Phase 3. Reinforcing change

A. Componente: Proceso (cont.)	
Práctica de gestión	Métricas modelo
BAI05.07 Sostener los cambios. Sostener los cambios mediante una capacitación efectiva del nuevo personal, campañas continuas de comunicación, compromiso permanente de la alta gerencia, monitorización de la adopción y compartir las lecciones aprendidas en toda la empresa.	a. Número de capacitaciones y transferencias de conocimientos realizadas b. Porcentaje de participación de la alta dirección en el refuerzo del cambio
Actividades	Nivel de capacidad
1. Sostener y reforzar el cambio a través de comunicación regular que demuestre el compromiso de la alta dirección.	2
2. Proporcionar asesoría, capacitación, tutoría y transferencia de conocimientos al personal nuevo para sostener el cambio.	3
3. Realizar revisiones periódicas de la operación y uso del cambio. Identificar mejoras.	4
4. Captar las lecciones aprendidas relacionadas con la implementación del cambio. Compartir el conocimiento con toda la empresa.	5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
PROSCI® 3-Phase Change Management Process	Phase 3. Reinforcing change

B. Componente: Estructuras organizativas																	
Práctica clave de gestión	Comité Ejecutivo	Director general ejecutivo	Director de operaciones	Director de TI	Director de tecnología	Director de tecnologías digitales	Consejo de gobierno de I&T	Dueños del proceso de negocio	Gestor de programas	Gestor de proyecto	Oficina de gestión de proyectos	Director de Recursos Humanos	Jefe de desarrollo	Jefe de operaciones de TI	Gestor de servicios	Gestor de seguridad de la información	Gestor de continuidad del negocio
BAI05.01 Establecer el deseo de cambiar.	R	A		R	R	R	R	R	R	R		R					
BAI05.02 Formar un equipo de implementación eficaz.	A			R	R	R			R	R	R		R				
BAI05.03 Comunicar la visión deseada.	A			R	R	R	R		R	R							
BAI05.04 Facultar a los roles participantes e identificar las ganancias a corto plazo.	A			R	R	R			R	R		R					
BAI05.05 Habilitar la operación y el uso.	A		R	R	R	R		R			R		R	R	R	R	R
BAI05.06 Incorporar nuevos enfoques.	A		R	R	R	R		R			R		R	R	R	R	R
BAI05.07 Sostener los cambios.	A		R	R	R	R		R	R	R	R		R	R	R	R	R
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)																	
Sin documentación relacionada para este componente.																	

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
BAI05.01 Establecer el deseo de cambiar.	De	Descripción	Descripción	A
	AP011.02	Resultados de la calidad del servicio, incluidos la retroalimentación de los clientes	Comunicaciones de la dirección ejecutiva sobre el compromiso de cambiar	Interna
	BAI02.01	• Repositorio de definiciones de requisitos • Criterios de aceptación confirmados por las partes interesadas	Comunicación de factores de cambio	Interna
	BAI02.03	• Registro de riesgos de los requisitos • Acciones de mitigación de riesgos		
	BAI03.01	Especificación de diseño de alto nivel aprobado		
	BAI03.02	Especificación de diseño detallado aprobado		
BAI05.02 Formar un equipo de implementación eficaz.	BAI02.01	Criterios de aceptación confirmados por las partes interesadas	Visión y metas comunes	BAI01.02
			Equipo y roles de implementación	BAI01.04
BAI05.03 Comunicar la visión deseada.			Plan de comunicación de la visión	BAI01.04
			Comunicaciones de la visión	BAI01.05
BAI05.04 Empoderar a los roles participantes e identificar las ganancias a corto plazo.	Fuera de COBIT	Estructura organizativa de la empresa	Objetivos de rendimiento de RR. HH alineados	AP007.04
			Ganancias rápidas identificadas.	BAI01.04
			Comunicación de beneficios	BAI01.06
BAI05.05 Habilitar la operación y el uso.	BAI03.03	Componentes documentados de la solución	Plan de operación y uso	AP008.04; BAI08.03; DSS01.01; DSS01.02; DSS06.02
	BAI03.10	Componentes de la solución actualizados y documentación relacionada	Mediciones y resultados del éxito	AP008.05; BAI07.07; BAI07.08; MEA01.03
BAI05.06 Incorporar nuevos enfoques.			Resultados de la revisión del desempeño de RR. HH.	AP007.04
			Comunicaciones de concienciación	Interna
			Resultados de la auditoría de cumplimiento	MEA02.02; MEA03.03
BAI05.07 Sostener los cambios.			Planes de transferencia del conocimiento	BAI08.02; BAI08.03
			Comunicaciones del compromiso de la dirección	Interna
			Revisiones del uso operativo	MEA02.02
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión del cambio del negocio	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.7. Business Change Management
Planificación y gestión de la implementación del cambio	Skills Framework for the Information Age V6, 2015	CIPM
Diseño e implementación en la organización	Skills Framework for the Information Age V6, 2015	ORDI

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de gestión de cambios organizativos	Proporciona un marco y señala principios para la gestión del cambio organizativo. Refleja la legislación actual y proporciona buenas prácticas de gestión de personal; garantiza un enfoque consistente a la hora de gestionar el cambio en la organización.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Obtener valor de las inversiones habilitadas por I&T requiere algo más que ofrecer soluciones y servicios de I&T. También requiere de cambios en los procesos de negocio, habilidades y competencias, cultura y comportamiento, etc.; todo ello debe incluirse en el caso de negocio de la inversión. La dirección debe crear una cultura de cambio continuo a través de flexibilidad, apertura y confianza y establecer el soporte y comunicación adecuados para la gestión del cambio.		

G. Componente: Servicios, infraestructura y aplicaciones	
<ul style="list-style-type: none"> Herramientas y canales de comunicación Herramientas de supervisión 	

Dominio: Construir, adquirir e implementar		Área prioritaria: Modelo Core de COBIT	
Objetivo de gestión: BAI06 – Gestionar los cambios de TI			
Descripción			
Gestionar todos los cambios de una manera controlada, incluidos los cambios estándar y los mantenimientos de emergencia en relación con los procesos de negocio, las aplicaciones y la infraestructura. Esto incluye estándares y procedimientos de cambio, evaluación del impacto, priorización y autorización, cambios de emergencia, seguimiento, informes, cierre y documentación.			
Propósito			
Facilitar una ejecución de cambios rápida y confiable para el negocio. Mitigar el riesgo de afectar negativamente la estabilidad o integridad del entorno que se ha modificado.			
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:			
Metas empresariales		➔	Metas de alineamiento
EG01 Portafolio de productos y servicios competitivos			AG06 Agilidad para convertir los requisitos del negocio en soluciones operativas
Métricas modelo para metas empresariales			Métricas modelo para metas de alineamiento
EG01 <ul style="list-style-type: none">a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercadob. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del clientec. Porcentaje de productos y servicios que proporcionan una ventaja competitivad. Plazo de comercialización para nuevos productos y servicios			AG06 <ul style="list-style-type: none">a. Nivel de satisfacción de los ejecutivos del negocio con la capacidad de respuesta de I&T a nuevos requisitosb. Plazo de comercialización promedio para servicios y aplicaciones nuevos relacionados con I&Tc. Tiempo promedio para convertir los objetivos estratégicos de I&T en iniciativas acordadas y aprobadasd. Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
BAI06.01 Evaluar, priorizar y autorizar solicitudes de cambio. Evaluar todas las solicitudes de cambio para determinar el impacto en los procesos de negocio y servicios de I&T; y evaluar si el cambio afectará negativamente al entorno operativo e introducirá riesgos inaceptables. Asegurarse de que los cambios se registran, priorizan, clasifican, evalúan, autorizan, planifican y programan.		a. Cantidad de retrabajo causado por cambios fallidos b. Porcentaje de cambios sin éxito debidos a evaluaciones de impacto inadecuadas
Actividades		Nivel de capacidad
1. Usar solicitudes de cambio formales para permitir a los propietarios de los procesos de negocio y a TI solicitar cambios a procesos de negocio, infraestructura, sistemas o aplicaciones. Asegurarse de que todos estos cambios surjan solo a través del proceso de gestión de solicitudes de cambio.		2
2. Categorizar todos los cambios solicitados (p. ej., procesos de negocio, infraestructura, sistemas operativos, redes, sistemas de aplicación, software de aplicación comprado/empaquetado) y relacionar los elementos de configuración afectados.		
3. Priorizar todos los cambios solicitados basándose en los requisitos de negocio y técnicos, recursos requeridos y las razones legales, regulatorias y contractuales para el cambio solicitado.		
4. Aprobar formalmente cada cambio por parte de los dueños de los procesos de negocio, gestores de servicios y partes interesadas técnicas de TI, según corresponda. Los cambios que son de bajo riesgo y relativamente frecuentes deben pre-aprobarse como cambios estándar.		
5. Planificar y programar todos los cambios aprobados.		
6. Planificar y evaluar todas las solicitudes de una manera estructurada. Incluir un análisis de impacto en los procesos de negocio, la infraestructura, los sistemas y las aplicaciones, los planes de continuidad del negocio (BCP) y los proveedores de servicios para asegurarse de que se hayan identificado todos los componentes afectados. Evaluar la probabilidad de afectar negativamente el entorno operativo y el riesgo de implementar el cambio. Considerar las implicaciones de seguridad, privacidad, legales, contractuales y de cumplimiento del cambio solicitado. Considerar también las interdependencias entre los cambios. Involucrar a los propietarios de los procesos de negocio en el proceso de evaluación, cuando sea conveniente.		3
7. Considerar el impacto de los proveedores de servicios contratados (p. ej., de procesamiento de negocio , infraestructura, desarrollo de aplicaciones y servicios compartidos externalizados) en el proceso de gestión de cambios. Incluir la integración de los procesos de gestión de cambios organizativos con los procesos de gestión de cambios de los proveedores de servicios y el impacto en términos contractuales y SLA.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISF, The Standard of Good Practice for Information Security 2016		SY2.4 Change Management
ISO/IEC 20000-1:2011(E)		9.2 Change management
ITIL V3, 2011		Service Transition, 4.2 Change Management
PMBOK Guide, 6.ª edición, 2017		Part 1: 4.6 Perform Integrated Change Control

A. Componente: Proceso (cont.)			
Práctica de gestión		Métricas modelo	
BAI06.02 Gestionar cambios de emergencia. Gestionar cuidadosamente los cambios de emergencia para minimizar futuros incidentes. Asegurar que el cambio de emergencia está controlado y se realiza de forma segura. Verificar que los cambios de emergencia se evalúan adecuadamente y se autorizan después del cambio.		a. Número de cambios de emergencia no autorizados después del incidente b. Porcentaje de cambios totales que son correcciones de emergencia	
Actividades		Nivel de capacidad	
1. Definir lo que constituye un cambio de emergencia.		2	
2. Asegurar que existe un procedimiento documentado para declarar, evaluar, aprobar inicialmente, autorizar después del cambio y registrar un cambio de emergencia.			
3. Verificar que todos los acuerdos de acceso de emergencia para los cambios se autoricen, documenten y revoquen adecuadamente después de que el cambio se haya aplicado.		3	
4. Monitorizar todos los cambios de emergencia y realizar las revisiones posteriores a la implementación con la participación de todas las partes interesadas. La revisión debe considerar e iniciar acciones correctivas basadas en las causas raíz, tales como problemas con los procesos de negocio, desarrollo y mantenimiento de sistemas de aplicación, entornos de desarrollo y pruebas, documentación y manuales, e integridad de datos.		4	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin documentación relacionada para esta práctica de gestión			
Práctica de gestión		Métricas modelo	
BAI06.03 Hacer seguimiento e informar sobre cambios de estado. Mantener un sistema de seguimiento e informes para documentar los cambios rechazados y comunicar el estado de los cambios aprobados, en proceso y finalizados. Asegurarse de que los cambios aprobados se implementan según lo previsto.		a. Número y antigüedad de las solicitudes de cambio pendientes b. Porcentaje de estado de peticiones de cambio comunicadas a las partes interesadas en el plazo adecuado	
Actividades		Nivel de capacidad	
1. Categorizar las solicitudes de cambio en el proceso de seguimiento (p. ej., rechazado; aprobado pero no iniciado; aprobado y en proceso; y cerrado).		4	
2. Implementar informes de estado de los cambios con métricas de rendimiento para permitir la gestión de la revisión y la monitorización, tanto del estado detallado de los cambios como del estado general (p. ej., análisis de la antigüedad de las solicitudes de cambio). Asegurarse de que los informes de estado formen una pista de auditoría para que los cambios puedan rastrearse posteriormente, desde su inicio hasta su eventual disposición.			
3. Monitorizar los cambios abiertos para asegurarse de que todos los cambios aprobados se cierren de manera oportuna, según su prioridad.			
4. Mantener un sistema de seguimiento e informes para todas las solicitudes de cambio.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
CMMI Cybermaturity Platform, 2018		IPCC Apply Change Control	
Práctica de gestión		Métricas modelo	
BAI06.04 Cerrar y documentar los cambios. Siempre que se implementen cambios, actualizar la solución, la documentación del usuario y los procedimientos afectados por el cambio.		a. Número de errores de revisión encontrados en la documentación b. Porcentaje de actualizaciones de procedimientos y documentación de usuario realizadas en el plazo oportuno	
Actividades		Nivel de capacidad	
1. Incluir los cambios en la documentación en el procedimiento de gestión. Algunos ejemplos de documentación son: procedimientos operativos de negocio y de TI, documentación de continuidad del negocio y recuperación ante desastres, información de configuración, documentación de aplicaciones, pantallas de ayuda y materiales de capacitación.		2	
2. Definir un período de retención adecuado para la documentación de los cambios y la documentación del sistema y del usuario antes y después del cambio.		3	
3. Someter la documentación al mismo nivel de revisión que el cambio en sí mismo.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin documentación relacionada para esta práctica de gestión			

B. Componente: Estructuras organizativas											
Práctica clave de gestión	Director de TI	Dueños del proceso de negocio		Gestor de programas	Gestor de proyecto	Jefe de desarrollo	Jefe de operaciones de TI	Gestor de servicios	Gestor de seguridad de la información	Gestor de continuidad del negocio	Director de privacidad
	A	R			R	R	R	R	R	R	R
	A				R	R	R	R			R
	A	R	R	R	R	R	R				
	A	R	R	R	R	R	R		R		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)					Referencia específica						
Sin documentación relacionada para este componente.											


C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
BAI06.01 Evaluar, priorizar y autorizar solicitudes de cambio.	De	Descripción	Descripción	A
	BAI03.05	Componentes de la solución integrados y configurados	Plan y cronograma de cambios	BAI07.01
	DSS02.03	Solicitudes de servicio aprobadas	Solicitudes de cambio aprobadas	BAI07.01
	DSS03.03	Soluciones propuestas a errores conocidos	Evaluaciones del impacto	Interna
	DSS03.05	Soluciones sostenibles identificadas		
	DSS04.08	Cambios aprobados a los planes		
	DSS06.01	Análisis de las causas raíz y recomendaciones		
BAI06.02 Gestionar cambios de emergencia.			Revisión posterior a la implementación	Interna
BAI06.03 Hacer seguimiento e informar sobre cambios de estado.	BAI03.09	Registro de todas las solicitudes de cambio aprobadas y aplicadas	Informes de estado de las solicitudes de cambio	BAI01.06; BAI10.03
BAI06.04 Cerrar y documentar los cambios.			Cambio en la documentación	Interna
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión de cambios	Skills Framework for the Information Age V6, 2015	CHMG
Soporte para cambios	e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework, 2016	C. Run - C.2. Change Support

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de gestión de cambios de TI	Comunica a la dirección la intención de que todos los cambios de TI de la empresa se gestionen e implementen de forma que se minimice el riesgo y el impacto en las partes interesadas. Cubre los activos afectados y el proceso de gestión de cambios estándar.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Los directivos deben crear una cultura de mejora continua a las soluciones y servicios de TI, con el reconocimiento de que la mejora implica que ellos entiendan el impacto del cambio tecnológico en la empresa, su riesgo inherente y la mitigación asociada, así como su coste. Los directivos deben balancear el impacto del cambio contra los beneficios esperados y su contribución a la estrategia de I&T y los objetivos empresariales.		

G. Componente: Servicios, infraestructura y aplicaciones	
<ul style="list-style-type: none"> Herramientas de gestión de la configuración Herramientas de gestión de cambios de TI 	

Dominio: Construir, adquirir e implementar		Objetivo de gestión: BAI07 – Gestionar la aceptación y la transición de los cambios de TI		Área prioritaria: Modelo Core de COBIT	
Descripción					
Aceptar formalmente y hacer operativas las nuevas soluciones. Incluir la planificación de la implementación, conversión de sistemas y datos, pruebas de aceptación, comunicación, preparación de la puesta en producción, paso a producción de nuevos o modificados procesos de negocio y servicios de I&T, soporte temprano de la producción y revisión posterior a la implementación.					
Propósito					
Implementar soluciones de forma segura y conforme a las expectativas y resultados acordados.					
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:					
Metas empresariales				Metas de alineamiento	
EG01 Portafolio de productos y servicios competitivos				AG06 Agilidad para convertir los requisitos del negocio en soluciones operativas	
Métricas modelo para metas empresariales				Métricas modelo para metas de alineamiento	
EG01 <ul style="list-style-type: none">a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercadob. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del clientec. Porcentaje de productos y servicios que proporcionan una ventaja competitivad. Plazo de comercialización para nuevos productos y servicios				AG06 <ul style="list-style-type: none">a. Nivel de satisfacción de los ejecutivos del negocio con la capacidad de respuesta de I&T a los nuevos requisitosb. Plazo de comercialización promedio para servicios y aplicaciones nuevos relacionados con I&Tc. Tiempo promedio para convertir los objetivos estratégicos de I&T en iniciativas acordadas y aprobadasd. Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas	

A. Componente: Proceso			
Práctica de gestión		Métricas modelo	
BAI07.01 Establecer un plan de implementación. Establecer un plan de implementación que cubra la conversión de sistemas y datos, criterios de pruebas de aceptación, comunicación, formación, preparación de puestas en producción, paso a producción, soporte temprano en producción, plan de fallback/backup y revisión posterior a la implementación. Obtener la aprobación de las partes interesadas.		a. Número y categoría de partes interesadas que aceptan el plan de implementación b. Número de planes de implementación robustos y que contienen todos los componentes necesarios	
Actividades			Nivel de capacidad
1. Crear un plan de implementación que refleje la estrategia global de implementación, secuencia de los pasos de implementación, requisitos de recursos, interdependencias, criterios de la dirección para la aceptación de la implementación a producción, establecimiento de requisitos de verificación, estrategia de transición para el soporte en producción y actualización de los planes de continuidad del negocio.			2
2. Obtener de los proveedores externos de soluciones el compromiso de su participación en cada paso de la implementación.			
3. Identificar y documentar los procesos de fallback y recuperación.			
4. Confirmar que todos los planes de implementación cuentan con la aprobación de las partes interesadas técnicas y de negocio y que están revisados por auditoría interna, cuando sea necesario.			3
5. Revisar formalmente el riesgo técnico y de negocio asociado con la implementación. Asegurar que considere el riesgo se y se aborde en el proceso de planificación.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
ITIL V3, 2011		Service Transition, 4.1 Transition Planning and Support	

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
BAI07.02 Planificar la conversión de procesos de negocio, sistemas y datos. Prepararse para la migración de los procesos de negocio, datos de servicios e infraestructura de I&T como parte de los métodos de desarrollo de la empresa. Incluir pistas de auditoría y un plan de recuperación si la migración falla.		a. Porcentaje de conversión realizada correctamente b. Porcentaje de ajustes necesarios realizados en los procedimientos (incluyendo la revisión de roles y responsabilidades y procedimientos de control)
Actividades		Nivel de capacidad
1. Definir un plan de migración del proceso de negocio, de los datos de servicios y de la infraestructura de I&T. En el desarrollo del plan, considerar, por ejemplo, el hardware, las redes, los sistemas operativos, el software, los datos de transacción, los archivos maestros, las copias de seguridad y archivos, las interfaces con otros sistemas (internos y externos), los posibles requisitos de cumplimiento, los procedimientos de negocio y la documentación del sistema.		2
2. En el plan de conversión del proceso de negocio, considerar todos los ajustes necesarios de los procedimientos, incluyendo la revisión de roles y responsabilidades y procedimientos de control.		
3. Confirmar que el plan de conversión de datos no requiere cambios en los valores de los datos, a menos que sea absolutamente necesario por razones de negocio. Documentar los cambios realizados en los valores de los datos y asegurar la aprobación del dueño de los datos del proceso de negocio.		
4. Planificar la retención de los datos de copias de seguridad y archivados de acuerdo con las necesidades del negocio y los requisitos de cumplimiento o regulatorios.		
5. Ensayar y probar la conversión antes de intentar una conversión en vivo.		
6. Coordinar y verificar los tiempos e integridad de la transición de la conversión rápida para que se produzca una transición continua y uniforme sin que se pierdan datos en la transición. Cuando sea necesario, si no existe otra alternativa, congelar las operaciones en vivo.		
7. Planificar una copia de seguridad de todos los sistemas y datos recopilados en el momento previo a la conversión. Mantener pistas de auditoría para poder tener un registro de los pasos de la conversión. Garantizar que haya un plan de recuperación que cubra el rollback de la migración y el fallback al procesamiento anterior si la migración falla.		3
8. Incorporar en el plan de conversión de datos métodos para recopilar, convertir y verificar los datos a convertir, e identificar y resolver cualquier error encontrado durante la conversión. Incluir la comparativa de los datos originales con los convertidos para comprobar su integridad y que están completos.		
9. Considerar el riesgo de los problemas de conversión, planificación de la continuidad del negocio y procedimientos de fallback en el proceso de negocio, plan de migración de datos e infraestructura en los que haya gestión de riesgo, necesidades del negocio o requisitos de cumplimiento/regulatorios.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ITIL V3, 2011		Service Transition, 4.1 Transition Planning and Support
Práctica de gestión		Métricas modelo
BAI07.03: Plan de pruebas de aceptación. Establecer un plan de pruebas basado en estándares de toda la empresa que defina roles, responsabilidades y criterios de entrada y salida. Asegurarse de que las partes interesadas aprueben el plan.		a. Porcentaje de partes interesadas satisfechas con la completitud del proceso de prueba b. Número de planes de pruebas documentados que incluyen todas las fases de las pruebas y escenarios de pruebas sólidos y adecuados para los requisitos y el entorno operativos

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Desarrollar y documentar el plan de pruebas, que esté alineado con el programa, el plan de calidad del proyecto y los estándares organizativos relevantes. Comunicar y consultar con los dueños del proceso de negocio y las partes interesadas de TI apropiadas.	2
2. Asegurar que el plan de pruebas refleje la evaluación del riesgo del proyecto y que se prueban todos los requisitos funcionales y técnicos. Con base en la evaluación del riesgo de fallo del sistema y los fallos en la implementación, incluir en el plan requisitos de rendimiento, estrés, usabilidad, piloto, pruebas de seguridad y privacidad.	
3. Garantizar que el plan de pruebas aborde la posible necesidad de acreditación interna o externa de los resultados del proceso de prueba (p. ej. requisitos financieros o regulatorios).	
4. Asegurar que el plan de pruebas identifique los recursos necesarios para ejecutar las pruebas y evaluar los resultados. Algunos ejemplos de recursos pueden ser la construcción de entornos de pruebas y el uso del tiempo del personal para el grupo de pruebas, incluida la posible sustitución temporal del personal de pruebas en los entornos de producción o desarrollo. Asegurar que se consulta a las partes interesadas sobre las implicaciones del plan de pruebas.	
5. Asegurar que el plan de pruebas identifique las fases de prueba apropiadas de acuerdo con los requisitos y entorno operativos. Algunos ejemplos de estas fases de pruebas son la inclusión de pruebas unitarias, pruebas de sistema, pruebas de integración, pruebas de aceptación del usuario, pruebas de rendimiento, pruebas de estrés, pruebas de conversión de datos, pruebas de seguridad, pruebas de privacidad, pruebas de preparación operativa, y pruebas de copias de seguridad y recuperación.	
6. Confirmar que el plan de pruebas considera la preparación de las pruebas (incluida la preparación de la instalación), requisitos de capacitación, instalación o actualización del entorno de pruebas definido, casos de pruebas de planificación/rendimiento/documentación/retención, manejo de errores y problemas, corrección y escalamiento, y aprobación formal.	
7. Confirmar que todos los planes de pruebas cuentan con la aprobación de las partes interesadas, incluidos los dueños del proceso de negocio y de TI, como corresponda. Las partes interesadas podrían incluir a los gestores del desarrollo de aplicaciones, gestores de proyecto y usuarios finales del proceso de negocio.	
8. Asegurar que el plan de pruebas establezca criterios claros para la medición del éxito de cada una de las fases de pruebas. Consultar con los dueños del proceso de negocio y las partes interesadas de TI para definir los criterios de éxito. Determinar que el plan establece los procedimientos de remediación cuando no se cumplen los criterios de éxito. Por ejemplo, si hay un fallo significativo en una fase de pruebas, el plan debe proporcionar unas directrices sobre si proceder a la fase siguiente, detener las pruebas o postergar la implementación.	3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin documentación relacionada para esta práctica de gestión	
Práctica de gestión	Métricas modelo
BAI07.04: Establecer un entorno de pruebas. Definir y establecer un entorno de pruebas seguro y representativo del proceso de negocio planificado y del entorno de operaciones de TI, en cuanto a rendimiento, capacidad, seguridad, controles internos, prácticas operativas, calidad de los datos, requisitos de privacidad y cargas de trabajo.	a. Nivel de comparación entre el entorno de pruebas y el entorno operativo y de negocio futuro b. Nivel de datos (y/o bases de datos) de pruebas borrados de forma segura (sanitizados) que son representativos del entorno de producción
Actividades	Nivel de capacidad
1. Crear una base de datos de pruebas que sea representativa del entorno de producción. Borrar en forma segura los datos usados en el entorno de pruebas y que vienen del entorno de producción, conforme a las necesidades de negocio y los estándares organizativos. Por ejemplo, considerar si los requisitos de cumplimiento o regulatorios obligan al uso de borrado seguro de datos.	2
2. Proteger los datos de prueba y resultados sensibles contra su divulgación, incluido el acceso, retención, almacenamiento y destrucción. Considerar el efecto de la interacción de los sistemas organizativos con los de terceros.	3
3. Establecer un proceso que permita la apropiada retención o eliminación (disposición) de los resultados de las pruebas, medios u otra documentación asociada, que permitan la revisión adecuada y el subsiguiente análisis o realización eficiente de nuevas pruebas, según lo requiera el plan de pruebas. Considerar el efecto de los requisitos de cumplimiento o regulatorios.	
4. Garantizar que el entorno de pruebas sea representativo del entorno operativo y de negocio futuro. Incluir procedimientos y roles del proceso de negocio, posible estrés por la carga de trabajo, sistemas operativos, software de aplicaciones necesario, sistemas de gestión de bases de datos e infraestructura de red y computación que se encuentre en el entorno de producción.	
5. Asegurar que el entorno de pruebas sea seguro e incapaz de interactuar con los sistemas de producción.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin documentación relacionada para esta práctica de gestión	

A. Componente: Proceso (cont.)		
Práctica de gestión	Métricas modelo	
BAI07.05 Realizar pruebas de aceptación. Probar los cambios de forma independiente de acuerdo con el plan de pruebas definido antes de la migración al entorno operativo en producción.	a. Número de brechas identificadas entre los resultados de las pruebas de aceptación y los criterios de éxito definidos b. Número de pruebas de aceptación satisfactorias	
Actividades	Nivel de capacidad	
1. Revisar la categorización del log de errores encontrados por el equipo de desarrollo en el proceso de pruebas. Comprobar que todos los errores se han solucionado o aceptado formalmente.	2	
2. Evaluar la aceptación final mediante comparación con los criterios de éxito e interpretar los resultados de las pruebas de aceptación final. Presentarlos de forma que sean entendibles para los dueños del proceso de negocio y de TI, para que pueda realizarse una evaluación y revisión informada.	3	
3. Aprobar la aceptación, con la confirmación formal de los dueños del proceso de negocio, terceros (si corresponde) y las partes interesadas de TI antes de su promoción.		
4. Garantizar que se llevan a cabo pruebas de los cambios conforme al plan de pruebas. Asegurar que las pruebas han sido diseñadas y ejecutadas por un grupo de pruebas, independiente del equipo de desarrollo. Considerar hasta qué punto están incluidos los dueños de los procesos de negocio y los usuarios finales en el grupo de pruebas. Asegurar que las pruebas se realicen solo dentro del entorno de pruebas.		
5. Asegurar que las pruebas y los resultados esperados se correspondan con los criterios de éxito definidos establecidos en el plan de pruebas.		
6. Considerar el uso de instructivos (guiones) de pruebas definidas claramente para implementar las pruebas. Asegurar que el grupo de pruebas independiente evalúe y apruebe cada guion de pruebas para confirmar que se han abordado adecuadamente los criterios de éxito de las pruebas establecidos en el plan de pruebas. Considerar el uso de guiones para comprobar hasta qué punto cumple el sistema con los requisitos de seguridad y privacidad.		
7. Considerar el equilibrio adecuado entre los guiones de pruebas automatizadas y las pruebas interactivas del usuario.		
8. Llevar a cabo pruebas a la seguridad conforme al plan de pruebas. Medir hasta qué punto existen debilidades o brechas de seguridad. Considerar el efecto de los incidentes de seguridad desde la creación del plan de pruebas. Considerar el efecto sobre los controles y los límites de acceso. Considerar la privacidad.		
9. Llevar a cabo pruebas de rendimiento del sistema y de las aplicaciones conforme al plan de pruebas. Considerar una serie de métricas de rendimiento (p. ej. tiempos de respuesta del usuario final y rendimiento de la actualización del sistema de gestión de base de datos).		
10. Cuando se lleven a cabo las pruebas, garantizar que se han considerado los elementos de fallback y rollback del plan de pruebas.		
11. Identificar, registrar y clasificar los errores (p. ej. menores, significativos, de misión crítica) durante las pruebas. Asegurar que esté disponible una pista de auditoría de los resultados de las pruebas. Según el plan de pruebas, comunicar los resultados de las pruebas a las partes interesadas para facilitar la corrección de errores y mejoras en la calidad.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
ITIL V3, 2011	Service Transition, 4.5 Service Validation and Testing	
Práctica de gestión	Métricas modelo	
BAI07.06 Promover a producción y gestionar las liberaciones (releases). Promover la solución aceptada al negocio y a las operaciones. Cuando sea apropiado, ejecutar la solución como una implementación piloto o en paralelo con la solución antigua durante un período definido y comparar el comportamiento y los resultados. Si se producen problemas significativos, volver al entorno original usando el plan de fallback/backup. Gestionar las liberaciones de los componentes de la solución.	a. Número y porcentaje de versiones no listas para lanzarse según el calendario b. Porcentaje de satisfacción de las partes interesadas con la solución implementada	
Actividades	Nivel de capacidad	
1. Prepararse para la transferencia de procedimientos del negocio y servicios de soporte, aplicaciones e infraestructura desde el entorno de pruebas al entorno de producción conforme a los estándares de gestión de cambios organizativos.	2	
2. Determinar hasta qué punto la implementación del piloto o el procesamiento paralelo de los sistemas nuevos y viejos está en línea con el plan de implementación.		
3. Actualizar rápidamente la documentación del proceso de negocio y del sistema, la información de configuración y los documentos de planes de contingencia relevantes, conforme corresponda.		
4. Garantizar que todas las bibliotecas de medios se actualizan rápidamente con la versión del componente de la solución transferido del entorno de pruebas al entorno de producción. Archivar la versión actual y su documentación soporte. Asegurar que la promoción a producción de sistemas, software de aplicaciones e infraestructura esté bajo el control de configuración.		
5. Si la distribución de componentes de soluciones se lleva a cabo de forma electrónica, controlar la distribución automática para garantizar que se notifica a los usuarios y que la distribución solo se realiza a destinatarios autorizados correctamente identificados. Incluir procedimientos de copia de seguridad en el proceso de liberación (release) para permitir que la distribución de los cambios se revise en caso de falla o error.		
6. Si la distribución se hace de forma física, mantener un registro formal de qué elementos se han distribuido, a quién y dónde se han implementado y cuándo se ha actualizado cada uno de ellos.		

A. Componente: Proceso (cont.)		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISO/IEC 20000-1:2011(E)		9.3 Release and deployment management
ITIL V3 2011		Service Transition, 4.4 Release and Deployment Management
Práctica de gestión		Métricas modelo
BAI07.07 Proporcionar soporte oportuno en producción. Proporcionar, durante un periodo de tiempo acordado, soporte oportuno a los usuarios y a las operaciones de I&T para resolver problemas y ayudar a estabilizar la nueva solución.		a. Número de recursos adicionales del sistema de I&T proporcionados para dar soporte b. Número de personal adicional proporcionado como soporte
Actividades		Nivel de capacidad
1. Proporcionar recursos adicionales, cuando se requiera, a los usuarios finales y personal de soporte hasta que se establezca la liberación.		3
2. Proporcionar recursos de sistemas de I&T adicionales, conforme se requiera, hasta que el lanzamiento esté en un entorno operativo estable.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
BAI07.08 Realizar una revisión post-implementación. Realizar una revisión post-implementación para confirmar los resultados, identificar las lecciones aprendidas y desarrollar un plan de acción. Evaluar el rendimiento y los resultados reales del servicio nuevo o modificado, en comparación con el rendimiento y resultados previstos por el usuario o cliente.		a. Número y porcentaje de análisis causa raíz completados b. Número o porcentaje de liberaciones que no se estabilizan dentro de un periodo aceptable c. Porcentaje de liberaciones que causan tiempo de inactividad
Actividades		Nivel de capacidad
1. Establecer procedimientos para garantizar que las revisiones post-implementación identifiquen, evalúen e informen sobre en qué medida han ocurrido los eventos siguientes: los requisitos de la empresa se han cumplido; los beneficios esperados se han logrado; el sistema se considera utilizable; las expectativas de las partes interesadas se han cumplido; han ocurrido impactos inesperados en la empresa; los riesgos clave se han mitigado; y los procesos de gestión de cambios, instalación y acreditación se han realizado de forma eficaz y eficiente.		3
2. Consultar a los dueños del proceso de negocio y los directivos técnicos de TI sobre la elección de métricas para la medición del éxito y consecución de requisitos y beneficios.		4
3. Llevar a cabo la revisión post-implementación conforme al proceso de gestión de cambios de la organización. Involucrar a los dueños del proceso de negocio y las terceras partes, como corresponda.		
4. Considerar los requisitos para la revisión post-implementación que surjan de fuera del negocio y de TI (p. ej. auditoría interna, ERM, cumplimiento).		
5. Acordar e implementar un plan de acción para solucionar los problemas identificados en la revisión post-implementación. Involucrar a los dueños del proceso de negocio y los directivos técnicos de TI en el desarrollo del plan de acción.		5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ITIL V3, 2011		Service Transition, 4.6 Change Evaluation

B. Componente: Estructuras organizativas											
	Director de TI	Dueños del proceso de negocio		Función de gestión de datos		Jefe de desarrollo	Jefe de operaciones de TI	Gestor de servicios	Gestor de seguridad de la información	Gestor de continuidad del negocio	Director de privacidad
Práctica clave de gestión											
BAI07.01 Establecer un plan de implementación.	A	R			R			R	R	R	
BAI07.02 Planificar la conversión de procesos de negocio, sistemas y datos.	A	R	R		R			R	R	R	
BAI07.03: Plan de pruebas de aceptación.	A	R			R	R			R	R	R
BAI07.04: Establecer un entorno de pruebas.	A	R			R	R			R	R	
BAI07.05 Realizar pruebas de aceptación.	A	R			R	R			R	R	R
BAI07.06 Promover a producción y gestionar las liberaciones (releases).	A	R			R	R	R			R	
BAI07.07 Proporcionar soporte oportuno en producción.	A	R			R	R	R				
BAI07.08 Realizar una revisión post-implementación	A	R			R	R	R				
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica										
Sin documentación relacionada para este componente.											

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
BAI07.01 Establecer un plan de implementación.	BAI01.07	Plan de gestión de la calidad	Implementación de procesos de fallback y recuperación	Interna
	BAI06.01	• Solicitudes de cambio aprobadas • Plan y calendario de cambios	Plan de implementación aprobado	Interna
	BAI11.05	Plan de gestión de la calidad del proyecto		
BAI07.02 Planificar la conversión de procesos de negocio, sistemas y datos.			Plan de migración	DSS06.02
BAI07.03: Plan de pruebas de aceptación.	BAI01.07	Requisitos para la verificación independiente de entregables	Plan de prueba de aceptación aprobado	BAI01.04; BAI11.04
	BAI03.07	• Plan de pruebas • Procedimientos de pruebas		
	BAI03.08	• Logs de resultados y pistas de auditoría de las pruebas • Comunicaciones de resultados de las pruebas		
	BAI11.05	Requisitos para la verificación independiente de entregables del proyecto		

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
BAI07.04: Establecer un entorno de pruebas.	De	Descripción	Descripción	A
			Datos de pruebas	Interna
BAI07.05 Realizar pruebas de aceptación.			Aceptación y liberación aprobada a producción	BAI01.04
			Evaluación de los resultados de aceptación	BAI01.06
			Registro de resultados de pruebas	Interna
BAI07.06 Promover a producción y gestionar las liberaciones (releases).			Plan de liberaciones	BAI10.01
			Registro de liberaciones	Interna
BAI07.07 Proporcionar soporte oportuno en producción.	AP011.02	Resultados de la calidad del servicio, incluyendo la retroalimentación de los clientes	Plan de soporte suplementario	APO08.04; APO08.05; DSS02.04
	BAI05.05	Mediciones y resultados del éxito		
BAI07.08 Realizar una revisión post-implementación.	AP011.03	• Resultados de la monitorización de la calidad para la prestación de servicios y soluciones • Causas raíz de los fallos de entrega de calidad	Plan de acciones correctivas	BAI01.09; BAI11.09
	AP011.04	Resultados de las revisiones y auditorías de calidad	Informe de la revisión post-implementación.	BAI01.09; BAI11.09
	BAI05.05	Mediciones y resultados del éxito		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Pruebas de los procesos de negocio	Skills Framework for the Information Age V6, 2015	BPTS
Liberación y despliegue	Skills Framework for the Information Age V6, 2015	RELM
Aceptación del servicio	Skills Framework for the Information Age V6, 2015	SEAC
Pruebas	Skills Framework for the Information Age V6, 2015	TEST
Evaluación de la experiencia del usuario	Skills Framework for the Information Age V6, 2015	USEV

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de gestión de cambios de TI	Comunica a la dirección la intención de que todos los cambios de TI de la empresa se gestionen e implementen de forma que se minimice el riesgo y el impacto en las partes interesadas. Cubre los activos afectados y el proceso de gestión de cambios estándar.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Establecer una cultura que garantice la comunicación oportuna de las solicitudes de cambio de TI a los grupos afectados; consultar con los grupos afectados la implementación y pruebas de los cambios.		

G. Componente: Servicios, infraestructura y aplicaciones	
<ul style="list-style-type: none"> • Herramientas de gestión de cambios de TI • Herramientas de gestión de liberaciones • Herramientas y servicios de pruebas 	

Dominio: Construir, adquirir e implementar Objetivo de gestión: BAI08 – Gestionar el conocimiento		Área prioritaria: Modelo Core de COBIT
Descripción		
Mantener disponible la información de gestión relevante, vigente, conocimiento validado y confiable con el fin de apoyar todas las actividades del proceso y facilitar la toma de decisiones relacionadas con el gobierno y la gestión de I&T de la empresa. Planificar la identificación, recopilación, organización, mantenimiento, uso y retirada del conocimiento.		
Propósito		
Proporcionar el conocimiento e información de gestión necesarios para apoyar a todo el personal en el gobierno y gestión de la I&T de la empresa y facilitar la toma de decisiones informada.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales		Metas de alineamiento
<ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG10 Habilidades, motivación y productividad del personal • EG13 Innovación de productos y negocio 		<ul style="list-style-type: none"> • AG12 Personal competente y motivado con entendimiento de la tecnología y el negocio • AG13 Conocimiento, experiencia e iniciativas para la innovación empresarial
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 <ul style="list-style-type: none"> a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios 		AG12 <ul style="list-style-type: none"> a. Porcentaje de personal de negocio con dominio de I&T (es decir, aquellos que tienen los conocimientos y el entendimiento de I&T requeridos para guiar, dirigir, innovar y ver las oportunidades de I&T en su área de especialización de negocio) b. Porcentaje de personal de I&T con dominio de negocio (es decir, aquellos que tienen los conocimientos y el entendimiento de los dominios de negocio relevantes para guiar, dirigir, innovar y ver las oportunidades de I&T para su dominio de negocio) c. Número o porcentaje de personal de negocio con experiencia en gestión de tecnología
EG10 <ul style="list-style-type: none"> a. Productividad del personal comparada con benchmarks b. Nivel de satisfacción de las partes interesadas con los niveles de conocimientos y habilidades del personal c. Porcentaje de personal cuyas habilidades son insuficientes con respecto a la competencia en su rol d. Porcentaje de personal satisfecho 		AG13 <ul style="list-style-type: none"> a. Nivel de conocimiento y comprensión de los ejecutivos del negocio sobre las posibilidades de innovación de las I&T b. Número de iniciativas aprobadas como resultado de ideas innovadoras de I&T c. Número de campeones en innovación reconocidos/premiados
EG13 <ul style="list-style-type: none"> a. Nivel de concienciación y comprensión de las posibilidades de innovación del negocio b. Satisfacción de las partes interesadas con los niveles de habilidades e ideas sobre innovación y productos c. Número de iniciativas de productos y servicios aprobadas como resultado de ideas innovadoras 		

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
BAI08.01 Identificar y clasificar las fuentes de información para el gobierno y la gestión de I&T. Identificar, validar y clasificar las diversas fuentes de información internas y externas requeridas para habilitar el gobierno y la gestión de I&T, incluidos los documentos estratégicos, reportes de incidentes e información de la configuración que surjan desde el desarrollo a las operaciones antes de ponerlo en marcha.		a. Porcentaje de información clasificada validada b. Porcentaje de pertinencia de los tipos de contenido, artefactos e información estructurada y no estructurada
Actividades		Nivel de capacidad
1. Identificar usuarios con conocimiento potenciales, incluidos dueños de información que tal vez deban contribuir y aprobar el conocimiento. Obtener requisitos de conocimiento y fuentes de información de los usuarios identificados.		2
2. Considerar los tipos de contenido (procedimientos, procesos, estructuras, conceptos, políticas, reglas, hechos, clasificaciones), artefactos (documentos, registros, video, voz) e información estructurada y no estructurada (expertos, redes sociales, correo electrónico, mensajes de voz, canales RSS (Rich Site Summary)).		
3. Clasificar las fuentes de información con base en el esquema de clasificación de contenidos (p. ej. el modelo de arquitectura de la información). Correlacionar las fuentes de información con el esquema de clasificación.		3
4. Recopilar, cotejar y validar las fuentes de información con base en los criterios de validación de la información (p. ej., comprensión, relevancia, importancia, integridad, precisión, consistencia, confidencialidad, vigencia y confiabilidad).		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
BAI08.02 Organizar y contextualizar la información en conocimiento. Organizar la información según los criterios de clasificación. Identificar y crear relaciones significativas entre los elementos de información y habilitar el uso de la información. Identificar a los dueños y aprovechar e implementar niveles de acceso a la información definidos por la empresa para la información de gestión y los recursos de conocimiento.		a. Número de relaciones identificadas entre las fuentes de información (etiquetado) b. Porcentaje de satisfacción de las partes interesadas con la organización y contextualización de la información en conocimiento
Actividades		Nivel de capacidad
1. Identificar atributos compartidos y relacionar sus fuentes de información , con la creación de relaciones entre los conjuntos de información (etiquetado de la información).		3
2. Crear vistas de conjuntos de datos relacionados, considerando los requisitos organizativos y de las partes interesadas.		
3. Idear e implementar un esquema para gestionar el conocimiento no estructurado que no está disponible a través de fuentes formales (p.ej. el conocimiento de expertos).		
4. Publicar y hacer que el conocimiento sea accesible a las partes interesadas relevantes, conforme a mecanismos de roles y acceso.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
COSO Enterprise Risk Management, junio de 2017		10. Information, Communication, and Reporting - Principle 18
Práctica de gestión		Métricas modelo
BAI08.03 Utilizar y compartir conocimiento. Transmitir los recursos de conocimiento disponibles a las partes interesadas correspondientes y comunicar cómo estos recursos pueden utilizarse para abordar diferentes necesidades (p. ej., resolución de problemas, aprendizaje, planificación estratégica y toma de decisiones).		a. Porcentaje de conocimiento disponible usado realmente b. Porcentaje de satisfacción del usuario con los conocimientos
Actividades		Nivel de capacidad
1. Establecer expectativas de gestión y demostrar la actitud adecuada en cuanto a la utilidad del conocimiento y la necesidad de compartir el conocimiento relacionado con el gobierno y la gestión de la I&T de la empresa.		2
2. Identificar usuarios potenciales de conocimiento por medio de la clasificación del conocimiento.		
3. Transferir el conocimiento a los usuarios del conocimiento, con base en un análisis de brechas de necesidades y técnicas de aprendizaje efectivas. Crear un entorno, herramientas y artefactos que respalden el intercambio y la transferencia de conocimiento. Asegurar que se cuenta con los controles de acceso adecuados, en línea con la clasificación de conocimiento definida.		3
4. Medir el uso de las herramientas y elementos de conocimiento y evaluar el impacto en los procesos de gobierno.		4
5. Mejorar la información y el conocimiento de los procesos de gobierno que muestran brechas de conocimientos.		5

A. Componente: Proceso (cont.)	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Cybermaturity Platform, 2018	PP.IS Apply Information Sharing; IR.ES Ensure Information sharing
ITIL V3, 2011	Service Transition, 4.7 Knowledge Management
PMBOK guide Sixth edition, 2017	Part 1: 4.4 Manage project knowledge
Práctica de gestión	Métricas modelo
BAI08.04 Evaluar y actualizar o retirar la información. Medir el uso y evaluar la aceptación y relevancia de la información. Actualizar la información o retirar la información obsoleta.	a. Frecuencia de actualización b. Nivel de satisfacción de los usuarios
Actividades	Nivel de capacidad
1. Definir los controles para la retirada de conocimientos y proceder a su retirada como corresponda.	3
2. Evaluar la utilidad, relevancia y valor de los elementos del conocimiento. Actualizar la información desactualizada que podría seguir siendo relevante y valiosa para la organización. Identificar la información relacionada que ya no es relevante para los requisitos de conocimiento de la empresa y retirarla o archivarla conforme a la política.	4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin documentación relacionada para esta práctica de gestión	

B. Componente: Estructuras organizativas																	
Práctica clave de gestión	Director de TI	Director de tecnología	Director de tecnologías digitales	Dueños del proceso de negocio	Gestor de portafolio	Gestor de programas	Gestor de proyecto	Función de gestión de datos	Jefe de arquitectura	Jefe de desarrollo	Jefe de operaciones de TI	Jefe de administración de TI	Gestor de servicios	Gestor de seguridad de la información	Gestor de continuidad del negocio	Director de privacidad	Asesor legal
BAI08.01 Identificar y clasificar las fuentes de información para el gobierno y la gestión de I&T.	A			R				R		R	R		R				
BAI08.02 Organizar y contextualizar la información en conocimiento.	A							R		R	R	R					
BAI08.03 Utilizar y compartir conocimiento.	A	R	R	R	R	R	R	R				R					R
BAI08.04 Evaluar y actualizar o retirar la información.	A			R		R	R	R	R	R	R	R	R	R	R	R	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica															
Sin documentación relacionada para este componente.																	

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
BAI08.01 Identificar y clasificar las fuentes de información para el gobierno y la gestión de I&T.	De	Descripción	Descripción	A
	Fuera de COBIT	Requisitos y fuentes de conocimiento	Clasificación de las fuentes de información	Interna
BAI08.02 Organizar y contextualizar la información en conocimiento.	BAI03.03	Componentes de la solución documentados	Repositorios de conocimiento publicados	APO07.03
	BAI05.07	Planes de transferencia de conocimiento		
BAI08.03 Utilizar y compartir conocimiento.	BAI03.03	Componentes de la solución documentados	Esquemas de concienciación y capacitación	APO07.03
	BAI05.05	Plan de operación y uso	Base de datos de usuarios de conocimiento	Interna
	BAI05.07	Planes de transferencia de conocimiento		
BAI08.04 Evaluar y actualizar o retirar la información.			Reglas para la retirada de conocimiento	Interna
			Resultados de la evaluación de uso del conocimiento	Interna
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión de la información y el conocimiento	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	D. Enable—D.10. Information and Knowledge Management

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de uso del conocimiento sobre gobierno	Guiar la creación y el uso de los activos de conocimientos relacionados con el gobierno de I&T. Los activos de conocimientos de I&T deberían ser accesibles para su consulta.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Implantar una cultura de intercambio de conocimientos en la empresa. Comunicar proactivamente el valor de los conocimientos para fomentar la creación, uso, reutilización e intercambio de conocimientos. Fomentar el intercambio y transferencia del conocimiento mediante la identificación y aprovechamiento de factores motivadores.		

G. Componente: Servicios, infraestructura y aplicaciones	
<ul style="list-style-type: none"> Plataforma de colaboración Repositorio de conocimientos 	

Dominio: Construir, adquirir e implantar Objetivo de gestión: BAI09 – Gestionar los activos		Área prioritaria: Modelo Core de COBIT
Descripción		
Gestionar los activos de I&T a través de su ciclo de vida para asegurarse de que su uso aporta valor a un coste óptimo, continúan operativos (adecuados a su propósito), y se tienen en cuenta y están físicamente protegidos. Asegurar que aquellos activos que son críticos para soportar la capacidad del servicio son confiables y están disponibles. Gestionar las licencias de software para asegurarse de que se adquiere, retiene y despliega la cantidad óptima en relación con el uso que requiere el negocio, y que el software instalado cumpla con los acuerdos de licencia.		
Propósito		
Tener en cuenta todos los activos de I&T y optimizar el valor proporcionado por su uso.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales	➔	Metas de alineamiento
<ul style="list-style-type: none"> • EG04 Calidad de la información financiera • EG07 Calidad de la información de gestión • EG09 Optimización de costes de los procesos del negocio 		AG04 Calidad de la información financiera relacionada con la tecnología
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG04 a. Encuesta de satisfacción de las partes interesadas clave con respecto al nivel de transparencia, comprensión y precisión de la información financiera de la empresa b. Coste de incumplimiento con respecto a regulaciones financieras		AG04 a. Satisfacción de partes interesadas clave con respecto al nivel de transparencia, comprensión y precisión de la información financiera de I&T b. Porcentaje de servicios de I&T con costes operativos y beneficios esperados definidos y aprobados
EG07 a. Grado de satisfacción del consejo de administración y la dirección ejecutiva con la información para la toma de decisiones b. Número de incidentes causados por decisiones erróneas de negocio basadas en información imprecisa c. Tiempo que se tarda en proporcionar la información que respalde la toma de decisiones de negocio eficaces d. Oportunidad de la información de gestión		
EG09 a. Proporción de coste vs. niveles de servicio logrados b. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con los costos de procesamiento del negocio		

A. Componente: Proceso		
Práctica de gestión	Métricas modelo	
BAI09.01 Identificar y registrar los activos actuales. Mantener un registro actualizado y preciso de todos los activos de I&T requeridos para ofrecer servicios y que son propiedad o están controlados por la organización a la espera de un futuro beneficio (incluidos recursos con valor económico, como hardware o software). Asegurar el alineamiento con la gestión de configuración y la gestión financiera.	a. Porcentaje de activos registrados correctamente en el registro de activos b. Porcentaje de activos que son adecuados para su propósito c. Porcentaje de activos en inventario y actualizados	
Actividades	Nivel de capacidad	
1. Identificar todos los activos adquiridos en un registro de activos que recoja el estado actual. Los activos se reportan en la hoja del balance; se compran o crean para aumentar el valor de una compañía o beneficiar las operaciones de la empresa (p. ej. hardware y software). Identificar todos los activos adquiridos y mantener el alineamiento con los procesos de gestión de la configuración y gestión de cambios, el sistema de gestión de la configuración y los datos de contabilidad financiera.	2	
2. Identificar requisitos legales, regulatorios o contractuales que deban abordarse al gestionar el activo.		
3. Comprobar que los activos son adecuados para su propósito (es decir, que se puedan usar).		
4. Garantizar la contabilidad de todos los activos.	3	
5. Comprobar la existencia de todos los activos adquiridos mediante comprobaciones y conciliación regulares de inventario físico y lógico. Incluir el uso de herramientas de descubrimiento de software.	4	
6. Determinar regularmente si cada activo continúa proporcionando valor. De ser así, estimar la vida útil esperada durante la que proporcionará valor.		

A. Componente: Proceso (cont.)		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		RI.AD Asset Discovery & Identification
ISF, The Standard of Good Practice for Information Security 2016		BA1.1 Business Application Register
ISO/IEC 27002:2013/Cor.2:2015(E)		8.1 Responsibility for assets
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.13 Physical and environmental protection (PE-9)
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016		CSC 1: Inventory of Authorized and Unauthorized Devices; CSC 2: Inventory of Authorized and Unauthorized Software
Práctica de gestión		Métricas modelo
BAI09.02 Gestionar activos críticos. Identificar los activos que son críticos para garantizar la capacidad de prestación del servicio. Maximizar su confiabilidad y disponibilidad para apoyar las necesidades de negocio.		a. Número de activos críticos b. Promedio de inactividad por activo crítico c. Número de tendencias de incidentes identificadas
Actividades		Nivel de capacidad
1. Identificar activos que son críticos para proporcionar la capacidad de servicio mediante la referencia a los requisitos en las definiciones de servicio, los SLA y el sistema de gestión de la configuración.		2
2. Considerar regularmente el riesgo de fallo o la necesidad de sustitución de cada activo crítico.		
3. Comunicar a los clientes y usuarios afectados el impacto esperado (p. ej. restricciones de rendimiento) de las actividades de mantenimiento.		
4. Incorporar al calendario global de producción las suspensiones planificadas. Programar actividades de mantenimiento para minimizar el impacto adverso en los procesos de negocio.		3
5. Mantener la resiliencia de los activos críticos aplicando un mantenimiento preventivo regular. Monitorizar el rendimiento y, de ser necesario, proporcionar activos alternativos y/o adicionales para minimizar la probabilidad de fallo.		
6. Establecer un plan de mantenimiento preventivo para todo el hardware considerando un análisis de coste beneficio, las recomendaciones de los proveedores, el riesgo de suspensión del servicio, el personal calificado y otros factores relevantes.		
7. Establecer acuerdos de mantenimiento que incluyan el acceso de terceros a las instalaciones de I&T de la organización a fin de realizar actividades en el sitio (on-site) o fuera de él (off-site) (p. ej. outsourcing). Establecer contratos de servicio formales que contengan o hagan referencia a todas las condiciones de seguridad y privacidad necesarias, incluidos procedimientos de autorización de acceso, para garantizar el cumplimiento con las políticas y estándares de seguridad/privacidad de la organización.		
8. Garantizar que los servicios de acceso remoto y los perfiles de usuario (y otros medios usados para el mantenimiento y el diagnóstico) estén activos solo cuando sea necesario.		4
9. Monitorizar el rendimiento de los activos críticos mediante el examen de tendencias de los incidentes. Cuando sea necesario, realizar acciones de reparación o sustitución.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, abril de 2018		ID.AM Asset Management
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.13 Physical and environmental protection (PE-20)
Práctica de gestión		Métricas modelo
BAI09.03: Gestionar el ciclo de vida del activo. Gestionar los activos desde su adquisición hasta su disposición. Asegurar que los activos se usen con la mayor eficacia y eficiencia posible y se puedan contabilizar y proteger físicamente hasta su correcta retirada.		a. Porcentaje de activos gestionados desde la adquisición hasta su disposición b. Porcentaje de uso por activo c. Porcentaje de activos desplegados que siguen el ciclo de vida de implementación estándar

A. Componente: Proceso (cont.)		
Actividades		Nivel de capacidad
1. Proporcionar todos los activos conforme a las solicitudes aprobadas y las políticas y prácticas de adquisición de la empresa.		2
2. Obtener, recibir, verificar, probar y registrar todos los activos de forma controlada, incluyendo etiquetas físicas, cuando se requiera.		
3. Aprobar los pagos y completar el proceso con los proveedores, conforme a las condiciones del contrato acordadas.		
4. Implementar los activos siguiendo el ciclo de vida de implementación estándar, incluida la gestión de cambios y las pruebas de aceptación.		3
5. Asignar los activos a usuarios, con responsabilidades de aceptación y confirmación, como corresponda.		
6. Siempre que sea posible, reasignar los activos cuando ya no se necesiten debido a un cambio de rol del usuario, redundancia en un servicio o retirada de un servicio.		
7. Planificar, autorizar e implementar actividades relacionadas con la retirada, mientras se conservan los registros correspondientes para satisfacer las necesidades regulatorias y de negocio en curso.		
8. Disponer de los activos de forma segura, tras considerar, por ejemplo, el borrado permanente de los datos registrados en los dispositivos y el daño potencial al medio ambiente.		4
9. Disponer de los activos de forma responsable cuando ya no sean de utilidad debido a la retirada de todos los servicios relacionados, tecnología obsoleta o la falta de usuarios, teniendo en consideración el impacto medioambiental.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		DP.ML Manage Asset Lifecycle
ISF, The Standard of Good Practice for Information Security 2016		IM2.1 Document Management; PA1.1 Hardware Life Cycle Management
ITIL V3, 2011		Service Transition, 4.3 Service Asset and Configuration Management
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, abril de 2018		PR.MA Maintenance
Práctica de gestión		Métricas modelo
BAI09.04 Optimizar el valor de los activos. Revisar periódicamente la base de activos para identificar formas de optimizar valor y mantener el alineamiento con las necesidades del negocio.		a. Costes de benchmarks b. Número de activos no utilizados
Actividades		Nivel de capacidad
1. Revisar regularmente toda la base de activos, considerando si está alineada con las necesidades del negocio.		3
2. Evaluar los costes de mantenimiento, considerar si son razonables e identificar opciones de menor coste. Cuando sea necesario, incluir reemplazos con nuevas alternativas .		4
3. Revisar las garantías y considerar la relación calidad-precio y las estrategias de reemplazo para determinar las opciones de menor coste.		5
4. Usar estadísticas de capacidad y uso para identificar activos subutilizados o redundantes que podrían considerarse para su eliminación o sustitución a fin de reducir costes.		
5. Revisar la base completa para identificar oportunidades de estandarización, suministro único y otras estrategias que podrían reducir los costes de adquisición, soporte y mantenimiento.		
6. Revisar el estado general a fin de identificar oportunidades para aprovechar las tecnologías emergentes o estrategias de suministro alternativas para reducir costes o incrementar la relación calidad-precio.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
BAI09.05 Gestionar las licencias. Gestionar las licencias de software para mantener el número de licencias óptimo y respaldar las necesidades del negocio. Garantizar que el número de licencias en propiedad sea suficiente para cubrir el software instalado en uso.		a. Porcentaje de licencias utilizadas frente a licencias adquiridas b. Porcentaje de licencias que se siguen pagando pero que no se usan c. Porcentaje de productos y licencias que deberían actualizarse para lograr un mayor valor

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Mantener un registro de todas las licencias de software adquiridas y los acuerdos de licencias asociados.	2
2. Realizar regularmente una auditoría para identificar todas las instancias de software con licencia instaladas.	3
3. Comparar el número de licencias instaladas con el número de licencias adquiridas. Garantizar que el método de medición de cumplimiento de licencias sea conforme a los requisitos de la licencia y del contrato.	4
4. Cuando las instancias sean inferiores al número de licencias adquiridas, decidir si se deben conservar o poner fin a esas licencias, considerando los posibles ahorros en mantenimiento, capacitación y otros costes innecesarios.	
5. Cuando las instancias sean superiores al número de licencias adquiridas, considerar en primer lugar desinstalar las instancias que ya no se requieran o no estén justificadas y comprar entonces, de ser necesario, licencias adicionales para cumplir con el acuerdo de licencias.	
6. Considerar de forma regular si puede ser más rentable actualizar los productos y las licencias asociadas.	5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin documentación relacionada para esta práctica de gestión	

B. Componente: Estructuras organizativas											
Práctica clave de gestión		Director de TI	Director de tecnología	Jefe de arquitectura	Jefe de desarrollo	Jefe de operaciones de TI	Jefe de administración de TI	Gestor de servicios	Gestor de seguridad de la información		
	BAI09.01 Identificar y registrar los activos actuales.		A			R	R				
	BAI09.02 Gestionar activos críticos.		A	R	R	R	R		R		R
	BAI09.03: Gestionar el ciclo de vida del activo.		A			R	R	R			
	BAI09.04 Optimizar el valor de los activos.	A	R	R	R	R	R	R			
	BAI09.05 Gestionar las licencias.	A	R		R	R	R				
	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica								
Sin documentación relacionada para este componente.											

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
BAI09.01 Identificar y registrar los activos actuales.	De	Descripción	Descripción	A
	BAI03.04	Actualizaciones del inventario de activos	Resultados de revisiones de idoneidad	AP002.02
	BAI10.02	Repositorio de configuraciones	Registro de activos	AP006.01; BAI10.03
Resultados de comprobaciones de inventario físicas			BAI10.03; BAI10.04; DSS05.03	
BAI09.02 Gestionar activos críticos.			Comunicaciones de suspensiones por mantenimiento planificados	AP008.04
			Contratos de mantenimiento	Interna
BAI09.03: Gestionar el ciclo de vida del activo.			Retiradas autorizadas de activos	BAI10.03
			Registro actualizado de activos	BAI10.03
			Solicitudes aprobadas de adquisiciones de activos	Interna
BAI09.04 Optimizar el valor de los activos.			Oportunidades para reducir los costes o aumentar el valor de los activos	AP002.02
			Resultados de las revisiones de optimización de costes	AP002.02
BAI09.05 Gestionar las licencias.			Plan de acción para ajustar el número y asignaciones de licencias	AP002.05
			Registro de licencias de software	BAI10.02
			Resultados de las auditorías a las licencias instaladas	MEA03.03
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión de activos	Skills Framework for the Information Age V6, 2015	ASMG
Instalación/desmantelamiento de sistemas	Skills Framework for the Information Age V6, 2015	HSIN

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de gestión de activos	Proporciona directrices para la gestión del ciclo de vida de los activos, medidas de protección de activos, clasificación y propiedad de sistemas, propiedad de datos, y clasificación de datos.		
Política de propiedad intelectual (PI)	Aborda el riesgo relacionado con el uso, la propiedad, venta y distribución de las salidas de los esfuerzos creativos relacionados con I&T realizadas por empleados (p. ej. el desarrollo de software). Exigir la documentación adecuada, nivel de detalle, etc. desde el comienzo del trabajo.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Establecer una cultura que identifica, evalúa e informa sobre el valor económico y estratégico relativo a cada activo de la empresa de forma abierta, consistente y transparente.		

G. Componente: Servicios, infraestructura y aplicaciones	
Herramientas de gestión de activos	

Dominio: Construir, adquirir e implementar Objetivo de gestión: BAI10 – Gestionar la configuración		Área prioritaria: Modelo Core de COBIT
Descripción		
Definir y mantener descripciones y relaciones entre recursos claves y las capacidades necesarias para ofrecer servicios habilitados por I&T. Incluir la recopilación de información sobre la configuración, estableciendo líneas de referencia, verificando y auditando esta información, y actualizando el repositorio de configuración.		
Propósito		
Proporcionar información suficiente sobre los activos de servicio para facilitar que el servicio se gestione de forma eficiente. Evaluar el impacto de los cambios y hacer frente a los incidentes del servicio.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales	➔	Metas de alineamiento
<ul style="list-style-type: none"> • EG02 Gestión del riesgo de negocio • EG06 Continuidad y disponibilidad del servicio del negocio 		AG07 Seguridad de la información, infraestructura de procesamiento, aplicaciones y, privacidad
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG02 <ul style="list-style-type: none"> a. Porcentaje de objetivos y servicios críticos de negocio cubiertos por la evaluación de riesgos b. Proporción de incidentes significativos que no fueron identificados en la evaluación de riesgos frente al total de incidentes c. Frecuencia de actualización del perfil de riesgo 		AG07 <ul style="list-style-type: none"> a. Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o descrédito público b. Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o descrédito público c. Número de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o descrédito público
EG06 <ul style="list-style-type: none"> a. Número de interrupciones del servicio al cliente o procesos de negocio que han causado incidentes significativos b. Coste empresarial de incidentes c. Número de horas de procesamiento de negocio perdidas debido a interrupciones no planificadas del servicio d. Porcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados 		

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
BAI10.01 Establecer y mantener un modelo de configuración. Establecer y mantener un modelo lógico de servicios, activos, infraestructura, y registro de los elementos de configuración (CI), incluyendo las relaciones entre estos. Incluir los CIs que se consideran necesarios para gestionar los servicios eficazmente y, proporcionar una única descripción confiable de los activos en un servicio.		a. Número de partes interesadas que aprueban el modelo de configuración b. Porcentaje de precisión de las relaciones entre los elementos de configuración
Actividades		Nivel de capacidad
1. Definir y acordar el alcance y nivel de detalle sobre la gestión de la configuración (es decir, qué elementos configurables de servicios, activos e infraestructura incluir).		3
2. Establecer y mantener un modelo lógico para la gestión de la configuración, incluida la información de los tipos de CI, atributos, tipos de relaciones, atributos de relaciones y códigos de estado.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Data Management Maturity Model, 2014		Supporting Processes - Configuration Management
ISF, The Standard of Good Practice for Information Security 2016		SY1 System Configuration
ISO/IEC 20000-1:2011(E)		9.1 Configuration management
ITIL V3, 2011		Service Transition, 4.3 Service Asset and Configuration Management
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.5 Configuration management (CM-6)

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
BAI10.02 Establecer y mantener un repositorio de configuración y una línea de referencia. Establecer y mantener un repositorio de gestión de la configuración y crear líneas de referencias de configuración controladas.		a. Número de elementos de configuración (CI) listados en el repositorio b. Porcentaje de precisión sobre las líneas de referencia de la configuración de un servicio, aplicación o infraestructura
Actividades		Nivel de capacidad
1. Identificar y clasificar CIs y poblar el repositorio.		2
2. Crear, revisar y acordar formalmente las líneas de referencia de la configuración de un servicio, aplicación o infraestructura.		3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
CMMI Cybermaturity Platform, 2018	IP.CB Apply Configuration Baselines	
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018	3.4 Implementation (Task 2)	
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.19 System and service acquisition (SA-10)	
Práctica de gestión		Métricas modelo
BAI10.03 Mantener y controlar los elementos de configuración. Mantener un repositorio actualizado de los elementos de configuración (CIs) incluyendo cualquier cambio en la configuración.		a. Frecuencia de cambios/actualizaciones al repositorio b. Porcentaje de precisión e integridad del repositorio de CIs
Actividades		Nivel de capacidad
1. Identificar regularmente todos los cambios a los CIs.		2
2. Para asegurar la integridad y precisión, revisar los cambios propuestos a los CIs comparándolos con las líneas de referencia.		
3. Actualizar los detalles de configuración para los cambios de CI aprobados.		
4. Crear, revisar y acordar formalmente los cambios en las líneas de referencia de la configuración, cuando sea necesario.		3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.5 Configuration management (CM-2)	
Práctica de gestión		Métricas modelo
BAI10.04 Generar informes de estado y de la configuración. Definir y generar informes de la configuración sobre los cambios de estado en los elementos de la configuración.		a. Número de cambios no autorizados identificados b. Porcentaje de precisión en los cambios de estado de los CIs en comparación con las líneas de referencia
Actividades		Nivel de capacidad
1. Identificar los cambios de estado de los CIs y compararlos con las líneas de referencia.		2
2. Relacionar todos los cambios de configuración con las solicitudes de cambio aprobadas para identificar los cambios no autorizados. Informar sobre cambios no autorizados a los gestores de cambios.		3
3. Identificar los requisitos de reporte de todas las partes interesadas, incluyendo el contenido, la frecuencia y el medio. Producir informes conforme a los requisitos identificados.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.5 Configuration management (CM-3)	
Práctica de gestión		Métricas modelo
BAI10.05 Verificar y revisar la integridad del repositorio de configuración. Revisar periódicamente el repositorio de configuración y verificar su integridad y precisión en comparación con la meta deseada.		a. Número de desviaciones entre el repositorio de configuración y la configuración real b. Número de discrepancias en relación con la información de configuración incompleta o faltante

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Comprobar periódicamente los elementos de configuración reales con respecto al repositorio de configuración, mediante comparación de las configuraciones físicas y lógicas y el uso de herramientas de descubrimiento adecuadas, conforme sea necesario.	4
2. Comunicar y revisar todas las desviaciones de las correcciones o acciones aprobadas para remover cualquier activo no autorizado.	
3. Comprobar regularmente que todos los elementos de configuración físicos, conforme a lo definido en el repositorio, existen físicamente. Informar de cualquier desviación a la dirección.	
4. Establecer y revisar periódicamente el objetivo para completar el repositorio de configuración conforme con las necesidades del negocio.	
5. Comparar periódicamente el grado de integridad y precisión contra los objetivos y llevar a cabo acciones correctivas, conforme sea necesario, para mejorar la calidad de los datos del repositorio.	5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.5 Configuration management (CM-4)

B. Componente: Estructuras organizativas									
Práctica clave de gestión									
BAI10.01 Establecer y mantener un modelo de la configuración.									
BAI10.02 Establecer y mantener un repositorio de configuración y una línea de referencia.									
BAI10.03 Mantener y controlar los elementos de configuración.									
BAI10.04 Generar informes de estado y de la configuración.									
BAI10.05 Verificar y revisar la integridad del repositorio de configuración.									
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)					Referencia específica				
Sin documentación relacionada para este componente.									

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
BAI10.01 Establecer y mantener un modelo de configuración.	De	Descripción	Descripción	A
	BAI07.06	Plan de liberaciones	Modelo lógico de configuración	Interna
			Alcance del modelo de gestión de configuración	Interna
BAI10.02 Establecer y mantener un repositorio de la configuración y una línea de referencia.	BAI09.05	Registro de licencias de software	Configuración de línea de referencia	BAI03.11; BAI03.12
			Repositorio de configuraciones	BAI09.01; DSS02.01
BAI10.03 Mantener y controlar los elementos de configuración.	BAI06.03	Informes de estado sobre las solicitudes de cambio	Cambios aprobados a la línea de referencia	BAI03.11
	BAI09.01	• Registro de activos • Resultados de comprobaciones sobre el inventario físico	Repositorio actualizado con CIs	DSS02.01
	BAI09.03	• Registro actualizado de activos • Retiradas autorizadas de activos		
BAI10.04 Generar informes de estado y de la configuración.	BAI09.01	Resultados de comprobaciones sobre el inventario físico	Informes de estado de la configuración	BAI03.11; DSS02.01
BAI10.05 Verificar y revisar la integridad del repositorio de configuración.			Resultados de las revisiones de integridad del repositorio	Interna
			Resultados de la comprobación física de CIs	Interna
			Desviaciones en licencias	MEA03.03
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
National Institute of Standards and Technology Special Publication 800-37, Revisión 2, septiembre de 2017		3.4 Implementation (Task 2): Inputs and Outputs		

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión de la configuración	Skills Framework for the Information Age V6, 2015	CFMG

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de gestión de la configuración	Comunica las directrices para el establecimiento y uso de un repositorio de configuración completo, incluidos todos los componentes tecnológicos, definiciones de configuración asociadas e interdependencias con otros componentes tecnológicos. Ayuda a garantizar que los cambios en los sistemas y el software sean mínimamente disruptivos para los servicios. Garantiza que los cambios se coordinen entre los grupos correspondientes, para que no se produzcan conflictos o duplicación de esfuerzos.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Establece una cultura que apoya un enfoque estructurado de la gestión de la configuración entre los departamentos, en la que los usuarios reconocen el valor de una gestión de configuración estricta (p. ej. evitar conflictos de versiones o esfuerzos duplicados) y aplican las reglas y procedimientos establecidos.		
G. Componente: Servicios, infraestructura y aplicaciones		
Herramientas y repositorios para la gestión de la configuración		

Página dejada en blanco intencionadamente

Dominio: Construir, adquirir e implementar Objetivo de gestión: BAI11 – Gestionar los proyectos		Área prioritaria: Modelo Core de COBIT
Descripción		
Gestionar todos los proyectos que se inician en la empresa, alineados con la estrategia de la empresa y de forma coordinada, con base en una estrategia de gestión de proyectos estándar. Iniciar, planificar, controlar y ejecutar proyectos, y concluir con una revisión post-implementación.		
Propósito		
Lograr los resultados definidos en el proyecto y reducir el riesgo de retrasos inesperados, costes y erosión del valor mediante la mejora de las comunicaciones y la participación del negocio y de los usuarios finales. Garantizar el valor y la calidad de los entregables del proyecto y maximizar su contribución a los programas definidos y al portafolio de inversiones.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales		Metas de alineamiento
<ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG08 Optimización de la funcionalidad de los procesos internos del negocio • EG12 Gestión de programas de transformación digital 	➔	<ul style="list-style-type: none"> • AG03 Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T • AG06 Agilidad para convertir los requisitos del negocio en soluciones operativas • AG09 Ejecución de programas dentro del plazo, sin exceder el presupuesto y que cumplan con los requisitos y estándares de calidad
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 <ul style="list-style-type: none"> a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios 		AG03 <ul style="list-style-type: none"> a. Porcentaje de inversiones habilitadas por la I&T en las que los beneficios previstos en el caso de negocio se cumplen o exceden b. Porcentaje de servicios de I&T para los que se han logrado los beneficios esperados (indicados en los acuerdos de nivel de servicio)
EG08 <ul style="list-style-type: none"> a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarial b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro 		AG06 <ul style="list-style-type: none"> a. Nivel de satisfacción de los ejecutivos de negocios con la capacidad de respuesta de I&T a los nuevos requisitos b. Plazo de comercialización promedio para servicios y aplicaciones nuevos relacionados con I&T c. Tiempo promedio para convertir los objetivos estratégicos de I&T en iniciativas acordadas y aprobadas d. Número de procesos de negocio críticos apoyados por infraestructura y aplicaciones actualizadas
EG12 <ul style="list-style-type: none"> a. Número de programas ejecutados a tiempo y dentro del presupuesto b. Porcentaje de partes interesadas satisfechas con la ejecución del programa c. Porcentaje de programas de transformación del negocio suspendidos d. Porcentaje de programas de transformación del negocio con actualizaciones del estado notificados regularmente 		AG09 <ul style="list-style-type: none"> a. Número de programas/proyectos ejecutados a tiempo y dentro del presupuesto b. Número de programas que necesitan una revisión significativa debido a defectos de calidad c. Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
BAI11.01 Mantener un enfoque estándar en la gestión de proyectos. Mantener una estrategia estándar para la gestión de proyectos que permita la revisión del gobierno y gestión, la toma de decisiones y las actividades de gestión de entrega. Estas actividades deberían centrarse consistentemente en el valor y los objetivos del negocio (es decir, los requisitos, riesgo, costes, calendario y objetivos de calidad).		a. Porcentaje de proyectos exitosos conforme con la estrategia estándar definida b. Número de actualizaciones de la estrategia de gestión de proyectos, buenas prácticas, herramientas y plantillas
Actividades		Nivel de capacidad
1. Mantener y hacer cumplir una estrategia estándar de gestión de proyectos, alineada con el entorno específico de la empresa y con las buenas prácticas, conforme a procesos definidos y al uso de la tecnología correcta. Asegurar que la estrategia cubra todo el ciclo de vida y las disciplinas a seguir, incluida la gestión del alcance, recursos, riesgo, coste, calidad, tiempo, comunicación, involucramiento de las partes interesadas, adquisiciones, control de cambio, integración y obtención de beneficios.		2
2. Proporcionar una capacitación en gestión de proyectos adecuada y considerar la certificación para los gestores de proyecto.		
3. Establecer una oficina de gestión de proyectos (PMO) que mantenga una estrategia estándar para la gestión de programas y proyectos en toda la organización. La PMO respalda todos los proyectos mediante la creación y mantenimiento de plantillas de documentación de proyectos requeridos, proveyendo formación y buenas prácticas para los gestores de proyecto, seguimiento de las métricas sobre el uso de buenas prácticas para la gestión de proyectos, etc. En algunos casos, la PMO podría también informar sobre el progreso del proyecto a la alta dirección y/o las partes interesadas, ayudar a priorizar proyectos y asegurar el respaldo de todos los proyectos con los objetivos globales de negocio de la empresa.		3
4. Evaluar las lecciones aprendidas sobre el uso de la estrategia de gestión de proyectos. Actualizar las buenas prácticas, herramientas y plantillas, conforme sea necesario.		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.15 Program management (PM-2)
Práctica de gestión		Métricas modelo
BAI11.02 Establecer e iniciar un proyecto. Definir y documentar la naturaleza y alcance del proyecto con el objetivo de confirmar y desarrollar un entendimiento común del alcance del proyecto entre las partes interesadas. Los patrocinadores del proyecto deben aprobar formalmente la definición.		a. Porcentaje de partes interesadas que aprueban la necesidad empresarial, alcance, resultado previsto y nivel de riesgo del proyecto b. Porcentaje de proyectos en los que las partes interesadas reciben una clara declaración por escrito que define la naturaleza, alcance y beneficio del proyecto
Actividades		Nivel de capacidad
1. Crear un entendimiento común sobre el alcance del proyecto entre las partes interesadas, proporcionarles una clara declaración por escrito que defina la naturaleza, el alcance y los entregables de cada proyecto.		2
2. Garantizar que cada proyecto tenga uno o más patrocinadores con la autoridad suficiente para gestionar la ejecución del proyecto dentro del programa global.		
3. Asegurar que las partes interesadas y los patrocinadores de la empresa (empresa y TI) acuerden y acepten los requisitos del proyecto, incluidas las definiciones de los criterios de éxito del proyecto (aceptación) y los indicadores clave de rendimiento (KPI).		
4. Nombrar a un gestor dedicado para el proyecto. Asegurar que el individuo tenga los conocimientos tecnológicos y de negocio requeridos y, las competencias y habilidades proporcionales para gestionar el proyecto de forma eficaz y eficiente.		
5. Asegurar que la definición del proyecto describe los requisitos de un plan de comunicación del proyecto que identifique las comunicaciones internas y externas del proyecto.		
6. Con la aprobación de las partes interesadas, mantener la definición del proyecto a lo largo del mismo y reflejar el cambio de requisitos.		
7. Hacer un seguimiento de la ejecución del proyecto, establecer mecanismos como la elaboración regular de informes en cada fase, revisiones por fases o liberaciones, de forma oportuna y con la aprobación correspondiente.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
PMBOK guide Sixth edition, 2017		Part 1: 4.1 Develop project charter; Part 1: 6. Project schedule management

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
BAI11.03 Gestionar la participación de las partes interesadas. Gestionar la participación de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna que llegue a todas las partes interesadas relevantes. Esto incluye planificar, identificar e involucrar a las partes interesadas y gestionar sus expectativas.		a. Nivel de satisfacción de las partes interesadas con la participación b. Porcentaje de partes interesadas efectivamente involucradas
Actividades		Nivel de capacidad
1. Planificar cómo las partes interesadas dentro y fuera de la organización se identificarán, analizarán, involucrarán y gestionarán durante el ciclo de vida del proyecto.		3
2. Identificar, involucrar y gestionar a las partes interesadas estableciendo y manteniendo los niveles de coordinación, comunicación y relación adecuadas para garantizar que estén involucrados en el proyecto.		
3. Analizar los intereses, requisitos y compromiso de las partes interesadas. Implementar medidas correctivas si fuera necesario.		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
PMBOK guide Sixth edition, 2017		Part 1: 13. Project stakeholder management Part 1: 10. Project communications management
Práctica de gestión		Métricas modelo
BAI11.04 Desarrollar y mantener el plan del proyecto. Establecer y mantener un plan de proyecto formal, integrado y aprobado (que cubra los recursos del negocio y de TI) para guiar la ejecución y el control del proyecto durante su ciclo de vida. El alcance de los proyectos debe definirse claramente y vincularse al desarrollo o mejora de las capacidades del negocio.		a. Porcentaje de proyectos activos llevados a cabo sin mapas de valor del proyecto válidas y actualizadas b. Porcentaje de hitos o tareas terminadas vs. el plan
Actividades		Nivel de capacidad
1. Desarrollar un plan de proyecto que proporcione información para permitir a la dirección controlar su progreso de forma progresiva. El plan debería incluir detalles de los entregables y los criterios de aceptación del proyecto, recursos y responsabilidades internos y externos requeridos, estructuras de división del trabajo y paquetes de trabajo claros, estimaciones sobre los recursos requeridos, plan / fases de hitos/liberaciones, dependencias clave, presupuesto y costes e identificación de una ruta crítica.		2
2. Mantener el plan del proyecto y los planes dependientes (p. ej., plan de riesgos, plan de calidad, plan de obtención de beneficios). Asegurar que los planes estén actualizados y reflejen el progreso actual y los cambios materiales aprobados.		
3. Asegurar que haya una comunicación efectiva de los planes del proyecto e informes de progresos. Asegurar que todos los cambios realizados a los planes individuales se reflejen en otros planes.		
4. Determinar las actividades, interdependencias y colaboración y comunicación requeridas en el proyecto y entre los múltiples proyectos de un programa.		
5. Asegurar que cada hito esté acompañado de un entregable significativo que requiere su revisión y confirmación.		
6. Establecer una línea de referencia del proyecto (p. ej. coste, calendario, alcance, calidad) que se revise, apruebe e incorpore adecuadamente al plan integrado del proyecto.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
PMBOK guide Sixth edition, 2017		Part 1: 4.2 Develop project management plan
Práctica de gestión		Métricas modelo
BAI11.05 Gestionar la calidad del proyecto. Preparar y ejecutar un plan de gestión de la calidad, procesos y prácticas, alineadas con el sistema de gestión de calidad (SGC). Describir el enfoque de calidad del proyecto y cómo se implementará. El plan debería evaluarse y aceptarse formalmente por todas las partes afectadas e incorporarse al plan integrado del proyecto.		a. Porcentaje de construcción de productos sin errores b. Número de proyectos cancelados

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Para proporcionar el aseguramiento de la calidad de los entregables del proyecto, identificar la propiedad y las responsabilidades, procesos de revisión de la calidad, criterios de éxito y métricas de rendimiento.	2
2. Identificar las tareas y prácticas de aseguramiento requeridas para respaldar la acreditación de sistemas nuevos o modificados durante la planificación del proyecto. Incluirlos en los planes integrados. Asegurar que las tareas garantizan que los controles internos y, las soluciones de seguridad y privacidad satisfacen los requisitos definidos.	3
3. Definir los requisitos para la validación y verificación independiente de la calidad de los entregables en el plan.	
4. Realizar actividades de aseguramiento y control de calidad conforme al plan de gestión de calidad y el SGC.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
PMBOK guide Sixth edition, 2017	Part 1: 8. Project quality management
Práctica de gestión	Métricas modelo
BAI11.06 Gestionar el riesgo del proyecto. Eliminar o minimizar el riesgo específico asociado a los proyectos mediante un proceso sistemático de planificación, identificación, análisis, respuesta, monitorización y control de las áreas o eventos que, potencialmente, pueden ocasionar un cambio no deseado. Definir y registrar cualquier riesgo al que se enfrenta la gestión del proyecto.	a. Número de retrasos y problemas identificados b. Número de proyectos con una gestión formal del riesgo alineada con el marco de gestión de riesgos empresariales (ERM, siglas en inglés).
Actividades	Nivel de capacidad
1. Establecer una estrategia formal de gestión de riesgos de proyectos alineada con el marco de gestión de riesgos empresariales (ERM). Asegurar que la estrategia incluya la identificación, análisis, respuesta, mitigación, monitorización y control del riesgo.	2
2. Asignar a personal adecuadamente calificado la responsabilidad de ejecutar el proceso de gestión de riesgos de proyectos de la empresa dentro de un proyecto y asegurar que esto se incorpore en las prácticas de desarrollo de soluciones. Considerar asignar este rol a un equipo independiente, sobre todo si se requiere un punto de vista objetivo o si un proyecto se considera crítico.	3
3. Identificar los dueños de las acciones para evitar, aceptar o mitigar el riesgo.	
4. Realizar la evaluación de riesgos del proyecto, identificando y cuantificando el riesgo continuamente durante todo el proyecto. Gestionar y comunicar el riesgo de forma adecuada dentro de la estructura de gobierno del proyecto.	
5. Reevaluar el riesgo del proyecto periódicamente, incluyendo un inicio a cada fase del proyecto principal como parte de evaluaciones de solicitudes de cambio mayores	
6. Mantener y revisar el registro de riesgos del proyecto, de todos los riesgos potenciales del proyecto y un registro de mitigación de riesgo de todos los problemas presentados y su resolución. Analizar periódicamente el log para ver las tendencias y problemas recurrentes con la finalidad de garantizar que se corrigen las causas raíz.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.15 Program management (PM-4)
PMBOK guide Sixth edition, 2017	Part 1: 11. Project risk management
Práctica de gestión	Métricas modelo
BAI11.07 Supervisar y controlar los proyectos. Medir el rendimiento del proyecto en comparación con los criterios clave, como son el calendario, la calidad, los costes y el riesgo. Identificar cualquier desviación de los objetivos esperados. Evaluar el impacto de las desviaciones en el proyecto y en el programa general e informar los resultados a las partes interesadas.	a. Porcentaje de actividades alineadas con el alcance y los resultados esperados b. Porcentaje de desviaciones del plan abordadas c. Frecuencia de revisiones del estado del proyecto

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Establecer y usar una serie de criterios de proyecto incluidos, pero no limitados a, el alcance, beneficio esperado para el negocio, calendario, calidad, coste y nivel de riesgo.	2
2. Informar a las partes interesadas identificadas clave acerca del progreso del proyecto, desviaciones con respecto a los criterios clave de rendimiento del proyecto establecidos (como, pero no limitado a, los beneficios empresariales esperados), y posibles efectos positivos y negativos en el proyecto.	
3. Documentar y enviar los cambios necesarios a las partes interesadas clave del proyecto para su aprobación antes de su adopción. Comunicar los criterios revisados a los gestores de proyecto para su uso en futuros informes de rendimiento.	
4. Para los entregables producidos en cada iteración, entrega o fase del proyecto, obtener aprobación y conformidad de los gestores y usuarios designados en las funciones de negocio y de TI afectadas.	
5. Basar el proceso de aprobación en criterios de aceptación definidos, acordados con las partes interesadas clave antes del comienzo de la fase del proyecto o iteración entregable.	3
6. Evaluar el proyecto en las fases, liberaciones o iteraciones mayores acordadas. Establecer decisiones formales de seguir o no seguir adelante conforme a los criterios críticos de éxito predeterminados.	
7. Establecer y activar un sistema de control de cambio para el proyecto con la finalidad de que todos los cambios de la línea de referencia del proyecto (p. ej. alcance, beneficios de negocio esperados, calendario, calidad, coste, nivel de riesgo) se revisen, aprueben e incorporen en el plan integrado del proyecto en línea con el marco de gobierno de proyectos y programas.	
8. Medir el rendimiento de los proyectos con respecto a los criterios clave de rendimiento del proyecto. Analizar las desviaciones causadas con respecto a los criterios clave de rendimiento del proyecto y evaluar los efectos positivos y negativos en el proyecto.	4
9. Supervisar los cambios en el proyecto y revisar los criterios clave de rendimiento del proyecto para determinar si siguen representando medidas de progreso válidas.	
10. Recomendar y supervisar medidas correctivas, cuando sea necesario, conforme al marco de gobierno del proyecto.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
PMBOK guide Sixth edition, 2017	Part 1: 4.5 Monitor and control project work
Práctica de gestión	Métricas modelo
BAI11.08 Gestionar los recursos del proyecto y los paquetes de trabajo. Gestionar los paquetes de trabajos asociados al proyecto mediante el establecimiento de requisitos formales para autorizarlos y aceptarlos y, asignar y coordinar los recursos de negocio y de TI apropiados.	a. Número de problemas de recursos (p. ej., habilidades, capacidad) b. Número de roles, responsabilidades y prerrogativas del gestor del proyecto, personal asignado y otras partes involucradas, claramente definidas
Actividades	Nivel de capacidad
1. Identificar las necesidades de recursos del negocio y de TI para el proyecto y asignar roles y responsabilidades adecuados, con escalamiento, y autoridad para la toma de decisiones acordadas y comprendidas.	2
2. Identificar las habilidades y tiempo requeridos por todos los individuos involucrados en las fases del proyecto con relación a los roles definidos. Asignar personal a los roles conforme a la información de habilidades disponibles (p. ej., matriz de habilidades de TI).	
3. Utilizar una gestión de proyectos experta y los recursos de líderes de equipo con las habilidades apropiadas al tamaño, complejidad y riesgo del proyecto.	
4. Considerar y definir claramente los roles y responsabilidades de otras partes involucradas, incluyendo finanzas, legal, adquisiciones, recursos humanos, auditoría interna y cumplimiento.	
5. Definir y acordar claramente la responsabilidad de la adquisición y gestión de productos y servicios de terceros y, gestionar la relación.	
6. Identificar y autorizar la ejecución del trabajo conforme al plan del proyecto.	
7. Identificar las brechas del plan del proyecto y proporcionar retroalimentación al gestor de proyectos para que las corrija.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
PMBOK guide Sixth edition, 2017	Part 1: 4.3 Direct and manage project work

A. Componente: Proceso (cont.)	
Práctica de gestión	Ejemplo de métricas
BAI11.09 Cerrar un proyecto o iteración. Al final de cada proyecto, liberación o iteración, requerir a las partes interesadas del proyecto para que determinen si el mismo ha dado los resultados previstos en cuanto a las capacidades y ha contribuido como se esperaba a los beneficios del programa. Identificar y comunicar las actividades pendientes necesarias para lograr los resultados planeados del proyecto y/o los beneficios del programa. Identificar y documentar las lecciones aprendidas para futuros proyectos, liberaciones iteraciones y programas.	a. Nivel de satisfacción de las partes interesadas expresado en la revisión de cierre del proyecto b. Porcentaje de resultados con aceptación en primera instancia
Actividades	Nivel de capacidad
1. Obtener la aceptación de las partes interesadas para los entregables del proyecto y transferir la propiedad.	2
2. Definir y aplicar los pasos claves para el cierre del proyecto, incluidas las revisiones post-implementación que evalúan si un proyecto ha alcanzado los resultados deseados.	3
3. Planificar y ejecutar revisiones post-implementación para determinar si los proyectos ofrecen los resultados esperados. Mejorar la gestión del proyecto y la metodología de procesos de desarrollo de sistemas.	
4. Identificar, asignar, comunicar y hacer un seguimiento a cualquier actividad incompleta requerida para garantizar que el proyecto ofrezca los resultados requeridos en términos de capacidades y, que los resultados contribuyen como se esperaba a los beneficios del programa.	
5. De forma regular, y al finalizar el proyecto, recopilar las lecciones aprendidas de los participantes del proyecto. Revisarlas junto con las actividades clave que llevaron a obtener beneficios y valor. Analizar los datos y realizar recomendaciones para mejorar el proyecto actual y el método de gestión de proyectos para proyectos futuros.	4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
PMBOK guide Sixth edition, 2017	Part 1: 4.7 Close project or phase

B. Componente: Estructuras organizativas										
Práctica clave de gestión	Director general ejecutivo	Director de riesgos	Director de TI	Director de tecnología	Dueños del proceso de negocio	Comité Estratégico (Programas/Proyectos)	Gestor de programas	Gestor de proyecto	Oficina de gestión de proyectos	Jefe de desarrollo
BAI11.01 Mantener un enfoque estándar en la gestión de proyectos.	A		R				R	R		
BAI11.02 Establecer e iniciar un proyecto.		R		R	R	A	R	R	R	
BAI11.03 Gestionar la participación de las partes interesadas.			R			A	R			
BAI11.04 Desarrollar y mantener el plan del proyecto.						A	R	R		
BAI11.05 Gestionar la calidad del proyecto.		R	R			A	R			R
BAI11.06 Gestionar el riesgo del proyecto.			R			A	R			R
BAI11.07 Supervisar y controlar los proyectos.					R	A	R	R	R	
BAI11.08 Gestionar los recursos del proyecto y los paquetes de trabajo.					R	A	R		R	R
BAI11.09 Cerrar un proyecto o iteración.						A	R	R		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica									
PMBOK guide Sixth edition, 2017	Part 1: 3. The role of the project manager									

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
BAI11.01 Mantener un enfoque estándar en la gestión de proyectos.	AP003.04	<ul style="list-style-type: none"> Requisitos de la arquitectura de gobierno Descripciones de la fase de implementación 	Enfoques de gestión de proyectos actualizados	Interna
	AP010.04	Riesgo identificado en las prestaciones de los proveedores		
	EDM02.03	Requisitos de las revisiones por fases		
	EDM02.04	Acciones para mejorar la entrega de valor		
BAI11.02 Establecer e iniciar un proyecto.			Definiciones del proyecto	Interna
			Declaraciones del alcance del proyecto	Interna
BAI11.03 Gestionar la participación de las partes interesadas.			Resultados de evaluaciones de eficacia sobre la participación de las partes interesadas	Interna
			Plan de participación de las partes interesadas	Interna
BAI11.04 Desarrollar y mantener el plan del proyecto.	BAI07.03	Plan de prueba de aceptación aprobado	Comunicaciones e informes del proyecto	Interna
			Línea de referencia de proyectos	Interna
			Planes de proyectos	Interna
BAI11.05 Gestionar la calidad del proyecto.	AP011.01	Planes de gestión de la calidad	Plan de gestión de la calidad del proyecto	BAI02.04; BAI03.06; BAI07.01
	AP011.02	Requisitos del cliente para la gestión de la calidad	Requisitos para la verificación independiente de entregables del proyecto	BAI07.03
BAI11.06 Gestionar el riesgo del proyecto.	AP012.02	Resultados del análisis de riesgo	Registro de riesgo del proyecto	Interna
	BAI02.03	<ul style="list-style-type: none"> Registro de los riesgos de los requisitos Acciones para la mitigación de riesgos 	Resultados sobre la evaluación de riesgos de proyectos	Interna
	Fuera de COBIT	Marco de gestión de riesgos empresariales (ERM)	Plan de gestión de riesgos del proyecto	Interna
BAI11.07 Supervisar y controlar los proyectos.			Cambios acordados al proyecto	Interna
			Informes de progreso del proyecto	Interna
			Criterios del desempeño del proyecto	Interna
BAI11.08 Gestionar los recursos del proyecto y los paquetes de trabajo.			Requisitos de recursos de proyectos	AP007.05; AP007.06
			Brechas en la planificación del proyecto	Interna
			Roles y responsabilidades del proyecto	Interna

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
BAI11.09 Cerrar un proyecto o iteración.	De	Descripción	Descripción	A
	BAI07.08	• Informe de revisión post-implementación • Plan de medidas correctivas	Resultados de la revisión post-implementación	AP002.04
			Confirmaciones de las partes interesadas sobre la aceptación del proyecto	Interna
			Lecciones aprendidas del proyecto	Interna
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
PMBOK guide Sixth edition, 2017		Part 1: 4. Project integration management: Inputs and Outputs; Part 1: 6. Project schedule management: Inputs and Outputs; Part 1: 10. Project communications management: Inputs & Outputs; Part 1: 11. Project risk management: Inputs and Outputs		

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Soporte para el portafolio, programas y proyectos	Skills Framework for the Information Age V6, 2015	PROF
Gestión de proyectos y portafolio	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.2. Project and Portfolio Management
Gestión de proyectos	Skills Framework for the Information Age V6, 2015	PRMG

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de gestión del programa/proyecto	Guías sobre la gestión de riesgos relacionados con programas y proyectos Detalle sobre la postura y expectativa de la dirección en relación a la gestión de programas y proyectos. Tratar la rendición de cuentas, metas y objetivos relacionados con el rendimiento, presupuesto y análisis de riesgo, reportes y mitigación de eventos adversos durante la ejecución del programa/proyecto.	PMBOK guide Sixth edition, 2017	Part 1: 2.3.1 Processes, policies and procedures


F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Establecer una cultura de gestión de proyectos en toda la empresa que garantice su implementación consistente y óptima, tomando en consideración la estructura organizativa y el entorno empresarial. Asegurar que todas las iniciativas se trasladen a proyectos (o cambios, cuando sean menores en el alcance); garantizar que no se realicen acciones ad hoc fuera del alcance de la gestión de proyectos.		

G. Componente: Servicios, infraestructura y aplicaciones
Herramientas de gestión de proyectos

4.4 ENTREGAR, DAR SERVICIO Y SOPORTE (DSS)

- 01 Gestionar las operaciones
- 02 Gestionar las peticiones y los incidentes del servicio
- 03 Gestionar los problemas
- 04 Gestionar la continuidad
- 05 Gestionar los servicios de seguridad
- 06 Gestionar los controles de los procesos de negocio

Página dejada en blanco intencionadamente

Dominio: Entregar, dar servicio y soporte		Área prioritaria: Modelo Core de COBIT	
Objetivo de gestión: DSS01 - Gestionar las operaciones			
Descripción			
Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar los servicios de I&T, internos y externalizados. Incluir la ejecución de procedimientos de operación estándar predefinidos y las actividades de supervisión requeridas.			
Propósito			
Proporcionar los resultados de los productos y servicios operativos de I&T según lo planeado.			
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:			
Metas empresariales			Metas de alineamiento
<ul style="list-style-type: none">• EG01 Portafolio de productos y servicios competitivos• EG08 Optimización de la funcionalidad de procesos del negocio internos			AG05 Prestación de servicios de I&T conforme a los requisitos del negocio
Métricas modelo para metas empresariales			Métricas modelo para metas de alineamiento
EG01 <ul style="list-style-type: none">a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercadob. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del clientec. Porcentaje de productos y servicios que proporcionan una ventaja competitivad. Plazo de comercialización para nuevos productos y servicios			AG05 <ul style="list-style-type: none">a. Porcentaje de partes interesadas del negocio satisfechas con la prestación de servicios de I&T que cumple con los niveles de servicio acordadosb. Número de interrupciones del negocio debido a incidentes de servicios de I&Tc. Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de I&T
EG08 <ul style="list-style-type: none">a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarialb. Niveles de satisfacción de los clientes con las capacidades de prestación de serviciosc. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro			

A. Componente: Proceso			
Práctica de gestión		Métricas modelo	
DSS01.01 Ejecutar procedimientos operativos.		<ul style="list-style-type: none"> a. Número de incidentes causados por problemas operativos b. Número de procedimientos operativos no estándar ejecutados 	
Actividades			Nivel de capacidad
1. Desarrollar y mantener los procedimientos operativos y las actividades relacionadas para respaldar todos los servicios prestados.			2
2. Mantener un calendario de las actividades operativas y ejecutar las actividades.			
3. Comprobar que todos los datos esperados para su procesamiento se reciban y procesen de forma completa, precisa y en el plazo debido. Entregar el producto conforme a los requisitos de la empresa. Soportar las necesidades de reinicios y reprocesamientos. Asegurar que los usuarios reciban los productos adecuados de forma segura y en el plazo debido.			3
4. Gestionar el rendimiento y throughput de las actividades programadas.			4
5. Monitorizar los incidentes y problemas relacionados con los procedimientos operativos y realizar las acciones adecuadas para mejorar la confiabilidad de las tareas operativas ejecutadas.			5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
CMMI Cybermaturity Platform, 2018		TPSE Safeguard Operational Environment	
HITRUST CSF versión 9, septiembre de 2017		09.01 Document Operating Procedures	
ISO/IEC 27002:2013/Cor.2:2015(E)		12.1 Operational procedures and responsibilities	
ITIL V3, 2011		Service Operation, 4.1 Event Management	
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.13 Physical and environmental protection (PE-13, PE-14, PE-15)	

A. Componente: Proceso (cont.)			
Práctica de gestión		Ejemplo de métricas	
DSS01.02 Gestionar servicios tercerizados de I&T. Gestionar la operación de los servicios tercerizados de I&T para mantener la protección de la información empresarial y la confiabilidad de la provisión del servicio.		a. Número de KPI específicos/SMART incluidos en los contratos de externalización b. Frecuencia de falla del socio subcontratista para cumplir con los KPI	
Actividades			Nivel de capacidad
1. Asegurar que los requisitos de los procesos de seguridad de la información de la empresa cumplan con los contratos y SLA de hosting de terceros o proveedores de servicios.			3
2. Asegurar que los requisitos de procesamiento operacional del negocio y de TI de la empresa y las prioridades para la prestación de servicios cumplan con los contratos y SLA de hosting de terceros o proveedores de servicios.			
3. Integrar los procesos de gestión de TI internos críticos con los de los proveedores de servicios externalizados. Esto debería cubrir, por ejemplo, la planificación de rendimiento y capacidad, gestión del cambio, gestión de la configuración, solicitud de servicios y gestión de incidentes, gestión de problemas, gestión de la seguridad, continuidad del negocio y monitorización del rendimiento y reporte del proceso.			
4. Planificar una auditoría independiente y el aseguramiento de los entornos operacionales de proveedores que proporcionen servicios externalizados para confirmar que se han abordado de forma adecuada los requisitos acordados.			4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
ISF, The Standard of Good Practice for Information Security 2016		SC1.2 Outsourcing	
ISO/IEC 20000-1:2011(E)		4.2 Governance of processes operated by other parties	
Práctica de gestión		Métricas modelo	
DSS01.03 Monitorizar la infraestructura de I&T. Monitorizar la infraestructura de I&T y eventos relacionados. Almacenar suficiente información cronológica en los logs de operación que permita la reconstrucción y revisión de las secuencias temporales de las operaciones y otras actividades asociadas o que apoyan las operaciones.		a. Porcentaje de tipos de eventos operativos críticos cubiertos por sistemas de detección automática b. Porcentaje de activos de infraestructura monitorizados conforme a la criticidad del servicio y la relación entre los elementos de configuración y servicios que dependen de ellos	
Actividades			Nivel de capacidad
1. Registrar los eventos. Identificar el nivel de información que debe registrarse, conforme a una consideración de riesgo y rendimiento.			2
2. Identificar y mantener una lista de activos de infraestructura que deben monitorizarse conforme a la criticidad del servicio y la relación entre los elementos de configuración y servicios que dependen de ellos			3
3. Definir e implementar reglas que identifiquen y registren incumplimientos de umbrales y los estados de eventos. Encontrar un equilibrio entre la generación de eventos menores insignificantes y eventos significativos para que los registros de eventos no estén sobrecargados de información innecesaria.			
4. Producir registros de eventos y conservarlos durante un periodo de tiempo adecuado para que ayuden en futuras investigaciones.			
5. Garantizar que se creen tickets de incidentes en el plazo debido a la hora de monitorizar desviaciones identificadas en los umbrales definidos.			4
6. Establecer procedimientos para monitorizar los registros de eventos. Llevar a cabo revisiones regulares.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.10 Maintenance (MA-2, MA-3)	
Práctica de gestión		Métricas modelo	
DSS01.04 Gestionar el medioambiente. Mantener medidas de protección contra los factores medioambientales. Instalar equipos y dispositivos especializados para monitorizar y controlar el ambiente.		a. Número de personas capacitadas para responder a los procedimientos de alarma medioambiental b. Número de escenarios de riesgo definidos para las amenazas medioambientales	

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Identificar los desastres naturales y causados por el hombre que podrían ocurrir en el área en la que se encuentran las instalaciones de TI. Evaluar el efecto potencial en las instalaciones de TI.	2
2. Identificar cómo el equipo de I&T, incluido el equipo móvil y el off-site, se protege de las amenazas medioambientales. Asegurar que la política limita o excluye el consumo de comida, bebida y fumar en áreas sensibles, y prohibir el almacenamiento de artículos de papelería y otros suministros que suponen un peligro de incendio en las salas de ordenadores.	
3. Mantener los centros de TI y salas de servidores limpios y seguros en todo momento (es decir, sin desorden, papel, cajas de cartón, papeleras llenas, productos químicos o materiales inflamables).	
4. Situar y construir las instalaciones de TI para minimizar y mitigar la susceptibilidad a las amenazas medioambientales (p. ej., robo, aire, incendio, humo, agua, vibración, terrorismo, vandalismo, químicos, explosivos). Considerar zonas de seguridad y/o células ignífugas específicas (p. ej., ubicar los entornos/servidores de producción y desarrollo apartado uno del otro).	3
5. Comparar las medidas y planes de contingencia con los requisitos de las políticas de seguros y los resultados del informe. Abordar los puntos de incumplimiento en el plazo debido.	
6. Responder a las alarmas medioambientales y a otras notificaciones. Documentar y probar los procedimientos, lo cual debería incluir la priorización de alarmas y contacto con las autoridades de respuesta a emergencia locales. Capacitar al personal en estos procedimientos.	
7. Monitorizar y mantener regularmente dispositivos que detecten proactivamente amenazas medioambientales (p. ej., fuego, agua, humo, humedad).	4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018	2.1 System and system elements; 3.2 Categorization (Task 5, 6)
Práctica de gestión	Métricas modelo
DSS01.05 Gestionar las instalaciones. Gestionar las instalaciones, incluidos los equipos de suministro eléctrico y comunicaciones, alineados con las leyes y reglamentos existentes, los requisitos técnicos y del negocio, las especificaciones del proveedor, y las directrices de salud y seguridad.	a. Tiempo transcurrido desde la última prueba del suministro de energía ininterrumpida b. Número de personas formadas en normas de salud y seguridad
Actividades	Nivel de capacidad
1. Examinar los requisitos de protección de las instalaciones de TI con respecto a las fluctuaciones y cortes eléctricos, junto con otros requisitos de planificación de continuidad del negocio. Procurar un equipo de suministro ininterrumpido adecuado (p. ej., baterías, generadores) para respaldar la planificación de continuación del negocio.	2
2. Probar regularmente los mecanismos de suministro eléctrico ininterrumpidos. Asegurar que la electricidad pueda cambiar a otra fuente de alimentación sin ningún efecto significativo en las operaciones del negocio.	
3. Asegurar que las instalaciones que acogen los sistemas de I&T cuenten con más de una fuente para las utilidades de servicios dependientes (p. ej., electricidad, telecomunicaciones, agua, gas). Separar la entrada física de cada utilidad de servicio.	
4. Confirmar que el cableado exterior de la instalación de TI se sitúe bajo tierra o tenga una protección alternativa adecuada. Determinar que el cableado de la instalación de TI se encuentre en conductos seguros, y el acceso a armarios de cableado esté restringido a personal autorizado. Proteger el cableado adecuadamente frente al daño causado por el fuego, el humo, el agua, la intercepción y la interferencia.	
5. Asegurar que el cableado y los parches de cableado físico (datos y teléfono) estén estructurados y organizados. Las estructuras de cableado y conducción deberían estar documentadas (p. ej., diagramas de cableado y planos de construcción).	
6. Educar al personal de forma regular sobre la legislación, las regulaciones y directrices en salud y seguridad relevantes. Educar al personal sobre simulacros de incendio y rescate para garantizar el conocimiento y las acciones tomadas en caso de fuego o incidentes similares.	
7. Asegurar que las instalaciones y el equipo de TI se mantengan conforme a los intervalos y especificaciones de servicio recomendados por el proveedor. Asegurar que el mantenimiento se realice solo por personal autorizado.	3
8. Analizar los sistemas de alojamiento de alta disponibilidad de las instalaciones para comprobar redundancia y requisitos de cableado a prueba de fallos (externo e interno).	
9. Asegurar que las instalaciones de TI cumplen con la legislación, regulaciones y, directrices de salud y seguridad y, las especificaciones de proveedores relevantes.	
10. Registrar, monitorizar, gestionar y resolver incidentes en las instalaciones en línea con el proceso de gestión de incidentes de I&T. Poner a disposición informes sobre incidentes en las instalaciones que la legislación y las regulaciones obligan a hacer públicos.	4
11. Analizar las alteraciones físicas de las instalaciones de TI para reevaluar el riesgo medioambiental (p. ej., daño por fuego o agua). Informar los resultados de este análisis a la dirección de instalaciones y continuidad del negocio.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin documentación relacionada para esta práctica de gestión	

B. Componente: Estructuras organizativas							
Práctica clave de gestión	Director de operaciones						
	Director de TI						
	Director de tecnología						
	Jefe de operaciones de TI						
	Gestor de seguridad de la información						
	Director de privacidad						
DSS01.01 Ejecutar procedimientos operativos.	R	A	R	R			
DSS01.02 Gestionar servicios tercerizados de I&T.		A	R	R	R	R	
DSS01.03 Monitorizar la infraestructura de I&T		R	A	R	R		
DSS01.04 Gestionar el medioambiente.		R	A	R	R		
DSS01.05 Gestionar las instalaciones.		R	A	R	R		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica						
Sin Documentación relacionada para este componente.							

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
DSS01.01 Ejecutar procedimientos operativos.	De	Descripción	Descripción	A
	BAI05.05	Plan de operación y uso	Registro de copias de seguridad	Interna
			Calendario operativo	Interna
DSS01.02 Gestionar servicios tercerizados de I&T.	AP009.03	• SLA • OLA	Planes independientes de aseguramiento	MEA04.02
	BAI05.05	Plan de operación y uso		
DSS01.03 Monitorizar la infraestructura de I&T.	BAI03.11	Definiciones de servicios	Reglas de monitorización de activos y estados de eventos	DSS02.01; DSS02.02
			Tickets de incidentes	DSS02.02
			Logs de eventos	Interna
DSS01.04 Gestionar el medioambiente.			Políticas medioambientales.	AP001.09
			Informes de políticas de seguros	MEA03.03
DSS01.05 Gestionar las instalaciones.			Concienciación de salud y seguridad	Interna
			Informes de evaluación de instalaciones	MEA01.03
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
National Institute of Standards and Technology Special Publication 800-37, Revisión 2, septiembre de 2017		3.2 Categorization (Task 5, 6): Inputs and Outputs		

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Detailed Reference
Administración de bases de datos	Skills Framework for the Information Age V6, 2015	DBAD
Gestión de instalaciones	Skills Framework for the Information Age V6, 2015	DCMA
Infraestructura de TI	Skills Framework for the Information Age V6, 2015	ITOP
Métodos y herramientas	Skills Framework for the Information Age V6, 2015	METL
Prestación de servicios	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	C. Run—C.3. Service Delivery
Gestión de almacenamiento	Skills Framework for the Information Age V6, 2015	STMG

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de gestión de servicios	Proporciona dirección y directrices para garantizar la gestión e implementación efectiva de todos los servicios de I&T para satisfacer los requisitos del negocio y del cliente, dentro de un marco de mediciones del rendimiento. Cubre la gestión de riesgos relacionado con los servicios de I&T. (El marco ITIL V3 ofrece directrices detalladas para la gestión de servicios y la optimización del riesgo relacionada con los servicios.)	(1) ISO/IEC 20000-1:2011(E); (2) ITIL V3, 2011	(1) 4.1.2 Service management policy; (2) Service Strategy, 3. Service strategy principles

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Crear una cultura habitual de excelencia en toda la organización. Animar a los empleados a sobresalir. Crear un entorno en el que los procedimientos operativos ofrezcan (más que) los servicios necesarios mientras que permitan a los empleados cuestionar el statu quo y probar nuevas ideas. Gestionar la excelencia operativa a través del compromiso de los empleados y la mejora continua. Aplicar el enfoque centrado en el cliente (tanto para clientes internos y externos).		

G. Componente: Servicios, infraestructura y aplicaciones	
<ul style="list-style-type: none"> • Servicios de alojamiento en la nube • Herramientas de monitorización de infraestructura • Herramientas de supervisión del nivel de servicio 	

Página dejada en blanco intencionadamente

Dominio: Entregar, dar Servicio y soporte Objetivo de gestión: DSS02 - Gestionar las peticiones y los incidentes de servicio		Área prioritaria: Modelo Core de COBIT
Descripción		
Proporcionar una respuesta oportuna y efectiva a las solicitudes de los usuarios y la resolución de todos los tipos de incidentes. Restaurar el servicio normal, registrar y completar las solicitudes de usuario; y registrar, investigar, diagnosticar, escalar y resolver los incidentes.		
Propósito		
Lograr una mayor productividad y minimizar las interrupciones mediante la resolución rápida de consultas e incidencias de los usuarios. Evaluar el impacto de los cambios y hacer frente a los incidentes del servicio. Resolver las solicitudes de los usuarios y restaurar el servicio como respuesta ante incidentes.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:		
Metas empresariales • EG01 Portafolio de productos y servicios competitivos • EG08 Optimización de la funcionalidad de procesos internos del negocio	➔	Metas de alineamiento AG05 Prestación de servicios de I&T en línea con los requisitos del negocio
Métricas modelo para metas empresariales EG01 a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios EG08 a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarial b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro		Métricas modelo para metas de alineamiento AG05 a. Porcentaje de partes interesadas del negocio satisfechas con que la prestación de servicios de I&T cumpla con los niveles de servicio acordados b. Número de interrupciones del negocio debido a incidentes de servicios de I&T c. Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de I&T

A. Componente: Proceso		
Práctica de gestión	Métricas modelo	
DSS02.01 Definir esquemas de clasificación para incidentes y peticiones de servicio. Definir esquemas de clasificación y modelos de incidentes y de peticiones de servicio.	a. Número total de solicitudes e incidentes de servicio por nivel de prioridad b. Número total de incidentes escalados	
Actividades	Nivel de capacidad	
1. Definir esquemas de priorización y clasificación de solicitudes de servicios e incidentes, y los criterios para el registro de problemas. Usar esta información para garantizar estrategias constantes a fin de gestionar e informar a los usuarios sobre los problemas y llevar a cabo análisis de tendencias.	3	
2. Definir modelos de incidentes sobre errores conocidos para permitir una resolución eficiente y eficaz.		
3. Definir modelos de solicitud de servicios conforme al tipo de solicitud de servicios para permitir la autoayuda y un servicio eficiente para solicitudes estándar.		
4. Definir las reglas y procedimientos de escalamiento de incidentes, sobre todo para incidentes importantes e incidentes de seguridad.		
5. Definir las fuentes de conocimiento sobre incidentes y solicitudes y describir cómo usarlas.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
CMMI Cybermaturity Platform, 2018	IA.IP Implement Incident Investigation Processes	
HITRUST CSF versión 9, septiembre de 2017	11.01 Reporting Information Security Incidents and Weaknesses	
ISF, The Standard of Good Practice for Information Security 2016	TM2 Security Incident Management	
ISO/IEC 20000-1:2011(E)	8.1 Incident and service request management	
ISO/IEC 27002:2013/Cor.2:2015(E)	16. Information security incident management	

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
DSS02.02 Registrar, clasificar y priorizar las peticiones e incidentes. Identificar, registrar y clasificar las peticiones de servicio y los incidentes, y asignarles una prioridad de acuerdo con la criticidad para el negocio y los acuerdos de servicio.		a. Número de tipos y categorías definidos para registrar solicitudes e incidentes de servicio b. Número de solicitudes e incidentes de servicio no clasificados
Actividades		Nivel de capacidad
1. Registrar todas las solicitudes e incidentes de servicio, mediante el registro de toda la información relevante, para que pueda gestionarse de forma eficaz y pueda mantenerse un registro histórico completo.		2
2. Permitir el análisis de tendencias, clasificar las solicitudes e incidentes de servicio, con identificación del tipo y categoría.		
3. Priorizar solicitudes e incidentes de servicio basados en la definición del servicio de SLA según el impacto y la urgencia para el negocio.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
DSS02.03 Verificar, aprobar y resolver peticiones de servicio. Seleccionar los procedimientos apropiados para peticiones y verificar que las solicitudes de servicio cumplan con los criterios de solicitud definidos. Obtener aprobación, si se requiere, y satisfacer las solicitudes.		a. Tiempo promedio transcurrido para la gestión de cada tipo de solicitud de servicio b. Porcentaje de solicitudes de servicio que cumplen con los criterios de solicitud definidos
Actividades		Nivel de capacidad
1. Comprobar el derecho a las solicitudes de servicio, utilizando un flujo de proceso predefinido y cambios estándar, cuando sea posible.		2
2. Obtener la aprobación y confirmación financiera y funcional, si fuera necesario, o las aprobaciones predefinidas para los cambios estándar acordados.		
3. Cumplir con las solicitudes realizando el proceso de solicitud seleccionado. Cuando sea posible, usar menús automáticos de autoayuda y modelos de solicitud predefinidas para elementos solicitados con frecuencia.		3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ITIL V3, 2011		Service Operation, 4.3 Request Fulfilment
Práctica de gestión		Métricas modelo
DSS02.04 Investigar, diagnosticar y asignar incidentes. Identificar y registrar los síntomas de los incidentes, determinar las causas posibles y asignarlos para su resolución.		a. Número de síntomas de incidentes identificados y registrados b. Número de causas de síntomas correctamente determinadas c. Número de problemas duplicados en el log de referencia
Actividades		Nivel de capacidad
1. Identificar y describir síntomas relevantes para establecer las causas más probables de los incidentes. Referenciar los recursos de conocimientos disponibles (incluidos errores y problemas conocido) para identificar posibles resoluciones de incidentes (soluciones temporales y/o permanentes).		2
2. Si un problema relacionado o error conocido no existe todavía y si el incidente satisface los criterios acordados para el registro de problemas, registrarlo como un problema nuevo.		
3. Asignar incidentes a funciones de especialista si se necesita una mayor habilidad. Contar con el nivel directivo adecuado, donde y si se necesita.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
DSS02.05 Resolver y recuperarse de los incidentes. Documentar, aplicar y probar las soluciones definitivas o temporales (workarounds) identificados. Realizar acciones de recuperación para restaurar el servicio relacionado con I&T.		a. Porcentaje de incidentes resueltos dentro de los SLA acordados b. Porcentaje de satisfacción de las partes interesadas con la solución y recuperación del incidente
Actividades		Nivel de capacidad
1. Seleccionar y aplicar las resoluciones de incidentes más adecuadas (solución workaround y/o solución permanente).		2
2. Registrar, si se usaron, workarounds para la resolución de incidentes.		
3. Aplicar medidas correctivas, si se requieren.		
4. Documentar la resolución de incidentes y evaluar si la resolución puede usarse como una fuente de conocimiento futura.		

A. Componente: Proceso (cont.)		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ITIL V3, 2011		Service Operation, 4.2 Incident Management
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, abril de 2018		RC.RP Recovery Planning
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.9 Incident response (IR-4, IR-5, IR-6)
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 201		CSC 19: Incident Response and Management
Práctica de gestión		Métricas modelo
DSS02.06 Cerrar las peticiones de servicio y los incidentes. Verificar la solución satisfactoria del incidente y/o el cumplimiento de la petición y su cierre.		a. Nivel de satisfacción del usuario con el cumplimiento de la petición de servicio b. Porcentaje de incidentes resueltos dentro del periodo de tiempo acordado/ aceptado
Actividades		Nivel de capacidad
1. Comprobar con los usuarios afectados que la solicitud de servicio se ha cumplido de forma satisfactoria o el incidente se ha resuelto de forma satisfactoria dentro de un plazo de tiempo acordado/aceptable.		2
2. Cerrar las peticiones e incidentes de servicio.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
DSS02.07 Hacer seguimiento al estado y producir informes. Hacer seguimiento, analizar e informar regularmente sobre los incidentes y el cumplimiento de las solicitudes. Examinar tendencias para proporcionar información para la mejora continua.		a. Tiempo promedio entre incidentes para el servicio habilitado por I&T b. Número y porcentaje de incidentes que causan interrupciones en procesos críticos del negocio
Actividades		Nivel de capacidad
1. Supervisar y hacer seguimiento al escalamientos y resoluciones de incidentes y solicitar procedimientos de manejo para progresar hacia la resolución o finalización de los mismos.		2
2 Identificar las partes interesadas en la información y sus necesidades de datos o informes. Identificar frecuencia y medio de elaboración de los reportes.		3
3. Producir y distribuir informes en el plazo debido o proporcionar un acceso controlado a los datos en línea.		4
4. Analizar incidentes y solicitudes de servicio por categoría y tipo. Establecer tendencias e identificar patrones de problemas recurrentes, violaciones o ineficiencias del SLA.		
5. Usar la información como un insumo a la planificación de la mejora continua.		5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		MI.IM Ensure Incident Mitigation; IR.IR Incident Reporting
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.9 Incident response (IR-7, IR-8)

B. Componente: Estructuras organizativas

	Director de tecnología	RDueños del proceso de negocio	Jefe de desarrollo	Jefe de operaciones de TI	Gestor de servicio	Gestor de seguridad de la información
Práctica clave de gestión						
DSS02.01 Definir esquemas de clasificación para incidentes y peticiones de servicio.	A		R	R	R	
DSS02.02 Registrar, clasificar y priorizar las peticiones e incidentes.	A			R	R	
DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	A	R	R	R	R	
DSS02.04 Investigar, diagnosticar y asignar incidentes.	A	R		R	R	
DSS02.05 Resolver y recuperarse de los incidentes.	A		R	R	R	R
DSS02.06 Cerrar las peticiones de servicio y los incidentes.	A			R	R	R
DSS02.07 Hacer seguimiento al estado y producir informes.	A			R	R	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica					
ISO/IEC 27002:2013/Cor.2:2015(E)	16.1.1 Responsibilities and procedures					

C. Componente: Flujos y elementos de información (ver también la sección 3.6)

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS02.01 Definir esquemas de clasificación para incidentes y peticiones de servicio.	AP009.03	SLA	Criterios para el registro de problemas	DSS03.01
	BAI10.02	Repositorio de configuraciones	Reglas para escalamiento de incidentes	Interna
	BAI10.03	Repositorio actualizado con elementos de configuración	Esquema y modelos de clasificación de peticiones de servicio e incidentes	Interna
	BAI10.04	Informes de estado de la configuración		
	DSS01.03	Reglas de monitorización de activos y estado de eventos		
	DSS03.01	Esquema de clasificación de problemas		
	DSS04.03	Acciones y comunicaciones para responder a incidentes		
DSS02.02 Registrar, clasificar y priorizar las peticiones e incidentes.	AP009.03	SLA	Peticiones de servicio e incidentes clasificadas y priorizadas	AP008.03; AP009.04; AP013.03; DSS03.05
	BAI04.05	Procedimiento de escalamiento de emergencia	Registro de solicitudes de servicio e incidentes	Interna; MEA04.07
	DSS01.03	• Reglas de monitorización de activos y estado de eventos • Tickets de incidentes		
	DSS05.07	Tickets de incidentes relacionados con la seguridad		


C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
DSS02.03: Verificar, aprobar y resolver peticiones de servicio.	De	Descripción	Descripción	A
	APO12.06	Causas raíz relacionadas con el riesgo	Peticiones de servicio aprobadas	BAI06.01
			Peticiones de servicio completadas	Interna
DSS02.04 Investigar, diagnosticar y asignar incidentes.	BAI07.07	Plan de soporte suplementario	Log de problemas	DSS03.01
			Síntomas de incidente	Interna
DSS02.05 Resolver y recuperarse de los incidentes.	APO12.06	Plan de respuesta a incidentes relacionados con riesgos	Resoluciones de incidentes	DSS03.03; DSS03.04; DSS03.05; MEA04.07
	DSS03.03	Registros de errores conocidos		
	DSS03.04	Comunicación de conocimientos aprendidos		
DSS02.06 Cerrar las peticiones de servicio y los incidentes.	DSS03.04	Registros de problemas cerrados	Confirmación del usuario del cumplimiento o resolución satisfactoria	APO08.03
			Cierre de peticiones de servicio e incidentes	APO08.03; APO09.04; DSS03.04
DSS02.07 Hacer seguimiento al estado y producir informes.	APO09.03	OLAs	Estado de incidentes e informe de tendencias	APO08.03; APO09.04; APO11.04; APO12.01; MEA01.03
	DSS03.01	Informe de estado del problema	Estado de cumplimiento de peticiones e informe de tendencias	APO08.03; APO09.04; APO11.04; MEA01.03
	DSS03.02	Informes de resolución de problemas		
	DSS03.05	Informes de monitorización de resolución de problemas		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Soporte de aplicaciones	Skills Framework for the Information Age V6, 2015	ASUP
Servicio de atención al cliente	Skills Framework for the Information Age V6, 2015	CSMG
Gestión de incidentes	Skills Framework for the Information Age V6, 2015	USUP
Soporte de redes	Skills Framework for the Information Age V6, 2015	NTAS
Soporte de usuarios	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	C. Run—C.1. User Support

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de solicitud de servicio	Establece los fundamentos y proporciona directrices para las peticiones de servicio e incidentes y su documentación.	ITIL V3, 2011	Service Operation, 3. Service operation principles

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Permitir a los empleados identificar incidentes de forma correcta y en el plazo debido e implementar las rutas de escalamiento adecuadas. Fomentar la prevención. Responder y resolver los incidentes de forma inmediata. Evitar una cultura de héroes.		

G. Componente: Servicios, infraestructura y aplicaciones		
Sistema y herramientas de seguimiento de incidentes		

Dominio: Entregar, dar servicio y soporte		Área prioritaria: Modelo Core de COBIT	
Objetivo de gestión: DSS03 - Gestionar los problemas			
Descripción			
Identificar y clasificar los problemas y su causa raíz. Ofrecer una solución oportuna para evitar incidentes recurrentes. Ofrecer recomendaciones de mejoras.			
Propósito			
Aumentar la disponibilidad, mejorar los niveles de servicio, reducir los costes y atender mejor las necesidades del cliente y lograr su satisfacción mediante una reducción del número de problemas operativos, e identificar las causas raíz como parte de la resolución de problemas.			
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:			
Metas empresariales			Metas de alineamiento
<ul style="list-style-type: none">• EG01 Portafolio de productos y servicios competitivos• EG08 Optimización de la funcionalidad de procesos del negocio interno			AG05 Prestación de servicios de I&T conforme a los requisitos del negocio
Métricas modelo para metas empresariales			Métricas modelo para metas de alineamiento
EG01	<ul style="list-style-type: none">a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercadob. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del clientec. Porcentaje de productos y servicios que proporcionan una ventaja competitivad. Plazo de comercialización para nuevos productos y servicios		AG05 <ul style="list-style-type: none">a. Porcentaje de partes interesadas del negocio satisfechas con la prestación de servicios de I&T que cumple con los niveles de servicio acordadosb. Número de interrupciones del negocio debido a incidentes de servicios de I&Tc. Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de I&T
EG08	<ul style="list-style-type: none">a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarialb. Niveles de satisfacción de los clientes con las capacidades de prestación de serviciosc. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro		

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
DSS03.01 Identificar y clasificar los problemas. Definir e implementar criterios y procedimientos para identificar e informar sobre los problemas. Incluir la clasificación, categorización y priorización del problema.		a. Porcentaje de incidentes mayores para los que se registraron problemas b. Porcentaje de incidentes resueltos conforme a los SLA acordados c. Porcentaje de problemas identificados correctamente, incluida la clasificación, categorización y priorización de los mismos.
Actividades		Nivel de capacidad
1. Identificar problemas a través de la correlación de informes de incidentes, registros de errores y otros recursos que permitan la identificación de problemas.		2
2. Gestionar todos los problemas formalmente con acceso a todos los datos relevantes. Incluir información del sistema de gestión de cambios de TI y de configuración/activo de TI y los detalles del incidente.		
3. Definir grupos de soporte adecuados para ayudar en la identificación de problemas, análisis de la causa raíz y determinación de soluciones para respaldar la gestión de problemas. Determinar grupos de soporte conforme a las categorías predefinidas, como hardware, red, software, aplicaciones y software de soporte.		
4. Definir niveles de prioridad a través de la consulta con el negocio para garantizar que la identificación del problema y el análisis de las causas raíz se gestionan en el plazo debido conforme a los SLA acordados. Basar los niveles de prioridad en el impacto y la urgencia del negocio.		
5. Informar del estado de los problemas identificados a la mesa de servicio, para que los clientes y gestores de TI puedan mantenerse informados.		
6. Mantener un único catálogo de gestión de problemas para registrar e informar sobre los problemas identificados. Usar el catálogo para establecer pistas de auditoría de los procesos de gestión de problemas incluido el estado de cada problema (es decir, abierto, reabierto, en curso o cerrado).		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISO/IEC 20000-1:2011(E)		8.2 Problem management

A. Componente: Proceso (cont.)			
Práctica de gestión		Métricas modelo	
DSS03.02 Investigar y diagnosticar problemas. Investigar y diagnosticar problemas con la ayuda de expertos en la materia para evaluar y analizar su causa raíz.		a. Número de problemas identificados clasificados como errores conocidos b. Porcentaje de problemas investigados y diagnosticados a lo largo de su ciclo de vida	
Actividades			Nivel de capacidad
1. Identificar problemas que podrían ser errores conocidos mediante una comparación de los datos de incidentes con la base de datos de errores conocidos y sospechados (p. ej., aquellos comunicados por proveedores externos) Clasificar los problemas como errores conocidos.			3
2. Asociar los elementos de configuración afectados con el error establecido/conocido.			
3. Producir informes para comunicar el progreso a la hora de resolver problemas y gestionar el impacto continuo de los problemas no resueltos. Monitorizar el estado del proceso de manejo de problemas a lo largo de su ciclo de vida, incluyendo los insumos de la gestión de cambios y de la configuración de TI.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin documentación relacionada para esta práctica de gestión			
Práctica de gestión		Métricas modelo	
DSS03.03 Presentar los errores conocidos. Tan pronto como se identifiquen las causas raíz de los problemas, crear registros de los errores conocidos, documentar las soluciones temporales apropiadas e identificar las soluciones potenciales.		a. Número de problemas con resolución satisfactoria que abordan las causas raíz b. Porcentaje de satisfacción de las partes interesada con la identificación de las causas raíz, la creación de registros de errores conocidos y soluciones temporales adecuadas, y la identificación de soluciones potenciales	
Actividades			Nivel de capacidad
1. Tan pronto como se identifiquen las causas raíz de los problemas, crear registros de los errores conocidos y desarrollar una solución temporal apropiada.			2
2. Identificar, evaluar, priorizar y procesar (a través de la gestión de cambio de TI) soluciones a los errores conocidos, conforme al coste/beneficio del caso de negocio, el impacto y la urgencia.			3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin documentación relacionada para esta práctica de gestión			
Práctica de gestión		Métricas modelo	
DSS03.04 Resolver y cerrar los problemas. Identificar e iniciar soluciones sostenibles dirigidas a la causa raíz del problema. Presentar solicitudes de cambio a través del proceso de gestión de cambio establecido, si es necesario, para resolver los errores. Asegurarse de que el personal afectado conoce las medidas adoptadas y los planes desarrollados para evitar que ocurran incidentes en el futuro.		a. Reducir el número de incidentes recurrentes causados por problemas no resueltos b. Porcentaje de soluciones temporales definidas para los problemas abiertos	
Actividades			Nivel de capacidad
1. Cerrar los registros de problemas después de la confirmación sobre la eliminación exitosa del error conocido o después del acuerdo con el negocio sobre cómo gestionar el problema de forma alternativa.			2
2. Informar a la mesa de servicio sobre el calendario de cierre de problemas (p. ej., el calendario para solucionar los errores conocidos, la posible solución temporal o el hecho de que el problema seguirá ahí hasta que se implemente el cambio) y las consecuencias de la estrategia llevada a cabo. Mantener a los usuarios y clientes afectados informados como corresponda.			3
3. A través del proceso de resolución, obtener informes regulares de gestión de cambios de TI relacionados con el progreso a la hora de resolver problemas y errores.			
4. Monitorizar el impacto continuo de los problemas y errores conocidos en los servicios.			4
5. Revisar y confirmar la resolución satisfactoria de problemas mayores.			
6. Asegurar que el conocimiento aprendido de la revisión se incorpore a la reunión de revisión de servicios con el cliente del negocio.			5
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica	
Sin documentación relacionada para esta práctica de gestión			

A. Componente: Proceso (cont.)	
Práctica de gestión	Métricas modelo
DSS03.05 Realizar una gestión proactiva de los problemas. Recopilar y analizar los datos operacionales (especialmente los registros del incidente y los cambios) para identificar las tendencias que están emergiendo que puedan indicar problemas. Guardar los registros de problemas para permitir su evaluación.	a. Porcentaje de problemas registrados como parte de la actividad de gestión de problemas proactiva b. Porcentaje de partes interesadas satisfechas con la comunicación de información de problemas relacionados con cambios e incidentes de TI
Actividades	Nivel de capacidad
1. Captar la información del problema relacionada con cambios e incidentes de I&T y comunicarla a las partes interesadas clave. Comunicar a través de informes y reuniones periódicas entre los dueños de los procesos de incidentes, problemas, cambios y gestión de la configuración para considerar los problemas recientes y las posibles acciones correctivas.	3
2. Garantizar que los dueños y gestores de los procesos de gestión de incidentes, problemas, cambios y configuración se reúnan regularmente para comentar los problemas conocidos y los cambios planificados futuros.	
3. Identificar e iniciar soluciones sostenibles (soluciones permanentes) que aborden la causa raíz. Presentar solicitudes de cambio a través de los procesos establecidos de gestión de cambios.	
4. Permitir a la empresa supervisar los costes totales de los problemas, captar los esfuerzos de cambios derivados de las actividades del proceso de gestión de problemas (p. ej., soluciones a problemas y errores conocidos) e informar al respecto.	4
5. Crear informes para supervisar la resolución de problemas en relación con los requisitos del negocio y los SLAs. Asegurar el escalamiento adecuado de los problemas, como comunicarlos al siguiente nivel directivo conforme a los criterios acordados, contactar con proveedores externos o consultar con el consejo asesor de cambios (CAB) para aumentar la prioridad de una solicitud de cambio urgente (RFC) para implementar una solución temporal.	
6. Optimizar el uso de recursos y reducir el uso de soluciones temporales; hacer un seguimiento a las tendencias de los problemas.	
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)	Referencia específica
CMMI Cybermaturity Platform, 2018	MI.IC Ensure Incident Containment
ITIL V3, 2011	Service Operation, 4.4 Problem Management

B. Componente: Estructuras organizativas							
Práctica clave de gestión	Comité Ejecutivo	Director de TI	Director de tecnología	Jefe de desarrollo	Jefe de operaciones de TI	Gestor de servicios	Gestor de seguridad de la información
		R	A	R	R	R	
			A		R	R	R
			A		R	R	R
			A		R	R	
	R		A		R	R	
	Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)						
Sin Documentación relacionada para este componente.							

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
DSS03.01 Identificar y clasificar los problemas.	De	Descripción	Descripción	A
	AP012.06	Causas raíz relacionadas con el riesgo	Esquema de clasificación de problemas	DSS02.01
	DSS02.01	Criterios para el registro de problemas	Informes de estado del problema	DSS02.07
	DSS02.04	Log de problemas	Registro de problemas	Interna
DSS03.02 Investigar y diagnosticar problemas.	AP012.06	Causas raíz relacionadas con el riesgo	Informes de resolución de problemas	DSS02.07
			Causas raíz de problemas	Interna; DSS03.05
DSS03.03 Presentar los errores conocidos.	AP012.06	Causas raíz relacionadas con el riesgo	Soluciones propuestas a errores conocidos	BAI06.01
	DSS02.05	Resoluciones de incidentes	Registros de errores conocidos	DSS02.05
DSS03.04 Resolver y cerrar los problemas.	DSS02.05	Resoluciones de incidentes	Comunicación de conocimientos aprendidos	AP008.04; DSS02.05
	DSS02.06	Cierre de peticiones de servicio e incidentes	Registros de problemas cerrados	DSS02.06
DSS03.05 Realizar una gestión proactiva de los problemas.	AP012.06	Causas raíz relacionadas con el riesgo	Soluciones sostenibles identificadas	BAI06.01
	DSS02.02	• Peticiones de servicio e incidentes clasificadas y priorizadas • Resoluciones de incidentes	Informes de supervisión de resolución de problemas	DSS02.07, MEA04.07
	DSS03.04	Causas raíz de los problemas		
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica		
Sin documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)	Referencia específica
Soporte de aplicaciones	Skills Framework for the Information Age V6, 2015	ASUP
Soporte de redes	Skills Framework for the Information Age V6, 2015	NTAS
Gestión de problemas	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	C. Run—C.4. Problem Management
Gestión de problemas	Skills Framework for the Information Age V6, 2015	PBMG

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de resolución de problemas	Documenta el razonamiento y proporciona directrices para abordar los problemas que surgen de incidentes e identificar soluciones temporales validadas.	ITIL V3, 2011	Service Operation, 3. Service strategy principles

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Respaldo una cultura de gestión de problemas proactiva (detección, acción y prevención) con roles y responsabilidades claramente definidos. Garantizar un entorno transparente y abierto para informar sobre problemas proporcionando mecanismos independientes de reporte y/o recompensas a las personas que comunican problemas.		
G. Componente: Servicios, infraestructura y aplicaciones		
Sistema de rastreo/resolución de problemas		

Página dejada en blanco intencionadamente

Dominio: Entregar, dar servicio y soporte Objetivo de gestión: DSS04 - Gestionar la continuidad		Área prioritaria: Modelo Core de COBIT
Descripción		
Establecer y mantener un plan que permita a las organizaciones empresariales y a TI responder a los incidentes y adaptarse rápidamente a las interrupciones. Esto permitirá la operación continua de los procesos críticos de negocio y de los servicios de I&T necesarios, y mantener la disponibilidad de recursos, activos e información en un nivel aceptable para la empresa.		
Propósito		
Adaptarse rápidamente, continuar con las operaciones del negocio y mantener la disponibilidad de los recursos y la información a un nivel aceptable para la empresa en caso de una interrupción significativa (p.ej., amenazas, oportunidades, demandas).		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales	➔	Metas de alineamiento
<ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG02 Gestión de riesgo de negocio • EG06 Continuidad y disponibilidad del servicio del negocio • EG08 Optimización de la funcionalidad del proceso interno de negocio 		<ul style="list-style-type: none"> • AG05 Prestación de servicios de I&T conforme a los requisitos de negocio • AG07 Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios		AG05 a. Porcentaje de partes interesadas del negocio satisfechas con que la prestación de servicios de I&T cumpla con los niveles de servicio acordados b. Número de interrupciones del negocio debido a incidentes de servicios de I&T c. Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de I&T
EG02 a. Porcentaje de objetivos y servicios empresariales críticos cubiertos por la evaluación de riesgos b. Proporción de incidentes significativos que no se identificaron en la evaluación de riesgos frente al total de incidentes c. Frecuencia de actualización del perfil de riesgo		AG07 a. Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o descrédito público b. Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o descrédito público c. Número de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o descrédito público
EG06 a. Número de interrupciones del servicio al cliente o procesos del negocio que han causado incidentes significativos b. Coste de los incidentes para el negocio c. Número de horas de procesamiento perdidas en el negocio debido a interrupciones inesperadas del servicio d. Porcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados		
EG08 a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso de negocio b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro		

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
DSS04.01 Definir la política de continuidad del negocio, sus objetivos y alcance. Definir la política y alcance de la continuidad del negocio, alineado con los objetivos de la empresa y de las partes interesadas, para mejorar la resiliencia del negocio.		a. Porcentaje de objetivos y alcance de continuidad del negocio reprocesados debido a procesos y actividades no identificados b. Porcentaje de partes interesadas clave que participan, definen y acuerdan la política y el alcance de continuidad
Actividades		Nivel de capacidad
1. Identificar procesos de negocio y actividades de servicio internos y externalizados que son críticos para las operaciones empresariales o necesarios para satisfacer las obligaciones legales y/o contractuales.		2
2. Identificar partes interesadas clave y los roles y responsabilidades para definir y acordar la política y el alcance de continuidad.		
3. Definir y documentar los objetivos de política mínimos acordados y el alcance de la resiliencia del negocio.		
4. Identificar procesos de negocio de soporte esenciales y servicios de I&T relacionados.		
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
HITRUST CSF versión 9, septiembre de 2017		12.01 Information Security Aspects of Business Continuity Management
ISF, The Standard of Good Practice for Information Security 2016		BC1.1 Business Continuity Strategy; BC1.2 Business Continuity Programme
ISO/IEC 27002:2013/Cor.2:2015(E)		17. Aspectos de seguridad de la información de la gestión de la continuidad del negocio
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.6 Contingency planning (CP-1)
Práctica de gestión		Métricas modelo
DSS04.02 Mantener la resiliencia del negocio. Evaluar las opciones de resiliencia del negocio y elegir una estrategia viable y rentable para asegurar la continuidad, la recuperación ante un desastre y la respuesta ante incidentes de la empresa ante un desastre u otro incidente o interrupción mayor.		a. Inactividad total derivada de un incidente o interrupción importante. b. Porcentaje de partes interesadas clave involucradas en el análisis de impacto del negocio que evalúan el impacto a lo largo del tiempo de duración de una interrupción de funciones críticas del negocio y el efecto que una interrupción tendría sobre ellas
Actividades		Nivel de capacidad
1. Identificar escenarios potenciales que podrían ocasionar eventos que darían lugar a incidentes disruptivos significativos.		2
2. Conducir un análisis de impacto del negocio para evaluar el impacto a lo largo del tiempo de duración de una interrupción de funciones críticas del negocio y el efecto que una interrupción tendría en ellas.		
3. Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y el entorno de I&T que lo soporta, conforme a una duración aceptable de interrupción del negocio y la suspensión tolerable máxima.		
4. Determinar las condiciones y los dueños de las decisiones clave que ocasionarán que se invoquen los planes de continuidad.		
5. Evaluar la probabilidad de amenazas que pudieran causar la pérdida de la continuidad del negocio. Identificar medidas que reducirán la probabilidad y el impacto a través de una mejor prevención y una mayor resiliencia.		3
6. Analizar requisitos de continuidad para identificar posibles opciones estratégicas empresariales y técnicas.		
7. Identificar los requisitos y costes de recursos para cada opción técnica estratégica y realizar recomendaciones estratégicas.		
8. Obtener la aprobación de ejecutivos del negocio para las opciones estratégicas seleccionadas.		
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
ISF, The Standard of Good Practice for Information Security 2016		BC1.3 Resilient Technical Environments
ITIL V3, 2011		Service Design, 4.6 IT Continuity Management
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.6 Contingency planning (CP-2)

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
DSS04.03 Desarrollar e implementar una respuesta de continuidad del negocio. Desarrollar un plan de continuidad del negocio (BCP) y un plan de recuperación de desastres (DRP) basados en la estrategia. Documentar todos los procedimientos necesarios para que la empresa continúe con sus actividades críticas en caso de incidente.		a. Número de sistemas críticos de negocio no cubiertos por el plan b. Porcentaje de partes interesadas clave involucradas en el desarrollo de BCPs y DRPs
Actividades		Nivel de capacidad
1. Definir acciones y comunicaciones de respuesta a incidentes que se deban tomar en caso de interrupción. Definir roles y responsabilidades relacionados, incluida la rendición de cuentas para la política y la implementación.		2
2. Garantizar que los proveedores clave y socios externalizados cuenten con planes de continuidad efectivos. Obtener evidencia auditada según se requiera.		
3. Definir las condiciones y los procedimientos de recuperación que permitirán la reanudación del procesamiento de negocio. Incluir la actualización y sincronización de bases de datos para preservar la integridad de la información.		
4. Desarrollar y mantener BCPs y DRPs operativos que contengan los procedimientos a seguir para permitir el funcionamiento continuo de procesos de negocio críticos y/o acuerdos de procesamiento temporales. Incluir vínculos a los planes de proveedores de servicios externalizados.		
5. Definir y documentar los recursos requeridos para respaldar los procedimientos de continuidad y recuperación, teniendo en cuenta las personas, las instalaciones y la infraestructura de TI.		
6. Definir y documentar los requisitos de copias de seguridad de la información necesarios para respaldar los planes. Incluir planes y documentos en papel, así como archivos de datos. Considerar la necesidad de seguridad y almacenamiento fuera de las instalaciones.		
7. Determinar las habilidades requeridas para los individuos involucrados en la ejecución del plan y los procedimientos.		
8. Distribuir los planes y la documentación soporte de forma segura a las partes interesadas debidamente autorizadas. Asegurar que los planes y la documentación son accesibles en todos los escenarios de desastre.		3
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
ISF, The Standard of Good Practice for Information Security 2016		BC1.4 Crisis Management; BC2.1 Business Continuity Planning
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.6 Contingency planning (CP-6, CP-9, CP-10)
Práctica de gestión		Métricas modelo
DSS04.04 Realizar ejercicios, probar y revisar el plan de continuidad del negocio (BCP) y el plan de respuesta ante desastres (DRP). Probar la continuidad de forma periódica para ver el comportamiento de los planes contra resultados predeterminados, mantener la resiliencia del negocio y permitir que se desarrollen soluciones innovadoras.		a. Frecuencia de las pruebas b. Número de ejercicios y pruebas que alcanzaron los objetivos de recuperación
Actividades		Nivel de capacidad
1. Definir objetivos para ejercitar y probar los sistemas del negocio, técnicos, logísticos, administrativos, procedimentales y operativos del plan para verificar la integridad de los BCP y DRP en el cumplimiento del riesgo del negocio.		2
2. Definir y acordar ejercicios con las partes interesadas que sean realistas y validen los procedimientos de continuidad. Incluir roles y responsabilidades y acuerdos de retención de datos que causen la mínima disrupción a los procesos del negocio.		
3. Asignar roles y responsabilidades para la ejecución de ejercicios y pruebas del plan de continuidad.		
4. Programar ejercicios y actividades de prueba de acuerdo a lo definido en los planes de continuidad.		3
5. Llevar a cabo una sesión informativa y un análisis luego del ejercicio para considerar lo alcanzado.		4
6. De acuerdo a los resultados de la revisión, desarrollar recomendaciones para mejorar los planes de continuidad actuales.		5
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		PP.RS Develop and Maintain Response Plans; PP.RP Develop and Maintain Recovery Plans
ISF, The Standard of Good Practice for Information Security 2016		BC2.3 Business Continuity Testing
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016		CSC 20: Penetration Tests and Red Team Exercises

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
DSS04.05 Revisar, mantener y mejorar los planes de continuidad. Conducir una revisión periódica de la capacidad de continuidad para asegurar su idoneidad, lo adecuado y su efectividad. Gestionar los cambios a los planes de acuerdo con el proceso de control de cambios para asegurar que los planes de continuidad se mantienen actualizados y reflejan continuamente los requisitos actuales del negocio.		a. Porcentaje de mejoras acordadas para el plan que se han incorporado al plan b. Porcentaje de planes de continuidad y evaluaciones del impacto en el negocio que se encuentran actualizados
Actividades		Nivel de capacidad
1. Revisar regularmente los planes de continuidad y la capacidad contra las hipótesis consideradas y los objetivos estratégicos y operativos actuales del negocio.		3
2. Revisar de forma regular los planes de continuidad para considerar el impacto de cambios nuevos o mayores en la organización empresarial, procesos de negocio, acuerdos con terceros, tecnologías, infraestructura, sistemas operativos y sistemas de aplicación.		
3. Considerar si pudiera necesitarse revisar la evaluación de impacto del negocio, dependiendo de la naturaleza del cambio.		
4. Recomendar cambios en la política, los planes, procedimientos, infraestructura y roles y responsabilidades. Comunicarlos como adecuados para la aprobación por la dirección y el procesamiento a través del proceso de gestión de cambios de TI.		
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
Sin Documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
DSS04.06 Realizar formación sobre el plan de continuidad. Proporcionar sesiones periódicas de formación sobre los procedimientos y sus roles y responsabilidades en caso de interrupción a todas las partes internas y externas involucradas.		a. Porcentaje de partes interesadas internas y externas que han recibido capacitación b. Porcentaje de partes internas y externas relevantes cuyas habilidades y competencias se encuentran actualizadas
Actividades		Nivel de capacidad
1. Realizar formación y concienciación sobre el BCP y el DRP.		2
2. Definir y mantener los requisitos y planes de formación para aquellas personas que realizan planificación de continuidad, evaluaciones de impacto, evaluaciones de riesgo, comunicación con medios de comunicación y respuesta a incidentes. Asegurar que los planes de formación consideren la frecuencia de capacitación y los mecanismos de prestación de la formación.		3
3. Desarrollar competencias basadas en formación práctica, incluida la participación en ejercicios y pruebas.		
4. De acuerdo a los resultados de los ejercicios y las pruebas, supervisar habilidades y competencias.		4
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.6 Contingency planning (CP-4)
Práctica de gestión		Métricas modelo
DSS04.07 Administrar los acuerdos de respaldo. Mantener la disponibilidad de la información crítica para el negocio.		a. Porcentaje de medios de respaldo transferidos y almacenados de forma segura b. Porcentaje de restauración exitosa y oportuna de copias de seguridad o copias de medios alternativos
Actividades		Nivel de capacidad
1. Hacer una copia de seguridad de los sistemas, aplicaciones, datos y documentación conforme a un calendario definido. Considerar una frecuencia (mensual, semanal, diario, etc.), modo de copia de seguridad (p. ej., disk mirroring para copias de seguridad en tiempo real frente a DVD-ROM para retención a largo plazo), tipo de copia de seguridad (p.ej., completa vs. incremental), y tipo de medios. Considerar también copias de seguridad online automatizadas, tipos de datos (p. ej. voz, ópticos), creación de logs, datos críticos de computación de usuario final (p. ej., hojas de cálculo), ubicación física y lógica de las fuentes de datos, derechos de acceso y seguridad, y encriptación.		2
2. Definir requisitos para el almacenamiento en las instalaciones (on-site) y fuera de ellas (off-site) de copias de seguridad de datos, conforme a los requisitos de negocio. Considerar el acceso requerido para hacer copias de seguridad de los datos.		
3. Probar y refrescar de forma periódica los datos archivados y las copias de seguridad de los datos.		
4. Garantizar que se haga una copia de seguridad o se aseguren de forma adecuada los sistemas, aplicaciones, datos y documentación mantenida o procesada por terceros. Considerar que se requiera que los terceros devuelvan las copias de seguridad. Considerar la opción de mantenimiento en fiducia (escrow, por su término en inglés) o acuerdos de depósitos.		

A. Componente: Proceso (cont.)	
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)	Referencia específica
CMMI Cybermaturity Platform, 2018	IPBP Apply Backup Processes
HITRUST CSF versión 9, septiembre de 2017	09.05 Information Back-Up
ISF, The Standard of Good Practice for Information Security 2016	SY2.3 Backup
ISO/IEC 27002:2013/Cor.2:2015(E)	12.3 Backup
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.6 Contingency planning (CP-3)
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016	CSC 10: Data Recovery Capability
Práctica de gestión	Métricas modelo
DSS04.08 Realizar revisiones post-reanudación. Evaluar la idoneidad del plan de continuidad del negocio (BCP) y el plan de respuesta ante desastres (DRP) tras la reanudación exitosa de los procesos y servicios del negocio después de una interrupción.	a. Porcentaje de problemas identificados que se han abordado posteriormente en el plan b. Porcentaje de problemas identificados que se han abordado posteriormente en los materiales de formación
Actividades	
1. Evaluar el cumplimiento de los BCP y DRP documentados.	4
2. Determinar la efectividad de los planes, capacidades de continuidad, roles y responsabilidades, habilidades y competencias, resiliencia a incidentes, infraestructura técnica y estructuras organizativas y relaciones.	
3. Identificar las debilidades u omisiones en los planes y capacidades y realizar recomendaciones de mejora. Obtener la aprobación de la dirección para cualquier cambio en los planes y aplicarlos a través del proceso de control de cambios de la empresa.	5
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)	Referencia específica
Sin documentación relacionada para esta práctica de gestión	

B. Componente: Estructuras organizativas																																	
	Comité Ejecutivo		Director de operaciones		Director de TI		Director de tecnología		Director de seguridad de la información		Dueños del proceso de negocio		Función de gestión de datos		Jefe de arquitectura		Jefe de desarrollo		Jefe de operaciones de TI		Gestor de servicios		Gestor de seguridad de la información		Gestor de continuidad del negocio								
Práctica clave de gestión																																	
DSS04.01 Definir la política de continuidad del negocio, sus objetivos y alcance.	R	A	R				R	R										R	R							R							
DSS04.02 Mantener la resiliencia del negocio.	R	A	R				R			R			R					R					R		R	R							
DSS04.03 Desarrollar e implementar una respuesta de continuidad del negocio.			R	R			R											R					R		A								
DSS04.04 Realizar ejercicios, probar y revisar el plan de continuidad del negocio (BCP) y el plan de respuesta ante desastres (DRP).			R	R			R											R					R		A								
DSS04.05 Revisar, mantener y mejorar los planes de continuidad.		A	R	R	R	R												R								R							
DSS04.06 Realizar formación sobre el plan de continuidad.			R	R			R										R	R					R		A								
DSS04.07 Administrar los acuerdos de respaldo.				A						R								R					R		R								
DSS04.08: Realizar revisiones post-reanudación.			R	R	R	R												R								A							
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)					Referencia detallada																												
Sin documentación relacionada para este componente.																																	

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
DSS04.01 Definir la política de continuidad del negocio, sus objetivos y alcance.	De	Descripción	Descripción	A
	APO09.03	SLAs	Política y objetivos para la continuidad del negocio	APO01.02
			Evaluaciones de capacidades y brechas de continuidad actuales	Interna
			Escenarios de incidentes disruptivos	Interna
DSS04.02 Mantener la resiliencia del negocio.	APO12.06	• Comunicación de impacto del riesgo • Causas raíz relacionadas con riesgos	Opciones estratégicas aprobadas	APO02.05
			BIAs	APO12.02
			Requisitos de continuidad	Interna
DSS04.03 Desarrollar e implementar una respuesta de continuidad del negocio.	APO09.03	OLAs	Acciones y comunicaciones para respuesta a incidentes	DSS02.01
			BCP	Interna
DSS04.04 Realizar ejercicios, probar y revisar el plan de continuidad del negocio (BCP) y el plan de respuesta ante desastres (DRP).			Resultados y recomendaciones de pruebas	Interna
			Ejercicios de prueba	Interna
			Objetivos de la prueba	Interna
DSS04.05 Revisar, mantener y mejorar los planes de continuidad.			Cambios recomendados a los planes	Interna
			Resultados de revisiones de planes	Interna
DSS04.06 Realizar formación sobre el plan de continuidad.	Recursos Humanos	Lista de personal que necesita formación	Supervisión de resultados de habilidades y competencias.	APO07.03
			Requisitos de formación	APO07.03
DSS04.07 Administrar los acuerdos de copia de seguridad.	APO14.10	• Plan de copias de seguridad • Plan de pruebas de copias de seguridad	Probar los resultados de las copias de seguridad de los datos	Interna
			Copia de seguridad de los datos	Interna; APO14.08
DSS04.08 Realizar revisiones post-reanudación.			Cambios aprobados a los planes	BAI06.01
			Informe de la revisión post-reanudación.	Interna
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica		
Sin documentación relacionada para este componente.				


D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)	Referencia específica
Gestión de la continuidad	Skills Framework for the Information Age V6, 2015	COPL

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de continuidad del negocio (BCP)	Señala el compromiso de la dirección con la evaluación de impacto del negocio (BIA), el plan de contingencia del negocio (incluida la recuperación confiable), los requisitos de recuperación para sistemas críticos, umbrales y disparadores de las contingencias definidos, plan de escalamiento, plan de recuperación de datos, formación y pruebas.		
Política de gestión de crisis	Establece las directrices y la secuencia de la respuesta ante crisis en áreas clave del riesgo. La gestión de crisis es, junto con la seguridad de I&T, la gestión de red, y la seguridad de los datos y la privacidad, una de las políticas a nivel operativo que debería considerarse para una gestión de riesgos de I&T completa.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Integrar la necesidad de resiliencia de negocio en la cultura empresarial. Informar de forma regular y frecuente a los empleados sobre los valores fundamentales, comportamientos deseados y objetivos estratégicos para conservar la compostura e imagen empresarial en cualquier situación. Probar de forma regular los procedimientos de continuidad y la recuperación de desastres.		

G. Componente: Servicios, infraestructuras y aplicaciones
<ul style="list-style-type: none"> • Servicios externos de hosting • Herramientas de monitorización de incidentes • Servicios de instalaciones para almacenamiento remoto

Página dejada en blanco intencionadamente

Dominio: Entregar, dar servicio y soporte		Área prioritaria: Modelo Core de COBIT	
Objetivo de gestión: DSS05 - Gestionar los servicios de seguridad			
Descripción			
Proteger la información de la empresa para mantener el nivel de riesgo de la seguridad de la información aceptable para la empresa, conforme con la política de seguridad. Establecer y mantener roles y privilegios de acceso de seguridad de la información. Realizar una monitorización de la seguridad.			
Propósito			
Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad de la información			
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:			
Metas empresariales			Metas de alineamiento
• EG02 Gestión de riesgo del negocio • EG06 Continuidad y disponibilidad del servicio del negocio			• AG02 Gestión de riesgo relacionado con I&T • AG07 Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad
Métricas modelo para metas empresariales			Métricas modelo para metas de alineamiento
EG02	a. Porcentaje de objetivos y servicios empresariales críticos cubiertos por la evaluación de riesgos b. Número de incidentes significativos que no se identificaron en la evaluación de riesgos frente al total de incidentes c. Frecuencia de actualización del perfil de riesgo	AG02	a. Frecuencia de actualización del perfil de riesgo b. Porcentaje de evaluaciones de riesgo empresarial que incluyen el riesgo relacionado con I&T c. Número de incidentes significativos relacionados con I&T que no se identificaron en la evaluación de riesgos
EG06	a. Número de interrupciones del servicio al cliente o procesos empresariales que causan incidentes significativos b. Coste de los incidentes para el negocio c. Número de horas de procesamiento perdidas en el negocio debido a interrupciones no planificadas del servicio d. Porcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados	AG07	a. Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o descrédito público b. Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o descrédito público c. Número de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o descrédito público

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
DSS05.01 Proteger contra software malicioso Implementar y mantener en toda la empresa medidas preventivas, detectivas y correctivas (especialmente parches de seguridad y control de virus actualizados) para proteger los sistemas de información y la tecnología del software malicioso (p. ej., ransomware, malware, virus, gusanos, spyware y spam).		a. Número de ataques exitosos de software malicioso b. Porcentaje de empleados que no pasan las pruebas de ataques maliciosos (p. ej., la prueba de correos electrónicos de phishing)
Actividades		Nivel de capacidad
1. Instalar y activar herramientas de protección contra software malicioso en todas las instalaciones de procesamiento, con archivos de definición de software malicioso que se actualizan según sea necesario (automáticamente o semiautomáticamente)		2
2. Filtrar el tráfico de entrada, como el correo electrónico y las descargas, para protegerlo de información no solicitada (p.ej. spyware, correos electrónicos de phishing).		
3. Comunicar acerca de concienciación sobre software malicioso y hacer cumplir los procedimientos y responsabilidades de prevención. Impartir formación periódica sobre malware en el uso de correo electrónico e Internet. Formar a los usuarios para que no abran e informen sobre correos electrónicos sospechosos y no instalen software compartido o no aprobado.		3
4. Distribuir todo el software de protección centralmente (versión y parches) usando una configuración centralizada y la gestión de cambios de TI.		
5. Revisar y evaluar la información sobre nuevas amenazas potenciales (p. ej., revisión de los consejos de seguridad de productos y servicios de proveedores) de forma regular.		4
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		DP.DC Detect Malicious Code; RI.VT Vulnerability and Threat Identification
HITRUST CSF versión 9, septiembre de 2017		09.04 Protection Against Malicious & Mobile Code
SF, The Standard of Good Practice for Information Security 2016		TS1 Security Solutions
SO/IEC 27002:2013/Cor.2:2015(E)		12.2 Protection against malware
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016		CSC 4: Continuous Vulnerability Assessment and Remediation; CSC 8: Malware Defenses

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
DSS05.02 Gestionar la seguridad de la conectividad y de la red. Usar medidas de seguridad y procedimientos de gestión relacionados para proteger la información a través de todos los métodos de conectividad.		a. Número de brechas del firewall b. Número de vulnerabilidades descubiertas c. Porcentaje de tiempo que la red y los sistemas no están disponibles debido a incidentes de seguridad
Actividades		Nivel de capacidad
1. Permitir que solo los dispositivos autorizados tengan acceso a la información corporativa y a la red de la empresa. Configurar estos dispositivos para forzar la introducción de contraseña.		2
2. Implementar mecanismos de filtrado de red, como firewalls y software de detección de intrusos. Hacer cumplir las políticas adecuadas para controlar el tráfico entrante y saliente.		
3. Aplicar protocolos de seguridad aprobados a las conexiones de red.		
4. Configurar el equipo de red de forma segura.		
5. Encriptar la información en tránsito de acuerdo a su clasificación.		3
6. Establecer y mantener una política para la seguridad de la conectividad con base en las evaluaciones de riesgo y los requisitos del negocio.		
7. Establecer mecanismos confiables para apoyar la transmisión y recepción segura de la información.		
8. Llevar a cabo pruebas de penetración periódicas para determinar la idoneidad de la protección de la red.		4
9. Llevar a cabo pruebas periódicas a la seguridad del sistema para determinar la idoneidad de la protección del sistema.		
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018	AC.MI Manage Network Integrity & Segregation; CM.MN Monitor Networks; AC.CP Manage Communication Protections	
HITRUST CSF versión 9, septiembre de 2017	01.04 Network Access Control	
ISF, The Standard of Good Practice for Information Security 2016	PA2.3 Mobile Device Connectivity; NC1.1 Network Device Configuration	
ISO/IEC 27002:2013/Cor.2:2015(E)	13.1 Network security management	
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.20 System and information integrity (SI-8)	
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016	CSC 9: Limitation and Control of Network Ports, Protocols, and Services; CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	
Práctica de gestión		Métricas modelo
DSS05.03 Gestionar la seguridad de endpoint. Garantizar que los dispositivos de punto final (Endpoint, término en inglés) (p. ej., ordenador portátil, ordenador de sobremesa, servidor y otros dispositivos móviles o de red o software) tengan una seguridad a un nivel igual o superior al de los requisitos de seguridad definidos para la información procesada, almacenada o transmitida.		a. Número de incidentes que involucran a dispositivos endpoint b. Número de dispositivos no autorizados detectados en la red o en el entorno de usuario final c. Porcentaje de personas que reciben formación de concienciación relacionada con el uso de dispositivos endpoint
Actividades		Nivel de capacidad
1. Configurar los sistemas operativos de forma segura.		2
2. Implementar mecanismos de bloqueo de dispositivos.		
3. Gestionar el acceso y control remotos (p.ej. dispositivos móviles, teletrabajo)		
4. Gestionar la configuración de red de forma segura.		
5. Implementar el filtrado de tráfico de red en dispositivos de punto final.		
6. Proteger la integridad del sistema.		
7. Proporcionar protección física a los dispositivos de punto final.		
8. Eliminar de forma segura los dispositivos Endpoint		
9. Gestionar el acceso malicioso a través del correo electrónico y los navegadores web. Por ejemplo, bloquear determinados sitios web y desactivar los clics a enlaces para los smartphones.		
10. Encriptar la información almacenada de acuerdo a su clasificación.		3

A. Componente: Proceso (cont.)		
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		IPMM Apply Mobile Device Management; TP:MP Apply Media Protection; DP:DP Detect Mobile Code and Browser Protection
ISF, The Standard of Good Practice for Information Security 2016		PM1.3 Remote Working; PA2.1 Mobile Device Configuration; PA2.4 Employee-owned Devices; PA2.5 Portable Storage Devices; NC1.6 Remote Maintenance
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.4 Assessment, authorization and monitoring (CA-8, CA-9); 3.19 System and communications protection (SC-10)
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016		CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers; CSC 7: Email and Web Browser Protections
Práctica de gestión		Métricas modelo
DSS05.04: Gestionar la identidad del usuario y el acceso lógico. Asegurarse de que todos los usuarios tienen derechos de acceso a la información de acuerdo con los requisitos del negocio. Coordinarse con las unidades del negocio que gestionan sus propios derechos de acceso en los procesos de negocio.		a. Tiempo promedio entre el cambio y la actualización de cuentas b. Número de cuentas (vs. número de usuarios/personal autorizado) c. Número de incidentes relacionados con el acceso no autorizado a la información
Actividades		Nivel de capacidad
1. Mantener los derechos de acceso de los usuarios de acuerdo con la función del negocio, los requisitos del proceso y las políticas de seguridad. Alinear la gestión de identidades y derechos de acceso con los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad-de-tener y necesidad-de-conocer.		2
2. Administrar oportunamente todos los cambios en los derechos de acceso (creación, modificación y eliminación), basándose únicamente en transacciones aprobadas y documentadas que hayan sido autorizadas por personas designadas por la dirección.		3
3. Segregar, reducir al mínimo necesario y gestionar activamente cuentas de usuario privilegiadas. Asegurar la supervisión de todas las actividades en estas cuentas.		
4. Identificar de forma unívoca y por roles funcionales todas las actividades de procesamiento de información. Coordinarse con las unidades de negocio para asegurarse de que todos los roles están definidos de manera consistente, incluidos los roles definidos por el propio negocio dentro de las aplicaciones de procesos del negocio.		
5. Autenticar todo el acceso a activos de información de acuerdo con el rol del individuo o a las reglas del negocio. Coordinarse con las unidades de negocio que gestionan la autenticación dentro de las aplicaciones utilizadas en los procesos de negocio, con el fin de asegurar que los controles de autenticación hayan sido administrados adecuadamente.		
6. Garantizar que todos los usuarios (internos, externos y temporales) y su actividad en los sistemas de TI (aplicación de negocio, infraestructura de TI, operaciones, desarrollo y mantenimiento de sistemas) se puedan identificar de manera unívoca.		4
7. Mantener un registro de auditoría del acceso a la información dependiendo de su sensibilidad y de los requisitos regulatorios.		
8. Llevar a cabo revisiones gerenciales periódicas de todas las cuentas y privilegios relacionados.		
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
HITRUST CSF versión 9, septiembre de 2017		10.03 Cryptographic Controls
ISF, The Standard of Good Practice for Information Security 2016		PM1.1 Employment Life Cycle; SA1 Access Management
ISO/IEC 27002:2013/Cor.2:2015(E)		7.3 Termination and change of employment; 9. Access control
ITIL V3, 2011		Service Operation, 4.5 Access Management
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.1 Access control (AC-11, AC-12); 3.11 Media protection (MP-2, MP-4, MP-7); 3.13 Physical and environmental protection (PE-2, PE-3, PE-6)
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016		CSC 1: Inventory of Authorized and Unauthorized Devices; CSC 2: Inventory of Authorized and Unauthorized Software; CSC 5: Controlled Use of Administrative Privileges; CSC 16: Account Monitoring and Control

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
DSS05.05 Gestionar el acceso físico a los activos de I&T. Definir e implantar procedimientos (incluyendo procedimientos de emergencia) para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas, de acuerdo con las necesidades del negocio. El acceso a las instalaciones, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Este requisito aplica a todas las personas que accedan a las instalaciones, incluyendo personal interno, personal temporal, clientes, proveedores, visitantes y cualquier otro tercero.		a. Calificación promedio de las evaluaciones de seguridad física b. Número de incidentes relacionados con la seguridad de la información física
Actividades		Nivel de capacidad
1. Registrar y monitorizar todos los puntos de entrada a las instalaciones de TI. Registrar a todos los visitantes al sitio, incluidos contratistas y proveedores.		2
2. Asegurar que todo el personal muestra una identificación debidamente autorizada en todo momento.		
3. Requerir a los visitantes que estén acompañados en todo momento durante su estancia en las instalaciones.		
4. Restringir y monitorizar el acceso a instalaciones sensibles de TI, mediante el establecimiento de restricciones al perímetro, como vallas, paredes y dispositivos de seguridad en puertas interiores y exteriores.		
5. Gestionar solicitudes para permitir el acceso debidamente autorizado a las instalaciones de cómputo.		3
6. Garantizar que los perfiles de acceso permanezcan actualizados. Basar el acceso a las instalaciones de TI (sala de servidores, edificios, áreas o zonas) en el cargo y las responsabilidades.		
7. Realizar formación sobre concienciación de la seguridad de la información física de forma regular.		
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		AC.MA Manage Access; ID.DI Determine Impacts
HITRUST CSF versión 9, septiembre de 2017		01.01 Business Requirement for Access Control; 01.02 Authorized Access to Information Systems; 02.0 Human Resources Security
ISF, The Standard of Good Practice for Information Security 2016		NC1.2 Physical Network Management
ISO/IEC 27002:2013/Cor.2:2015(E)		11. Physical and environmental security
Práctica de gestión		Métricas modelo
DSS05.06: Gestionar documentos sensibles y dispositivos de salida. Establecer protecciones físicas apropiadas, prácticas contables y gestión de inventario relativa a activos sensibles de I&T, como formas especiales, instrumentos negociables, impresoras para fines especiales o tokens de seguridad.		a. Número de dispositivos de salida robados. b. Porcentaje de documentos sensibles y dispositivos de salida identificados en el inventario
Actividades		Nivel de capacidad
1. Establecer procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa.		2
2. Asegurar que se han establecido controles criptográficos para proteger información sensible almacenada electrónicamente.		
3. Asignar privilegios de acceso a documentos sensibles y dispositivos de salida con base en el principio de menor privilegio, manteniendo un equilibrio entre el riesgo y los requisitos del negocio.		3
4. Establecer un inventario de documentos sensibles y dispositivos de salida y realizar reconciliaciones periódicas.		
5. Establecer salvaguardas físicas adecuadas para documentos sensibles.		

A. Componente: Proceso (cont.)		
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		CM.Ph Monitor Physical
HITRUST CSF versión 9, septiembre de 2017		01.06 Application & Information Access Control; 01.07 Mobile Computing & Teleworking; 08.0 Physical & Environmental Security; 10.03 Cryptographic Controls; 10.04 Security of System Files
ISF, The Standard of Good Practice for Information Security 2016		IR2.3 Business Impact Assessment - Confidentiality Requirements; IR2.4 Business Impact Assessment - Integrity Requirements; IR2.5 Business Impact Assessment - Availability Requirements; IM2.2 Sensitive Physical Information; PA2.2 Enterprise Mobility Man
ISO/IEC 27002:2013/Cor.2:2015(E)		10. Cryptography
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.1 Access control (AC-2, AC-3, AC-4, AC-5, AC-6, AC-13, AC-24); 3.7 Identification and authentication (IA-2, IA-10, IA-11)
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016		CSC 15: Wireless Access Control
Práctica de gestión		Métricas modelo
DSS05.07 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad. Mediante el uso de un portafolio de herramientas y tecnologías (p.ej. herramientas de detección de intrusión), gestionar las vulnerabilidades y monitorizar la infraestructura para detectar accesos no autorizados. Asegurar que las herramientas, tecnologías y detección de seguridad están integradas en la monitorización general de eventos y la gestión de incidentes.		a. Número de pruebas de vulnerabilidad llevadas a cabo en dispositivos perimetrales b. Número de vulnerabilidades descubiertas durante las pruebas c. Tiempo dedicado a remediar vulnerabilidades d. Porcentaje de tickets creados de forma oportuna cuando los sistemas de monitorización identifican posibles incidentes de seguridad.
Actividades		Nivel de capacidad
1. Usar de forma continua un portafolio de tecnologías, servicios y activos soportados (p. ej., escáneres de vulnerabilidad, fuzzers y sniffers, analizadores de protocolos) para identificar vulnerabilidades de seguridad de la información.		2
2. Definir y comunicar escenarios de riesgo para que se puedan reconocer con facilidad y se pueda entender su probabilidad e impacto.		
3. Revisar regularmente los logs de eventos para detectar posibles incidentes.		
4. Garantizar que se creen tickets relativos a incidentes de seguridad de forma oportuna cuando la monitorización identifique posibles incidentes.		
5. Registrar eventos relacionados con la seguridad y conservar los registros durante el periodo de tiempo apropiado.		3
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
ISF, The Standard of Good Practice for Information Security 2016		IR2.6 Threat Profiling
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.7 Identification and authentication (IA-3); 3.11 Media protection (MP-1); 3.13 Physical and environmental protection (PE-5); 3.19 System and communications protection (SC-15)
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016		Maintenance, Monitoring, and Analysis of Audit Logs

B. Componente: Estructuras organizativas									
	Director de TI	Director de seguridad de la información	Dueños del proceso de negocio	Director de Recursos Humanos	Jefe de desarrollo	Jefe de operaciones de TI	Gestor de seguridad de la información	Director de privacidad	
Práctica clave de gestión									
DSS05.01 Proteger contra software malicioso		A	R	R	R	R	R		
DSS05.02 Gestionar la seguridad de la conectividad y de la red.		A			R	R	R		
DSS05.03 Gestionar la seguridad de endpoint.		A			R	R	R		
DSS05.04 Gestionar la identidad del usuario y el acceso lógico.		A	R			R	R	R	
DSS05.05 Gestionar el acceso físico a los activos de I&T.		A				R	R	R	
DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	A					R		R	
DSS05.07 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad.		A				R	R	R	
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica							
Sin documentación relacionada para este componente.									

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS05.01 Proteger contra software malicioso			Política de prevención de software malicioso	AP001.02
			Evaluaciones de amenazas potenciales	AP012.02; AP012.03
DSS05.02 Gestionar la seguridad de la conectividad y de la red.	AP001.07	Directrices de clasificación de datos	Política de seguridad de la conectividad	AP001.02
	AP009.03	SLAs	Resultados de pruebas de penetración	MEA04.07
DSS05.03 Gestionar la seguridad de endpoint.	AP003.02	Modelo de arquitectura de la información	Políticas de seguridad para dispositivos Endpoint	AP001.02
	AP009.03	• SLAs • OLAs		
	BAI09.01	Resultados de comprobaciones de inventario físicas		
	DSS06.06	Informes de violaciones		
DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	AP001.05	Definición de roles y responsabilidades relacionadas con I&T	Resultados de revisiones de cuentas de usuarios y privilegios	Interna
	AP003.02	Modelo de arquitectura de la información	Derechos de acceso de usuario aprobados	Interna

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
DSS05.05 Gestionar el acceso físico a los activos de I&T.	De	Descripción	Descripción	A
			Registros de acceso	DSS06.03, MEA04.07
			Solicitudes de acceso aprobadas	Interna
DSS05.06: Gestionar documentos sensibles y dispositivos de salida.	APO03.02	Modelo de arquitectura de la información	Privilegios de acceso	Interna
			Inventario de documentos y dispositivos sensibles	Interna
DSS05.07 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad.			Tickets relacionados con incidentes de seguridad	DSS02.02
			Características de los incidentes de seguridad	Interna
			Logs de eventos de seguridad	Interna
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica		
Sin documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)	Referencia específica
Seguridad de la información	Skills Framework for the Information Age V6, 2015	SCTY
Gestión de seguridad de la información	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage— E.8. Information Security Management
Pruebas de penetración	Skills Framework for the Information Age V6, 2015	PENT
Administración de seguridad	Skills Framework for the Information Age V6, 2015	SCAD

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de seguridad de la información	Establecer directrices para proteger la información corporativa y los sistemas e infraestructura asociados.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Crear una cultura de concienciación con respecto a la responsabilidad del usuario de mantener prácticas de seguridad y de privacidad.	1) HITRUST CSF versión 9, septiembre de 2017; (2) ISF, The Standard of Good Practice for Information Security 2016	(1) 01.03 User Responsibilities; (2) PM2.1 Security Awareness Program

G. Componente: Servicios, infraestructuras y aplicaciones	
<ul style="list-style-type: none"> • Servicios de directorio • Sistemas de filtrado de correo electrónico • Sistema de gestión de acceso e identidad • Servicios de concienciación sobre seguridad • Herramientas de seguridad de la información y de gestión de eventos (SIEM) • Servicios del centro de operaciones de seguridad (SOC) • Servicios de evaluación de seguridad de terceros • Sistemas de filtrado de URL 	

Página dejada en blanco intencionadamente

Dominio: Entregar, dar servicio y soporte Objetivo de gestión: DSS06 - Gestionar los controles de procesos de negocio		Área prioritaria: Modelo Core de COBIT
Descripción		
Definir y mantener los controles apropiados de los procesos de negocio para asegurar que la información relacionada y procesada por procesos de negocio internos o externalizados cumpla con todos los requisitos relevantes de control de la información. Identificar los requisitos relevantes de control de la información. Gestionar y operar los controles adecuados de entrada, throughput y salida (controles de aplicación) para asegurar que la información y el procesamiento de la información cumpla con estos requisitos.		
Propósito		
Mantener la integridad de la información y la seguridad de los activos de información manejados dentro de los procesos de negocio, dentro de la empresa u operación externalizada.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales	➔	Metas de alineamiento
<ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG05 Cultura de servicio orientada al cliente • EG08 Optimización de la funcionalidad de procesos internos del negocio • EG12 Programas de transformación digital gestionados 		AG08 Habilitar y dar soporte a procesos de negocio mediante la integración de aplicaciones y tecnología
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios		AG08 a. Plazo para la ejecución de servicios y procesos empresariales b. Número de programas empresariales facilitados por I&T retrasados o que incurren en costes adicionales debido a problemas de integración tecnológica c. Número de cambios en los procesos de negocio que se deben aplazar o revisar debido a problemas de integración tecnológica d. Número de aplicaciones o infraestructuras críticas que operan en silos y no están integradas
EG05 a. Número de interrupciones del servicio al cliente b. Porcentaje de partes interesadas del negocio satisfechas de que la prestación de servicios al cliente cumpla con los niveles acordados c. Número de quejas de clientes d. Tendencia de los resultados de la encuesta de satisfacción al cliente		
EG08 a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarial b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro		
EG12 a. Número de programas ejecutados a tiempo y dentro del presupuesto b. Porcentaje de partes interesadas satisfechas con la ejecución del programa c. Porcentaje de programas de transformación del negocio parados d. Porcentaje de programas de transformación del negocio con actualizaciones regulares del estado reportado		

A. Componente: Proceso	
Práctica de gestión	Métricas modelo
DSS06.01 Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales. Evaluar y monitorizar continuamente la ejecución de las actividades de los procesos de negocio y los controles relacionados (basados en el riesgo empresarial) para asegurarse de que los controles de procesamiento están alineados con las necesidades del negocio.	a. Porcentaje de inventario de procesos críticos y controles clave completado b. Porcentaje de controles de procesamiento alineados con las necesidades empresariales

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Identificar y documentar las actividades de control necesarias para procesos clave del negocio para satisfacer los requisitos de control para los objetivos estratégicos, operativos, de reporte y de cumplimiento.	2
2. Priorizar las actividades de control de acuerdo al riesgo inherente al negocio. Identificar controles clave.	
3. Garantizar la propiedad de las actividades de control clave.	
4. Implementar controles automáticos.	3
5. Monitorizar continuamente las actividades de control de principio a fin para identificar oportunidades de mejora.	4
6. Mejorar de forma continua el diseño y operación de los controles de proceso del negocio.	5
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)	Referencia específica
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018	3.1 Preparation (Task 10, 11)
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016	CSC 14: Controlled Access Based on the Need to Know
Práctica de gestión	Métricas modelo
DSS06.02: Controlar el procesamiento de información. Gestionar la ejecución de las actividades de los procesos del negocio y los controles relacionados, con base en el riesgo empresarial. Garantizar que el procesamiento de información sea válido, completo, preciso, oportuno y seguro (p. ej., refleja el uso legítimo y autorizado del negocio).	a. Número de incidentes y hallazgos de auditoría que indican un fallo de los controles clave b. Porcentaje de cobertura de controles clave dentro de los planes de prueba
Actividades	Nivel de capacidad
1. Autenticar al originador de las transacciones y comprobar que el individuo tiene la autoridad para originar la transacción.	2
2. Garantizar una adecuada segregación de tareas con relación al origen y aprobación de las transacciones.	
3. Comprobar que las transacciones son precisas, completas y válidas. Los controles podrían incluir secuencia, límite, rango, validez, razonabilidad, comprobación de tablas, existencia, verificación de clave, dígito de verificación, completitud, comprobaciones de duplicados y relaciones lógicas y ediciones temporales. Los criterios y parámetros de validación deberían estar sujetos a revisiones y confirmaciones periódicas. Validar los datos de entrada y editarlos o, cuando sea aplicable, devolverlos para su corrección lo más cerca posible del punto de origen.	3
4. Sin comprometer los niveles de autorización de la transacción original, corregir y reenviar los datos que se introdujeron de forma errónea. Cuando sea adecuado para la reconstrucción, conservar documentos fuente originales durante el periodo de tiempo adecuado.	
5. Mantener la integridad y la validez de los datos durante el ciclo de procesamiento. Asegurar que la detección de transacciones erróneas no interrumpa el procesamiento de transacciones válidas.	
6. Manipular el resultado de forma autorizada, entregarlo al destinatario adecuado y proteger la información durante la transmisión. Verificar la exactitud e integridad del resultado.	
7. Mantener la integridad de los datos durante interrupciones inesperadas en el procesamiento del negocio. Confirmar la integridad de los datos después de fallos en el procesamiento.	
8. Antes de pasar datos de transacciones entre aplicaciones internas y funciones operativas/de negocio (dentro o fuera de la empresa), comprobar el trato adecuado, la autenticidad del origen y la integridad del contenido. Mantener la autenticidad y la integridad durante la transmisión o el transporte.	
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)	Referencia específica
HITRUST CSF versión 9, septiembre de 2017	13.01 Openness and Transparency; 13.02 Individual Choice and Participation
ISF, The Standard of Good Practice for Information Security 2016	BA1.4 Information Validation

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad. Gestionar los roles de negocio, responsabilidades, niveles de autoridad y segregación de funciones necesarias para apoyar los objetivos de los procesos de negocio. Autorizar el acceso a todos los activos de información relacionados con los procesos de información del negocio, incluidos aquellos bajo custodia del negocio, de TI y de terceros. Esto asegura que la empresa sepa dónde están los datos y quién está manejando los datos en su nombre.		a. Número de incidentes y hallazgos de auditoría debido a violaciones de acceso o de separación de funciones b. Porcentaje de roles de procesos de negocio con derechos de acceso y niveles de autoridad asignados c. Porcentaje de roles de proceso de negocio con clara separación de funciones
Actividades		Nivel de capacidad
1. Asignar roles y responsabilidades conforme a las descripciones del cargo y las actividades aprobadas del proceso de negocio.		2
2. Asignar niveles de autoridad para la aprobación de transacciones, límites de transacción y cualquier otra decisión relacionada con el proceso de negocio, conforme a roles de trabajo aprobados.		
3. Asignar roles para actividades sensibles para que haya una clara segregación de funciones.		
4. Asignar derechos de acceso y privilegios basado en lo mínimo requerido para realizar las actividades laborales, conforme a roles de trabajo predefinidos. Eliminar o revisar derechos de acceso de forma inmediata si el rol de trabajo cambia o si un miembro del personal deja el área de proceso de negocio. Revisar periódicamente para asegurar que el acceso sea adecuado para las amenazas, riesgo, tecnología y necesidades empresariales actuales.		3
5. Concienciar y formar regularmente sobre los roles y responsabilidades, para que todos entiendan sus responsabilidades; la importancia de los controles; y la seguridad, integridad, confidencialidad y privacidad de la información de la compañía en todas sus formas.		
6. Garantizar que los privilegios administrativos están asegurados, rastreados y controlados de forma suficiente y eficaz para prevenir el mal uso.		
7. Revisar periódicamente las definiciones de control de acceso, los logs y los informes de excepción. Asegurar que todos los privilegios de acceso son válidos y están alineados con los miembros actuales del personal y sus roles asignados.		4
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
HITRUST CSF versión 9, septiembre de 2017		13.04 Collection, Use and Disclosure
ISO/IEC 27002:2013/Cor.2:2015(E)		7. Human resource security
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016		CSC 5: Controlled Use of Administrative Privileges
Práctica de gestión		Métricas modelo
DSS06.04 Gestionar errores y excepciones. Gestionar las excepciones y los errores del proceso del negocio y facilitar su corrección, mediante la ejecución de las acciones correctivas definidas y su escalamiento, si fuera necesario. Este tratamiento de excepciones y errores ofrece garantía de la precisión e integridad de los procesos de información del negocio.		a. Frecuencia de las ineficiencias de procesamiento debido a entradas de datos incompletas b. Número de errores detectados a tiempo c. Número de errores de procesamiento de datos que se solucionaron de forma eficiente
Actividades		Nivel de capacidad
1. Revisar errores, excepciones y desviaciones.		2
2. Hacer un seguimiento, corregir, aprobar y reenviar los documentos fuente y las transacciones.		
3. Mantener evidencia de acciones correctivas.		
4. Definir y mantener procedimientos para asignar la propiedad de errores y excepciones, corregir errores, anular errores y manejar condiciones fuera del balance.		3
5. Informar de manera oportuna sobre errores relevantes de procesamiento de la información del negocio para realizar un análisis de causa raíz y de tendencia.		4
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
DSS06.05 Asegurar la trazabilidad y la rendición de cuentas de los eventos de información. Asegurarse de que la información de negocio puede rastrearse hasta el evento de negocio que la originó y se puede asociar a las partes que rinden cuentas. Esta capacidad de descubrimiento ofrece la garantía de que la información de negocio es confiable y que se ha tratado de acuerdo con los objetivos definidos.		a. Número de incidentes en los que no se puede recuperar el historial de transacciones b. Porcentaje de integridad del log de transacciones rastreables
Actividades		Nivel de capacidad
1. Obtener la información fuente, evidencias de soporte y el registro de transacciones.		2
2. Definir los requisitos de retención de acuerdo a los requisitos del negocio para cumplir con las necesidades operativas, de reportes financieros y de cumplimiento.		3
3. Disponer de la información fuente, las evidencias de soporte y el registro de las transacciones conforme a la política de retención.		
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
DSS06.06 Asegurar los activos de información. Asegurar los activos de información accesibles por el negocio a través de métodos aprobados, incluyendo información en formato electrónico (p.ej. dispositivos de medios portátiles, aplicaciones de usuarios y dispositivos de almacenamiento, u otros métodos que crean nuevos activos de cualquier tipo), información en formato físico (p.ej. documentos fuente o informes de salida) e información durante el tránsito. Esto beneficia al negocio porque ofrece una protección de principio a fin de la información.		a. Casos de datos de transacciones sensibles enviados al destinatario erróneo b. Frecuencia de integridad de datos críticos comprometida
Actividades		Nivel de capacidad
1. Restringir el uso, distribución y el acceso físico a la información de acuerdo con su clasificación.		2
2. Proporcionar una concienciación y formación adecuada sobre el uso.		
3. Aplicar las políticas y procedimientos de seguridad para la clasificación y uso aceptable de datos y para proteger los activos de información que están bajo control del negocio.		3
4. Identificar e implantar procesos, herramientas y técnicas para verificar el cumplimiento de forma razonable.		
5. Informar al negocio y a otras partes interesadas sobre violaciones y desviaciones.		4
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		AC.MP Manage Access Permissions
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016		CSC 18: Application Software Security

B. Componente: Estructuras organizativas									
	Comité Ejecutivo	Director de TI	Consejo de gobierno de I&T	Director de seguridad de la información	Dueños del proceso de negocio	Función de gestión de datos	Gestor de servicios	Gestor de seguridad de la información	Asesor jurídico
Práctica clave de gestión									
DSS06.01 Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales.	R		A		R				
DSS06.02 Controlar el procesamiento de información.		R	A	R	R	R			R
DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad.		R	A	R	R			R	
DSS06.04 Gestionar errores y excepciones.		R		R	A		R		
DSS06.05 Asegurar la trazabilidad y la rendición de cuentas de los eventos de información.		R		R	A				
DSS06.06 Asegurar los activos de información.		R		R	A				
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)	Referencia específica								
Sin documentación relacionada para este componente.									

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS06.01 Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales.	APO01.07	<ul style="list-style-type: none"> Directrices de clasificación de datos Procedimientos de integridad de datos 	Análisis de causa raíz y recomendaciones	BAI06.01; MEA02.04; MEA04.04; MEA04.06; MEA04.07
			Resultados de las revisiones de la efectividad del procesamiento	MEA02.04
DSS06.02: Controlar el procesamiento de información.	BAI05.05	Plan de operación y uso	Informes de control del procesamiento	Interna
	BAI07.02	Plan de migración		
DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad.	APO11.01	Roles, responsabilidades y derechos de decisión del sistema de gestión de la calidad (SGC)	Niveles de autoridad asignados	APO01.05
	APO13.01	Declaración del alcance del sistema de gestión de seguridad de la información (SGSI)	Roles y responsabilidades asignados	APO01.05
	DSS05.05	Logs de acceso	Derechos de acceso asignados	APO07.04
	EDM04.02	Responsabilidades asignadas para la gestión de recursos		

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
DSS06.04 Gestionar errores y excepciones.	De	Descripción	Descripción	A
			Informes de error y análisis de causa raíz	Interna
			Evidencia de corrección y solución de errores	MEA02.04
DSS06.05 Asegurar la trazabilidad y la rendición de cuentas de los eventos de información.			Registro de transacciones	Interna
			Requisitos de retención	Interna; AP014.09
DSS06.06 Asegurar los activos de información.			Informes de violaciones	DSS05.03
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica		
National Institute of Standards and Technology Special Publication 800-37, Revisión 2, septiembre de 2017		3.1 Preparation (Task 10, 11): Inputs and Outputs		

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)	Referencia específica
Seguridad de la información	Skills Framework for the Information Age V6, 2015	SCTY
Administración de seguridad	Skills Framework for the Information Age V6, 2015	SCAD

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Guía de los controles del negocio	Define los controles del proceso de negocio para garantizar un control adecuado y reducir el riesgo de fraude y errores. Identifica controles manuales para proteger documentos (p.ej. fuente, entrada, procesamiento y documentos de salida); identifica los controles de supervisión para revisar el flujo de documentos y garantizar su correcto procesamiento. Incluye controles generales de I&T (p.ej. seguridad física, acceso y autenticación y gestión de cambios) y controles de aplicación (p.ej. comprobación de edición, configuración del sistema y ajustes de seguridad).		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Crear una cultura que adopte la necesidad de controles sólidos en los procesos de negocio, mediante su incorporación en las aplicaciones en desarrollo o exigiéndolos en aplicaciones adquiridas o accedidas como un servicio. Animar a todos los empleados a que sean conscientes de los controles para proteger todos los activos de la organización (p.ej. registros en papel e instalaciones)		

G. Componente: Servicios, infraestructura y aplicaciones
<ul style="list-style-type: none"> • Controles automatizados de aplicación • Herramientas de auditoría de log de eventos

4.5 MONITORIZAR, EVALUAR Y VALORAR (MEA)

- 01 Gestionar la monitorización del rendimiento y la conformidad
- 02 Gestionar el sistema de control interno
- 03 Gestionar el cumplimiento de los requisitos externos
- 04 Gestionar el aseguramiento

Página dejada en blanco intencionadamente

Dominio: Monitorizar, evaluar y valorar Objetivo de gestión: MEA01 – Gestionar la supervisión del rendimiento y la conformidad		Área prioritaria: Modelo Core de COBIT
Descripción		
Recopilar, validar y evaluar las metas y métricas de alineamiento de la empresa. Supervisar que los procesos y las prácticas se desempeñen según las metas y métricas de rendimiento y conformidad acordadas. Proporcionar informes sistemáticos y oportunos.		
Propósito		
Proporcionar transparencia en el rendimiento y la conformidad e impulsar la consecución de las metas.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales <ul style="list-style-type: none"> • EG01 Portafolio de productos y servicios competitivos • EG04 Calidad de la información financiera • EG07 Calidad de la información de gestión • EG08 Optimización de la funcionalidad de procesos internos del negocio 	➔	Metas de alineamiento <ul style="list-style-type: none"> • AG05 Prestación de servicios de I&T conforme a los requisitos del negocio • AG10 Calidad de la información de gestión de I&T
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG01 a. Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado b. Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente c. Porcentaje de productos y servicios que proporcionan una ventaja competitiva d. Plazo de comercialización para nuevos productos y servicios		AG05 a. Porcentaje de partes interesadas del negocio satisfechas con que la prestación del servicio de I&T cumpla con los niveles de servicio acordados b. Número de interrupciones del negocio debido a incidentes de servicios de I&T c. Porcentaje de usuarios satisfechos con la calidad de la prestación del servicio de I&T
EG04 a. Encuesta de satisfacción de las partes interesadas clave con respecto a la transparencia, comprensión y precisión de la información financiera de la empresa b. Coste de incumplimiento con regulaciones relacionadas con finanzas		AG10 a. Nivel de satisfacción del usuario con la calidad, puntualidad y disponibilidad de la información de gestión relacionada con I&T, teniendo en cuenta los recursos disponibles b. Proporción y alcance de las decisiones erróneas de negocio en las que la información errónea o no disponible relacionada con I&T fue un factor clave c. Porcentaje de información que satisface los criterios de calidad
EG07 a. Grado de satisfacción del consejo de administración y la dirección ejecutiva con la información para la toma de decisiones b. Número de incidentes causados por decisiones erróneas de negocio basadas en información imprecisa c. Tiempo que se tarda en proporcionar información que respalde decisiones eficaces de negocio d. Puntualidad de la información de gestión		
EG08 a. Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso del negocio b. Niveles de satisfacción de los clientes con las capacidades de prestación de servicios c. Niveles de satisfacción de los proveedores con las capacidades de la cadena de suministro		

A. Componente: Proceso	
Práctica de gestión	Métricas modelo
MEA01.01 Establecer un enfoque de supervisión. Involucrar a las partes interesadas a fin de establecer y mantener un enfoque de supervisión para definir los objetivos, el alcance y el método con los que medir la solución del negocio, la entrega de servicios y la contribución a los objetivos de la empresa. Integrar este enfoque con el sistema de gestión de rendimiento corporativo.	a. Porcentaje de procesos con metas y métricas definidos b. Porcentaje de integración del enfoque de supervisión en el sistema de gestión de rendimiento corporativo

A. Componente: Proceso (cont.)		
Actividades		Nivel de capacidad
1. Identificar a las partes interesadas (p. ej., dirección, dueños del proceso y usuarios).		2
2. Colaborar con las partes interesadas y comunicar los requisitos y objetivos empresariales de supervisión, recopilación y reporte, por medio del uso de definiciones comunes (p. ej., glosario empresarial, metadatos y taxonomía), análisis de referencia y benchmarking.		
3. Alinear y mantener continuamente el enfoque de supervisión y evaluación con el enfoque de la empresa y las herramientas a utilizar para la recopilación de datos y la generación de informes empresariales (p. ej., aplicaciones de inteligencia de negocio).		
4. Acordar los tipos de metas y métricas (p. ej., conformidad, rendimiento, valor, riesgo), taxonomía (clasificación y relaciones entre metas y métricas) y retención de datos (evidencia).		
5. Solicitar, priorizar y asignar recursos para la supervisión, considerar la idoneidad, eficiencia, efectividad y confidencialidad.		
6. Validar periódicamente el enfoque usado e identificar partes interesadas, requisitos y recursos nuevos o cambiados.		3
7. Acordar una gestión del ciclo de vida y un proceso de control de cambio para la supervisión y la presentación de informes. Incluir oportunidades de mejora para el reporte, métricas, enfoque, análisis de referencia y benchmarking.		
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
CMMI Data Management Maturity Model, 2014	Supporting Processes - Measurement and Analysis	
SF, The Standard of Good Practice for Information Security 2016	SI2 Security Performance	
ISO/IEC 27001:2013/Cor.2:2015(E)	9.1 Monitoring, measurement, analysis and evaluation	
ISO/IEC 27004:2016(E)	6. Characteristics; 7. Types of measures; 8. Processes	
ISO/IEC 38500:2015(E)	5.5 Principle 4: Performance; 5.6 Principle 5: Conformidad	
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018	3.1 Preparation (Task 13); 3.3 Selection (Task 2); 3.7 Monitoring (Task 1)	
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.4 Assessment, authorization and monitoring (CA-2, CA-7); 3.20 System and information integrity (SI-4)	
Práctica de gestión		Métricas modelo
MEA01.02 Establecer objetivos de rendimiento y conformidad. Trabajar con las partes interesadas para definir, revisar periódicamente, actualizar y aprobar los objetivos de rendimiento y conformidad dentro del sistema de medición de desempeño.		a. Porcentaje de metas y métricas aprobadas por las partes interesadas b. Porcentaje de procesos con revisión y mejora de la efectividad de metas y métricas
Actividades		Nivel de capacidad
1. Definir las metas y métricas. Revisarlas periódicamente con las partes interesadas para identificar cualquier elemento significativo faltante y definir la razonabilidad de objetivos y tolerancias.		2
2. Evaluar si las metas y métricas de gestión son adecuadas, es decir, específicas, medibles, alcanzables, relevantes y con tiempos determinados (SMART).		
3. Comunicar los cambios propuestos a los objetivos y tolerancias (relacionado con las métricas) de desempeño y conformidad con partes interesadas clave (p.ej. legal, auditoría, recursos humanos, ética, cumplimiento, finanzas) de debida diligencia.		
4. Publicar a los usuarios de esta información los objetivos y tolerancias modificados.		
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)		Referencia específica
CMMI Data Management Maturity Model, 2014	Supporting Processes - Process Management	
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.4 Assessment, authorization and monitoring (CA-5)	
Práctica de gestión		Métricas modelo
MEA01.03 Recopilar y procesar los datos de rendimiento y conformidad Recopilar y procesar datos oportunos y precisos alineados con los enfoques de la empresa.		a. Porcentaje de procesos críticos supervisados b. Porcentaje del entorno de controles que es supervisado, analizado comparativamente y mejorado para cumplir con los objetivos de la organización

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Recopilar datos de procesos definidos (automatizados, cuando sea posible).	2
2. Evaluar la eficiencia (esfuerzo con relación a la visión proporcionada) y la idoneidad (utilidad y significado) de los datos recopilados y validar la integridad de los datos (precisión y completitud).	
3. Agregar datos para respaldar la medición de métricas acordadas.	
4. Alinear los datos agregados al enfoque y objetivos del reporte empresarial.	3
5. Usar herramientas y sistemas adecuados para el procesamiento y análisis de datos.	4
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)	Referencia específica
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.20 System and information integrity (SI-2)
Práctica de gestión	Métricas modelo
MEA01.04 Analizar e informar sobre el rendimiento. Revisar e informar periódicamente sobre el rendimiento en comparación con los objetivos. Usar un método que ofrezca una visión global sucinta del rendimiento de I&T y que se adapte al sistema de supervisión de la empresa.	a. Porcentaje de metas y métricas alineadas con el sistema de supervisión de la empresa b. Porcentaje de informes de desempeño enviados conforme al plazo c. Porcentaje de procesos con resultado asegurado en línea con los objetivos y dentro de las tolerancias
Actividades	Nivel de capacidad
1. Diseñar informes de desempeño de proceso que sean concisos, fáciles de entender y personalizados conforme a las distintas necesidades de la dirección y audiencias. Facilitar una toma de decisiones efectiva y oportuna (p.ej. cuadros de mando, informes light de semáforos). Asegurar que la causa y el efecto entre las metas y las métricas se comunica de forma comprensible.	3
2. Distribuir informes a las partes interesadas relevantes.	4
3. Analizar la causa de las desviaciones con respecto a los objetivos, iniciar medidas correctivas, asignar responsabilidades para su corrección y hacer seguimiento. En los momentos oportunos, revisar todas las desviaciones y buscar las causas raíz, cuando sea necesario. Documentar los problemas para mayor orientación por si el problema se repite. Documentar los resultados.	
4. Cuando sea posible, integrar el desempeño y el cumplimiento en los objetivos de desempeño de los miembros del personal y vincular el logro de los objetivos de desempeño al sistema de compensación de recompensas organizativo.	
5. Comparar los valores de desempeño con los objetivos y benchmarks internos y, cuando sea posible, con los benchmarks externos (industria y competidores clave).	
6. Analizar tendencias de desempeño y cumplimiento y tomar las medidas oportunas.	5
7. Recomendar cambios a las metas y métricas, cuando corresponda.	
Documentación relacionada (Estándares, Marcos, Requisitos de Cumplimiento)	Referencia específica
CMMI Data Management Maturity Model, 2014	Supporting Processes - Measurement and Analysis
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.3 Audit and accountability (AU-6)
Práctica de gestión	Métricas modelo
MEA01.05 Asegurar la implementación de acciones correctivas. Ayudar a las partes interesadas a identificar, iniciar y rastrear las acciones correctivas para abordar las anomalías.	a. Número de anomalías recurrentes b. Número de acciones correctivas implementadas
Actividades	Nivel de capacidad
1. Revisar las respuestas, opciones y recomendaciones de la dirección para abordar problemas y desviaciones importantes.	2
2. Asegurar que se mantenga la asignación de responsabilidades para las acciones correctivas.	
3. Hacer un seguimiento a los resultados de las acciones comprometidas.	
4. Comunicar los resultados a las partes interesadas.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
ITIL V3, 2011	Continual Service Improvement, 4.1 The 7-Step Improvement Process
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018	3.7 Monitoring (Task 3)
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.3 Audit and accountability (AU-5)

B. Componente: Estructuras organizativas													
Práctica clave de gestión	Comité Ejecutivo	Director general ejecutivo	Director general financiero	Director de operaciones	Director de TI	Consejo de gobierno de I&T	Dueños del proceso de negocio	Gestor de relaciones	Jefe de desarrollo	Jefe de operaciones de TI	Gestor de servicios		
MEA01.01 Establecer un enfoque de supervisión.	R	A	R	R	R	R							
MEA01.02 Establecer los objetivos de rendimiento y conformidad.	A						R	R	R	R	R		
MEA01.03 Recopilar y procesar los datos de rendimiento y conformidad.					A		R	R	R	R	R		
MEA01.04 Analizar e informar sobre el rendimiento.					A		R	R	R	R	R		
MEA01.05 Asegurar la implementación de acciones correctivas.					A		R	R	R	R	R		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica												
Sin documentación relacionada para este componente.													

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
MEA01.01 Establecer un enfoque de supervisión.	EDM05.01	<ul style="list-style-type: none"> Evaluación de los requisitos de reporte de la empresa Principios de comunicación y reporte 	Metas y métricas de supervisión aprobadas	Interna
			Requisitos de supervisión	Interna
	EDM05.02	Reglas para la validación y aprobación de informes obligatorios		
	EDM05.03	Evaluación de la eficacia de la elaboración de informes		
MEA01.02 Establecer objetivos de rendimiento y conformidad.	AP001.11	Metas de rendimiento y métricas para el seguimiento de la mejora de los procesos	Supervisión de objetivos	Todos los APO; Todos los BAI; Todos los DSS; Todos los MEA

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
MEA01.03 Recopilar y procesar los datos de rendimiento y conformidad.	AP001.11	Evaluaciones de la capacidad de los procesos	Datos de supervisión procesados	Interna
	AP005.03	Informes de rendimiento del portafolio de inversiones		
	AP009.04	Informes de rendimiento del nivel de servicio		
	AP010.05	Resultados de la revisión de los mecanismos de supervisión del cumplimiento de los proveedores		
	BAI01.06	Resultados de las revisiones del rendimiento del programa		
	BAI04.04	Informes de revisión de disponibilidad, rendimiento y monitorización de la capacidad		
	BAI05.05	Medidas de éxito y resultados		
	DSS01.05	Informes de evaluación de instalaciones		
	DSS02.07	<ul style="list-style-type: none"> Estado de incidentes e informe de tendencias Estado de cumplimiento de peticiones e informe de tendencias 		
MEA01.04 Analizar e informar sobre el rendimiento.			Informes de desempeño	Todos los APO; Todos los BAI; Todos los DSS; Todos los MEA; EDM01.03
MEA01.05 Asegurar la implementación de acciones correctivas.	AP001.09	Acciones correctivas del incumplimiento	Acciones correctivas y tareas	Todos los APO; Todos los BAI; Todos los DSS; Todos los MEA
	EDM05.02	Directrices de escalamiento	Estado y resultados de las acciones	EDM01.03
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
National Institute of Standards and Technology Special Publication 800-37, Revisión 2, septiembre de 2017		3.1 Preparation (Task 13): Inputs and Outputs; 3.3 Selection (Task 2): Inputs and Outputs; 3.7 Monitoring (Task 1, Task 3): Inputs and Outputs		

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Revisión de conformidad	Skills Framework for the Information Age V6, 2015	CORE
Gestión de calidad de Tecnología de la información y las telecomunicaciones (ICT)	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.6. ICT Quality Management
Aseguramiento de la calidad	Skills Framework for the Information Age V6, 2015	QUAS

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de autoevaluación	Proporciona directrices a los responsables de gestión para evaluar las operaciones como parte del programa de mejora continua. Usado a menudo para informar internamente a los ejecutivos o al consejo de administración sobre capacidades, progresos y mejoras actuales, conforme a los requisitos del negocio. Se podrían usar evaluaciones durante o después de un programa de mejora de procesos (es decir, para evaluar el progreso luego de haber realizado una mejora).		
Política de protección de denunciantes	Fomentar que los empleados transmitan sus preocupaciones y preguntas con toda confianza. Garantiza a los empleados que recibirán una respuesta y podrán escalar sus preocupaciones si no están satisfechos con la respuesta. Garantiza que los empleados estén protegidos cuando informan sobre un problema y que no teman represalias.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Fomentar una cultura de mejora continua de los procesos del negocio y de I&T para lograr las metas de la organización y optimizar el rendimiento.		

G. Componente: Servicios, infraestructura y aplicaciones
<ul style="list-style-type: none"> • Sistema de medición del desempeño (p. ej., cuadro de mando integral, herramientas de gestión de competencias) • Herramientas de autoevaluación

Dominio: Monitorizar, evaluar y valorar Objetivo de gestión: MEA02 – Gestionar el sistema de control interno		Área prioritaria: Modelo Core de COBIT
Descripción		
Supervisar y evaluar continuamente el entorno de control, incluyendo autoevaluaciones y autoconcienciación. Habilitar a la gerencia para identificar deficiencias e ineficiencias de control e iniciar acciones de mejora. Planificar, organizar y mantener estándares para la evaluación del control interno y la eficacia del control de procesos.		
Propósito		
Dar información transparente a las partes interesadas clave sobre la idoneidad del sistema de controles internos que permita, proporcionar confianza en las operaciones, confianza en el logro de los objetivos de la empresa y una comprensión adecuada del riesgo residual.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primarias:		
Metas empresariales	➔	Metas de alineamiento
<ul style="list-style-type: none"> • EG03 Cumplimiento de leyes y regulaciones externas • EG11 Cumplimiento de las políticas internas 		AG11 Cumplimiento de I&T con las políticas internas
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG03 <ul style="list-style-type: none"> a. Coste de incumplimiento regulatorio, incluidos acuerdos y multas b. Número de problemas de incumplimiento regulatorio que causan comentarios públicos o publicidad negativa c. Número de problemas de incumplimiento señalados por los reguladores d. Número de problemas de incumplimiento regulatorio en relación con acuerdos contractuales con socios empresariales 		AG11 <ul style="list-style-type: none"> a. Número de incidentes asociados con el incumplimiento de las políticas relacionadas con I&T. b. Número de excepciones a las políticas internas c. Frecuencia de revisión y actualización de la política
EG11 <ul style="list-style-type: none"> a. Número de incidentes relacionados con el incumplimiento de la política b. Porcentaje de las partes interesadas que entienden las políticas c. Porcentaje de políticas respaldadas por estándares y prácticas de trabajo eficaces 		

A. Componente: Proceso		
Práctica de gestión	Métricas modelo	
MEA02.01 Supervisar los controles internos. Supervisar, hacer benchmark y mejorar continuamente el entorno de control y el marco de control de I&T, para alcanzar los objetivos de la organización.	a. Número de brechas mayores de control interno b. Porcentaje de entorno de controles y marco supervisados, analizados comparativamente y mejorados continuamente para cumplir con los objetivos de la organización	
Actividades	Nivel de capacidad	
1. Identificar los límites del sistema de control interno. Por ejemplo, considerar cómo los controles internos de la organización, tienen en cuenta las actividades de desarrollo o producción externalizadas y/o ubicadas en otro país (offshore, término en inglés).	3	
2. Evaluar el estado de los controles internos de los proveedores de servicios externos. Confirmar que los proveedores de servicio cumplen con los requisitos legales y regulatorios y con sus obligaciones contractuales.		
3. Realizar actividades de supervisión y evaluación del control interno basadas en estándares de gobierno de la organización y marcos y prácticas aceptados por la industria. Incluye también la supervisión y evaluación de la eficacia y eficiencia de las actividades de supervisión gerencial.		
4. Asegurar que las excepciones de control se comuniquen, se sigan y analicen prontamente, y que se prioricen e implementen acciones correctivas apropiadas, conforme al perfil de gestión de riesgos (p. ej., clasificar algunas excepciones como riesgo clave y otras como riesgo no clave).		
5. Considerar evaluaciones independientes del sistema de control interno (p. ej., por auditoría interna o compañeros).		
6. Mantener el sistema de control interno, considerando los cambios continuos en el riesgo del negocio y de I&T, el entorno de control de la organización y los procesos del negocio y de I&T relevantes. Si hay una brecha, evaluar y recomendar cambios.	4	
7. Evaluar regularmente el desempeño del marco de control, a través de una comparación con estándares y buenas prácticas aceptadas por la industria. Considerar la adopción formal de una estrategia de mejora continua de la supervisión del control interno.	5	

A. Componente: Proceso (cont.)		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
HITRUST CSF versión 9, septiembre de 2017		09.10 Monitoring
ISO/IEC 38502:2017(E)		5.5 Governance and internal control
National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017		3.3 Audit and accountability (AU-2)
Práctica de gestión		Métricas modelo
MEA02.02 Revisar la eficacia de los controles del proceso de negocio. Revisar la operación de los controles, incluidas la supervisión y la evidencia de las pruebas, para asegurar que los controles de los procesos de negocio operan eficazmente. Incluir actividades para mantener evidencia de la operación efectiva de los controles mediante mecanismos, como pruebas periódicas, supervisión continua, evaluaciones independientes, centros de mando y control , y centros de operaciones de red. Estas evidencias garantizan al negocio que los controles cumplen con los requisitos relacionados con las responsabilidades de negocio, regulatorias y sociales.		a. Número de debilidades identificadas por calificaciones externas e informes de certificación b. Número de controles supervisados y probados para garantizar que los controles de los procesos de negocio operen de forma eficaz
Actividades		Nivel de capacidad
1. Entender y priorizar el riesgo de los objetivos de la organización.		3
2. Identificar controles clave y desarrollar una estrategia adecuada para validar los controles.		
3. Identificar información que indicará si un entorno de control interno está funcionando de forma eficaz.		
4. Conservar evidencias de la eficacia del control.		4
5. Desarrollar e implementar procedimientos rentables para obtener esta información de acuerdo a los criterios de calidad de la información correspondientes.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
MEA02.03 Realizar autoevaluaciones de control. Alentar a la gerencia y a los dueños de los procesos para que mejoren los controles de forma proactiva mediante un programa continuo de autoevaluación que evalúe la integridad y la efectividad del control de la gestión de los procesos, políticas y contratos.		a. Número de autoevaluaciones realizadas b. Número de brechas identificadas en la autoevaluación frente a los estándares o buenas prácticas de la industria
Actividades		Nivel de capacidad
1. Definir una estrategia acordada y consistente para realizar autoevaluaciones de control y coordinarse con auditores internos y externos.		3
2. Mantener planes de evaluación e identificación de criterios y alcance para llevar a cabo las autoevaluaciones. Planificar la comunicación de los resultados del proceso de autoevaluación al negocio, a TI y a la dirección general y al consejo de administración. Considerar estándares de auditoría interna en el diseño de las autoevaluaciones.		
3. Determinar la frecuencia de las autoevaluaciones periódicas, considerando globalmente la eficacia y eficiencia de la supervisión continua.		
4. Asignar las responsabilidades de la autoevaluación a los individuos adecuados para garantizar la objetividad y la competencia.		
5. Proporcionar revisiones independientes para garantizar la objetividad de la autoevaluación y permitir que se compartan buenas prácticas de control interno de otras empresas.		
6. Comparar los resultados de las autoevaluaciones con los estándares y buenas prácticas de la industria.		4
7. Resumir e informar de los resultados de las autoevaluaciones y benchmarking para tomar acciones correctivas.		5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISO/IEC 27001:2013/Cor.2:2015(E)		9.3 Management review
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018		3.7 Monitoring (Task 2)

A. Componente: Proceso (cont.)	
Práctica de gestión	Métricas modelo
MEA02.04 Identificar e informar las deficiencias de control. Identificar las deficiencias de control y analizar e identificar sus causas raíz subyacentes. Escalar las deficiencias de control e informar a las partes interesadas.	a. Tiempo transcurrido entre la ocurrencia de la deficiencia de control interno y el reporte b. Tiempo transcurrido entre la identificación de la excepción y las acciones planteadas acordadas c. Porcentaje de implementación de acciones correctivas derivadas de las evaluaciones de control
Actividades	Nivel de capacidad
1. Comunicar procedimientos para el escalamiento de las excepciones de control, análisis de la causa raíz y notificación a los dueños del proceso y a las partes interesadas de I&T.	3
2. Considerar el riesgo empresarial relacionado para establecer umbrales para el escalamiento de las excepciones de control y fallos.	
3. Identificar, reportar y registrar las excepciones de control. Asignar responsabilidades para su resolución e informar de su estado.	
4. Decidir qué excepciones de control deberían comunicarse a la persona responsable de la función y qué excepciones deberían escalarse. Informar a los dueños del proceso y a las partes interesadas.	
5. Hacer un seguimiento de todas las excepciones para garantizar que se han abordado las acciones acordadas.	4
6. Identificar, iniciar, seguir e implementar acciones correctivas que surjan de las evaluaciones de control y los reportes.	5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin documentación relacionada para esta práctica de gestión	

B. Componente: Estructuras organizativas														
Práctica clave de gestión	Director general financiero	Director de riesgos	Director de TI	Director de tecnología	Consejo de gobierno de I&T	Dueños del proceso de negocio	Oficina de gestión de proyectos	Jefe de desarrollo	Jefe de operaciones de TI	Jefe de administración de TI	Gestor de servicios	Gestor de seguridad de la información	Gestor de continuidad del negocio	Director de privacidad
		R	A	R		R	R	R	R	R	R	R	R	R
	R		A	R	R	R								
		R	A	R		R	R	R	R	R	R	R	R	R
			A	R		R	R	R	R	R	R	R	R	R
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)					Referencia específica									
Sin documentación relacionada para este componente.														

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
MEA02.01 Supervisar los controles internos.	De	Descripción	Descripción	A
	AP012.04	Resultados de evaluaciones de riesgos de terceros	Resultados de benchmarking y otras evaluaciones	Todos los APO; Todos los BAI; Todos los DSS; Todos los MEA; EDM01.03
	AP013.03	Reportes de auditoría del sistema de gestión de seguridad de la información (SGSI)	Resultados de la supervisión del control interno y sus revisiones	Todos los APO; Todos los BAI; Todos los DSS; Todos los MEA; EDM01.03
	Fuera de COBIT	Estándares y buenas prácticas de la industria		
MEA02.02 Revisar la eficacia de los controles del proceso de negocio.	BAI05.06	Resultados de la auditoría de cumplimiento	Evidencia de la efectividad de los controles	Interna
	BAI05.07	Revisiones del uso operativo		
MEA02.03 Realizar autoevaluaciones de control.			Planes y criterios de autoevaluación	Todos los APO; todos los BAI; todos los DSS; todos los MEA
			Resultados de las revisiones de las autoevaluaciones	Todos los APO; todos los BAI; Todos los DSS; todos los MEA; EDM01.03
			Resultados de las autoevaluaciones	Interna
MEA02.04 Identificar e informar las deficiencias de control.	AP011.03	Causas raíz del fracaso a la hora de ofrecer calidad	Acciones correctivas	Todos los APO; todos los BAI; Todos los DSS; todos los MEA
	AP012.06	Causas raíz relacionadas con el riesgo	Deficiencias de control	Todos los APO; todos los BAI; Todos los DSS; todos los MEA
	DSS06.01	• Resultados de las revisiones de eficiencia del procesamiento • Análisis de causas raíz y recomendaciones		
	DSS06.04	Evidencia de corrección y solución de errores		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
National Institute of Standards and Technology Special Publication 800-37, Revisión 2, septiembre de 2017		3.7 Monitoring (Task 2): Inputs and Outputs		

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión de riesgos	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.3. Risk Management

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de control interno	Comunica los objetivos del control interno a la dirección. Establece estándares para el diseño y funcionamiento del sistema de control interno empresarial para minimizar la exposición a todos los riesgos. Proporciona directrices para la supervisión y evaluación continua del entorno de control, incluida la autoconcienciación y la autoevaluación.		
Directrices de la autoevaluación del control interno	Recomienda la supervisión continua de los controles internos para identificar deficiencias y brechas de eficacia, determinar sus causas raíz e iniciar planes de acción e hitos de corrección para informar a las partes interesadas.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Fomentar la concienciación sobre la importancia de un entorno de control eficaz. Fomentar una cultura proactiva de autoconcienciación del riesgo, incluido el compromiso con la autoevaluación y las revisiones de aseguramiento independientes.		

G. Componente: Servicios, infraestructura y aplicaciones	
<ul style="list-style-type: none"> • COBIT y productos/herramientas relacionadas • Servicios de autoevaluación del control interno de terceros 	

Página dejada en blanco intencionadamente

Dominio: Monitorizar, evaluar y valorar Objetivo de gestión: MEA03 – Gestionar el cumplimiento de los requisitos externos		Área prioritaria: Modelo Core de COBIT
Descripción		
Evaluar si los procesos de I&T y los procesos de negocio apoyados por I&T cumplen con las leyes, regulaciones y requisitos contractuales. Asegurar que los requisitos se han identificado y cumplido; integrar el cumplimiento de TI con el cumplimiento general de la empresa.		
Propósito		
Asegurarse de que la empresa cumpla con todos los requisitos externos aplicables.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:		
Metas empresariales	➔	Metas de alineamiento
EG03 Cumplimiento de leyes y regulaciones externas		AG01 Cumplimiento de I&T y soporte al cumplimiento del negocio con leyes y regulaciones externas
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG03 <ul style="list-style-type: none"> a. Coste de incumplimiento regulatorio, incluidos acuerdos y multas b. Número de problemas de incumplimiento regulatorio que causan comentarios públicos o publicidad negativa c. Número de problemas de incumplimiento señalados por los reguladores d. Número de problemas de incumplimiento regulatorio en relación con acuerdos contractuales con socios empresariales 		AG01 <ul style="list-style-type: none"> a. Coste de incumplimiento de TI, incluidos acuerdos y multas, y el impacto de la pérdida reputacional b. Número de problemas de incumplimiento relacionados con TI notificados al consejo de administración o que causan comentarios o descrédito públicos c. Número de problemas de incumplimiento en relación con acuerdos contractuales con los proveedores de servicios de TI

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
MEA03.01 Identificar los requisitos externos de cumplimiento. Supervisar de forma continua los cambios en las leyes y regulaciones locales e internacionales, así como otros requisitos externos e identificar las obligaciones para el cumplimiento desde una perspectiva de I&T.		a. Frecuencia de revisiones de requisitos de cumplimiento b. Porcentaje de satisfacción de las partes interesadas clave en el proceso de revisión del cumplimiento normativo.
Actividades		Nivel de capacidad
1. Asignar la responsabilidad de identificar y supervisar los cambios en los requisitos legales, regulatorios y otros requisitos contractuales externos, relevantes para el uso de recursos de TI y el procesamiento de la información dentro de las operaciones empresariales y de TI.		2
2. Identificar y evaluar todos los posibles requisitos de cumplimiento y su impacto en las actividades de I&T, en áreas como flujo de datos, privacidad, controles internos, informes financieros, regulaciones específicas de la industria, propiedad intelectual, salud y seguridad en el trabajo.		
3. Evaluar el impacto de los requisitos legales y regulatorios relacionados con I&T sobre contratos con terceros relacionados con las operaciones de TI, proveedores de servicio y otros socios comerciales de negocios.		
4. Definir las consecuencias del incumplimiento.		
5. Obtener asesoría independiente cuando corresponda, sobre los cambios en la legislación, regulaciones y estándares vigentes.		3
6. Mantener un registro actualizado de todos los requisitos legales, regulatorios y contractuales; de su impacto y las acciones requeridas.		
7. Mantener un registro global, armonizado e integrado, de los requisitos de cumplimiento externo para la empresa.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		BC.RR Determine Legal / Regulatory Requirements
HITRUST CSF versión 9, septiembre de 2017		06.01 Compliance with Legal Requirements
ISF, The Standard of Good Practice for Information Security 2016		SM2.3 Legal and Regulatory Compliance

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
MEA03.02 Optimizar la respuesta a los requisitos externos. Revisar y ajustar las políticas, principios, estándares, procedimientos y metodologías para asegurarse de que se aborden y comuniquen los requisitos legales, regulatorios y contractuales. Considerar la adopción y adaptación de los estándares de la industria, los códigos y guías de buenas prácticas.		a. Tiempo promedio entre la identificación de los problemas de cumplimiento externo y su resolución b. Porcentaje de satisfacción del personal relevante con la comunicación de los requisitos de cumplimiento regulatorio, nuevos y modificados
Actividades		Nivel de capacidad
1. Revisar y ajustar continuamente las políticas, principios, estándares, procedimientos y metodologías para que sean eficaces en garantizar el cumplimiento necesario y abordar el riesgo empresarial. Usar expertos internos y externos, cuando sea necesario.		3
2. Comunicar los requisitos nuevos y modificados a todo el personal relevante.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
King IV Report on Corporate Governance for South Africa, 2016		Part 5.4: Governance functional areas - Principle 13
Práctica de gestión		Métricas modelo
MEA03.03 Confirmar el cumplimiento externo. Confirmar el cumplimiento de las políticas, principios, estándares, procedimientos y metodologías con los requisitos legales, regulatorios y contractuales.		a. Número de problemas críticos de incumplimiento identificados cada año b. Porcentaje de dueños de procesos que aprueban y confirman el cumplimiento
Actividades		Nivel de capacidad
1. Evaluar regularmente las políticas, estándares, procedimientos y metodologías organizativas en todas las funciones de la empresa, para garantizar el cumplimiento de todos los requisitos legales y regulatorios relevantes relacionados con el procesamiento de la información.		3
2. Tratar las brechas de cumplimiento en políticas, estándares y procedimientos con la debida oportunidad.		
3. Evaluar periódicamente los procesos y actividades del negocio y de TI para asegurar el cumplimiento de los requisitos legales, regulatorios y contractuales vigentes.		
4. Revisar regularmente los patrones recurrentes de fallos de cumplimiento y evaluar las lecciones aprendidas.		4
5. Mejorar las políticas, estándares, procedimientos, metodologías y sus procesos y actividades asociadas con base en la revisión y las lecciones aprendidas.		5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
MEA03.04 Obtener aseguramiento de cumplimiento externo. Obtener e informar del aseguramiento del cumplimiento y adherencia a las políticas, principios, estándares, procedimientos y metodologías. Confirmar que las acciones correctivas para abordar las brechas de cumplimiento se cierren de manera oportuna.		a. Número de informes de cumplimiento obtenidos b. Porcentaje de cumplimiento de los proveedores de servicio basado en revisiones independientes c. Tiempo transcurrido entre la identificación de la brecha de cumplimiento y la acción correctora d. Número de informes de acciones correctivas que tratan brechas de cumplimiento cerradas oportunamente
Actividades		Nivel de capacidad
1. Obtener confirmación periódica del cumplimiento con las políticas internas por parte de los dueños de los procesos de negocio y de TI y los jefes de unidades.		2
2. Realizar periódicamente revisiones internas y externas (independientes, cuando sea posible,) para evaluar los niveles de cumplimiento.		
3. Si se requiere, obtener declaraciones de los proveedores de servicio externos de I&T sobre sus niveles de cumplimiento con las leyes y regulaciones aplicables		
4. Si se requiere, obtener declaraciones de los socios de negocio sobre sus niveles de cumplimiento con leyes y regulaciones aplicables, en la medida en que estén relacionados con las transacciones electrónicas entre empresas.		
5. Integrar los informes sobre los requisitos legales, regulatorios y contractuales a nivel global de la empresa, involucrando a todas las unidades de negocio.		3
6. Supervisar y comunicar los problemas de incumplimiento y, cuando sea necesario, investigar la causa raíz.		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Data Management Maturity Model, 2014		Supporting Processes - Process Quality Assurance
ISO/IEC 27002:2013/Cor.2:2015(E)		18. Cumplimiento

B. Componente: Estructuras organizativas																	
Práctica clave de gestión																	
	Director general ejecutivo	Director general financiero	Director de operaciones	Director de TI	Consejo de gobierno de I&T	Dueños del proceso de negocio	Oficina de gestión de proyectos	Jefe de desarrollo	Jefe de operaciones de TI	Jefe de administración de TI	Gestor de servicios	Gestor de seguridad de la información	Gestor de continuidad del negocio	Director de privacidad	Asesor legal	Cumplimiento	Auditoría
MEA03.01 Identificar los requisitos externos de cumplimiento.				R		R								R	R	A	R
MEA03.02 Optimizar la respuesta a los requisitos externos.	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	A
MEA03.03 Confirmar el cumplimiento externo.	R	R	R	R	R	R								R	R	A	
MEA03.04 Obtener aseguramiento de cumplimiento externo				R											R	A	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)														Referencia específica			
Sin documentación relacionada para este componente.																	

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
MEA03.01 Identificar los requisitos externos de cumplimiento.	Fuera de COBIT	Requisitos de cumplimiento legal y regulatorio.	Log de acciones de cumplimiento requeridas	Interna
			Registro de requisitos de cumplimiento	Interna
MEA03.02 Optimizar la respuesta a los requisitos externos.			Comunicaciones de cambios en los requisitos de cumplimiento	Todos los APO; Todos los BAI; Todos los DSS; Todos los MEA; EDM01.01
			Políticas, principios, procedimientos y estándares actualizados	AP001.09; AP001.11
MEA03.03 Confirmar el cumplimiento externo.	BAI05.06	Resultados de las auditorías de cumplimiento	Confirmaciones de cumplimiento	EDM01.03
	BAI09.05	Resultados de auditoría a las licencias instaladas	Brechas de cumplimiento identificadas	MEA04.08
	BAI10.05	Desviaciones de licencias		
	DSS01.04	Informes de políticas de seguros		
MEA03.04 Obtener aseguramiento de cumplimiento externo.	EDM05.02	Reglas para la validación y aprobación de informes obligatorios	Informes de aseguramiento del cumplimiento	EDM01.03
	EDM05.03	Evaluación de la eficacia de reporte	Informes de los problemas de incumplimiento y sus causas raíz	EDM01.03; MEA04.04
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)				
Referencia específica				
Sin documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Seguridad de la información	Skills Framework for the Information Age V6, 2015	SCTY

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de cumplimiento	Identifica los requisitos de cumplimiento regulatorios, contractuales e internos. Explica el proceso para evaluar el cumplimiento de los requisitos regulatorios, contractuales e internos. Listas de roles y responsabilidades de distintas actividades en el proceso y proporciona directrices sobre las métricas para medir el cumplimiento. Obtiene informes de cumplimiento y confirma el cumplimiento o las acciones correctivas para abordar la solución de las brechas de cumplimiento de manera oportuna.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Proporcionar una cultura de concienciación sobre el cumplimiento, incluida una tolerancia cero con el incumplimiento de requisitos legales y regulatorios.		

G. Componente: Servicios, infraestructura y aplicaciones	
<ul style="list-style-type: none"> Servicios de vigilancia regulatoria Servicios de evaluación al cumplimiento de terceros 	

Dominio: Monitorizar, evaluar y valorar Objetivo de gestión: MEA04 – Gestionar el aseguramiento		Área prioritaria: Modelo Core de COBIT
Descripción		
Planificar, delimitar y ejecutar iniciativas de aseguramiento para cumplir con requisitos internos, leyes, regulaciones y objetivos estratégicos. Permitir que la dirección ofrezca una garantía adecuada y sostenible en la empresa, con la realización de revisiones y actividades de aseguramiento independiente.		
Propósito		
Facilitar a la organización el diseño y desarrollo de iniciativas de aseguramiento eficaces y eficientes proporcionando una guía sobre la planificación, alcance, ejecución y seguimiento de las revisiones de aseguramiento con una hoja de ruta basada en estrategias de aseguramiento ampliamente aceptadas.		
El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:		
Metas empresariales	➔	Metas de alineamiento
<ul style="list-style-type: none"> • EG03 Cumplimiento de leyes y regulaciones externas • EG11 Cumplimiento de las políticas internas 		AG11 Cumplimiento de I&T con las políticas internas
Métricas modelo para metas empresariales		Métricas modelo para metas de alineamiento
EG03 <ul style="list-style-type: none"> a. Coste de incumplimiento regulatorio, incluidos acuerdos y multas b. Número de problemas de incumplimiento regulatorio que causan comentarios públicos o publicidad negativa c. Número de problemas de incumplimiento señalados por los reguladores d. Número de problemas de incumplimiento regulatorio en relación con acuerdos contractuales con socios empresariales 		AG11 <ul style="list-style-type: none"> a. Número de incidentes relacionados con el incumplimiento de las políticas relacionadas con I&T. b. Número de excepciones a las políticas internas c. Frecuencia de revisión y actualización de la política
EG11 <ul style="list-style-type: none"> a. Número de incidentes relacionados con el incumplimiento de la política b. Porcentaje de partes interesadas que entienden las políticas c. Porcentaje de políticas respaldadas por estándares y prácticas de trabajo eficaces 		

A. Componente: Proceso		
Práctica de gestión		Métricas modelo
MEA04.01 Asegurar que los proveedores de aseguramiento sean independientes y estén cualificados. Asegurar que las entidades que realizan la evaluación sean independientes de la función, grupos u organizaciones incluidos en el alcance. Las entidades que realizan la evaluación deben demostrar una actitud y apariencia apropiadas, competencia en las habilidades y conocimientos necesarios para realizar el aseguramiento, y adherencia a los códigos de ética y a los estándares profesionales.		a. Porcentaje de procesos que reciben una revisión independiente b. Porcentaje de cualificaciones y competencias satisfechas por los proveedores de servicio
Actividades		Nivel de capacidad
1. Establecer la adherencia a los códigos éticos y de estándares vigentes (p. ej. código de ética profesional de ISACA) y otros estándares de aseguramiento de la industria y específicos de la localización geográfica [p. ej. los IT Audit and Assurance Standards of ISACA y el International Framework for Assurance Engagements (IAASB Assurance Framework) del International Auditing and Assurance Standards Board (IAASB's)].		2
2. Establecer la independencia de los proveedores del aseguramiento.		
3. Establecer la competencia y la cualificación de los proveedores del aseguramiento.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
HITRUST CSF versión 9, septiembre de 2017		06.03 Information System Audit Considerations

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
MEA04.02 Desarrollar una planificación de iniciativas de aseguramiento basada en riesgos. Determinar objetivos de aseguramiento basados en evaluaciones del entorno y contextos interno y externo, el riesgo de no lograr las metas empresariales, y las oportunidades asociadas al logro de esas mismas metas.		a. Porcentaje de iniciativas de aseguramiento que siguen los estándares del programa y plan de aseguramiento b. Porcentaje de iniciativas del plan de aseguramiento basadas en el riesgo
Actividades		Nivel de capacidad
1. Entender la estrategia y prioridades de la empresa.		2
2. Entender el contexto interno de la empresa. Esta comprensión ayudará al profesional de aseguramiento a evaluar mejor las metas empresariales y la importancia relativa de las metas de alineamiento y metas empresariales, así como las amenazas más importantes para estas metas. A su vez, esto contribuirá a definir un mejor y más relevante alcance para el compromiso con el aseguramiento.		
3. Entender el contexto externo de la empresa. Esta comprensión ayudará al profesional del aseguramiento a comprender mejor las metas empresariales y la importancia relativa de las metas de alineamiento y metas empresariales, así como las amenazas más importantes para estas metas. A su vez, esto contribuirá a definir un mejor y más relevante alcance para el compromiso con el aseguramiento.		
4. Desarrollar un plan anual global para las iniciativas de aseguramiento que incluya los objetivos consolidados de aseguramiento.		3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
King IV Report on Corporate Governance for South Africa, 2016		Part 5.4: Governance functional areas—Principle 15
Práctica de gestión		Métricas modelo
MEA04.03 Determinar los objetivos de la iniciativa de aseguramiento. Definir y acordar con todas las partes interesadas los objetivos de la iniciativa de aseguramiento.		a. Porcentaje de objetivos alcanzados durante la iniciativa de aseguramiento b. Porcentaje de satisfacción de las partes interesadas con los objetivos de la iniciativa de aseguramiento
Actividades		Nivel de capacidad
1. Definir el objetivo de aseguramiento de la iniciativa de aseguramiento mediante la identificación de las partes interesadas en esta iniciativa de aseguramiento y sus intereses.		2
2. Acordar los objetivos de alto nivel y los límites organizativos del compromiso de aseguramiento.		
3. Considerar el uso de la cascada de metas de COBIT y sus distintos niveles para expresar el objetivo del aseguramiento.		3
4. Asegurar que los objetivos del compromiso del aseguramiento consideren los tres componentes de valor del objetivo: obtener beneficios que respalden los objetivos estratégicos, optimizar el riesgo de que no se alcancen los objetivos estratégicos y optimizar los niveles de recursos requeridos para lograr los objetivos estratégicos.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Data Management Maturity Model, 2014		Supporting Processes - Process Quality Assurance
Práctica de gestión		Métricas modelo
MEA04.04 Definir el alcance de la iniciativa de aseguramiento. Definir y acordar con todas las partes interesadas el alcance de la iniciativa de aseguramiento, con base en los objetivos de aseguramiento.		a. Número de planes de compromiso, basados en el alcance, que consideran la información a recopilar y las entrevistas a las partes interesadas b. Porcentaje de satisfacción de las partes interesadas con el alcance de la iniciativa del aseguramiento, conforme a los objetivos de aseguramiento
Actividades		Nivel de capacidad
1. Definir todos los componentes de gobierno en el alcance de la revisión, es decir, los principios, políticas y marcos de referencia; procesos; estructuras organizativas; cultura, ética y comportamiento; información; servicios, infraestructura y aplicaciones; personas, habilidades y competencias		2
2. Basándose en el alcance establecido, definir un plan de compromiso, que incluya la información que debe recopilarse y las partes interesadas que deben entrevistarse		3
3. Confirmar y perfeccionar el alcance con base en el conocimiento de la arquitectura empresarial.		
4. Perfeccionar el alcance del compromiso de aseguramiento, conforme a los recursos disponibles		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		TP.LA Apply Logging and Audit Processes

A. Componente: Proceso (cont.)		
Práctica de gestión		Métricas modelo
MEA04.05 Definir el programa de trabajo para la iniciativa de aseguramiento. Definir un programa de trabajo detallado para la iniciativa de aseguramiento, estructurado conforme al alcance de los objetivos de gestión y los componentes de gobierno.		a. Porcentaje de controles de gestión identificados como débiles, sin prácticas definidas para reducir el riesgo residual b. Número de controles revisados c. Porcentaje de satisfacción de las partes interesadas con el programa de trabajo de la iniciativa de aseguramiento
Actividades		Nivel de capacidad
1. Definir pasos detallados para la recopilación y evaluación de la información de los controles de gestión considerados en el alcance. Centrarse en evaluar la definición y aplicación de buenas prácticas relacionadas con el diseño de controles y el logro de los objetivos de control, relacionados con la eficacia del control.		2
2. Entender el contexto de los objetivos de gestión y los controles de gestión que los respaldan y que se ponen en práctica. Entender cómo estos controles de gestión contribuyen a lograr las metas de alineamiento y las metas empresariales.		
3. Entender a todas las partes interesadas y sus intereses.		
4. Acordar las buenas prácticas esperadas para los controles de gestión.		3
5. Si un control de gestión fuera débil, definir las prácticas para identificar el riesgo residual (como preparación para el reporte).		
6. Entender la fase del ciclo de vida de los controles de gestión y acordar los valores esperados.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		
Práctica de gestión		Métricas modelo
MEA04.06 Ejecutar la iniciativa de aseguramiento, enfocándose en la efectividad del diseño. Ejecutar la iniciativa de aseguramiento planificada. Validar y confirmar el diseño de los controles internos existentes. Adicional y especialmente en las tareas de auditoría interna, considerar la rentabilidad del diseño del componente de gobierno.		a. Porcentaje de iniciativas de aseguramiento que consideran la rentabilidad del diseño b. Porcentaje de satisfacción de las partes interesadas con el diseño de la iniciativa de aseguramiento
Actividades		Nivel de capacidad
1. Perfeccionar el entendimiento del sujeto de aseguramiento de TI.		2
2. Perfeccionar el alcance del sujeto de aseguramiento de TI.		
3. Observar/inspeccionar y revisar la estrategia de control de gestión. Validar el diseño con el dueño del control en cuanto a su completitud, relevancia, oportunidad y facilidad de medición.		3
4. Preguntar al dueño del control si se han asignado las responsabilidades globales del componente de gobierno y de la rendición de cuentas. Confirmar la respuesta. Comprobar si la rendición de cuentas y las responsabilidades se han entendido y aceptado. Comprobar que están disponibles las habilidades adecuadas y los recursos necesarios.		
5. Reconsiderar el equilibrio entre prevención y detección y los tipos de corrección de las actividades de control de gestión.		
6. Considerar el esfuerzo dedicado a mantener los controles de gestión y su rentabilidad asociada.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISF, The Standard of Good Practice for Information Security 2016		SI1 Security Audit
ISO/IEC 27001:2013/Cor.2:2015(E)		9.2 Internal audit
Práctica de gestión		Métricas modelo
MEA04.07 Ejecutar la iniciativa de aseguramiento, enfocándose en la eficacia operativa. Ejecutar la iniciativa de aseguramiento planificada. Probar si los controles internos establecidos son adecuados y suficientes. Probar el resultado de los objetivos clave de gestión en el alcance de la iniciativa de aseguramiento.		a. Porcentaje de iniciativas de aseguramiento que prueban el resultado de los objetivos clave de gestión dentro del alcance b. Porcentaje de satisfacción de las partes interesadas con la ejecución de la iniciativa de aseguramiento

A. Componente: Proceso (cont.)	
Actividades	Nivel de capacidad
1. Evaluar si se han alcanzado los resultados esperados para cada uno de los controles de gestión en el alcance. Es decir, evaluar la efectividad del control de gestión (eficacia del control).	3
2. Asegurar que el profesional del aseguramiento prueba el resultado o la efectividad del control de gestión mediante la búsqueda de evidencias directas e indirectas del impacto en las metas de los controles de gestión. Esto implica la justificación directa e indirecta de la contribución medible de las metas de gestión a las metas de alineamiento y de este modo se registran las evidencias directas e indirectas de que se han alcanzado realmente los resultados esperados.	
3. Determinar si el profesional del aseguramiento obtiene evidencias directas o indirectas de los elementos/periodos seleccionados al aplicar una selección de técnicas de pruebas para garantizar que el control de gestión bajo revisión funciona de forma efectiva. Asegurar que el profesional del aseguramiento realice también una revisión limitada de la idoneidad de los resultados del control de gestión y determine el nivel de pruebas sustantivas y el trabajo adicional necesarios para proporcionar aseguramiento de que el desempeño del control de gestión es adecuado.	
4. Investigar si un control de gestión puede ser más eficiente y si su diseño puede ser más efectivo optimizando los pasos y buscando sinergias con otros controles de gestión.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
ISF, The Standard of Good Practice for Information Security 2016	SI1 Security Audit
SO/IEC 27001:2013/Cor.2:2015(E)	9.2 Internal audit
Práctica de gestión	Métricas modelo
MEA04.08 Informar y hacer seguimiento a la iniciativa de aseguramiento. Ofrecer opiniones positivas de la evaluación cuando sea apropiado, así como recomendaciones de mejora relacionadas con el rendimiento operacional identificado, el cumplimiento externo y las debilidades del control interno.	a. Aceptación de las partes interesadas del informe de aseguramiento b. Aceptación de las partes interesadas de las recomendaciones de mejora relativas al rendimiento operacional identificado, el cumplimiento externo y las debilidades del control interno.
Actividades	Nivel de capacidad
1. Documentar el impacto de las debilidades del control.	2
2. Comunicarse con la dirección durante la ejecución de la iniciativa para que haya un claro entendimiento del trabajo realizado y un acuerdo y aceptación de los hallazgos preliminares y las recomendaciones.	
3. Proporcionar a la dirección un informe (alineado con los términos de referencia, alcance y estándares de informes acordados) que sustente los resultados de la iniciativa y permita centrarse claramente en los problemas clave y las acciones importantes.	3
4. Supervisar las actividades de aseguramiento y garantizar que el trabajo está finalizado, cumple con los objetivos y tiene una calidad aceptable. Revisar el enfoque o los pasos detallados si se detecta una calidad deficiente.	4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin documentación relacionada para esta práctica de gestión	
Práctica de gestión	Métricas modelo
MEA04.09 Hacer seguimiento a las recomendaciones y a las acciones. Acordar, hacer seguimiento e implementar las recomendaciones de mejoras identificadas.	a. Número de debilidades recurrentes b. Número de debilidades identificadas resueltas
Actividades	Nivel de capacidad
1. Acordar e implementar internamente, dentro de la organización, las acciones necesarias para resolver las debilidades y brechas identificadas.	2
2. Hacer un seguimiento, dentro de la organización, para determinar si se llevaron a cabo acciones correctivas y las debilidades de control interno se resolvieron.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Sin documentación relacionada para esta práctica de gestión	

B. Componente: Estructuras organizativas													
	Director de operaciones	Director de riesgos	Director de TI	Director de tecnología	Comité de riesgos empresariales	Dueños del proceso de negocio	Función de gestión de datos	Jefe de operaciones de TI	Gestor de servicios	Gestor de seguridad de la información	Gestor de continuidad del negocio	Asesor legal	Auditoría
Práctica clave de gestión													
MEA04.01 Asegurar que los proveedores de aseguramiento sean independientes y estén cualificados.			R	R	R	R						R	A
MEA04.02 Desarrollar una planificación de iniciativas de aseguramiento basada en los riesgos.	R	R	R	R		R						R	A
MEA04.03 Determinar los objetivos de la iniciativa de aseguramiento.	R	R	R	R		R						R	A
MEA04.04 Definir el alcance de la iniciativa de aseguramiento.	R	R	R	R		R						R	A
MEA04.05 Definir el programa de trabajo para la iniciativa de aseguramiento.	R		R	R		R						R	A
MEA04.06 Ejecutar la iniciativa de aseguramiento, enfocándose en la efectividad del diseño.	R		R	R		R	R	R	R	R	R	R	A
MEA04.07 Ejecutar la iniciativa de aseguramiento, enfocándose en la eficacia operativa.	R		R	R		R	R	R	R	R	R	R	A
MEA04.08 Informar y hacer seguimiento a la iniciativa de aseguramiento.	R		R	R		R						R	A
MEA04.09 Hacer seguimiento a las recomendaciones y a las acciones.	R	R	A	R		R		R				R	R
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica												
Sin documentación relacionada para este componente.													

C. Componente: Flujos y elementos de información (ver también la sección 3.6)				
Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
MEA04.01 Asegurar que los proveedores del aseguramiento sean independientes y estén cualificados.			Resultados de evaluaciones del proveedor del aseguramiento	Interna
MEA04.02 Desarrollar una planificación de iniciativas de aseguramiento basada en los riesgos.	BAI01.05	Planes de auditoría de programas	Planes de aseguramiento	Todos los APO; Todos los BAI; Todos los DSS; Todos los MEA; EDM01.03
	DSS01.02	Planes independientes de aseguramiento	Criterios de evaluación	Interna
			Evaluaciones de alto nivel	Interna
MEA04.03 Determinar los objetivos de la iniciativa de aseguramiento.	MEA04.02	Planes de aseguramiento	Objetivos del aseguramiento y beneficios esperados	Interna
MEA04.04 Definir el alcance de la iniciativa de aseguramiento.	AP011.03	Causas raíz del fracaso a la hora de ofrecer calidad	Prácticas de revisión del aseguramiento	Interna
	AP012.06	Causas raíz relacionadas con el riesgo	Plan de compromiso	Interna
	DSS06.01	Análisis de la causa raíz y recomendaciones		
	MEA03.04	Informes de los problemas y causas raíz del incumplimiento	Alcance de la revisión del aseguramiento	Interna

C. Componente: Flujos y elementos de información (ver también la sección 3.6) (cont.)				
Práctica de gestión	Entradas		Salidas	
MEA04.05 Definir el programa de trabajo para la iniciativa de aseguramiento.	De	Descripción	Descripción	A
	AP012.04	Análisis de riesgos e informes del perfil de riesgo para las partes interesadas	Alcance redefinido Programa detallado del trabajo de aseguramiento	Interna MEA04.06
MEA04.06 Ejecutar la iniciativa de aseguramiento, enfocándose en la efectividad del diseño.	AP012.06	Causas raíz relacionadas con el riesgo	Diseño de controles internos documentados	MEA04.07
	DSS06.01	Análisis de la causa raíz y recomendaciones		
	MEA04.05	Programa detallado del trabajo de aseguramiento		
MEA04.07 Ejecutar la iniciativa de aseguramiento, enfocándose en la eficacia operativa.	DSS02.02	Log de peticiones de servicio e incidentes	Pruebas de la eficacia del control.	MEA04.08; MEA04.09
	DSS02.05	Resoluciones de incidentes		
	DSS03.05	Informes de supervisión de la resolución de problemas		
	DSS05.02	Resultados de las pruebas de penetración		
	DSS05.05	Logs de acceso		
	DSS06.01	Análisis de la causa raíz y recomendaciones		
	MEA04.06	Diseño documentado de controles internos		
MEA04.08 Informar y hacer seguimiento a la iniciativa de aseguramiento.	MEA03.03	Brechas de cumplimiento identificadas	Informes de revisión del aseguramiento	Todos los APO; todos los BAI; Todos los DSS; todos los MEA; EDM05.03
	MEA04.07	Pruebas de la eficacia del control.	Resultados de la revisión del aseguramiento	Todos los APO; todos los BAI; Todos los DSS; todos los MEA; EDM05.03; MEA04.09
MEA04.09 Hacer seguimiento a las recomendaciones y a las acciones.	MEA04.07	Pruebas de la eficacia del control.	Acciones correctivas	Todos los APO; todos los BAI; Todos los DSS; todos los MEA
	MEA04.08	Resultados de la revisión de aseguramiento		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin documentación relacionada para este componente.				

D. Componente: Personas, habilidades y competencias		
Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Hay una serie de principios fundamentales descritos por el Instituto de auditores internos®, que respaldan la efectividad y la eficiencia de la función de auditoría (interna). Estos principios incluyen, entre otros, la importancia de la independencia, habilidades de comunicación efectiva, proactividad, etc.	Core Principles for the Professional Practice of Internal Auditing, The Institute of Internal Auditors	cfr. IIA website—Standards & Guidance - Core Principles
Gestión de riesgos	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.3. Risk Management

E. Componente: Políticas y procedimientos			
Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Guía de aseguramiento	Proporciona directrices sobre la realización de actividades de aseguramiento. Permite el desarrollo eficaz y eficiente de iniciativas de aseguramiento de I&T, incluidas la planificación, la definición del alcance y la ejecución de revisiones de aseguramiento, conforme a enfoques de aseguramiento ampliamente aceptados. Proporciona los pasos de aseguramiento para poner a prueba el diseño del control, probar el resultado de su efectividad operativa y documentar las debilidades del control y su impacto.		
Estatuto de auditoría interna	Proporciona independencia para llevar a cabo revisiones de auditoría e informar sobre los hallazgos y recomendaciones directamente a la alta dirección. La función de auditoría interna debería ser una entidad separada reportando al director general ejecutivo o al director de operaciones. Con respecto a I&T, el estatuto debería estipular que la función de auditoría es responsable de la revisión de los controles generales y de aplicaciones para determinar si los controles se han diseñado de acuerdo con la dirección de la gerencia, los estándares y procedimientos establecidos, los requisitos legales conocidos, y si estos controles están funcionando de forma eficaz para proporcionar confiabilidad y seguridad en cuanto a los datos que se procesan (es decir, confidencialidad, integridad y disponibilidad). El estatuto debería estipular que la función de auditoría interna es responsable de la revisión del diseño, desarrollo e implementación de nuevos sistemas o modificaciones mayores de los sistemas actuales.		

F. Componente: Cultura, ética y comportamiento		
Elementos culturales clave	Documentación relacionada	Referencia específica
Crea una cultura que adopta la auditoría interna y los hallazgos y recomendaciones de aseguramiento, conforme al análisis de las causas raíz. Los líderes deben garantizar que la auditoría interna y el aseguramiento formen parte de las iniciativas estratégicas y reconocer la necesidad (y el valor) de la auditoría y de los informes de aseguramiento.		
Garantizar una cultura ética de auditoría interna a través de un código ético adecuado.	Código de ética, el Instituto de Auditores internos	cfr. IIA website—Standards & Guidance—Code of Ethics

G. Componente: Servicios, infraestructura y aplicaciones
<ul style="list-style-type: none"> • Herramientas de compromiso de aseguramiento • Herramientas de auditoría para el log de eventos • Servicios de prestación de aseguramiento por terceros

Apéndices

A.1 Anexo A: Cascada de metas: Tablas de relacionamiento

Las tablas de relacionamiento del anexo A muestran la cascada de metas. La primera tabla relaciona las metas de alineamiento con las metas empresariales; la segunda tabla relaciona los objetivos de gobierno y gestión con los objetivos de alineamiento. La «P» de la tabla se refiere a primario y la «S» se refiere a secundario.

A.1.1 Tabla de relacionamiento: Metas empresariales—Metas de alineamiento

Figura A.1—Relacionamiento de metas empresariales y metas de alineamiento														
		EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	EG13
		Portafolio de productos y servicios competitivos	Gestión del riesgo del negocio	Cumplimiento con leyes y regulaciones externas	Calidad de la información financiera	Cultura de servicio orientado al cliente	Continuidad y disponibilidad del servicio del negocio	Calidad de la información sobre gestión	Optimización de la funcionalidad de los procesos internos de negocio	Optimización de costos de los procesos de negocio	Habilidades, motivación y productividad del personal	Cumplimiento con las políticas internas	Gestión de programas de transformación digital	Innovación de productos y negocios
AG01	Cumplimiento y soporte de I&T para el cumplimiento del negocio con leyes y regulaciones externas		S	P								S		
AG02	Gestión de riesgo relacionado con I&T		P				S							
AG03	Beneficios obtenidos del portafolio de inversiones y servicios habilitados por I&T	S				S			S	S			P	
AG04	Calidad de la información financiera relacionada con la tecnología				P			P		P				
AG05	Prestación de servicios I&T conforme a los requisitos del negocio	P				S	S		S				S	
AG06	Agilidad para convertir los requisitos del negocio en soluciones operativas	P				S			S				S	S
AG07	Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad		P				P							
AG08	Habilitar y dar soporte a procesos de negocio mediante la integración de aplicaciones y tecnología	P				P			S		S		P	S
AG09	Ejecución de programas dentro del plazo, sin exceder el presupuesto, y que cumplen con los requisitos y estándares de calidad	P				S			S	S			P	S
AG10	Calidad de la información sobre gestión de I&T				P			P		S				
AG11	Cumplimiento de I&T con las políticas internas		S	P								P		
AG12	Personal competente y motivado con un entendimiento de la tecnología y del negocio					S					P			
AG13	Conocimiento, experiencia e iniciativas para la innovación empresarial	P		S									S	P

A.1.2 Tabla de relacionamiento: Metas de alineamiento—Objetivos de gobierno y gestión

Figura—A.2 Relacionamiento de objetivos de gobierno y gestión con metas de alineamiento														
		AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13
		Cumplimiento y soporte de I&T para el cumplimiento del negocio con leyes y regulaciones externas	Gestión de riesgo relacionado con I&T	Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T	Calidad de la información financiera relacionada con la tecnología	Prestación de servicios de I&T conforme a los requisitos del negocio	Agilidad para convertir los requisitos del negocio en soluciones operativas	Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad	Habilitar y dar soporte a procesos de negocio mediante la integración de aplicaciones y tecnología	Ejecución de programas dentro del plazo, sin exceder el presupuesto, y que cumplan con los requisitos y estándares de calidad	Calidad de la información sobre gestión de I&T	Cumplimiento de I&T con las políticas internas	Personal competente y motivado con un entendimiento de la tecnología y del negocio	Conocimiento, experiencia e iniciativas para la innovación empresarial
EDM01	Asegurar el establecimiento y el mantenimiento del marco de gobierno	P	S	P					S			S		
EDM02	Asegurar la obtención de beneficios			P		S	S		S					S
EDM03	Asegurar la optimización del riesgo	S	P					P				S		
EDM04	Asegurar la optimización de recursos			S		S	S		S	P			S	
EDM05	Asegurar el compromiso de las partes interesadas				S						P	S		
AP001	Gestionar el marco de gestión de I&T	S	S	P		S		S	S	S	S	P		
AP002	Gestionar la estrategia			S		S	S		P				S	S
AP003	Gestionar la arquitectura empresarial			S		S	P	S	P					
AP004	Gestionar la innovación			S			P		S				S	P
AP005	Gestionar el portafolio			P		P	S		S	S				
AP006	Gestionar el presupuesto y los costes			S	P					P	S			
AP007	Gestionar los recursos humanos			S		S				S			P	P
AP008	Gestionar las relaciones			S		P	P		S	S			P	P
AP009	Gestionar los acuerdos de servicio					P			S					
AP010	Gestionar los proveedores					P	S			S				
AP011	Gestionar la calidad			S	S	S				P	P			
AP012	Gestionar el riesgo		P					P						
AP013	Gestionar la seguridad	S	S					P						
AP014	Gestionar los datos	S	S		S			S			P			
BAI01	Gestionar los programas			P			S		S	P				
BAI02	Gestionar la definición de requisitos			S		P	P		S	P			S	
BAI03	Gestionar la identificación y construcción de soluciones			S		P	P		S	P				
BAI04	Gestionar la disponibilidad y la capacidad					P		S		S				
BAI05	Gestionar el cambio organizativo			P		S	S		P	P			S	
BAI06	Gestionar los cambios de TI		S			S	P		S					
BAI07	Gestionar la aceptación y la transición de los cambios de TI		S				P			S				
BAI08	Gestionar el conocimiento			S			S		S	S			P	P
BAI09	Gestionar los activos				P						S			
BAI10	Gestionar la configuración					S		P						
BAI11	Gestionar los proyectos			P		S	P			P				
DSS01	Gestionar las operaciones					P			S					
DSS02	Gestionar las peticiones y los incidentes del servicio		S			P		S						
DSS03	Gestionar los problemas		S			P		S						
DSS04	Gestionar la continuidad		S			P		P						
DSS05	Gestionar los servicios de seguridad	S	P			S		P				S		
DSS06	Gestionar los controles de procesos de negocio		S			S		S	P			S		
MEA01	Gestionar la supervisión del rendimiento y la conformidad	S		S		P				S	P	S		
MEA02	Gestionar el sistema de control interno	S	S		S	S		S		S	S	P		
MEA03	Gestionar el cumplimiento de los requisitos externos	P										S		
MEA04	Gestionar el aseguramiento	S	S		S	S		S			S	P		

A.2 Anexo B: Estructuras organizativas: Visión general y descripciones

En la guía detallada del capítulo 4, los componentes de las estructuras organizativas se derivan de los roles y estructuras señalados en la **figura A.3** (ver también la sección 3.5 para obtener una visión general del componente de estructuras organizativas).

En las empresas, la nomenclatura aplicada a cada rol o estructura podría seguramente ser distinta. Con base en las descripciones siguientes, cada empresa podría identificar, los roles y estructuras más adecuados (dado su propio contexto de negocio, organización y entorno operativo) y asignar niveles de rendición de cuentas y responsabilidad, según corresponda.

Figura A.3—Roles y estructuras organizativas de COBIT

Rol/estructura	Descripción
Consejo de Administración	Grupo de altos ejecutivos y/o directores no ejecutivos que rinden cuentas sobre el gobierno y control total de los recursos de la empresa
Comité ejecutivo	Grupo de altos ejecutivos nombrados por el consejo de administración para garantizar que el consejo participe y esté informado de las principales decisiones. (El comité ejecutivo rinde cuentas sobre la gestión de los portafolios de inversiones de I&T, de los servicios y activos de I&T; garantizando que se ofrece valor; y se gestiona el riesgo. El comité suele estar presidido por un miembro del consejo de administración).
Director general ejecutivo	Director de más alto rango— encargado de la gestión global de la empresa
Director general financiero	Director de más alto rango que rinde cuentas sobre todos los aspectos de la gestión financiera, incluido el riesgo y los controles financieros, así como de una contabilidad confiable y precisa
Director de operaciones	Director de más alto rango que rinde cuentas sobre la operación de la empresa
Director de riesgos	Director de más alto rango que rinde cuentas sobre todos los aspectos de la gestión de riesgos de la empresa (Una función de director de riesgos de I&T podría establecerse para supervisar el riesgo de I&T).
Director de TI	Director de más alto rango que rinde cuentas sobre el alineamiento de las TI y las estrategias del negocio y rinde cuentas por la planificación, gestión de recursos y prestación de servicios y soluciones de I&T
Director de tecnología	Director de más alto rango encargado de los aspectos técnicos de I&T, incluida la gestión y supervisión de decisiones relacionadas con servicios, soluciones e infraestructura de I&T (Este rol podría también realizarlo el director de información).
Director de tecnologías digitales	Director de más alto rango encargado de poner en práctica la transformación digital de la empresa o de las unidades de negocio (Este rol podría también realizarlo el director de información u otro miembro del comité ejecutivo).
Consejo de gobierno de I&T	Grupo de partes interesadas y expertos que rinden cuentas sobre la dirección de los asuntos y decisiones relacionadas con I&T, incluidas la gestión de inversiones habilitadas por I&T, la obtención de valor y la supervisión del riesgo
Consejo de arquitectura	Grupo de partes interesadas y expertos que rinden cuentas sobre la dirección de los asuntos y decisiones relacionados con la arquitectura empresarial y de establecer las políticas y estándares de la misma.
Comité de riesgos corporativos	Grupo de ejecutivos que rinden cuentas sobre el nivel de colaboración y consenso requeridos para respaldar las actividades y decisiones de gestión de riesgos empresariales (ERM). (Podría establecerse un consejo de riesgos de I&T para considerar el riesgo de I&T más detalladamente y asesorar al comité de riesgos corporativos).
Director de seguridad de la información	El director de más alto rango que rinde cuentas sobre todos los aspectos de la gestión de seguridad de la empresa
Dueño del proceso de negocio	Persona que rinde cuentas sobre la ejecución de los procesos y/o el logro de los objetivos de los procesos, conducir la mejora de los procesos y aprobar los cambios a los procesos.
Gestor de portafolio	Persona responsable de dirigir la gestión del portafolio, asegurar una selección adecuada de programas y proyectos y gestionar y supervisar programas y proyectos para obtener un valor óptimo, así como alcanzar los objetivos estratégicos a largo plazo de forma eficaz y eficiente
Comité estratégico (programas/proyectos)	Grupo de personas interesadas y expertos que rinden cuentas sobre la dirección de programas y proyectos, incluidos planes de gestión y supervisión, asignación de recursos, obtención de beneficios y valor y gestión del riesgo de los programas y proyectos.
Gestor de programas	Persona responsable de dirigir un programa específico, incluidos la articulación y el seguimiento de las metas y objetivos del programa y la gestión del riesgo y su impacto en el negocio

Figura A.3—Roles y estructuras organizativas de COBIT (cont.)

Rol/estructura	Descripción
Gestor de proyecto	Persona responsable de dirigir un proyecto específico, incluidos la coordinación y delegación del tiempo, presupuesto, recursos y tareas del equipo del proyecto
Oficina de gestión de proyectos	Función responsable de respaldar a los gestores de proyecto y de programa y de recopilar, evaluar y comunicar información sobre la ejecución de los programas y los proyectos que los componen
Función de gestión de datos	Función responsable de respaldar los activos de datos de la empresa durante su ciclo de vida y gestionar la estrategia, infraestructura y repositorios de datos
Director de recursos humanos	El director de más alto rango que rinde cuentas sobre la planificación y las políticas relacionadas con los recursos humanos de la empresa
Gestor de relaciones	Persona experta responsable de supervisar y gestionar la interfaz y comunicaciones internas entre las funciones del negocio y de I&T
Jefe de arquitectura	Persona experta encargada del proceso de arquitectura empresarial.
Jefe de desarrollo	Persona experta que rinde cuentas sobre los procesos de desarrollo de soluciones de I&T
Jefe de operaciones de TI	Persona experta que rinde cuentas sobre los entornos operativos e infraestructura de TI
Jefe de administración de TI	Persona experta que rinde cuentas sobre los registros de I&T y es responsable de apoyar en labores administrativas de I&T
Gestor de servicios	Persona que gestiona el desarrollo, la implementación, la evaluación y el mantenimiento continuo de productos y servicios nuevos o ya existentes, para un cliente específico (usuario) o grupo de clientes (usuarios)
Gestor de seguridad de la información	Persona que gestiona, diseña, supervisa y/o evalúa la seguridad de la información de una empresa
Gestor de continuidad del negocio	Persona que gestiona, diseña, supervisa y/o evalúa la capacidad de continuidad del negocio de una empresa, para garantizar que sus funciones críticas sigan operando después de eventos disruptivos
Director de privacidad	Persona responsable de supervisar el riesgo e impacto de las leyes sobre privacidad en el negocio y de dirigir y coordinar la implementación de políticas y actividades que garanticen el cumplimiento de las directivas de privacidad (En algunas empresas, el puesto podría denominarse oficial o responsable de protección de datos).
Asesor Legal	Función responsable de la asesoría en asuntos legales y regulatorios
Cumplimiento	Función responsable de asesorar sobre todo el cumplimiento externo
Auditoría	Función responsable de la realización de auditorías internas

A.3 Anexo C: Lista de referencias detallada

Los estándares y directrices siguientes contribuyen a las referencias detalladas de los 40 objetivos de gobierno y gestión de COBIT® 2019.

- CIS® Center for Internet Security®, *The CIS Critical Security Controls for Effective Cyber Defense*, Versión 6.1, agosto de 2016
- CMMI® Cybermaturity Platform, 2018
- CMMI® Data Management Maturity (DMM)SM model, 2014
- Committee of Sponsoring Organizations (COSO) Enterprise Risk Management (ERM) Framework, junio de 2017
- European Committee for Standardization (CEN), *e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework*, EN 16234-1:2016

- HITRUST® Common Security Framework, versión 9, septiembre de 2017
- Information Security Forum (ISF), *The Standard of Good Practice for Information Security 2016*
- International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) standards
 - ISO/IEC 20000-1:2011(E)
 - ISO/IEC 27001:2013/Cor.2:2015(E)
 - ISO/IEC 27002:2013/Cor.2:2015(E)
 - ISO/IEC 27004:2016(E)
 - ISO/IEC 27005:2011(E)
 - ISO/IEC 38500:2015(E)
 - ISO/IEC 38502:2017(E)
- Information Technology Infrastructure Library (ITIL®) v3, 2011
- Institute of Internal Auditors® (IIA®), “Core Principles for the Professional Practice of Internal Auditing”• *King IV Report on Corporate Governance™*, 2016
- *King IV Report on Corporate Governance™*, 2016
- US National Institute of Standards and Technology (NIST) standards
 - *Framework for Improving Critical Infrastructure Cybersecurity* V1.1, abril de 2018
 - Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018
 - Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017
- *A Guide to the Project Management Body of Knowledge: PMBOK® Guide Sixth Edition*, 2017
- PROSCI® 3-Phase Change Management Process
- Scaled Agile Framework for Lean Enterprises (SAFe®)
- Skills Framework for the Information Age (SFIA®) V6, 2015
- The Open Group IT4IT® Reference Architecture, versión 2.0
- The Open Group Standard TOGAF® versión 9.2, 2018

Página dejada en blanco intencionadamente