Guía del profesional de riesgos de TI

ISACA

Acerca de ISACA

Durante más de 50 años, ISACA® (*www.isaca.org*) ha promovido el mejor talento, experiencia y aprendizaje en tecnología. ISACA ofrece conocimiento, credenciales, educación y comunidad para que los individuos progresen en sus carreras profesionales y transformen sus organizaciones, y permitan que las empresas formen y desarrollen equipos de calidad. ISACA es una organización de aprendizaje y una asociación global de profesionales que aprovecha la experiencia de sus 145 000 miembros que trabajan en seguridad de la información, gobierno, aseguramiento, riesgo y privacidad para impulsar la innovación a través de la tecnología. Está presente en 188 países, con más de 220 capítulos a nivel mundial.

Descargo de responsabilidad

ISACA ha diseñado y creado la *Guía del profesional de riesgos de TI, 2ª Edición*(el "Trabajo") fundamentalmente como un recurso educativo para profesionales. ISACA no pretende que el uso de cualquier parte del Trabajo garantice un resultado satisfactorio. No se debería considerar que el Trabajo incluye toda la información, los procedimientos y las pruebas apropiadas, ni que excluye otro tipo de información, procedimientos y pruebas que estén orientadas razonablemente hacia la obtención de los mismos resultados. Para determinar la pertinencia de cualquier información, procedimiento o prueba específicos, los profesionales deberían aplicar su propio criterio profesional a las circunstancias específicas presentadas por los sistemas o entorno de tecnología de la información particular.

Reserva de derechos

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA
Phone: +1.847.660.5505
Fax: +1.847.253.1755
Contact us: https://support.isaca.org
Website: www.isaca.org

Participate in the ISACA Online Forums: https://engage.isaca.org/onlineforums

Twitter: http://twitter.com/ISACANews
LinkedIn: www.linkedin.com/company/isaca
Facebook: www.facebook.com/ISACAGlobal
Instagram: www.instagram.com/isacanews/

Guía del profesional de riesgos de TI, 2ª Edición
ISBN 978-1-60420-836-8

Agradecimientos

ISACA desea reconocer a las siguientes personas:

Desarrollador líder
Lisa Young, CISA, CISM, CISSP, Axio, EE.UU.

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

Revisores expertos
Luis Alberto Capua, CRISC, CISM, Argentina
Tom Conkle, CISSP, Optic Cyber Solutions, EE.UU.
Andrew Foo, CISA, CRISC, CISM, CGEIT, CBCP, CCSK, CISSP, PMP, Dulwich College International, China
Sandra Fonseca, Ph.D., CISA, CRISC, CISM, CICA, Northcentral University, EE.UU.
Yalcin Gerek, CISA, CRISC, CGEIT, COBIT 5 Trainer, DASA DevOps Coach, ISO 20000LI, ISO 27001LA, ITIL Expert, PRINCE2, Resilia Practitioner, TAC, Turquía
Ahmad M. El Ghazouly, Ph.D., CISA, CRISC, CISM, PMI-ACP, AMBCI, BISL, PBA, PMP, PMI-RMP, TOGAF, PGESCo, Egipto
Demetri Gittens, CISA, CRISC, Central Bank of Trinidad and Tobago, Trinidad y Tobago
Rob Hanson, CISA, CRISC, CISM, CGEIT, CRMA, Australian Data Standards Body, Canberra, ACT, Australia
Ken Hendrie, CISA, CRISC, CISM, CGEIT, ISO27001 LI, ITIL, PRINCE2, IRAP, Cyconsol, Australia
John Hoffoss, CISA, CISSP, CGIH, CliftonLarsonAllen, EE.UU.
Mike Hughes, CISA, CRISC, CGEIT, MIoD, Prism RA, Reino Unido
John E. Jasinski, CISA, CRISC, CISM, CGEIT, CSX, COBIT 5 Assessor, COBIT and ITIL Accredited Instructor, AWS Practitioner, CCSK, Certified Scrum Master and Product Owner, ISO 20000, IT4IT, ITIL Expert, Lean IT, MOF, ServiceNow and RSA Archer Certified System Administrator, Six Sigma Blackbelt, TOGAF, EE.UU.
Jack Jones, CISA, CRISC, CISM, CISSP, RiskLens, EE.UU.
Linda Kostic, CISA, CISSP, CPA, Doctor of IT-Cybersecurity & Information Assurance, PRMIA Complete Course in Risk Management at George Washington University (GWU), Citi, EE.UU.
Jerry M. Kathingo, CRISC, CISM, Hatari Security, Kenia
Kamal Khan, CISA, CISSP, CITP, MBCS, Reino Unido
Shruti S. Kulkarni, CISA, CRISC, CCSK, CISSP, ITIL v3, Interpublic Group, Reino Unido
Jim Lipkis, Monaco Risk Analytics Inc., EE.UU.
Tony Martin-Vegue, CISM, CISSP, Netflix
Andre Pitkowski, CRISC, CGEIT, COBIT 5 Assessor, APIT Consultoria de Informatica Ltda, Brasil
Eduardo Oscar Ritegno, CISA, CRISC, Banco Nación, Argentina
Gurvinder Pal Singh, CISA, CRISC, CISM, Qantas Airways, Australia
Katsumi Sakagawa, CISA, CRISC, Japón
Darron Sun, CISA, CRISC, CISSP, CMA, CPA (Australia), CRMA, FIPA, Hong Kong Housing Society, China
Peter C. Tessin, CISA, CRISC, CISM, CGEIT, Discover Financial Services, EE.UU.
Alok Tuteja, CRISC, CGEIT, CIA,CISSP, BRS Ventures, Emiratos Árabes Unidos
Ashish Vashishtha, CISA, CRISC, CISM, CIPT, CISSP, AWS Certified Cloud Practitioner, HITRUST CSF Practitioner, PROSCI Change Practitioner, AdventHealth, EE.UU.
Greet Volders, CGEIT, Voquals N.V., Bélgica
Jonathan Waldo, CISA, CRISC, ITIL 4 Foundation, CH Robinson, EE.UU.
Larry G. Wlosinski, CISA, CRISC, CISM, CAP, CBCP, CCSP, CDP, CIPM, CISSP, ITIL v3, PMP, Coalfire-Federal, EE.UU.
Prometheus Yang, CISA, CRISC, CISM, CFE, Standard Chartered Bank, Hong Kong

Agradecimientos *(cont.)*

Revisores expertos (cont.)
Dušan Žikić, CISA, CRISC, CISM, CSX-P, Cybersecurity Audit, Cybersecurity Fundamentals, COBIT 5 Foundation, COBIT 2019 Foundation, COBIT 2019 Design and Implementation, ITIL (2011) Foundation, ITIL 4 Foundation, IBM Data Science, NIS Gazprom Neft, Serbia

Grupo de trabajo de riesgos de TI
Steven Babb, CRISC, CGEIT, ITIL, MUFG Investor Services, Reino Unido
Urs Fischer, CISA, CRISC, CPA (Swiss), UBS Business Solutions AG, Suiza
Jack Freund, Ph.D., CISA, CRISC, CISM, CISSP, RiskLens, EE.UU.
Apolonio Garcia, CRISC, Open FAIR, HealthGuard, EE.UU.
Jimmy Heschl, CISA, CISM, CGEIT, Red Bull, Austria
Gladys Rouissi, CISM, CRISC, ANC Wealth, Australia
James C. Samans, CISA, CRISC, CISM, CBCP, CISSP-ISSEP, CPP, PMP, American Institutes for Research, EE.UU.
Ekta Singh-Bushell, CISA, CGEIT, CISSP, CPA, Datatec, EE.UU.
Dirk Steuperaert, CISA, CRISC, CGEIT, IT In Balance, Bélgica
Evan Wheeler, CRISC, IASO, Edelman Financial Engines, EE.UU.

Consejo de dirección
Tracey Dedrick, Chair, Former Chief Risk Officer, Hudson City Bancorp, EE.UU.
Rolf von Roessing, Vice-Chair, CISA, CISM, CGEIT, CDPSE, CISSP, FBCI, Partner, FORFA Consulting AG, Suiza
Gabriela Hernandez-Cardoso, Independent Board Member, México
Pam Nigro, CISA, CRISC, CGEIT, CRMA, Vice President–Information Technology, Security Officer, Home Access Health, EE.UU.
Maureen O'Connell, Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., EE.UU.
David Samuelson, Chief Executive Officer, ISACA, EE.UU.
Gerrard Schmid, President and Chief Executive Officer, Diebold Nixdorf, EE.UU.
Gregory Touhill, CISM, CISSP, President, AppGate Federal Group, EE.UU.
Asaf Weisberg, CISA, CRISC, CISM, CGEIT, Chief Executive Officer, introSight Ltd., Israel
Anna Yip, Chief Executive Officer, SmarTone Telecommunications Limited, Hong Kong
Brennan P. Baybeck, CISA, CRISC, CISM, CISSP, ISACA Board Chair, 2019-2020, Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, EE.UU.
Rob Clyde, CISM, ISACA Board Chair, 2018-2019, Independent Director, Titus, and Executive Chair, White Cloud Security, EE.UU.
Chris K. Dimitriadis, Ph.D., CISA, CRISC, CISM, ISACA Board Chair, 2015-2017, Group Chief Executive Officer, INTRALOT, Grecia

TABLA DE CONTENIDOS

Esta página se dejó en blanco intencionalmente

LISTA DE FIGURAS

Capítulo 1. Presentación de la Guía del profesional de riesgos de TI

Capítulo 2. Establecimiento del contexto y el alcance de las actividades de la gestión de riesgos

Capítulo 3. Conceptos esenciales del gobierno de riesgos

Capítulo 4. Fundamentos de evaluación de riesgos

Capítulo 5. Definición de escenarios de riesgo

Capítulo 6. Orientación para construir escenarios de riesgo

Capítulo 7. Conceptos esenciales de la respuesta al riesgo

Esta página se dejó en blanco intencionalmente

Capítulo 1
Presentación de la *Guía del profesional de riesgos de TI*

1.1 Visión general de riesgos de TI

La *Guía del profesional de riesgos de TI* se refiere a los riesgos de información y tecnología (I&T); en otras palabras, el riesgo para el negocio o la misión que está relacionado con el uso o la dependencia de la tecnología de la información y comunicación (TIC),[1] la tecnología operacional (TO),[2] la red o internet de las cosas (IoT),[3] los datos electrónicos, y las comunicaciones digitales o electrónicas. La conexión con el negocio o la misión se encuentra en los principios en los que se elabora el *Marco de riesgos de TI*, *2ª Edición* publicado por separado como un documento relacionado con esta guía; es decir, el gobierno y la gestión efectivos de la empresa de todos los tipos de riesgos relacionados con la tecnología y la información.

La denominación I&T, tal como se usa en este documento, incluye, pero no se limita a, la seguridad de la información, el aseguramiento de la información y la ciberseguridad como subtipos del riesgo de I&T.

La *Guía del profesional de riesgos de TI* (esta publicación) contiene una orientación práctica y, a veces, más detallada sobre cómo llevar a cabo algunas de las actividades descritas en su publicación complementaria, el *Marco de riesgos de TI*. El *Marco de riesgos de TI* describe las tareas y las actividades o, de manera más simple, el "qué hacer" para gestionar los riesgos de I&T. En esta publicación, se hace referencia a términos y conceptos que se presentan en el *Marco de riesgos de TI*, como "taxonomía de riesgo", "apetito de riesgo", "identificación del riesgo", "análisis de riesgos" e "indicadores clave de riesgo (KRI)". El lector de este documento podría querer familiarizarse con las definiciones del *Marco de riesgos de TI* y el apéndice B de la presente publicación, antes de aplicar las tareas y las actividades en su empresa.

La gestión de riesgos es una capacidad empresarial o, simplemente, una capacidad que acciona una empresa que describe un conjunto colectivo de actividades que se desarrollan para lograr un resultado específico. La capacidad de gestión de riesgos sustenta todos los procesos del negocio para garantizar que la empresa continúe creando y aportando valor. Las actividades de la gestión de riesgos precisan de personas, procesos y tecnología y podrían automatizarse con software y sistemas, así como también supervisarse por los más altos niveles de la organización. La gestión de riesgos funciona mejor cuando está integrada en el flujo de trabajo habitual del personal y la dirección, en lugar de ser una actividad añadida.

Los beneficios de la gestión de riesgos de I&T efectiva incluyen:

- una mejor supervisión de los activos de la organización;
- unas pérdidas reducidas o minimizadas;
- un uso más rentable de los recursos;
- la identificación proactiva de amenazas, vulnerabilidades y potenciales impactos;
- la priorización de los esfuerzos de respuesta al riesgo para que se corresponda con las prioridades y las metas de la organización;
- una base más holística y un planteamiento para el cumplimiento legal y regulatorio;
- una mayor probabilidad de éxito de los proyectos;
- un mejor rendimiento en la empresa, que conduce a una mayor confianza de las partes interesadas;

[1] NIST, "Information and Communications Technology (ICT)," Computer Security Resource Center, *https://csrc.nist.gov/glossary/term/information_and_communications_technology*
[2] NIST, "Operational Technology (OT)," Computer Security Resource Center, *https://csrc.nist.gov/glossary/term/operational_technology*
[3] Voas, Jeffrey; "Network of 'Things'," 800-183, NIST, July 2016, *https://csrc.nist.gov/publications/detail/sp/800-183/final*

- la creación de una cultura consciente de los riesgos con menor dependencia exclusiva de los especialistas de riesgos;
- una mejor gestión de la continuidad de negocios y los incidentes;
- unos factores relevantes para el diseño de controles eficientes con una supervisión y presentación de informes mejoradas;
- una mejor toma de decisiones como resultado de un acceso más profuso a información oportuna y precisa;
- un aumento de la capacidad para conseguir los objetivos del negocio y crear valor.

Para los lectores que buscan una estructura global sobre la que reflexionar en relación con la gestión de riesgos, se recomienda consultar el *Marco de riesgos de TI* (publicado por separado).

Para los lectores que buscan orientación sobre el gobierno de la gestión de riesgos, los capítulos 1, 2, 3 y 6 de la *Guía del profesional de riesgos de TI* resultan más aplicables.

Para los lectores que buscan orientación sobre la gestión o los factores relevantes para la implementación de las actividades de gestión de riesgos, los capítulos 1, 2, 4, 5 y 6 de la *Guía del profesional de riesgos de TI* son los más aplicables.

Para aquellos lectores que están más familiarizados con los procesos de COBIT® 2019 y, en consonancia, con los principios de ISACA de que el gobierno y la gestión son conjuntos diferenciados de actividades, este documento está dividido acorde a las secciones que incluyen cada área definida de gobierno y gestión. Ver la **figura 1.1**.

1.1.1 El lenguaje del riesgo

Las evaluaciones de riesgo de I&T y las decisiones significativas sobre los riesgos de I&T requieren que el riesgo de I&T se exprese en términos inequívocos y claros que sean relevantes para el negocio o la misión relacionados con cuestiones tales como las finanzas, los ingresos o la capacidad para alcanzar los resultados estratégicos deseados. Una gestión de riesgos efectiva requiere una comprensión mutua entre el área de I&T y el resto del negocio sobre qué riesgo debe gestionarse, y por qué. Todas las partes interesadas deben tener la capacidad de comprender y expresar cómo los eventos adversos, también conocidos como incidentes o riesgos materializados, podrían afectar a los objetivos del negocio o la misión. Esto significa que existe un entendimiento compartido de que:

- Los fallos relacionados con I&T, los errores o los eventos pueden impactar en los objetivos de la empresa y dar resultado a pérdidas directas (costes, p. ej. financieros) o indirectas (información, p. ej. datos sensibles de clientes), provocando daños reputacionales.
- Para la empresa, las pérdidas de los eventos relacionados con la I&T pueden afectar a la capacidad de que una organización ofrezca sus productos y servicios clave. Esto es cierto incluso cuando la empresa depende de proveedores de I&T para suministrar bienes y servicios que son esenciales para sus objetivos estratégicos.

La comunicación sobre los riesgos precisa que los términos utilizados en la empresa para expresar y describir el riesgo tengan un significado de común entendimiento. Una **taxonomía** de riesgo constituye un esquema para clasificar las fuentes y las categorías del riesgo. El tránsito entre una amenaza cibernética o área de preocupación y un riesgo requiere que la descripción de riesgos se descomponga en componentes sobre los que se pueda actuar. Una taxonomía de riesgo proporciona un lenguaje común para discutir y comunicar el riesgo a las partes interesadas. Consulte el Apéndice A: Recursos de riesgos para referencias de fuentes de información relacionadas con el riesgo, las taxonomías de riesgo y la gestión de riesgo.

Los conceptos clave de riesgo se tratan en diferentes contextos a lo largo de esta publicación. Es frecuente que las personas que carecen de una comprensión plena sobre los términos de riesgos los utilicen indistintamente, pero al hacerlo pueden crear confusión, impedir una gestión de riesgo satisfactoria y sembrar dudas sobre su competencia profesional. Por ejemplo, cuando los términos “amenaza”, “vulnerabilidad”, “instancia” y “riesgo” se usan de

manera indistinta o inconsistente no siempre queda claro lo que se está comunicando. El profesional de riesgos debería asegurarse de dedicar el tiempo suficiente a estudiar el lenguaje para obtener un conocimiento confiable y básico de los diferentes términos y de cómo se relacionan entre sí. Para obtener información más detallada sobre la terminología de riesgos, consulte el Capítulo 1 del *Marco de riesgos de TI* (publicado por separado).

El riesgo se puede tratar en términos cuantitativos (usando números) o cualitativos (usando palabras descriptivas), y las definiciones específicas del riesgo suelen variar de fuente a fuente. La naturaleza fundamental del riesgo es la incertidumbre. Esto supone que la incertidumbre de que el riesgo se materialice y conduzca a pérdidas o daños podría suceder, o no, y generalmente se trata usando términos como "probabilidad", "verosimilitud", "volatilidad" y "frecuencia". Otra parte de la incertidumbre es lo que supondrían las pérdidas o los daños para la organización si ese riesgo se materializara y, generalmente, se trata usando términos tales como "impacto", "magnitud" o "consecuencia". Los intentos primigenios para definir el riesgo observaron que la probabilidad de que algo sucediera era una combinación de dos cosas: que sucediese algo con potencial de daño (p. ej. ataques de denegación de servicio [DoS], correos electrónicos enviados por error al destinatario equivocado, eventos meteorológicos peligrosos), y que el objetivo del evento fuese propenso al ataque (vulnerabilidad). La mayor parte del tiempo, una empresa tiene poco control sobre las amenazas, las vulnerabilidades u otras condiciones del entorno en el que opera. Sin embargo, la empresa sí tiene control directo sobre cómo se identifica, evalúa o analiza y gestiona el riesgo.

A medida que se ha desarrollado la práctica de la gestión de riesgos, los profesionales de riesgos han comenzado a distinguir entre las condiciones (factores de riesgo) y el grado en el que esos factores afectan a las actividades de creación de valor de la organización (impacto). En la actualidad, es habitual distinguir entre diferentes tipos de amenazas, evaluarlas en base a los activos de I&T específicos de la organización contra los que pueden dirigirse, y analizar esos activos en términos de sus debilidades individuales (vulnerabilidades) que podrían explotarse para impactar en el negocio o la misión.

A medida que se ha desarrollado la práctica de la gestión de riesgos, los profesionales de riesgos han comenzado a distinguir entre las condiciones (factores de riesgo) y el grado en el que esos factores afectan a las actividades de creación de valor de la organización (impacto).

El *Marco de riesgos de TI* y la *Guía del profesional de riesgos de TI* están diseñados para ayudar a desarrollar, implementar o mejorar la práctica de la gestión de riesgos al:

- vincular el contexto de negocio con los activos de I&T específicos;
- trasladar el centro de atención a las actividades sobre las que la empresa tenga un control significativo, como dirigir y gestionar de manera activa el riesgo, minimizando a la vez la atención a las condiciones sobre las que la empresa tiene poco control (agentes de las amenazas);
- extender el planteamiento del uso de un lenguaje de riesgo común que etiquete correctamente los elementos que deben gestionarse bien para crear valor.

Cuando se contempla desde la perspectiva de la forma en que los activos de I&T se usan dentro de la organización, los activos tienen valor por causa del propósito de negocio o la misión a la que prestan servicio. Un activo de I&T, por sí mismo, puede ser fácilmente reemplazable, como el hardware de un servidor, o muy susceptible a las vulnerabilidades, como el software. Sin embargo, sin el contexto del negocio o la misión, no es posible entender por completo la criticidad de los activos de I&T. Este paso de la evaluación de riesgos (en general cualitativa) al análisis de riesgos (habitualmente cuantitativo) hace posible comunicar de manera más clara el impacto en términos de productividad perdida y otras medidas específicas de valor, que es útil por muchos motivos:

1. El uso de un valor cuantitativo para las pérdidas (o ganancias), empleando términos monetarios, temporales, unidades de productividad u otros valores medibles, es más fácil de comunicar a todos.
2. Establecer si cada consecuencia es o no aceptable en docenas o más áreas diferentes de funciones del negocio o la misión, usando sólo etiquetas cualitativas (bajo, alto, catastrófico) con escalas de medición diferentes, no permite la toma de decisiones sobre el riesgo seguras o justificadas.

3. La cuantificación de las pérdidas potenciales u otros impactos negativos asociados al riesgo proporciona una base para decidir cómo responder ante el riesgo que esté fuera de la tolerancia de los niveles aceptables, y cuándo puede ser aplicable un planteamiento de mitigación tradicional basado en controles.
4. No todos los activos de I&T son iguales, y el presupuesto necesario para responder al riesgo debería estar en consonancia con el valor o la criticidad del activo en el logro de los objetivos del negocio y la misión.

Para las empresas que desean mejorar sus prácticas de gestión de riesgos, la *Guía del profesional de riesgos de TI* puede proporcionar un acelerador de soluciones, no de manera prescriptiva, sino como una plataforma sólida sobre la que se puede construir una práctica de gestión de riesgos mejorada. La *Guía del profesional de riesgos de TI* se puede utilizar para ayudar a establecer una estructura de gestión de riesgos de I&T en la empresa, y para mejorar las prácticas de gestión de riesgos de I&T ya existentes.[4]

El marco de riesgos de TI se describe en detalle en la publicación del *Marco de riesgos de TI*. Para facilitar la consulta, la **figura 1.1** contiene una visión general gráfica sobre el marco de riesgos de TI y sus componentes, y cómo los principios se alinean con los objetivos de COBIT EDM03 *Asegurar la optimización del riesgo* y APO12 *Riesgo gestionado*.

[4] Esta guía no pretende ser completa o integral. Además de las técnicas y prácticas descritas aquí, existen otras técnicas y soluciones viables que pueden aplicarse para la gestión de riesgos de I&T.

Figura 1.1—Marco de riesgos de TI

Se alinea a EDM03 Asegurar la optimización del riesgo	Se alinea con APO12 Riesgo gestionado
Gobierno de riesgos Asegurar que el apetito y la tolerancia al riesgo de la empresa se entiendan, evidencien y comuniquen, y de que el riesgo para el valor empresarial relacionado con el uso de I&T se identifique y se gestione.	**Gestión de riesgos** Identificar, evaluar y reducir continuamente los riesgos relacionados con I&T hasta los niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
Dirigir la gestión de riesgos. Dirigir el establecimiento de las prácticas de gestión de riesgos para proporcionar un aseguramiento razonable de que las prácticas de gestión de riesgos de I&T son apropiadas, y de que el riesgo actual de I&T no sobrepase al apetito de riesgo del consejo.	**Recopilar datos.** Identificar y recopilar datos relevantes para habilitar la identificación efectiva, el análisis y el informe de los riesgos relacionados con la I&T.
Monitorizar la gestión de riesgos. Monitorizar las metas y las métricas clave de los procesos de gestión de riesgos. Determinar cómo se identificarán las desviaciones o problemas, se hará su seguimiento y se comunicarán para su reparación.	**Analizar el riesgo.** Desarrollar una visión fundamentada del riesgo real de I&T, que soporte las decisiones de riesgo.
Evaluar la gestión de riesgos. Examinar y evaluar continuamente el efecto del riesgo sobre el uso empresarial actual y futuro de la I&T. Considerar si el apetito de riesgo de la empresa es apropiado, y asegurarse de que se identifique y gestione el riesgo para el valor empresarial relacionado con el uso de I&T.	**Mantener un perfil del riesgo.** Mantener un inventario de los riesgos conocidos y los atributos del riesgo, incluyendo la frecuencia esperada, el impacto potencial y las respuestas. Documentar los recursos, las capacidades y las actividades de control actuales relacionadas con elementos de riesgo.
	Evidenciar 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 elaborar una respuesta apropiada.
	Definir un catálogo de acciones de gestión de riesgos. Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como una cartera (portfolio).
	Responder al riesgo. Responder de manera oportuna a eventos de riesgo materializados con medidas efectivas para limitar la magnitud de las pérdidas.

Fuente: ISACA, *The Risk IT Framework, 2nd Edition*, USA, 2020, figura 3.1, *https://www.isaca.org/bookstore/bookstore-risk-digital/ritf2*

Hay más orientación disponible en el artículo técnico de ISACA *Getting Started with Risk Management (Cómo empezar con la gestión de riesgos)*, la publicación del *Marco de riesgos de TI* y las referencias a COBIT® cuando corresponda.

Capítulo 2
Establecimiento del contexto y el alcance de las actividades de la gestión de riesgos

2.1 Establecimiento del contexto para la gestión de riesgos

El posicionamiento del riesgo en el contexto de la misión, la estrategia y los objetivos de la empresa es el primer paso para asegurarse de que las actividades de gestión de riesgos aportan valor al proceso general de la gestión de riesgos de la empresa. Esto se conoce como establecimiento del contexto para la gestión de riesgos. Combinar un enfoque basado en riesgos con una visión estratégica de la empresa permite comunicar y aclarar qué incertidumbres, o riesgos, tienen mayor potencial para impedir que la empresa cumpla con las metas, los objetivos y la misión previstos. Para aquellos profesionales que están más familiarizados con COBIT 2019, las actividades de este capítulo están relacionadas con el objetivo APO12 *Riesgo gestionado*.[5]

El establecimiento de los criterios frente a los que se vaya a evaluar el riesgo identificado es también una parte importante del proceso general de gestión de riesgos. El desarrollo del apetito de riesgo y las tolerancias al riesgo pueden ayudar a la rápida evaluación y comprensión sobre los riesgos que se encuentran en consonancia con los objetivos de la dirección para la adopción de riesgos y los riesgos que precisan de más análisis o investigación para determinarlo.

La gestión del riesgo de I&T de la empresa comienza por la definición del universo de riesgo. Un universo de riesgo describe el entorno (del riesgo) general (es decir, define los límites de las actividades de la gestión de riesgos) y proporciona una estructura para gestionar el riesgo de I&T. La selección de los elementos incluidos en las actividades de riesgo generalmente se basa en la comprensión del universo de riesgo completo, seguida de la selección de la parte específica de la empresa a la que se aplicarán las actividades de riesgo. Esto suele llamarse alcance del riesgo. El universo del riesgo:

- Tiene en cuenta la misión global y los objetivos de la empresa, los procesos de negocio y las dependencias en toda la empresa. La identificación de las dependencias de la I&T ayudará a entender el riesgo que afecta a las diferentes funciones y operaciones de la organización.
- Describe los componentes, los procesos, los activos y la infraestructura de I&T que respaldan los objetivos del negocio y la misión.
- Describe el riesgo en un lenguaje completo y exhaustivo para que pueda contemplarse desde una perspectiva de extremo a extremo del negocio o la misión.
- Tiene en cuenta la cadena de valor completa de la empresa para incluir filiales, unidades de negocio, clientes, suministradores y proveedores de servicios. Estas designaciones pueden ser merecedoras de atención al establecer el alcance de las actividades de riesgo.
- Incluye una segmentación lógica y práctica del panorama de riesgo global en el que opera la empresa (p. ej. unidades o subunidades organizativas; procesos o servicios de negocio; ubicaciones geográficas; tipos de tecnología, tal como función interna de TI en contraposición con componentes en la nube; y otras áreas en las que pueda haber oportunidades para alinear visiones distintas en toda la empresa).
- Alinea la planificación estratégica de la organización con la identificación de los tipos de riesgo que tendrían el mayor impacto en el logro de la estrategia y los objetivos de negocio.
- También está influido por el clima de negocio o el entorno geopolítico en el que opera la empresa.

[5] Ver ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018, *https://www.isaca.org/bookstore/bookstore-cobit_19-print/cb19fgm*.

2.1.1 Alcance de las actividades de gestión de riesgos de I&T

La gestión de riesgos precisa que se establezca el alcance del panorama del riesgo, o universo del riesgo, y que se definan los criterios frente a los que se evaluará y analizará el riesgo identificado. La gestión de riesgos comienza con la comprensión de la organización, pero el profesional de riesgos debería tener en cuenta que la organización está fuertemente influenciada por el entorno, o contexto, en el que opera. Esto es especialmente cierto en organizaciones que operan en un mismo sector de actividad económica, como los servicios financieros, el manufacturero o los servicios de salud, porque existe una fuerte dependencia de muchas de las mismas cadenas de suministro.

El alcance debería determinarse en el contexto de los objetivos de la organización. El establecimiento del contexto ayudará a identificar dónde encaja el alcance de la evaluación de riesgos inicial en el contexto general de la empresa (p. ej. en una función del negocio, como la contabilidad). Se puede elaborar una definición de un alcance inicial, preliminar, para las actividades de gestión de riesgos utilizando una evaluación de alto nivel sobre los riesgos de I&T globales a los que se enfrenta la empresa. En la práctica, esto puede lograrse examinando los componentes del negocio, la misión u otros componentes del panorama de riesgo. El contexto preliminar proporciona una perspectiva del riesgo inherente de la empresa (es decir, una evaluación de riesgos de I&T sin tener en cuenta ningún resultado de análisis detallado del riesgo y, por lo tanto, sin considerar los controles existentes u otras respuestas al riesgo).

Otros factores que pueden considerarse incluyen:

- la dependencia de la organización de una cadena de suministro, especialmente con sede en otra región geográfica del mundo o con entrega 'justo a tiempo';
- las influencias de la financiación, la deuda y los socios o las partes interesadas importantes;
- la vulnerabilidad a los cambios en las condiciones políticas o económicas;
- los cambios en los patrones y las tendencias del mercado;
- la aparición de nueva competencia;
- el impacto de nueva legislación;
- la existencia de posibles desastres naturales;
- las restricciones causadas por los sistemas heredados y la tecnología obsoleta;
- las relaciones de trabajo tensas y la gestión rígida;
- el clima geopolítico, las consideraciones regulatorias y de privacidad;
- cualquier obligación contractual que introduzca un riesgo en la empresa si no se gestiona bien, como cláusulas de responsabilidad del producto o de indemnización por daños y perjuicios.

El resultado de la actividad de alcance de riesgo se usa para centrar y priorizar las actividades más detalladas de gestión de riesgos. La evaluación:

- permite la identificación de las áreas potenciales con riesgos de alto impacto en toda la empresa;
- proporciona una visión general de los factores de riesgo significativos a los que está sujeta la empresa, tenga o no la capacidad de influir en ellos;
- recopila datos sobre cualquier obligación general de cumplimiento, regulatoria, de privacidad o de otro tipo (p. ej. el Reglamento General de Protección de Datos [RGPD], la Ley de Portabilidad y Responsabilidad de Seguro de Salud [HIPAA], o las regulaciones específicas del país), u obligaciones contractuales que comprometan a la empresa a actividades específicas de gestión de riesgos;
- Proporciona las primeras pistas sobre los principales escenarios de riesgo, que son contribuciones importantes para la fase de desarrollo de escenarios de las actividades de análisis de riesgos más detalladas que deben llevarse a cabo en una etapa posterior.

La actividad de alcance de riesgo de la empresa podría tener que repetirse periódicamente. Esto puede consistir en una simple confirmación anual de resultados previos si no se han producido cambios importantes en ninguno de los factores de riesgo, pero si se han producido cambios importantes para la empresa (p. ej. fusiones, nuevos mercados), la actividad de definición del alcance debería reiterarse por completo. En entornos estables, se recomienda una actualización o confirmación anual del alcance preliminar. También se recomienda evaluar periódicamente las actividades de riesgo para asegurarse de que los activos y los servicios más importantes estén incluidos en el alcance. Algunas empresas comienzan con los activos de alto valor que respaldan los productos, los procesos y las líneas de negocio más críticas, y luego extienden el alcance cuando la capacidad de gestión de riesgos madura.

Un ejercicio de definición del alcance del riesgo de I&T de la empresa involucra a todas las partes interesadas principales de la empresa. En el Capítulo 4 del *Marco de riesgos de TI* se identifican las partes interesadas para la gestión de riesgos. La evaluación debería ser facilitada por un profesional de gestión de riesgos experimentado que garantice la imparcialidad y la coherencia en toda la empresa.

Los datos que hay que recopilar en la actividad de definición del alcance incluyen:

- las unidades o subunidades organizativas, los procesos de negocio o, y las ubicaciones geográficas que estarán sujetos a las actividades de la gestión de riesgos;
- los criterios de impacto, p. ej. las posibles consecuencias del riesgo materializado, y las declaraciones del apetito de riesgo y la tolerancia al riesgo de la empresa;
- la calificación actual, los índices de severidad, u otros criterios de métricas o mediciones de riesgo que se usen en la empresa;
- la intensidad y la extensión previstas para las actividades de gestión de riesgos;
- las áreas definidas que estarán sujetas a los requisitos de análisis y presentación de informes;
- el perfil de riesgo actual de la entidad organizativa, si es que existe;
- las autoevaluaciones de riesgo y los controles que pudiesen haberse realizado;
- las prioridades de auditoría o de cumplimiento.

Una reunión o discusión, en forma de ejercicio de simulación o de “recorrido de escenario”, usando una preocupación común que puedan tener muchas partes interesadas, es una manera práctica de reunir a las líneas de negocio, las áreas funcionales y otras áreas de riesgo específicas.Esto es especialmente útil para las empresas que están tratando de contemplar las perspectivas tanto de línea de negocio, como funcional. Por ejemplo, si la protección de los datos de clientes de un interés relevante para el negocio, una preocupación común puede ser el riesgo de una violación de la privacidad, o la pérdida o destrucción de los registros de datos. También podría haber hallazgos recurrentes de auditoría relacionados con muchas áreas funcionales que podrían usarse como un caso inicial para aplicar las prácticas de gestión de riesgos en toda la organización, en lugar de abordar el problema tan solo en un área funcional, o silo, de la organización.

Una reunión o discusión, en forma de ejercicio de simulación o de “recorrido de escenario”, usando una preocupación común que puedan tener muchas partes interesadas, es una manera práctica de reunir a las líneas de negocio, las áreas funcionales y otras áreas de riesgo específicas.

2.1.2 Flujo de trabajo de la gestión de riesgos

El flujo de trabajo de la gestión de riesgos consta de los siguientes pasos. Los pasos no tienen por qué realizarse de manera lineal o secuencial. Cada organización deberá desarrollar un flujo de trabajo que constituya la forma más eficiente y efectiva de realizar estos pasos. Para facilitar su posterior referencia, la **figura 2.1** incluye una visión gráfica general de los pasos.

Figura 2.1—Flujo de trabajo de la gestión de riesgos

Fuente: ISACA, *The Risk IT Framework, 2nd Edition*, USA, 2020, figura 5.1, *https://www.isaca.org/bookstore/bookstore-risk-digital/ritf2*

El ejemplo del flujo de trabajo de la gestión de riesgos (que ilustra la **figura 2.1**) incluye los siguientes pasos:

1. Como parte del establecimiento del contexto:
   a. Definición del alcance de la evaluación de riesgos: Definir los objetivos y los límites de la evaluación. Incluir la información relevante, idealmente derivada de o vinculada a las declaraciones de apetito de riesgo y tolerancia al riesgo. Realizar la evaluación conjuntamente con los representantes de negocio involucrados. La dirección del negocio y el personal que trabaja en primera línea de las actividades del negocio o la misión suelen ser las mejores fuentes para determinar las áreas de preocupación que podrían necesitar más investigación o análisis.
   b. Recopilación de datos: Asegurarse de que se utilizan todas las fuentes posibles para recopilar datos importantes sobre amenazas, vulnerabilidades, condiciones, áreas de preocupación o riesgos conocidos para los objetivos del negocio o la misión. Esto incluye los repositorios de incidentes de I&T, los informes de vulnerabilidades de la tecnología y logs de cambios, así como informes de riesgos previos y datos externos, tales como análisis de tendencias de I&T y cambios regulatorios.
2. Como parte de la identificación y evaluación del riesgo:
   a. Identificación de los factores de riesgo comunes: Verificar que los eventos interrelacionados estén agrupados por tipo. Los factores de riesgo comunes pueden obtenerse de una taxonomía de riesgo o de un catálogo de controles. Estos factores pueden influir en la frecuencia y el impacto de los eventos que podrían tener un impacto significativo en el negocio.

   b. Identificación de las áreas de preocupación: La dirección y el personal suelen preocuparse por las tareas y las actividades que podrían exponer a la empresa o hacer que la empresa se vuelva más susceptible a ciertos tipos de riesgo. A veces, los profesionales de la ciberseguridad o de la seguridad de la información pueden denominar como "superficie de ataque" al aumento de la exposición al riesgo. Este es un paso apropiado en el que involucrar a las partes interesadas para garantizar una identificación minuciosa de todas las preocupaciones.

3. Como parte del análisis de riesgos y el impacto en el negocio:
   a. Análisis del riesgo de I&T: Realizar una evaluación cualitativa o un análisis cuantitativo para estimar la frecuencia y el impacto de los escenarios, teniendo en cuenta los factores de riesgo (que pueden incluir a los controles actuales). Los escenarios y la manera de utilizarlos se explican con más detalle en el Capítulo 4 de esta publicación. Los niveles definidos de tolerancia al riesgo (como se explica en el Capítulo 3 de esta publicación) también deben considerarse. Estos servirán como la base para determinar la respuesta al riesgo. Este paso debe ser realizado con los representantes del negocio relevantes y en colaboración con las funciones de supervisión de riesgos, si estas existen.
4. Como parte de la respuesta al riesgo:
   a. Identificación de las opciones de respuesta al riesgo: Este paso debería realizarse en cooperación con los propietarios relevantes de procesos de negocio que dependan de las áreas de I&T que están siendo evaluadas.
   b. Comprensión de los controles o procesos que ya están actualmente implementados o que deben diseñarse, y de cómo funcionan para prevenir, detectar, mitigar, transferir o monitorizar el riesgo.
5. Como parte de la presentación de informes y comunicación de riesgos:
   a. Revisión de la evaluación: En la revisión del resultado de la evaluación debe incluirse a las partes interesadas relevantes de la parte empresarial. Esto mejorará la aceptación del negocio de los resultados de la evaluación, y también servirá como una manera de incluir sus aportaciones en las acciones de respuesta.
   b. Presentación de informes: Proporcionar a la directiva los resultados de la evaluación y los análisis correspondientes para respaldar la toma de decisiones.

COBIT 2019 adopta un enfoque similar, pero ligeramente diferente, de un flujo de trabajo de riesgo (ver la **figura 2.2**).[6]

Figura 2.2—COBIT 2019 APO12 *Riesgo gestionado*

2.1.3 Ejemplo de flujo de trabajo de gestión de riesgos usando un diagrama de cadena de responsabilidad (funcional)

Esta sección describe un ejemplo de flujo de trabajo de gestión de riesgos en un diagrama funcional (ver la **figura 2.3**). Este diagrama funcional, también conocido como diagrama de cadena de responsabilidad (swimlane), hace referencia a varios tipos de actividades de la gestión de riesgos y no constituye la única manera de llevar a cabo las actividades.

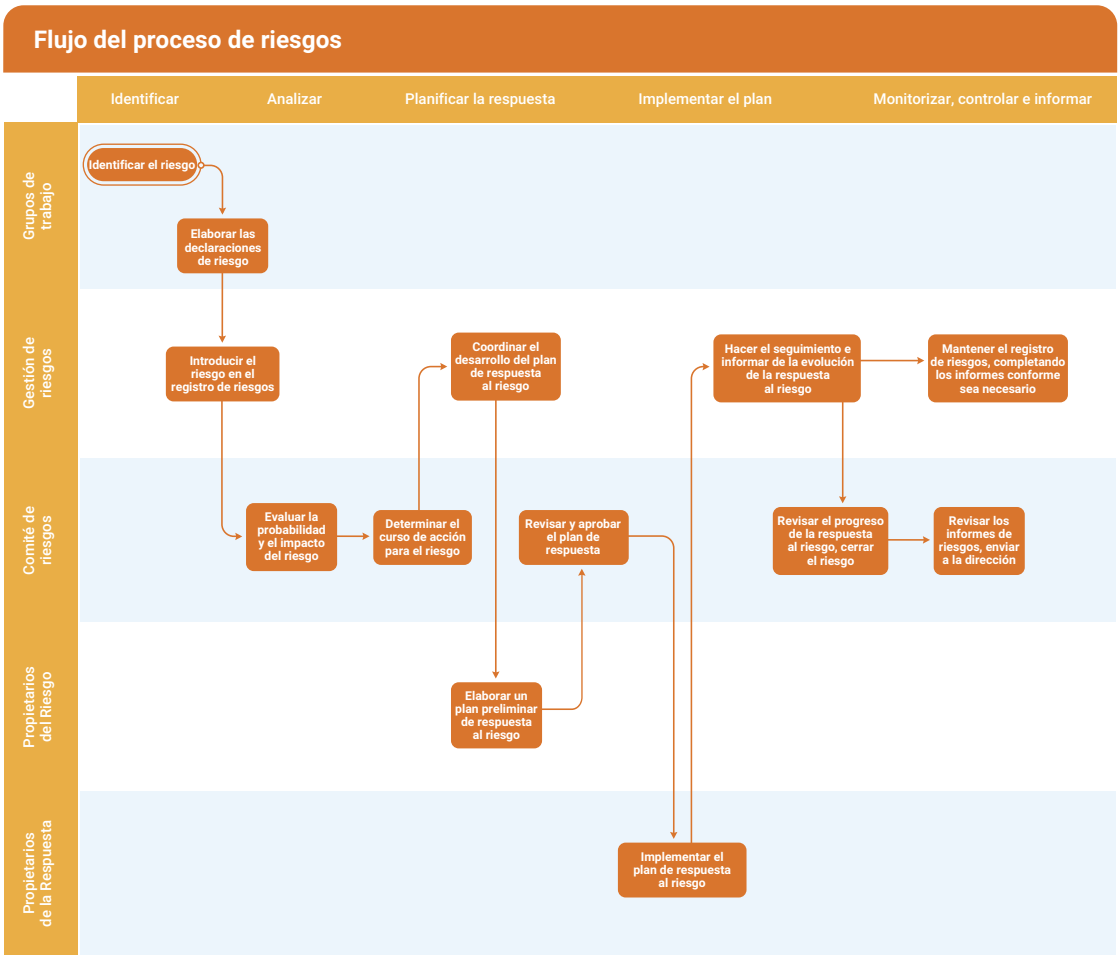
[6] Para conocer las actividades que soportan el flujo de trabajo de riesgo de COBIT 2019, consulte ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, APO12 *Managed risk*.

La guía aquí provista aúna varios conceptos y actividades para ayudar a que las prácticas sean más utilizables de manera apropiada. En este contexto, se usan los siguientes supuestos:

- El gobierno de riesgos está implementado y funcionando correctamente en la empresa. Esto significa que se realizan evaluaciones de riesgos periódicas, usando una escala de impacto o un conjunto de criterios definidos organizacionalmente, y están definidos el apetito de riesgo y las tolerancias que se pueden utilizar para establecer umbrales operativos, indicadores o disparadores usados para iniciar las actividades de gestión de riesgos.
- Los criterios de evaluación y análisis de riesgos se utilizan para actualizar el registro de riesgos, los mapas de riesgo y el perfil de riesgo, si lo hay.

El riesgo se identifica de manera proactiva, usando diversas técnicas y métodos, y hay forma de obtener o aceptar los informes de un área de preocupación para que pueda investigarse más a fondo.

Figura 2.3—Ejemplo de diagrama funcional (o de cadena de responsabilidad)



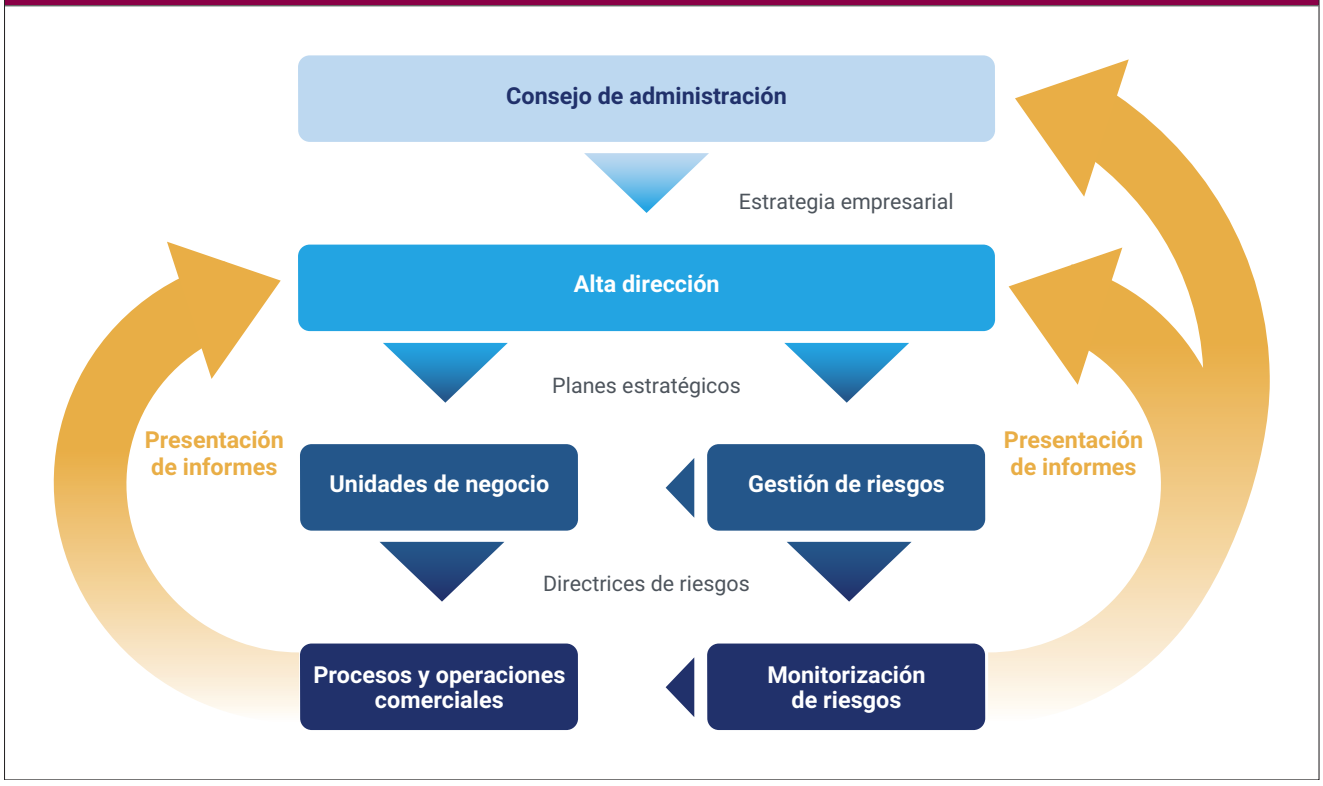
Capítulo 3
Conceptos esenciales del gobierno de riesgos

3.1 Gobierno

El término "gobierno" ha pasado a la vanguardia del pensamiento empresarial como respuesta a los ejemplos que prueban la importancia de una supervisión efectiva, por una parte, y los graves perjuicios para el negocio global derivados de una supervisión deficiente, por otra. El gobierno corporativo es el sistema mediante el que las organizaciones se evalúan, dirigen y monitorizan. Por lógica, el gobierno corporativo de la I&T es el sistema mediante el cual se evalúa, dirige y monitoriza el uso actual y futuro de la I&T. El objetivo de cualquier sistema de gobierno es permitir que las organizaciones creen valor para sus partes interesadas o promover la creación de valor. La creación de valor, a su vez, incluye la obtención de beneficios, la optimización de los riesgos y la optimización de los recursos. La optimización de los riesgos es una parte fundamental para cualquier sistema de gobierno, y no se puede considerar aisladamente de la obtención de beneficios o de la optimización de los recursos. Para aquellos lectores que están familiarizados con COBIT, el contenido de esta sección es coherente con el objetivo de gobierno de COBIT 2019 EDM03 *Asegurar la optimización del riesgo*.[7]

El gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para establecer que deben alcanzarse unos objetivos empresariales equilibrados y acordados; la dirección se establece por medio de la priorización y la toma de decisiones; y se monitoriza el desempeño, el cumplimiento y el progreso respecto de la dirección y los objetivos acordados. En la mayoría de las empresas, el gobierno es responsabilidad del consejo de administración bajo el liderazgo del presidente, como muestra la **figura 3.1**.

Figura 3.1—Gobierno de riesgos



[7] Ver ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, EDM03 *Ensured risk optimization*.

Un buen gobierno implica que la optimización de los riesgos forme parte de los planes vigentes, y que la información sobre los riesgos esté incluida en el proceso de toma de decisiones. Al mismo tiempo, la función de riesgo debe gobernarse: es decir, debe estar provista de dirección y monitorizada.

Los temas tratados en este capítulo incluyen:

1. el apetito de riesgo y la tolerancia al riesgo;
2. la cultura de riesgos;
3. la política de riesgos;
4. los indicadores clave de riesgo (KRI);
5. el perfil del riesgo;
6. los mapas de riesgos y agregación de riesgos para la toma de decisiones del consejo y la ejecutiva.

El tema de la "capacidad de riesgo" se trata en el *Marco de riesgos de TI* (publicado por separado) y no se repite en este documento.

3.1.1 El apetito de riesgo y la tolerancia al riesgo

Al formular sus estrategias y planes operativos, una empresa se expone a cierto nivel de riesgo para lograr sus objetivos. La cantidad de riesgo se expresa, generalmente, como el apetito de riesgo y la tolerancia al riesgo. En COBIT, esto se denomina optimización, que significa mantener al riesgo dentro de la tolerancia al apetito de riesgo, lo que debería constituir la meta. El apetito de riesgo y la tolerancia al riesgo son conceptos que se utilizan con frecuencia, pero hay una gran posibilidad de malinterpretarlos. Algunas personas utilizan los conceptos indistintamente, otras ven una clara diferencia. El apetito de riesgo puede ser, y será, diferente en cada empresa; no existe una norma absoluta o un estándar sobre lo que constituye un riesgo aceptable e inaceptable.

La gestión de riesgos efectiva comienza en los niveles más altos de la organización, con unas declaraciones sobre el apetito de riesgo bien conformadas y claramente expresadas. Las declaraciones, cuando se entienden con claridad, se comunican y se ejercitan, sirven como guía para los comportamientos, las decisiones, los límites y las políticas que establecen las fronteras dentro de las que se desarrollan las prácticas de gestión de riesgos en una empresa.

Como recordatorio, el apetito de riesgo es la cantidad de riesgo que una entidad (empresa, organización, compañía pública o privada) está dispuesta a asumir para lograr sus objetivos estratégicos. Por ejemplo, una declaración de apetito de riesgo para un proveedor de atención médica podría ser: "Situamos la seguridad del paciente como nuestra principal prioridad. También reconocemos la necesidad de equilibrar el nivel de respuesta inmediata a todas las necesidades del paciente con los costes de prestar dicho servicio". Esto demuestra un bajo apetito para el riesgo que podría impactar en la seguridad del paciente, compensado con un mayor apetito relacionado con la respuesta a la atención del paciente y al servicio al cliente.

La tolerancia al riesgo es la magnitud de la variación en los parámetros utilizados para medir el apetito de riesgo. En otras palabras, la tolerancia al riesgo es la respuesta al apetito de riesgo específico. Para el proveedor de atención médica indicado en el párrafo anterior, el ejemplo de apetito de riesgo y la correspondiente declaración de tolerancia podría ser: "Planificamos nuestro volumen de personal para permitir el tratamiento de todos los pacientes en menos de cinco minutos a partir del horario de su cita, y de los pacientes de urgencias sin cita previa en menos de 15 minutos. Sin embargo, la dirección acepta que en contadas situaciones (5 por ciento de las veces), los pacientes que requieren de una atención que no ponga en riesgo sus vidas puedan recibir esa atención en un período de hasta cuatro horas".

La tolerancia al riesgo es la magnitud de la variación en los parámetros utilizados para medir el apetito de riesgo.

A continuación, se facilitan algunos consejos para evaluar el apetito de riesgo, y consideraciones para elaborar declaraciones que puedan probarse y mejorarse a lo largo del tiempo:

- ¿Las entidades de gestión y gobierno de la organización están alineadas con unos resultados de negocio que son inaceptables para la empresa? ¿Cuál es el proceso para evaluar periódicamente las declaraciones de apetito de riesgo de la empresa si hay cambios significativos en el negocio, la misión u otras condiciones?
- ¿Está claro cuáles son los resultados inaceptables, y se comunican a todos los que deben conocerlos? ¿Tienen todos claro cuáles son los tipos de riesgo que la empresa desea asumir en contraposición con los que quiere evitar?
- Si alguien se da cuenta de un riesgo potencial, ¿hay alguna manera de plantear una inquietud o realizar una consulta antes de que ocurra un evento negativo? ¿Cómo se determinaría la efectividad del proceso organizativo para identificar, evaluar e informar el riesgo en relación con el apetito de riesgo declarado?
- ¿Las personas en la primera línea de la empresa saben cuáles son las fronteras, los parámetros, los límites de control u otras restricciones para la toma de decisiones de su rol? Un ejemplo de límites de control en un banco podría estar relacionado con el límite financiero autorizado a varios miembros del personal para abonar un cheque: el límite financiero máximo de un miembro del personal junior será menor que el de un miembro del personal senior, cuyo límite más alto se justifica por su mayor experiencia y formación en el entorno operativo. En muchos negocios, existen límites superiores e inferiores para la toma de decisiones que están integrados en el flujo de trabajo para ayudar a asegurar que se mantiene el apetito de riesgo óptimo.
- ¿Existen límites publicados, claramente definidos y comunicados para las pérdidas financieras; el cumplimiento regulatorio; las interrupciones del negocio; el desempeño operativo; la vida, la salud, o la seguridad? ¿Tales límites publicados existen para la seguridad de la información, la ciberseguridad, y los eventos o los incidentes tecnológicos?

Crear concienciación sobre el riesgo en una organización conlleva el reconocer que la incertidumbre, o riesgo, es una parte integral del negocio. Esto no implica que deban evitar o eliminar todos los riesgos, sino que estos se deben comunicar de manera efectiva y ser bien entendidos por todos. El riesgo de I&T es identificable, y la empresa que emplea un lenguaje común para expresar y describir el riesgo podrá con mayor facilidad detectarlo, reconocerlo y utilizar los recursos adecuados para gestionarlo.

Crear concienciación sobre el riesgo en una organización conlleva el reconocer que la incertidumbre, o riesgo, es una parte integral del negocio.

La definición y el desarrollo de un conjunto de declaraciones empresariales de apetito de riesgo y de tolerancia al riesgo son tan sólo una parte de los criterios de éxito para la gestión de riesgos. También es necesario un lenguaje de uso común para que todas las partes interesadas puedan recibir, entender y actuar conforme a las políticas, y las actividades necesarias para garantizar que no se materialice ningún riesgo que pudiera impedir que se logren los objetivos del negocio o la misión. La presentación de informes y la comunicación son partes clave de este proceso; para los responsables de la toma de decisiones y las partes interesadas (incluidos los consejos) es fundamental recibir información precisa y oportuna sobre el riesgo sobre la que poder actuar.

Hablar acerca del riesgo puede originar algunas conversaciones incómodas, puesto que el riesgo conlleva incertidumbres respecto del futuro que es posible que nunca se materialicen. Sin embargo, es imprescindible que se practique una buena comunicación del riesgo antes de que se materialice como una instancia, un incidente o una crisis importante.

Hay multitud de alternativas para expresar el riesgo de I&T en términos de negocio, y no hay opciones correctas o incorrectas. Es fundamental elegir la opción que mejor se adapte a la empresa y complementar este esquema con una serie de escalas para cuantificar el riesgo durante el análisis de riesgos.

La **figura 3.2** muestra ejemplos de declaraciones de apetito de riesgo y de expresiones de la tolerancia. Cada empresa debe definir sus propios niveles de apetito de riesgo y revisarlos de forma regular. Esta definición debería estar en consonancia con la cultura general de riesgos que la empresa desea declarar (es decir, abarcando desde la

muy aversa al riesgo hasta la asunción de riesgos/busca de oportunidades). El apetito de riesgo y la tolerancia al riesgo deberían aplicarse en todas las tomas de decisiones de I&T.

Figura 3.2—Ejemplos de declaraciones de apetito de riesgo y tolerancia al riesgo empresarial

Tipo de empresa	Ejemplo de declaración de apetito de riesgo	Ejemplo de declaración de tolerancia al riesgo
Universidad o instituto de enseñanza superior	El sistema de la universidad está dispuesto a asumir tipos crediticios de interés del X por ciento para préstamos (de una determinada cantidad financiera o porcentaje de activos) para financiar nuevas iniciativas.	La calificación crediticia de la universidad no puede caer más de un grado de su nivel actual.
Universidad o instituto de enseñanza superior	El sistema de la universidad acepta una inversión de X USD por persona en el reclutamiento y la formación de nuevos empleados.	Sobre toda la base universitaria, la rotación de empleados debe ser menor a X por ciento en cualquier período dado de 90 días.
Proveedor de energía o de servicios públicos	La reputación y la condición financiera de la empresa podrían verse afectados de manera negativa debido a las obligaciones que tiene la empresa de cumplir con las regulaciones, las leyes, y otros requisitos legales federales y estatales que rigen el cumplimiento de las operaciones, las evaluaciones, el almacenamiento, el cierre, la corrección, la eliminación y la monitorización.	Sobre la base de toda la empresa, las penalizaciones por incumplimiento deben ser menores al X por ciento en un período de 12 meses.
Proveedor de energía o de servicios públicos	La empresa trata de mantener un 99,999 por ciento de disponibilidad de la energía para sus clientes, y de restituir la energía a sus clientes en no más de X horas a partir de recibir la notificación de una interrupción del servicio.	Las interrupciones del servicio a más del X por ciento de clientes por menos de (período Y de tiempo) son aceptables.
Institución financiera	El banco tiene un bajo apetito para los incidentes relacionados con los sistemas de TI que son debidos a malas prácticas de gestión de cambios.	El X por ciento de los activos tecnológicos del banco deben tener aprobados los parámetros de configuración que se hayan establecido e implementado, y que estén manteniéndose. Otro ejemplo de declaración de tolerancia para la gestión de cambios podría establecer un porcentaje aprobado de cambios con éxito en activos críticos del negocio durante un período de tiempo específico.
Institución financiera	El banco se compromete a garantizar que la información de sus clientes es correcta, está debidamente clasificada, correctamente protegida y gestionada conforme a los requisitos legislativos y de negocio.	El banco mantendrá una frecuencia (X) y estricta puntualidad para los respaldos de activos de información y las pruebas con éxito de los respaldos. Otra declaración de tolerancia para la información de clientes podría establecer una cantidad permitida de violaciones de las políticas relacionadas con la confidencialidad y privacidad de la información de clientes.

El ejemplo del mapa de riesgos de la **figura 3.3** es un procedimiento de representación del riesgo en un gráfico bidimensional, usando las dimensiones de frecuencia e impacto. El apetito de riesgo puede visualizarse usando los mismos mapas de riesgos: se pueden definir diferentes niveles de severidad del riesgo, representados por cuadrados coloreados en el mapa de riesgos.

La aceptación del riesgo es binaria: algo es o no es aceptable. En la práctica, esto se refiere a cuán rápidamente una organización responde a una condición relacionada con el riesgo. Puede ser que no se necesite ninguna respuesta porque la condición esté comprendida en las tolerancias definidas (es decir, es aceptable o incluso supone una

oportunidad para asumir un riesgo adicional); que se requiera una respuesta porque una condición se encuentra fuera de la tolerancia o se dirige en esa dirección (es decir, es inaceptable pero no es urgente); o que una condición sea de una naturaleza tal que requiera de una respuesta inmediata porque rebasa con creces la tolerancia.

En el ejemplo de la **figura 3.3**, se definen cuatro niveles de severidad:

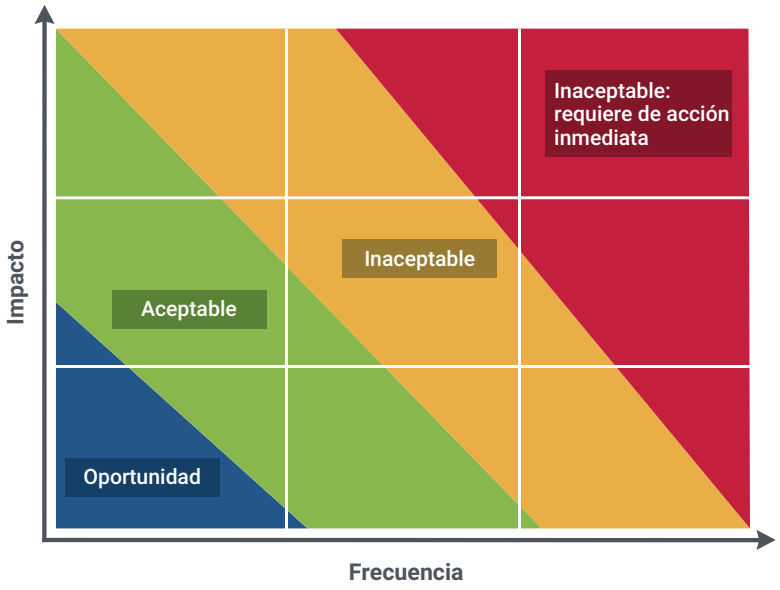
- El **rojo** indica un riesgo inaceptable que requiere de una acción inmediata.
- El **amarillo** indica un riesgo inaceptable (rebasando también el apetito de riesgo).
- El **verde** indica un nivel aceptable de riesgo sin que se requiera de ninguna acción especial.
- El **azul** indica muy bajo nivel de riesgo. Esta podría ser un área en la que pudiesen encontrarse eficiencias u oportunidades de ahorro de costes disminuyendo el grado de control, o pudiese estar indicado asumir más riesgo.

Figura 3.3—Ejemplo de mapa de riesgos

	Frecuencia		
Impacto	Inaceptable	Inaceptable: se requiere una acción inmediata	Inaceptable: se requiere una acción inmediata
	Aceptable	Inaceptable	Inaceptable: se requiere una acción inmediata
	Oportunidad	Aceptable	Inaceptable

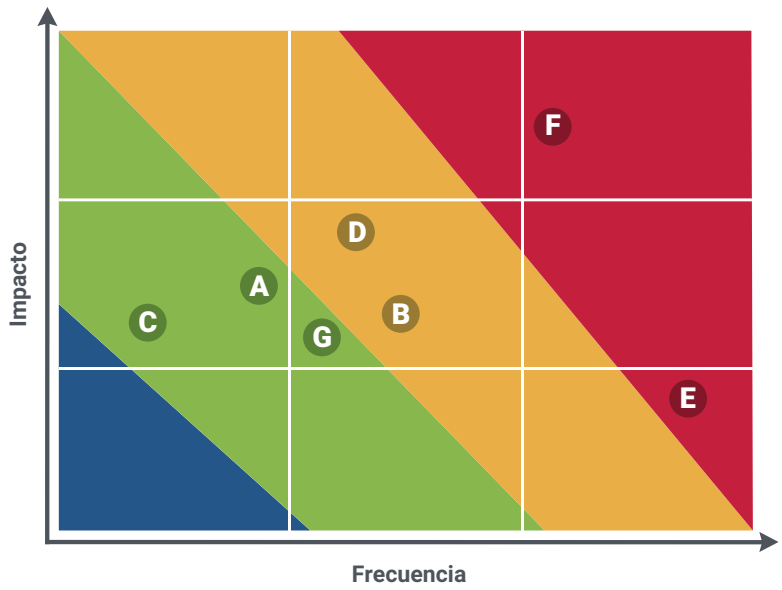
Normalmente, existen múltiples áreas de riesgo. Como resultado, es útil que la alta dirección tenga una visión sobre dónde se halla cada área en relación con el apetito de riesgo general de la empresa. La **figura 3.4** es un ejemplo de cómo puede representarse el riesgo dentro de bandas dependiendo del impacto y de la frecuencia de cada riesgo.

Figura 3.4—Mapa de riesgos que muestra las bandas de apetito de riesgo



El esquema de apetito de riesgo de la figura 3.5 es un ejemplo ilustrativo. Las letras denotan diversos riesgos que pueden existir en una empresa. El apetito de riesgo se puede explicar y representar mediante un mapa de riesgos.

Figura 3.5—Ejemplo de mapa de riesgos con apetito de riesgo



La práctica actual y los métodos de evaluación cualitativa de los riesgos pueden no estar lo suficientemente maduros como para proporcionar un nivel de precisión como el que ilustra la **figura 3.5**.

El apetito de riesgo se define por la alta dirección a nivel empresarial.[8] Hay diversos beneficios asociados con la definición del apetito de riesgo a nivel empresarial. Este enfoque:

- apoya y proporciona evidencia del proceso de toma de decisiones basado en riesgos;
- rastrea y presenta las decisiones para cada tipo de respuesta al riesgo;
- facilita la comprensión de cómo cada componente de la empresa contribuye al perfil de riesgo general;
- muestra cómo las diferentes estrategias de asignación de recursos pueden tener un impacto sobre las opciones de respuesta al riesgo y los resultados deseados para las opciones de respuesta al riesgo;
- permite la trazabilidad y la justificación de las acciones de respuesta al riesgo;
- respalda la consistencia en las decisiones de la gestión de riesgos;
- apoya la priorización de las acciones de respuesta al riesgo;
- identifica las áreas específicas donde el riesgo debería recibir una respuesta.

El apetito y la tolerancia al riesgo de una empresa cambian con el tiempo. Nueva tecnología, nuevas estructuras organizacionales, nuevas condiciones del mercado, nueva estrategia comercial y muchos otros factores exigen que la empresa revalúe su cartera (portfolio) de riesgo a intervalos regulares. Estos desarrollos también precisan que la empresa reconfirme su apetito de riesgo a intervalos regulares, y pueden desencadenar revisiones de la política de riesgos.

El apetito de riesgo y la tolerancia al riesgo van de la mano. La tolerancia al riesgo se define a nivel empresarial y se refleja en las políticas establecidas por los ejecutivos. A niveles inferiores (tácticos) de la empresa, pueden tolerarse excepciones (o definirse diferentes umbrales), siempre y cuando a nivel empresarial la exposición global no exceda el apetito de riesgo deseado.

[8] *Ibid.*

Cualquier iniciativa de negocio incluye un componente de riesgo, por lo que la dirección debería ser prudente al buscar nuevas oportunidades hasta alcanzar el nivel del apetito de riesgo. Hay situaciones en las que las políticas se basan en requisitos específicos legales, regulatorios o industriales, haciendo apropiado el no tener tolerancia al riesgo para no incumplir el requisito. Un ejemplo de esto puede estar relacionado con las regulaciones de privacidad específicas de algunos países cuyo incumplimiento puede acarrear multas o sanciones financieras extremadamente grandes.

3.1.2 Cultura de riesgos

La gestión de riesgos trata de ayudar a que una empresa maximice el valor que genera, a la vez que evita las pérdidas que pueden impactar de manera negativa en su capacidad para lograr su misión o en su capacidad para continuar operando. Una cultura de consciencia de riesgos, facilita típicamente un entorno en el que se discuten abiertamente los componentes de riesgo, y se entienden y mantienen niveles aceptables del riesgo. Una cultura de consciencia de riesgos comienza desde la alta dirección, con el consejo de administración y los ejecutivos de negocio que establecen la dirección, comunican la toma de decisiones consciente de riesgos y recompensan los comportamientos de gestión de riesgos efectivos. La consciencia de riesgos también implica que toda la dirección y el personal de cualquier nivel dentro de la empresa sepan cómo y por qué responder a los eventos adversos de I&T.

La cultura de riesgos es un concepto que no es fácil de describir. Consiste en una serie de comportamientos, como muestra la **figura 3.6**.

Figura 3.6—Comportamientos relevantes para el gobierno y la gestión de riesgos

Comportamiento	Objetivo clave/Criterios apropiados/Resultado
Comportamiento general	
En toda la empresa existe una cultura de consciencia de riesgos y cumplimientos, incluyendo la identificación proactiva y el escalamiento del riesgo.	La cultura debe definir un planteamiento de gestión de riesgos y un apetito de riesgo. Debe establecerse una tolerancia cero para el incumplimiento de los requisitos regulatorios y legales.
Hay políticas vigentes definidas que se han comunicado y que promueven el comportamiento.	Todo el personal entiende e implementa los requisitos de la empresa conforme se han definido en las políticas.
La empresa muestra un comportamiento positivo con respecto al planteamiento de problemas o a los resultados negativos.	Los denunciantes se consideran como una contribución positiva para la empresa. Se evita la cultura de culpabilidad. El personal entiende la necesidad de la concienciación del riesgo y la denuncia de posibles debilidades.
La empresa reconoce el valor del riesgo.	El personal entiende la importancia que da la empresa a mantener la concienciación del riesgo, y el valor que la gestión de riesgos aporta a sus funciones.
La empresa fomenta una cultura transparente y participativa como un aspecto de interés importante.	La comunicación es abierta y manifiesta; por lo tanto, los hechos no se omiten, tergiversan o subestiman. Se evita el impacto negativo de las agendas ocultas.
Las partes interesadas muestran respeto mutuo.	Se alienta la colaboración entre partes interesadas y los evaluadores de riesgos. Se respeta a las personas como profesionales y se las trata como expertos en sus funciones.
El negocio acepta la propiedad del riesgo.	Se incorporan prácticas de riesgo en toda la empresa. Las obligaciones de rendición de cuentas son claras y están aceptadas. El riesgo de negocio relacionado con la TI es propiedad del negocio y no es visto como responsabilidad exclusiva del departamento de TI de la función de riesgo.
La empresa permite la aceptación del riesgo como una opción válida.	La dirección entiende la probabilidad y las consecuencias del impacto de la aceptación del riesgo. Se determina que el impacto va a estar dentro del apetito de riesgo de la empresa.

Figura 3.6—Comportamientos relevantes para el gobierno y la gestión de riesgos *(cont.)*	
Comportamiento	**Objetivo clave/Criterios apropiados/Resultado**
Comportamiento del profesional de riesgos	
Se realizan esfuerzos para entender qué es el riesgo para cada parte interesada y cómo este impacta en los objetivos de la parte interesada.	Los profesionales de riesgos entienden la realidad empresarial de los impactos del riesgo. Esto puede incluir requisitos de cumplimiento, regulatorios, operativos y competitivos. Si bien pueden existir riesgos que son comunes a un determinado sector de actividad económica, cada empresa es única en términos de cómo los elementos de esos riesgos impactan en sus objetivos específicos.
Los profesionales de riesgos generan concienciación y comprensión de la política de riesgos.	La alineación entre la capacidad de riesgo, el apetito de riesgo y la política de la empresa conduce a estrategias de riesgos efectivas.
Se apoya la colaboración y la comunicación bidireccional durante la evaluación de riesgos.	La evaluación del riesgo es esencialmente exacta y completa, y aborda las necesidades de las partes interesadas.
El apetito de riesgo de la empresa es claro y se comunica de manera oportuna a las partes interesadas relevantes.	Las partes interesadas gestionan el riesgo de manera más efectiva, y hay una alineación adecuada con las estrategias y los esfuerzos organizativos.
Las políticas reflejan el apetito de riesgo y la tolerancia al riesgo.	Los empleados y la dirección operan dentro de la tolerancia al riesgo. Las líneas de negocio aplican el apetito de riesgo y tolerancia al riesgo formales a la práctica diaria. Existe un proceso claro para proponer y realizar cambios en los niveles del apetito de riesgo, con la consideración y aprobación de la alta dirección.
La cultura de la empresa soporta las prácticas de riesgo efectivas.	Las partes interesadas entienden el riesgo desde visiones de carteras (portfolio) comunes (productos, procesos), y aplican la toma de decisiones basada en el riesgo a la práctica diaria.
Los KRI se usan como una alerta temprana.	Los KRI están vinculados con métricas válidas y pueden utilizarse como un indicador de fallo de proceso o de control. Las métricas de KRI se encuentran disponibles y accesibles para la elaboración regular de informes, y están relacionadas con los objetivos.
Se actúa sobre los indicadores o eventos de riesgo que rebasen la tolerancia y el apetito.	Los indicadores de riesgo están relacionados con la respuesta al riesgo y las actividades de corrección de la dirección.
Comportamiento de la dirección	
La cúpula directiva establece la dirección y muestra un apoyo visible y genuino a las prácticas de riesgo.	La calidad de las prácticas de gestión de riesgos se mantiene a través del apoyo genuino de la alta dirección.
La dirección se compromete con todas las partes interesadas relevantes a acordar acciones y hacer seguimientos de los planes de acción.	Se involucra de manera adecuada a las partes interesadas apropiadas para garantizar la resolución oportuna de los problemas y el logro de los planes de negocio.
Se obtiene un compromiso genuino, y se asignan recursos para la ejecución de las acciones.	Se faculta al personal para que ejecute las acciones requeridas por las decisiones de la gestión de riesgos.
La dirección alinea las políticas y las acciones con el apetito de riesgo.	La dirección toma las decisiones de riesgo adecuadas cumpliendo con las políticas. Los ingresos ajustados al riesgo están alineados con las expectativas de la dirección.
La dirección supervisa de forma proactiva el riesgo y el progreso del plan de acción.	Se completan los planes de corrección dentro de los plazos de negocio esperados, y tienen un impacto positivo en los objetivos de la empresa.
Se informa a la dirección sobre las tendencias de riesgos.	La presentación oportuna de informes sobre las tendencias de riesgos gestiona el riesgo de forma proactiva y evita la pérdida de oportunidades.
Se recompensa la gestión de riesgos efectiva.	Se reconocen las buenas prácticas de riesgos. Los objetivos de desempeño de los empleados y las estructuras de las recompensas se establecen para estimular las prácticas de gestión de riesgos efectivas y la ejecución adecuada de las acciones de mitigación.

La cultura de riesgos incluye:

- El comportamiento frente a la adopción de riesgos: ¿Cuáles son las normas y las actitudes para la adopción de riesgos, la identificación de riesgos y el análisis de riesgos?
- El comportamiento frente al cumplimiento de la política: ¿La política es algo que existe pero que no se cumple? ¿Las políticas promueven el comportamiento? ¿Las políticas son fáciles de leer, comprender y cumplir?
- El comportamiento frente a los resultados negativos: ¿Cómo trata la empresa los resultados negativos, las excepciones a la política, los eventos de pérdida, los ciberincidentes, las oportunidades desaprovechadas, los hallazgos de auditoría y las investigaciones postincidente? ¿Aprenderá de ellos e intentará adaptarse, o se atribuirán culpas sin abordar la causa raíz?

Algunos síntomas de una cultura de riesgos inadecuada o problemática incluyen:

- La falta de alineación entre el apetito de riesgo, las tolerancias declaradas y su traducción en políticas, las directrices cuando las políticas no están alineadas con el rumbo de la dirección, y las normas de la organización sobre el cumplimiento de la política.
- Un gran número de excepciones a la política, que sugiere o bien que las políticas y los estándares no representan de hecho el apetito/tolerancia de riesgo de la organización, o bien que la organización no examina correctamente las solicitudes de excepción.
- La existencia de una cultura de culpabilidad. Este tipo de cultura debería evitarse, ya que es el inhibidor más eficaz de la comunicación relevante y eficiente. En una cultura de culpabilidad, las unidades de negocio tienden a señalarse con el dedo entre sí cuando no se cumplen los objetivos. Al hacerlo, no se percatan de cómo adelantar la participación de la unidad de negocio afecta el éxito del proyecto. En casos extremos, la unidad de negocio puede culpar por no cumplirse unas expectativas que nunca había comunicado de forma clara. La atribución de culpas sólo resta valor a la comunicación efectiva entre las unidades, provocando aún más retrasos. Los líderes ejecutivos deben identificar y controlar rápidamente una cultura de culpabilidad si se desea fomentar la colaboración en la empresa.

3.1.3 Política de riesgos

La buena práctica de la gestión de riesgos requiere que las políticas formen parte de un marco de gobierno y gestión integral, proporcionando una estructura (jerárquica) en la que deberían encuadrarse todas las políticas y proporcionar respaldo a los principios subyacentes.

Como parte de la inclusión de las normas o condiciones de gestión de riesgos en el marco de las políticas de la empresa, también deberían describirse los siguientes elementos en las políticas de riesgos:

- el alcance y la autoridad, vinculados con las declaraciones de apetito y de tolerancia al riesgo;
- los roles y las responsabilidades de las partes interesadas;
- las consecuencias de no cumplir con la política;
- la forma de tratar las excepciones;
- la manera en que se controlará y medirá el cumplimiento de la política.

Las políticas deberían estar alineadas con el apetito de riesgo de la empresa. Las políticas son un componente clave del sistema de control interno de una empresa, cuyo propósito es garantizar que una empresa cumpla con sus objetivos establecidos. Como parte de las actividades del gobierno de riesgos, se define el apetito de riesgo de la empresa, y este apetito de riesgo debería verse reflejado en las políticas. Esto no quiere decir que las declaraciones del apetito de riesgo o la tolerancia al riesgo se deban incluir en los documentos de las políticas, sino que las políticas deben estar alineadas con la cultura de adopción de riesgos de la empresa. Las políticas deben revalidarse y actualizarse a intervalos regulares para garantizar su relevancia para los requisitos y las prácticas de negocio.

Como parte de las actividades del gobierno de riesgos, se define el apetito de riesgo de la empresa, y este apetito de riesgo debería verse reflejado en las políticas.

Las políticas proporcionan una guía detallada sobre cómo poner en práctica los principios, y cómo estos influenciarán la toma de decisiones. Algunos ejemplos de los tipos de políticas de riesgo se encuentran recogidos en la **figura 3.7**. No están incluidas todas las políticas relevantes, ni estas son propiedad de las áreas de TI, de seguridad de la información, de privacidad de la información o de la función de riesgo.

Figura 3.7—Ejemplos de tipos de políticas de riesgo

Políticas	Descripción
Política de riesgo de TI principal	Define a nivel estratégico, táctico y operativo cómo el riesgo de una empresa debe gobernarse y gestionarse conforme a sus objetivos de negocio. Esta política traslada el gobierno de la empresa a los principios y las políticas del gobierno de riesgo, y elabora las actividades de gestión de riesgos.
Política de seguridad de la información	Establece las normas para proteger la información corporativa y los sistemas e infraestructuras asociados. Los requisitos del negocio relativos a la seguridad y el almacenamiento son más dinámicos que la gestión de riesgos de TI; por lo tanto, para su efectividad, su gobierno debería tratarse por separado del gobierno de riesgo de TI. Sin embargo, por eficiencia operativa, es necesario mantener la política de seguridad de la información sincronizada con la política de riesgo de TI.
Política de gestión de crisis	Al igual que la seguridad de TI, la gestión de redes y la seguridad de los datos, la gestión de crisis de TI es una de las políticas que debe considerarse a nivel operativo para una gestión completa de los riesgos de TI. Establece las directrices sobre cómo actuar en situaciones de crisis, y detalla la secuencia en la que se debe tratar cada una de las áreas identificadas de riesgo (clave).
Política de gestión de prestación de servicios de TI de terceros	Establece las directrices para gestionar el riesgo relacionado con los servicios de terceros. Establece un marco de expectativas sobre el comportamiento y las precauciones de seguridad adoptados por los proveedores de servicios externos para gestionar el riesgo relacionado con la prestación del servicio.
Política de continuidad del negocio (BCP)	Incluye el compromiso y la visión de la dirección sobre: • el análisis del impacto en el negocio (BIA); • los planes de contingencia del negocio con recuperación confiable; • los requisitos de recuperación para sistemas críticos; • los umbrales establecidos y los disparadores para contingencias; • la manera de tratar el escalamiento de incidentes; • el plan de recuperación ante desastres (PRD); • la formación y las pruebas.
Política de gestión de programas/proyectos	Se ocupa de la gestión de los riesgos vinculados con los proyectos y los programas. Detalla la postura y las expectativas de la dirección sobre la gestión de programas y proyectos. Asimismo, se encarga de la rendición de cuentas, las metas y los objetivos con relación al desempeño, el presupuesto, el análisis de riesgos, la presentación de informes, y la mitigación de eventos adversos durante la ejecución de programas y proyectos.
Políticas de recursos humanos (RR.HH.)	Detallan qué pueden esperar los empleados de la empresa, y qué espera la empresa de los empleados. Pormenorizan los comportamientos aceptables e inaceptables de los empleados y, al hacerlo, gestionan el riesgo que está vinculado con el comportamiento humano.
Política de riesgo de fraude	Se ocupa de proteger la marca, la reputación y los activos de la empresa frente a las pérdidas y/o los daños derivados de incidentes de fraude y/o de malas conductas. La política proporciona una guía para todos los empleados sobre cómo denunciar actividades sospechosas y la forma de tratar informaciones sensibles y evidencias. Ayuda a crear una cultura antifraude y concienciación del riesgo.

Figura 3.7—Ejemplos de tipos de políticas de riesgo *(cont.)*

Políticas	Descripción
Política de cumplimiento	Explica el proceso de evaluación relativo al cumplimiento de los requisitos regulatorios, contractuales e internos. Enumera los roles y las responsabilidades para las distintas actividades del proceso, y facilita directrices sobre las métricas que deben usarse para medir el cumplimiento.
Política de ética	Define los aspectos esenciales de cómo van a interactuar las personas dentro de una empresa entre sí y con los clientes a los que atienden.
Política de gestión de la calidad	Detalla la visión de la dirección sobre los objetivos de calidad de la empresa, el nivel aceptable de calidad y las funciones de los departamentos específicos para garantizar la calidad.
Política de gestión de servicios	Proporciona dirección y orientación para garantizar la gestión e implementación efectivas de todos los servicios de TI para cumplir con los requisitos del negocio y del cliente en un marco de medición del desempeño. También se ocupa de la gestión del riesgo relacionado con los servicios de TI. El marco ITIL incluye una guía detallada sobre la gestión del servicio y la optimización del riesgo relacionado con los servicios.
Política de gestión de cambios	Comunica el propósito de la dirección de que los cambios al área de TI de la empresa se gestionen e implementen de manera tal que se minimice el riesgo y el impacto para las partes interesadas. La política incluye información sobre los activos dentro de su alcance y el proceso estándar de gestión de cambios establecido.
Política de delegación de autoridad	Detalla: • la autoridad que el consejo de administración retiene estrictamente para sí mismo; • los principios generales de la delegación de autoridad; • un programa de delegación de autoridad (incluyendo límites claros); • una definición clara de las estructuras organizativas en las que el consejo delega su autoridad.
Política de denunciantes	Debe: • fomentar que los empleados transmitan sus preocupaciones y preguntas; • proporcionar vías para que los empleados transmitan sus preocupaciones con toda confianza; • garantizar a los empleados que recibirán una respuesta por las preocupaciones transmitidas, y que podrán escalar una preocupación si no están satisfechos con la respuesta; • reafirmar a los empleados que están protegidos cuando informan un problema y que no deberían temer represalias.
Política de control interno	El propósito es: • comunicar los objetivos de control interno de la dirección; • establecer los estándares para el diseño y el funcionamiento del sistema empresarial de controles internos para reducir la exposición a todos los riesgos a que hace frente la empresa.
Política de propiedad intelectual (PI)	Asegura que todos los riesgos relacionados con el uso, la propiedad, la venta y la distribución de los resultados de los esfuerzos creativos relacionados con TI de los empleados de una empresa, como el desarrollo de software, estén detallados de manera adecuada desde el comienzo de un trabajo.
Política de privacidad de datos	Describe las formas en que una parte recopila, usa, divulga y gestiona los datos personales. La información personal puede ser cualquiera que se pueda usar para identificar a un individuo, incluyendo, pero sin limitarse, a, su nombre, domicilio, fecha de nacimiento, estado civil, información de contacto, la fecha de emisión y caducidad de su documento de identidad, sus registros financieros, su información crediticia, historial médico, destino de viaje, y sus intenciones de adquirir bienes y servicios. La política define cómo una empresa recopila, almacena y divulga la información personal que reúne. Informa al cliente sobre la información específica que se recopila y si se

Figura 3.7—Ejemplos de tipos de políticas de riesgo *(cont.)*	
Políticas	**Descripción**
	mantiene confidencial, se comparte con socios, o se vende a otras compañías o empresas. Además, la política garantiza el cumplimiento con la legislación relevante relacionada con la protección de datos.

3.1.4 Indicadores clave de riesgo (KRI)

Cualquier medición que pueda usarse para describir y rastrear un riesgo es un indicador de ese riesgo. Los indicadores de riesgo son específicos de cada empresa. El desarrollo y la selección de los KRI dependen de una serie de parámetros de los entornos interno y externo, tales como el tamaño y la complejidad de la empresa, si está funcionando en un mercado altamente regulado, y sus objetivos estratégicos.

La identificación de los indicadores de riesgo debería tener en cuenta los siguientes aspectos:

- La consideración de las diferentes partes interesadas en la empresa. Los indicadores de riesgo pueden y deberían identificarse para las partes interesadas en función de sus necesidades de información específicas. La involucración de las partes interesadas apropiadas en la selección de los indicadores de riesgo también asegurará una mayor aceptación y propiedad.
- Seleccionar equilibradamente los indicadores de riesgo, incluyendo los indicadores retrospectivos (que indican el riesgo después de que hayan ocurrido los eventos), los indicadores progresivos (que indican qué capacidades existen para evitar que ocurran eventos) y las tendencias (que analizan los indicadores a través del tiempo o que estudian las correlaciones de los indicadores para obtener información). Los indicadores seleccionados deben profundizar en la causa raíz de los eventos (ser indicativos de la causa raíz y no sólo de los síntomas).
- Los indicadores que se relacionan directamente con las declaraciones establecidas de apetito de riesgo y tolerancia al riesgo serán más significativos para hacer el seguimiento de los resultados deseados del programa de gestión de riesgos.

Los KRI son las métricas o los datos que sirven de señal de alerta temprana de que algo no está funcionando como se esperaba, o de que hay una mayor exposición al riesgo en una o más áreas de la empresa. Este tipo de indicador es similar a un detector de humo que emite una alarma al primer indicio de humo. Un indicador que cumple con el requisito de alerta temprana es conocido como un indicador progresivo. Puede que un indicador progresivo no sea totalmente confiable, o que haya alertas que resulten indicar falsos positivos.

Ninguna discusión de indicadores de riesgo estaría completa sin presentar a los indicadores clave de desempeño (KPI). Los KPI están diseñados para proporcionar una visión general de alto nivel del desempeño pasado, y casi siempre se derivan de datos históricos. Los KPI son conocidos como indicadores retrospectivos, y proporcionan información sobre si han logrado o no los objetivos de un requisito de cumplimiento, o si se han controlado los gastos de un proyecto a su finalización.

Puede ser necesario usar tanto los KRI como los KPI al comenzar las mediciones de la gestión de riesgos, hasta que haya suficientes datos para mejorar el proceso. Idealmente, los KRI son indicadores progresivos pero no siempre son viables en las primeras etapas de la gestión de riesgos. Algunos ejemplos de KRI se muestran en la **figura 3.8**.

Figura 3.8—Ejemplos de indicadores clave de riesgo
Porcentaje de áreas críticas del negocio que han finalizado una evaluación de riesgo en los últimos 12 meses
Porcentaje de cumplimiento o régimen de pruebas de controles para activos críticos finalizado en los últimos 12 meses
Porcentaje de riesgos no mitigados en el registro de riesgos para los que no existe un plan de respuesta
Porcentaje de procesos de negocio en los que se utilizan datos personales de clientes

Figura 3.8—Ejemplos de indicadores clave de riesgo *(cont.)*
Porcentaje de incidentes en los que se pierden/roban datos personales de clientes
Porcentaje de entregas de productos que se pierden o retrasan debido a fallos de TI
Porcentaje de proveedores que suministran sistemas de TI críticos que han implementado un marco de control de seguridad aprobado
Porcentaje de planes de recuperación ante desastres (PRD) probados con éxito en los últimos 12 meses (retrospectivo)
Porcentaje de PRD cuyas pruebas están programadas en los próximos 12 meses (prospectivo)

Una empresa puede desarrollar un extenso conjunto de métricas que sirvan como indicadores de riesgo; sin embargo, no es ni posible ni viable mantener un conjunto completo de métricas como KRI. Un KRI se diferencia por ser extremadamente relevante, y por tener una alta probabilidad de predecir o indicar un riesgo importante. Los criterios para seleccionar KRI incluyen:

- **Impacto**: los indicadores de riesgos con alto impacto en el negocio o aquellos vinculados directamente con las declaraciones de tolerancia al riesgo tienen mayor probabilidad de ser KRI.
- **Esfuerzo** (de implementación, medida o informe): entre diferentes indicadores que tengan una sensibilidad equivalente, puede constituir un buen punto de partida aquel para el que sea más fácil la recopilación de datos.
- **Confiabilidad**: el indicador debe poseer una alta correlación con el riesgo, y ser un buen predictor o una buena medida de sus resultados.
- **Sensibilidad**: el indicador debe ser representativo de los factores de riesgo, y capaz de indicar con exactitud las variaciones de los factores de riesgo.

El riesgo que deba introducirse en el flujo de trabajo de gestión de riesgos se monitoriza, informa, o cierra cuando se considera que se encuentra en un rango aceptable para la empresa. En esta etapa de la gestión de riesgos, dos métodos que se usan comúnmente para desarrollar indicadores de riesgo, algunos de los cuales derivan en KRI, son el análisis de causa raíz (ACR o RCA)[9] y el procedimiento Objetivos-Preguntas-Indicadores-Métricas (OPIM o GQIM).[10] Ambos métodos ayudan al desarrollo de indicadores y mejoran el bucle de retroalimentación (feedback) que se precisa para aumentar la madurez del proceso de gestión de riesgos a lo largo del tiempo.

3.1.5 Mapas y agregación de riesgos para la toma de decisiones del consejo y los ejecutivos

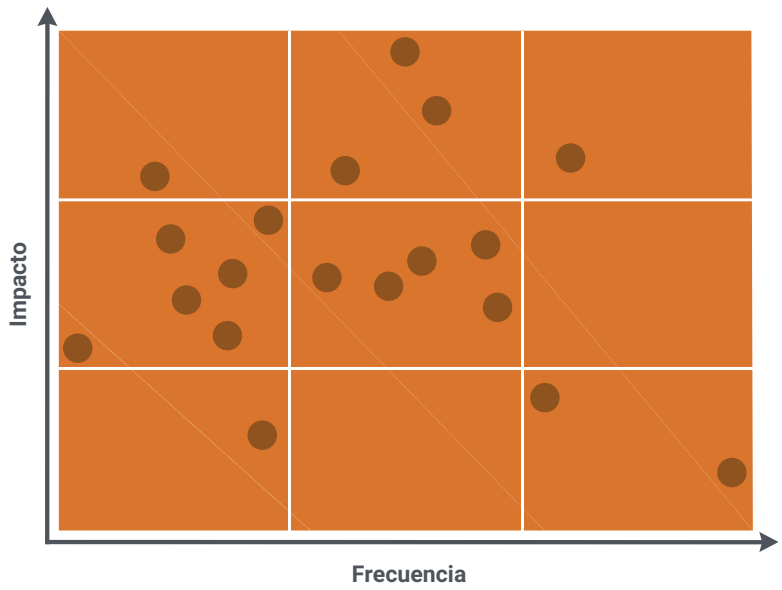
Una técnica muy común e intuitiva para presentar el riesgo es el mapa de riesgos, también conocido como mapa de calor (heatmap), en el que el riesgo se representa en un diagrama bidimensional, cuyas dos dimensiones más comunes (ejes X e Y) son la frecuencia y el impacto. En la **figura 3.9** se muestra un ejemplo de mapa de riesgos. El mapa puede ser útil para facilitar un ejercicio de clasificación de prioridades, pero es posible que no aporte a la dirección suficiente información para adoptar una decisión sobre la acción apropiada.

Aunque los mapas de riesgos se emplean ampliamente en muchas empresas, a menudo son objeto de muchas críticas y muchos analistas de riesgos cuantitativos los desestiman por tener poco valor, y algunos analistas se refirieren a ellos como prácticamente inútiles. Como se describe con más detalle en las secciones de análisis de riesgos cualitativo y cuantitativo posteriormente en esta publicación, el mapa de riesgos debería ser una expresión del riesgo que se ha evaluado usando criterios de impacto bien definidos e inequívocos. Los mapas iniciales o una agregación de tipos de riesgos pueden ser útiles para que un analista desarrolle tendencias o perfiles comunes para los que las actividades de respuesta al riesgo podrían hacerse más eficientes, pero pueden no ser la técnica adecuada para la toma de decisiones de la dirección. La mayoría de las veces, si una organización está utilizando sólo métodos cualitativos de evaluación de riesgos, es muy difícil, si no imposible, agregar riesgos significativamente.

[9] Durmesevic-Mutapcic, A.; "How Root Cause Analysis Fits Into Various Audit Types," *ISACA® Journal*, 1 March 2019, *https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/how-root-cause-analysis-fits-into-various-audit-types*

[10] Stewart, K.; Allen, J.; Valdez, M.; Young, L; "Measuring What Matters Workshop Report," Software Engineering Institute, CERT Division, January 2015, *https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_433525.pdf*

Figura 3.9—Ejemplo de mapa de riesgos

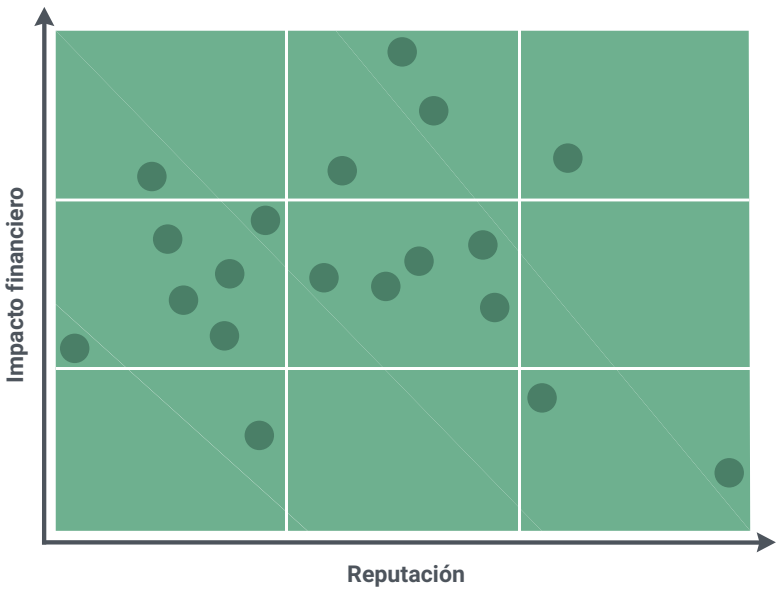


Si una empresa utiliza actualmente mapas de riesgos, tiene una oportunidad para comenzar el tránsito entre la "medición" cualitativa del riesgo y la medición cuantitativa del riesgo. Por ejemplo, se puede comenzar el tránsito con algunos pasos sencillos, como evolucionar desde las descripciones cualitativas del riesgo (alto, medio o bajo) asociando a estos términos números específicos o, más exactamente, rangos numéricos específicos.

Una vez que los analistas de riesgo de empresa y las partes interesadas se encuentren cómodos usando y comunicándose con el mapa de riesgos básico, se puede extender el concepto a mapas más avanzados que incluyan criterios cuantitativos adicionales para la agregación de riesgos y la toma de decisiones priorizada (ver la **figura 3.10**). Esta es un área de rápido cambio y adaptación en el campo de la gestión de riesgos que se abordará mediante varias nuevas herramientas, técnicas y métodos en el futuro. Un artículo publicado en *ISACA Journal*, titulado "Evolving from Qualitative to Quantitative Risk Assessment" (Evolucionando desde la evaluación de riesgos cualitativa a la cuantitativa) facilita información adicional y ejemplos relevantes.[11]

[11] Heynderickx, B.; "Evolving From Qualitative to Quantitative Risk Assessment," *ISACA Journal*, 1 July 2019, *https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/evolving-from-qualitative-to-quantitative-risk-assessment*

Figura 3.10—Ejemplo de mapa de riesgos específicos



Por ejemplo, en la **figura 3.10**, el análisis se realiza sobre los factores de riesgo relacionados con el coste financiero directo en que se puede incurrir si ocurre una brecha de datos (en el eje X), con el eje Y reemplazado con un recuento frecuencial de la cantidad de veces en que la organización se ha mencionado en las noticias u otros medios.

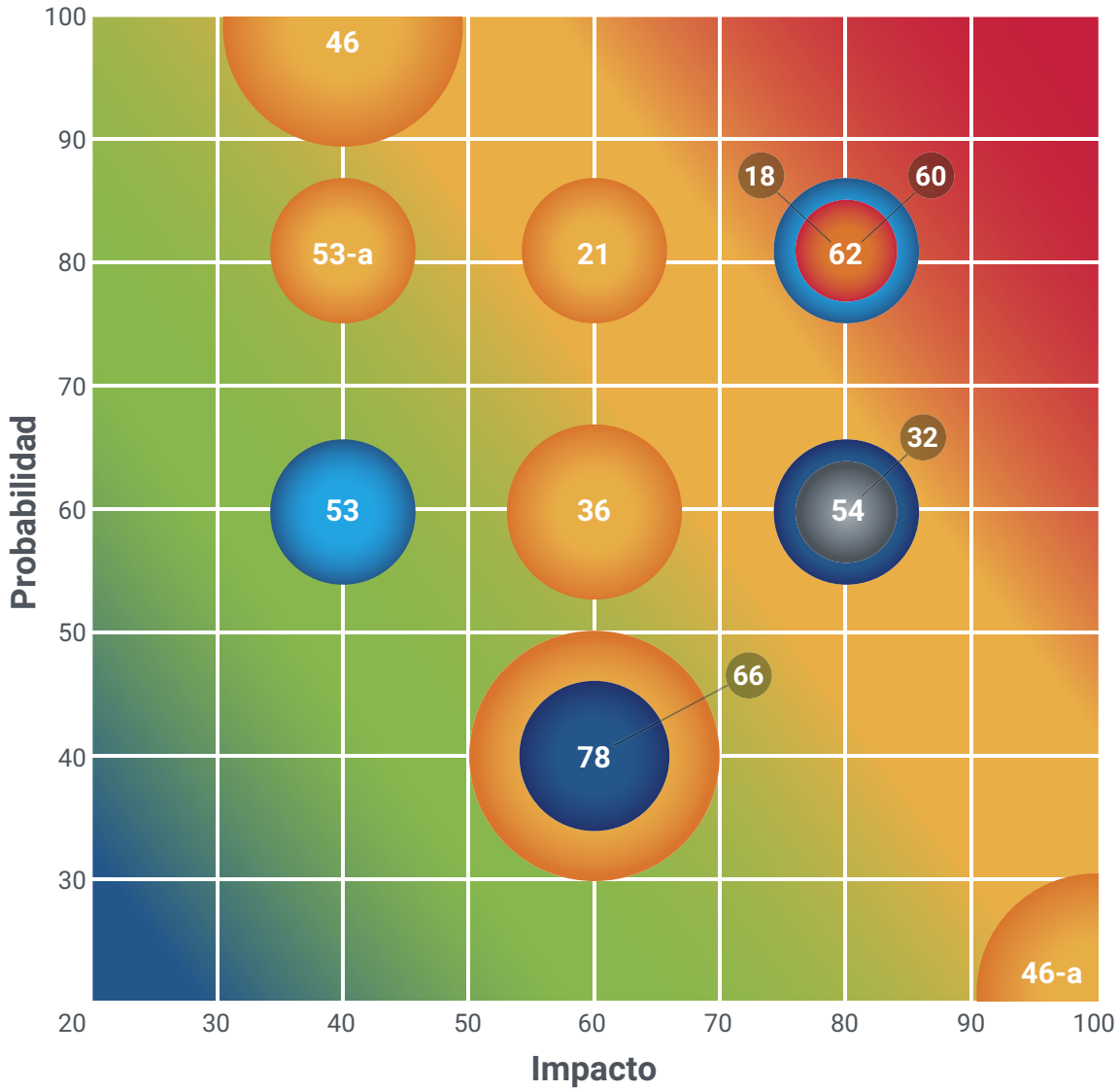
Si el consejo y la dirección requieren que se cuantifique el riesgo en términos financieros, la técnica más común consiste en cambiar el procedimiento al cálculo de la máxima pérdida probable (PML)[12] o de la máxima pérdida previsible (MFL).[13] El uso de la PML o la MFL permite que el riesgo se analice con respecto al impacto que tendrá en la organización en el caso de que se materialice. Estas técnicas se usan para garantizar que la empresa disponga de las protecciones financieras adecuadas en caso de que se materialice un riesgo.

El impacto financiero del riesgo suele agregarse con fines de presentación de informes para el consejo o la dirección en rangos de pérdidas monetarias que podrían esperarse si se materializaran ciertos tipos de riesgos. En muchas organizaciones, hay un conjunto de criterios de impacto y de tolerancias al riesgo expresados en términos financieros. A menudo, esta representación del riesgo también se plasma en un mapa de riesgos, usando círculos de varios tamaños para representar el impacto financiero: un círculo grande que representa un mayor impacto financiero que un círculo más pequeño, como muestra **figura 3.11**.

El impacto financiero del riesgo suele agregarse con fines de presentación de informes para el consejo o la dirección en rangos de pérdidas monetarias que podrían esperarse si se materializaran ciertos tipos de riesgos.

[12] Investopedia, "Probable Maximum Loss," *https://www.investopedia.com/terms/p/probable-maximum-loss-pml.asp*
[13] Investopedia, "Maximum Foreseeable Loss," *https://www.investopedia.com/terms/m/maximum-foreseeable-loss.asp*

Figura 3.11—Impacto financiero del riesgo



En el sector financiero, la agregación de riesgos y la presentación de informes cuantitativos de riesgos son un requisito actual para muchas instituciones financieras sujetas al proceso supervisor del Comité de Basilea sobre Supervisión Bancaria (Comité de Basilea).[14] Este requisito está suscitando el debate sobre los mejores métodos para la agregación y la cuantificación del riesgo, de modo que el riesgo de I&T pueda informarse y gestionarse acordemente con otros riesgos que requieran una toma de decisiones informada.

La agregación permite que el riesgo que se extiende por toda la empresa se haga visible e informa la toma de decisiones de la dirección sobre las respuestas al riesgo. El riesgo, cuando se agrega a nivel empresarial, puede estar tan lejos del rango de tolerancia de la organización que requiera de una acción inmediata o de respuestas generalizadas. La agregación de riesgos es el principal impulsor para desarrollar y perfeccionar los criterios de impacto del riesgo que reflejan las escalas de medición comunes y específicas en la organización necesarias para

[14] BIS, "Launch of the consolidated Basel Framework," 16 December 2019, *https://www.bis.org/bcbs/publ/d491.htm*

gestionar verdaderamente el riesgo de I&T de manera acorde con otros riesgos empresariales. La maduración de las funciones de gestión de riesgos y los procesos hasta el nivel de capacidad que permite una mayor certeza en la toma de decisiones crea un valor mayor para la organización que el de la mera gestión de un único riesgo. La toma de decisiones informada es verdaderamente el valor de un proceso de gestión cuantitativa de riesgos maduro.

Esta página se dejó en blanco intencionalmente

Capítulo 4
Fundamentos de evaluación de riesgos

4.1 Componentes esenciales

Este capítulo analiza los componentes esenciales de la evaluación de riesgos. La dirección de la empresa es responsable de las actividades de planificación, construcción, implementación y monitorización de acuerdo con la dirección establecida por el órgano de gobierno para lograr los objetivos de la empresa. En la mayoría de las empresas, la dirección es responsabilidad de la dirección ejecutiva, bajo el liderazgo del director general ejecutivo (CEO).

Como se explicó en el Capítulo 3, el gobierno es el sistema mediante el que se evalúan, dirigen y monitorizan las organizaciones. Hay una clara distinción entre gobierno y gestión. La gestión se centra en planificar, construir, ejecutar y monitorizar las actividades de acuerdo con la dirección establecida por el órgano de gobierno para crear valor mediante el logro de los objetivos. Una organización bien gestionada sujeta a un gobierno deficiente creará y ejecutará planes claros y efectivos para lograr objetivos que no crean valor. De forma similar, la gestión de riesgos intenta prever los desafíos para lograr los objetivos y disminuir las probabilidades de que ocurran resultados negativos (o sus impactos en caso de que ocurran), pero la efectividad de la gestión de riesgos depende, en gran medida, de las decisiones adoptadas por los responsables del gobierno de riesgos. Para los profesionales que están más familiarizados con COBIT 2019, las actividades de este capítulo están relacionadas con el objetivo APO12 *Riesgo gestionado*.[15]

Los temas tratados aquí incluyen:

1. los criterios de riesgos: expresar el impacto en términos de negocio;
2. la identificación del riesgo;
3. la evaluación y el análisis del riesgo;
4. los planteamientos cuantitativos y cualitativos;
5. los mapas de riesgos (heatmaps);
6. los escenarios de riesgo de I&T;
7. el registro de riesgos.

4.1.1 Criterios de riesgos: expresar el impacto en términos de negocio

La gestión de riesgos es una actividad empresarial que mejora con un planteamiento estructurado y estandarizado que pueda aplicarse a toda la empresa sin una modificación ni personalización sustancial. Se puede identificar el riesgo sistema a sistema o proyecto a proyecto, pero como resultado, dicho planteamiento crea el riesgo de una falsa confianza al no tener ni consistencia ni interoperabilidad entre los métodos, las técnicas o los procesos de riesgos que se han implementado. Sin un procedimiento estructurado, el riesgo se puede medir de manera diferente en distintas partes de la organización, creando confusión y conduciendo a la gestión del riesgo individual en lugar de una gestión de riesgos para toda la empresa.

La gestión de riesgos es una actividad empresarial que mejora con un planteamiento estructurado y estandarizado que pueda aplicarse a toda la empresa sin una modificación ni personalización sustancial.

Una técnica de análisis que es útil en esta etapa es el desarrollo de los criterios de impacto específicos de la organización.

[15] Ver ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, APO12 *Managed risk.*

Los criterios de impacto dan significado al riesgo, y ayudan a que la empresa establezca los apetitos de riesgo o tolerancias al riesgo específicos de la organización. Los criterios pueden ser de naturaleza cualitativa o cuantitativa. Una razón para desarrollar criterios de impacto con rangos cuantitativos definidos (umbrales) es que los criterios pueden actuar como contribuciones o controles dobles para las declaraciones del apetito de riesgo y la tolerancia al riesgo.

Los criterios de impacto se aplican a la empresa, no a un activo específico de I&T, y reflejan las áreas que son más relevantes para los objetivos del negocio o la misión. Un buen conjunto inicial de criterios de impacto genérico debería, como mínimo, incluir el financiero, el de productividad, el de la interrupción del negocio o las tolerancias de disponibilidad de los sistemas, el de pérdidas tangibles (p. ej. propiedad, maquinaria, equipos), el de seguridades física, vida, salud, laboral, y el de las multas y las sanciones legales. A medida que los criterios de impacto se van perfeccionando con el tiempo, puede ser útil para la dirección distinguir entre los tipos de riesgo que conducirían a costos directos inmediatos de los que darían lugar a futuras pérdidas de ingresos o responsabilidades para la organización. Un ejemplo de una tabla de criterios de impacto[16] aparece en la **figura 4.1.**

Figura 4.1—Tabla de criterios de impacto

Área de impacto	Bajo	Moderado	Alto
Reputación	• La reputación se ve mínimamente afectada; se necesita poco o ningún esfuerzo o gasto para recuperarla. El impacto se limita a clientes internos/pocos clientes.	• La reputación se daña, y se requiere cierto esfuerzo y gasto para recuperarla. El impacto se limita a una área local específica del mercado.	• La reputación se ve destruida o dañada de forma permanente. Todas las áreas geográficas del mercado se ven afectadas.
Pérdida de clientes claves	• Reducción de menos del 1 por ciento de clientes durante entre uno y 30 días debido a la pérdida de confianza.	• Reducción del 1 al 5 por ciento de clientes durante entre uno y 30 días debido a la pérdida de confianza.	• Reducción de más del 5 por ciento de clientes durante entre uno y 30 días debido a la pérdida de confianza.
Financiera	• Se imponen multas inferiores a 50 000 USD. • Se presentan demandas fundamentadas inferiores a 250 000 USD contra la organización, o se presentan demandas frívolas contra la empresa.	• Se imponen multas de entre 50 000 y 100 000 USD. • Se presentan demandas fundamentadas contra la empresa superiores a 250 000 USD, pero menores de 500 000 USD.	• Se imponen multas superiores a 100 000 USD. • Se presentan demandas fundamentadas contra la empresa superiores a 500 000 USD.
Productividad / horas de personal	• Las horas de trabajo del personal aumentan en menos de un 5 por ciento durante entre uno y 30 días. • Menos del 25 por ciento del personal está ausente durante una semana o menos.	• Las horas de trabajo del personal aumentan entre un 3 y un 7 por ciento durante entre 30 y 60 días. • Más del 25 por ciento del personal está ausente de una a tres semanas.	• Las horas de trabajo del personal aumentan en más del 8 por ciento durante más de 60 días. • Más del 25 por ciento del personal está ausente durante más de tres semanas.

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

[16] Procedente de Software Engineering Institute, Carnegie Mellon University, http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419

Al analizar escenarios de riesgo, se deben evaluar dos propiedades de cada uno de ellos: frecuencia e impacto. "Magnitud" e "impacto" suelen usarse indistintamente en conversaciones de riesgo corrientes, a pesar de que pueden conllevar pequeños matices. La "magnitud" es una descripción más objetiva y firme de cuán grande es algo, mientras que el "impacto" es una descripción más subjetiva de lo que esto significa para las empresas, y la consecuencia que tiene en los objetivos del negocio. La técnica para describir el impacto, explicada en esta sección, incluye ambos aspectos.

El análisis de riesgos requiere el cálculo de la frecuencia de eventos adversos y su impacto (expresado en términos de negocio). Muchas empresas utilizan sus propias escalas desarrolladas para tal propósito, basándose en una de las técnicas descritas en esta sección. Es beneficioso usar los mismos grupos de métricas para la frecuencia y el impacto en toda la empresa (ampliada): permite una mejor comprensión del riesgo y unas comparaciones más fáciles en las cadenas de valor. En última instancia, la mayoría de los métodos de análisis de riesgos requieren datos de pérdidas específicos, rangos de datos de pérdidas reales, rangos estimados de pérdidas de datos potenciales, o alguna combinación de estos tipos de datos para comprender el posible impacto.

Los datos estadísticos pueden estar disponibles en diferentes cantidades y calidades, que van en una escala continua desde casi inexistentes a profusamente disponibles. Cuando se dispone de una amplia variedad de datos estadísticos, el método preferido de evaluación de riesgos podría ser una evaluación cuantitativa. Con datos escasos, incompletos o deficientes, o en una situación en la que la organización desea saber más sobre las características del riesgo, se puede utilizar un conjunto más amplio de rangos cuantitativos para representar fielmente la incertidumbre que surge de los datos escasos. Cuanto mejores sean las entradas del proceso cualitativo o cuantitativo, más fiables serán los resultados. Contar con entradas de datos incompletos, deficientes o imprecisos, o con estimaciones erróneas afecta a la fiabilidad tanto de los métodos cuantitativos como de los cualitativos.

Los métodos híbridos de evaluación de riesgos se pueden aplicar a situaciones comprendidas entre los extremos aquí descritos. Cuando hay menos datos disponibles, el uso de métodos y mediciones más simples puede ser un buen comienzo, teniendo en cuenta que las estimaciones usadas en el análisis pueden introducir incertidumbre en el mismo. También es importante comunicar a las partes interesadas el nivel de confianza en los datos o las estimaciones. Esto da transparencia a la precisión de los resultados del análisis y confianza al analista para fiarse de esos resultados.

4.1.2 Identificación del riesgo

Esta etapa exige la identificación de amenazas, condiciones, áreas de preocupación o riesgos conocidos para los objetivos del negocio o la misión. A menudo, en una empresa no existe un proceso proactivo de identificación de riesgo, lo que significa que no hay manera de elevar un área de preocupación al nivel adecuado en la organización para la toma de decisiones. Cuando se trabaja con consejos o comités de gobierno, el riesgo se plantea a través del proceso de auditoría en lugar de hacerlo por un proceso proactivo de identificación del riesgo.

En las instancias de riesgo, crisis o incidente, es muy probable que haya alguien que supiera que existía una condición o circunstancia que podía conducir a que sucediera algo malo, pero no había manera de que la persona lo articulara o planteara una preocupación que luego pudiese someterse a los procesos de análisis y las técnicas de toma de decisiones necesarias.

A menudo, las organizaciones son mucho mejores respondiendo ante el riesgo materializado que evitando que este ocurra cuando tienen un sólido proceso o capacidad de identificación de riesgos. Hoy en día, muchas empresas se encuentran más cómodas con el planteamiento de evaluación de riesgos que intenta determinar la frecuencia con que sucede un evento o incidente (riesgo materializado), que luego se combina con una escala de gravedad definida organizacionalmente, un índice del impacto o una calificación numérica ordinal del impacto que produciría la materialización del riesgo. La dificultad de usar este tipo de análisis es que la probabilidad y el impacto son importantes, pero no constituyen la representación completa de la totalidad del riesgo al que hace frente la organización.

El proceso de identificación del riesgo trata de mejorar la confianza en el conocimiento y la comprensión del riesgo que tiene el potencial de impedir la capacidad de la empresa para cumplir con sus objetivos estratégicos. El proceso de identificación del riesgo puede realizarse en contextos formales (p. ej. talleres o sesiones de lluvia de ideas) o informales (p. ej. problemas identificados en reuniones o durante "conversaciones en el dispensador de agua"). Cuando sucede durante una sesión de lluvia de ideas, suele comenzar con una relación de cosas que quitan el sueño a los participantes, ciberamenazas o áreas de preocupación.

El proceso de identificación del riesgo trata de mejorar la confianza en el conocimiento y la comprensión del riesgo que tiene el potencial de impedir la capacidad de la empresa para cumplir con sus objetivos estratégicos.

El profesional de riesgos cuenta con varias fuentes posibles para la identificación del riesgo, que incluyen:

- Métodos históricos o basados en la evidencia, tales como una revisión de:
  - informes de auditorías o incidentes;
  - medios de comunicación (p. ej. periódicos, televisión);
  - comunicados de prensa e informes anuales.
- Planteamientos sistemáticos (opinión de expertos) en los que un equipo de riesgos examina y cuestiona un proceso de negocio de manera sistemática para determinar los puntos potenciales de fallo, tales como:
  - evaluaciones de vulnerabilidades;
  - revisión de los PCN y PRD;
  - entrevistas y talleres con directivos, empleados, clientes, proveedores y auditores;
  - métodos inductivos (análisis teórico), en los que un equipo examina un proceso para determinar el posible punto de ataque o compromiso, como las pruebas de penetración.

La recopilación de información del personal es un método valioso para obtener información sobre el negocio de las personas más cercanas a los procesos y con más probabilidades de entender su funcionamiento fundamental. Sin embargo, las entrevistas plantean ciertos desafíos de los que el profesional de riesgos debe ser consciente. Uno es que muchas personas quieren ser vistas como participantes esenciales en la misión de la organización, lo que las puede llevar exagerar su propia importancia y la de sus equipos o departamentos. Otro es que las personas podrían no entender por completo los procesos generales de negocio o las dependencias entre sus departamentos y otros departamentos. En algunos casos, como en los de negligencia demostrable o conducta indebida, alguien podría proporcionar información incorrecta intencionalmente.

La recopilación de información del personal es un método valioso para obtener información sobre el negocio de las personas más cercanas a los procesos y con más probabilidades de entender su funcionamiento fundamental.

El profesional de riesgos puede mejorar la posibilidad de que una entrevista genere información útil al adoptar las siguientes buenas prácticas:

- Designar un intervalo de tiempo específico y que no se exceda dicho tiempo sin mutuo acuerdo.
- Cuando se le dice a un directivo que un miembro del personal deberá ausentarse durante 45 minutos, este no debería descubrir que la entrevista duró 90 minutos.
- Saber todo lo posible sobre el proceso del negocio antes de la entrevista, para reducir el tiempo dedicado a explicaciones generales de las funciones principales del negocio.
- Forjar una alianza con el equipo de auditoría interna responsable del alcance específico del proyecto o compromiso. El beneficio de la transparencia en los procesos de riesgo, con auditoría como socio, no puede menospreciarse.
- Antes de la entrevista, obtener y revisar la documentación relevante relacionada con el alcance del panorama del riesgo, como los mapas de procesos, los procedimientos operativos estándar, los resultados de evaluaciones de impacto y las topologías de red.

- Preparar las preguntas y facilitárselas a los entrevistados con antelación para que puedan aportar cualesquiera documentos justificativos, informes o datos que pudiesen ser necesarios.
- Realizar entrevistas con significados interlocutores para garantizar un conocimiento profundo de la empresa, incluyendo cada aspecto de cada operación de negocio. Los significados interlocutores pueden incluir miembros del consejo de administración, administradores, terceros prestadores de servicios críticos, clientes, proveedores y directores.
- Alentar a los entrevistados a mostrarse abiertos sobre los desafíos a que se enfrentan y el riesgo que les preocupa, así como también cualquier posible oportunidad perdida o problemas asociados con sus procesos, sistemas y servicios/productos actuales.
- Evitar que se establezcan expectativas incorrectas sobre la confidencialidad de las respuestas de la entrevista. La gente puede preocuparse por las repercusiones de discutir fallos u oportunidades perdidas. Solo se puede prometer confidencialidad si esta realmente se mantendrá.

4.1.3 Evaluación y análisis del riesgo

La "evaluación de riesgos" suele usarse como un término genérico para describir cualquier proceso utilizado para identificar y valorar el riesgo, independientemente de que la valoración del riesgo esté sujeta a métodos de análisis cuantitativos o cualitativos. En su planteamiento más sencillo, una evaluación de riesgos consiste en entender qué podría posiblemente salir mal, la probabilidad de que un evento particular suceda, y su impacto potencial en la empresa.

La evaluación de riesgos es ligeramente más amplia que el análisis de riesgos e incluye las actividades de clasificación o priorización del riesgo identificado según los umbrales de riesgo (basados en las tolerancias) definidos en la empresa, el agrupamiento de tipos de riesgos parecidos para su mitigación, y la documentación de los controles existentes que proporcionan la mitigación para tipos similares de riesgos. Independientemente de los métodos de evaluación o análisis usados en una empresa, el profesional de riesgos puede producir un resultado más significativo si adopta las siguientes buenas prácticas:

- Realizar algunas evaluaciones (en general, cualitativas) o análisis (en general, cuantitativos) de la amenaza, condición o preocupación para determinar el curso de acción. Las amenazas, condiciones o preocupaciones que se evalúan o analizan por tener un impacto suficientemente significativo en el negocio, si se materializan, también podrían valorarse para determinar la probabilidad de que ocurran. Un método de análisis común en esta etapa del proceso es utilizar los métodos de análisis cuantitativo de MFL o PML. Estos métodos pueden ayudar a la dirección a entender cuál sería el impacto financiero total en la empresa si el riesgo se materializara. Las técnicas MFL y PML combinan mejor con un conjunto completo de escenarios de riesgo relevantes con supuestos bien establecidos.
- Si se identifica un riesgo, introducirlo en un inventario, en ocasiones denominado registro de riesgos, y determinar cuál será el siguiente paso en el análisis o la respuesta. Este paso en el proceso de gestión de riesgos necesita con frecuencia un análisis adicional de los factores de riesgo para determinar un curso de acción eficaz o de coste-justificación para un plan de corrección. Un proceso de análisis de decisiones recomendado es el uso del método de análisis de Monte Carlo[17] de modelado y simulación para graduar-secuenciar, o priorizar, el inventario de preocupaciones de riesgo de un registro de riesgos para obtener respuestas adecuadas. Las simulaciones de Monte Carlo, como las utilizadas en el método de Análisis de factores de riesgo de la información[18] (FAIR™), contempla el riesgo como una función de la probabilidad (frecuencia con la que pasa algo) y el impacto. El modelo analítico completo de FAIR permite los análisis de Monte Carlo; sin embargo, se puede utilizar para evaluar estáticamente los resultados de los mejores y peores casos de escenarios a efectos de permitir su clasificación. La cuestión es que la probabilidad y el impacto no constituyen una representación completa cuando se analiza el riesgo. Los eventos improbables ocurren con demasiada frecuencia, y muchos eventos probables nunca se materializan.

[17] Brownlee, J.; "A Gentle Introduction to Monte Carlo Sampling for Probability," Machine Learning Mastery, 4 November 2019, h*ttps://machinelearningmastery.com/monte-carlo-sampling-for-probability/*

[18] The Open Group, Open FAIR™standards, *https://publications.opengroup.org/standards/open-fair-standards*

- La expectativa de pérdidas anuales (ALE) suele utilizarse para distribuir las pérdidas probables durante cierto período de tiempo dependiendo de la precisión de los datos usados en el modelado. Puede que el uso del método ALE combinado con un análisis de Monte Carlo no sea útil para adoptar decisiones sobre transferencias de riesgos. ALE distribuye las pérdidas a lo largo de un plazo que puede distorsionar o minimizar las pérdidas financieras reales en que se incurriría si el riesgo se materializara. Por ejemplo, supongamos que el uso de una simulación de Monte Carlo para un escenario dado determina que, de materializarse, el impacto de que ocurriese un ciberriesgo específico sería de 350 millones de USD. La probabilidad de que el riesgo se materialice es de una vez cada 10 años. Al combinar el resultado del análisis de modelo de Monte Carlo de un impacto de 350 millones de USD con ALE con la probabilidad de que este riesgo se materialice una vez cada 10 años se distribuye el impacto de 350 millones de USD durante un período de 10 años. El análisis de este ciberriesgo específico conduce a su introducción en el registro de riesgos como una pérdida potencial de 35 millones de USD, que podría estar dentro de la tolerancia de la organización. Sin embargo, cuando ese ciberriesgo específico realmente se materializa en un año dado, la empresa tiene un evento de pérdida de 350 millones de USD, no de 35 millones de USD. La organización podría haber respondido con diferentes opciones de mitigación o de transferencia del riesgo si hubiese conocido el impacto potencial completo (MFL/PML) de la pérdida antes de que se materializara.

Hay varios métodos para el análisis de riesgos, que van desde los de alto nivel y principalmente cualitativos, hasta otros muy detallados y/o cuantitativos, con híbridos entre ambos. Puede que se necesiten diversas modalidades en las diferentes etapas del proceso de gestión de riesgos. Por ejemplo, al análisis cualitativo tiende a ser mejor en la etapa inicial de evaluación del riesgo para realizar una clasificación rápida del riesgo identificado, y el análisis cuantitativo puede proporcionar más rigor y exactitud para los tipos o las áreas de riesgo seleccionados que necesitan más análisis. Hay multitud de buenas fuentes de datos para soportar el análisis de riesgos, y existen varias fuentes de las que pueden obtenerse estos datos internamente, incluyendo colegas de otras disciplinas que pueden estar recopilando datos similares.

La cultura de la empresa, sus recursos, sus habilidades y su conocimiento sobre la gestión de riesgos de I&T, su entorno, su apetito de riesgo, y su planteamiento actual de la GRE determinarán qué metodología se utiliza.

4.1.4 Planteamientos cualitativos y cuantitativos

Un planteamiento cualitativo de evaluación de riesgos utiliza opiniones de expertos para estimar la frecuencia y el impacto en el negocio de eventos adversos. La frecuencia y el impacto se estiman usando descripciones cualitativas, tales como alta, media o baja. Estas etiquetas pueden variar dependiendo de las circunstancias y los diferentes entornos. Para explicar con más detalle esta cuestión, en general, no es útil agrupar el riesgo usando un descriptor cualitativo porque no hay manera de saber qué riesgo “alto” es mayor que otro riesgo “alto” del mismo grupo. Alternativamente, no hay manera de saber si aglutinar un grupo de riesgos “bajos” es equivalente a uno o más riesgos “medios”, o a uno “alto”. Los métodos cualitativos tampoco soportan la agregación de riesgos de manera significativa cuando se trata de examinar el riesgo en toda la empresa.

Los métodos cualitativos se usan de forma efectiva para identificar las características similares o distintas con fines de agrupación, y pueden ayudar a mejorar la eficiencia en la aplicación de los controles o de las técnicas de mitigación para responder al riesgo que serían efectivos frente a tipos de riesgo comunes. Por ejemplo, se puede reducir la incertidumbre agrupando todos los riesgos “altos”, y evaluando más a fondo si alguno de estos puede mitigarse o responderse de una manera efectiva que aporte valor a la empresa. Esto puede conducir a mejores procedimientos, objetivos de cumplimiento racionalizados, u objetivos de control optimizados. Los planteamientos cualitativos no pretenden ser un método de medición. La medición del riesgo debería ayudar a una empresa en la toma de decisiones sobre la incertidumbre de la materialización de un escenario de riesgo.

Los métodos cualitativos se usan de forma efectiva para identificar las características similares o distintas con fines de agrupación, y pueden ayudar a mejorar la eficiencia en la aplicación de los controles o de las técnicas de mitigación para responder al riesgo que serían efectivos frente a tipos de riesgo comunes.

Cuando se usan valores cuantitativos (p. ej. rangos estimados, financieros, temporales) para definir valores cualitativos, o cuando solo se utilizan valores cuantitativos, se trata de un análisis cuantitativo. Por ejemplo, muchas organizaciones que actualmente usan una escala de medición alta, media y baja asignarán arbitrariamente la escala de calificación de riesgo a los números 1 (alta), 2 (media) o 3 (baja) para graduar-secuenciar un inventario de riesgos. El uso de una escala numérica para representar el riesgo identificado en un gráfico no equivale a un análisis de riesgos cuantitativo. La esencia de la evaluación cuantitativa del riesgo consiste en obtener la frecuencia y el impacto de los escenarios de riesgo, a partir de mediciones, métodos estadísticos y datos.

El análisis basado en opiniones individuales o datos estimados puede ser insuficiente para adoptar decisiones mejores, y puede que no proporcione valor a la empresa. ¿Qué seguridad puede tener uno de los resultados de la evaluación de riesgos si las entradas que conducen a los resultados son deficientes, sesgadas o incorrectas? Queda además la cuestión de la incertidumbre. Hay algunos métodos avanzados para aumentar la fiabilidad de las evaluaciones de riesgos, pero éstos requieren de ciertos conocimientos y habilidades estadísticas. Actualmente, la calibración de los profesionales de riesgos no se basa en métodos estadísticos pese a que mejoran el proceso de estimación y la fiabilidad de las entradas cuantitativas cuando los datos son escasos. La calibración es el ajuste fino de la capacidad de los profesionales de riesgos para mejorar sus estimaciones a lo largo del tiempo tiempo, reconocer tanto sus propios sesgos como otros sesgos, y disminuir la subjetividad en la etapa de análisis. El análisis cuantitativo del riesgo, tal como se aplica actualmente en la práctica, se encuentra esencialmente en las primeras etapas de madurez en el campo de la I&T, y la inversión en métodos cuantitativos avanzados no siempre da como resultado el valor o el retorno de la inversión previsto.

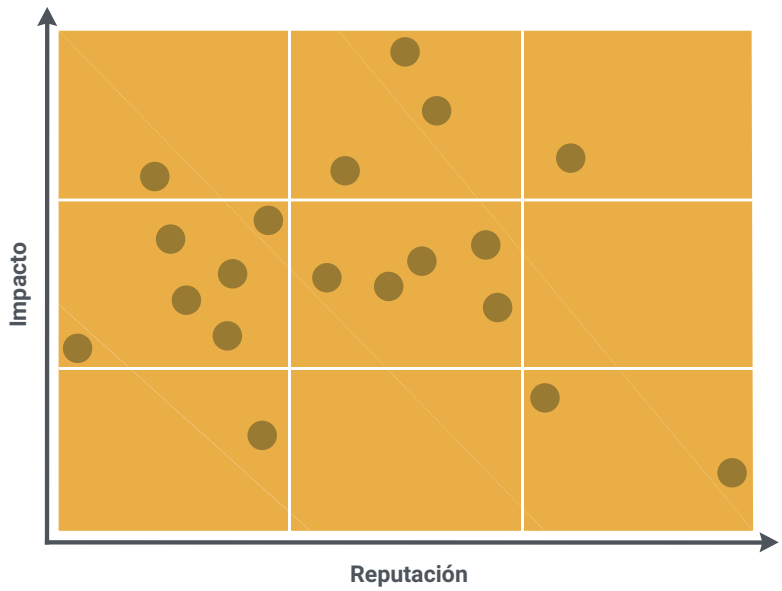
Los diferentes métodos, cuantitativos y cualitativos, tienen algunas limitaciones comunes:

- Ningún método es totalmente objetivo, y los resultados de las evaluaciones y los análisis pueden estar sujetos a sesgos personales, a los conocimientos y habilidades del encargado de la evaluación, y a los datos disponibles utilizados en la evaluación.
- Las evaluaciones que son sólo cuantitativas están sujetas a crear exceso de confianza en modelos complejos basados en datos insuficientes.
- Las evaluaciones que son sólo cualitativas también están sujetas a resultados poco fiables debido a la naturaleza sobresimplificada del uso de una escala de medición ordinal o basada en una taxonomía.

4.1.5 Mapas de riesgos (heatmaps)

Como se mencionó anteriormente en este documento, los mapas de riesgos (o heatmaps) se han convertido en el método común para visualizar el contexto y el alcance del riesgo. En estos mapas, el riesgo se representa en un diagrama bidimensional cuyas dos dimensiones son la frecuencia y el impacto. En la **figura 4.2.** se muestra un ejemplo de mapa de riesgos.

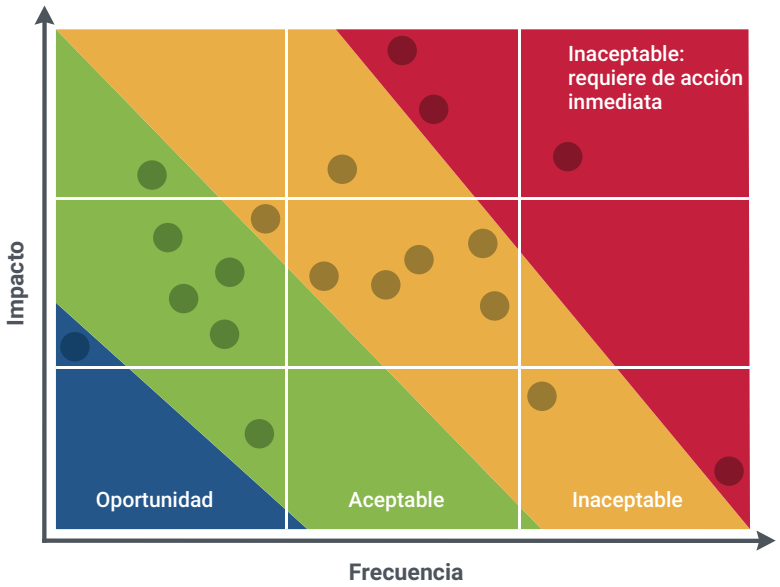
Figura 4.2—Ejemplo de mapa de riesgos



El mapa de riesgos se hace más útil cuando se combina con las diferentes zonas del apetito de riesgo (ver el Capítulo 3). Los diferentes grupos de importancia del apetito de riesgo se designan en el mapa de riesgos usando zonas coloreadas, lo que lleva al ejemplo de la **figura 4.3**. Esta versión del mapa de riesgos identifica inmediatamente los riesgos que son realmente inaceptables y requieren de una respuesta inmediata, tal como se establece en las declaraciones de apetito de riesgo de la empresa.

En el otro extremo del espectro, el mapa de riesgos también podría permitir la identificación de oportunidades para relajar los controles o asumir más riesgo, como indica la zona azul de la **figura 4.3.**

Figura 4.3—Ejemplo de mapa de riesgos con apetito de riesgo



El uso de un mapa de riesgos es valioso si los criterios de medida subyacentes y las escalas de impacto están bien definidos, y la organización entiende bien el lenguaje. A medida que maduran el proceso de gestión de riesgos y la toma de decisiones, suele haber un alejamiento del cálculo de la probabilidad de que un riesgo ocurra para prestar mayor atención al impacto financiero que podría tener en la empresa el riesgo materializado. Esto ocurre cuando el consejo y la dirección establecen el requisito de cuantificar el riesgo en términos financieros; para ello, las técnicas más comunes son cambiar el procedimiento al cálculo de la PML o la MFL. El uso de la PML o la MFL permite que el riesgo se analice respecto de su impacto financiero en la organización, en caso de materializarse. Estas técnicas se usan para garantizar que la empresa disponga de las protecciones financieras adecuadas en caso de que se materialice un riesgo.

A medida que maduran el proceso de gestión de riesgos y la toma de decisiones, suele haber un alejamiento del cálculo de la probabilidad de que un riesgo ocurra para prestar mayor atención al impacto financiero que podría tener en la empresa el riesgo materializado.

Una consideración final para calcular el impacto durante el análisis y la evaluación de riesgos es que la mejor manera de obtener estimaciones fiables y aceptables consiste en involucrar a todas las partes interesadas en los ejercicios de análisis de escenarios. Esto puede llevarse a cabo mediante evaluaciones separadas o a través de talleres, seguidos de discusiones en grupo para alcanzar el consenso. El personal que realiza el trabajo es una fuente excelente de escenarios verosímiles, o puede contar con información sobre las cuasi-pérdidas que se hayan producido. El nivel de confianza de la evaluación es la confianza que se tiene en las fuentes de datos o las estimaciones calibradas usadas en el análisis, y las ventajas de comunicar ese nivel a las audiencias no puede menospreciarse. Esto puede resultar especialmente importante cuando se utilizan procedimientos menos sofisticados de calificación o visualización del riesgo, para garantizar que los responsables de la toma de decisiones se hagan una idea de cuánto pueden confiar en los resultados de la evaluación.

4.1.6 Registro de riesgos

Se denomina **registro de riesgos** a un inventario de áreas de riesgo que se han identificado, analizado y priorizado. Un registro de riesgos es el inventario de los eventos adversos potenciales que se han identificado y analizado para entender su posible impacto, en caso materializarse. El registro de riesgos no es una lista de deficiencias de controles o de parches de software que faltan en un servidor. Si no hay incertidumbre, la deficiencia de control es una instancia o un problema, no un riesgo. La gestión de instancias o problemas trasciende del alcance de esta publicación, pero podría considerarse como parte del establecimiento de la función de riesgo. El registro de riesgos puede considerarse como una extensión del mapa de riesgos (ver la **figura 3.3**), que ofrece una información detallada sobre cada riesgo identificado, incluyendo:

- la identificación del riesgo;
- el propietario del riesgo;
- los detalles del escenario de riesgo;
- la organización o unidad de negocio;
- la fecha de la identificación del riesgo;
- la fuente del riesgo (si se conoce);
- el propietario del riesgo/el punto de contacto;
- el título del riesgo;
- la descripción del riesgo;
- el índice (cualitativo) de severidad (mapa);
- información sobre los resultados detallados de análisis o los índices (cuantitativos);
- información detallada sobre la respuesta al riesgo;
- el estado actual de la respuesta al riesgo;
- información sobre los controles (si corresponde);
- la categoría principal del riesgo;
- la categoría secundaria del riesgo (si se utiliza);
- el estado de la corrección o el despliegue;
- la fecha del estado actual;
- la fecha de seguimiento;
- los comentarios.

No hay informaciones nuevas en el registro de riesgos que no se hayan recogido en las secciones previas. Un registro de riesgos es simplemente una técnica práctica para almacenar y mantener toda la información recopilada en un formato útil para todas las partes interesadas. A menudo, cuando una empresa decide comprar una herramienta comercial para gestionar el riesgo, ésta incluye una plantilla de registro de riesgos lista para usuarse que puede personalizarse específicamente para dicha organización.

Capítulo 5
Definición de escenarios de riesgo

5.1 Introducción

Los escenarios de riesgo facilitan la comunicación en la gestión de riesgos al construir una narrativa que puede inspirar a las personas a actuar. El uso de escenarios de riesgo puede mejorar el trabajo de la gestión de riesgos al ayudar al equipo de riesgos a comprender y explicar el riesgo a los propietarios de los procesos de negocio, y a otras partes interesadas. Además, un escenario bien desarrollado proporciona una visión realista y práctica del riesgo que está más alineada con los objetivos de negocio, los eventos históricos y las amenazas emergentes previstas por la organización de lo que se habría conseguido consultando un estándar o un catálogo de controles de aplicación general. Estos beneficios hacen que los escenarios de riesgo sean valiosos como medio para recopilar y enmarcar la información usada en los siguientes pasos del proceso de gestión de riesgos.

Uno de los desafíos para la gestión de riesgos de I&T es identificar el riesgo importante y relevante entre todo aquello que posiblemente pueda salir mal en el área de I&T o en relación con la I&T, debido a la presencia generalizada de la I&T y a la dependencia que tiene el negocio de ella. Una de las técnicas para superar este desafío es el desarrollo y uso de escenarios de riesgo. Es un planteamiento esencial para aportar realismo, conocimiento, compromiso organizacional, análisis mejorado, y estructura a la compleja cuestión del riesgo de I&T. Una vez que se han desarrollado estos escenarios, se utilizan durante el análisis de riesgos, en el que se estiman la frecuencia y los impactos en el negocio.

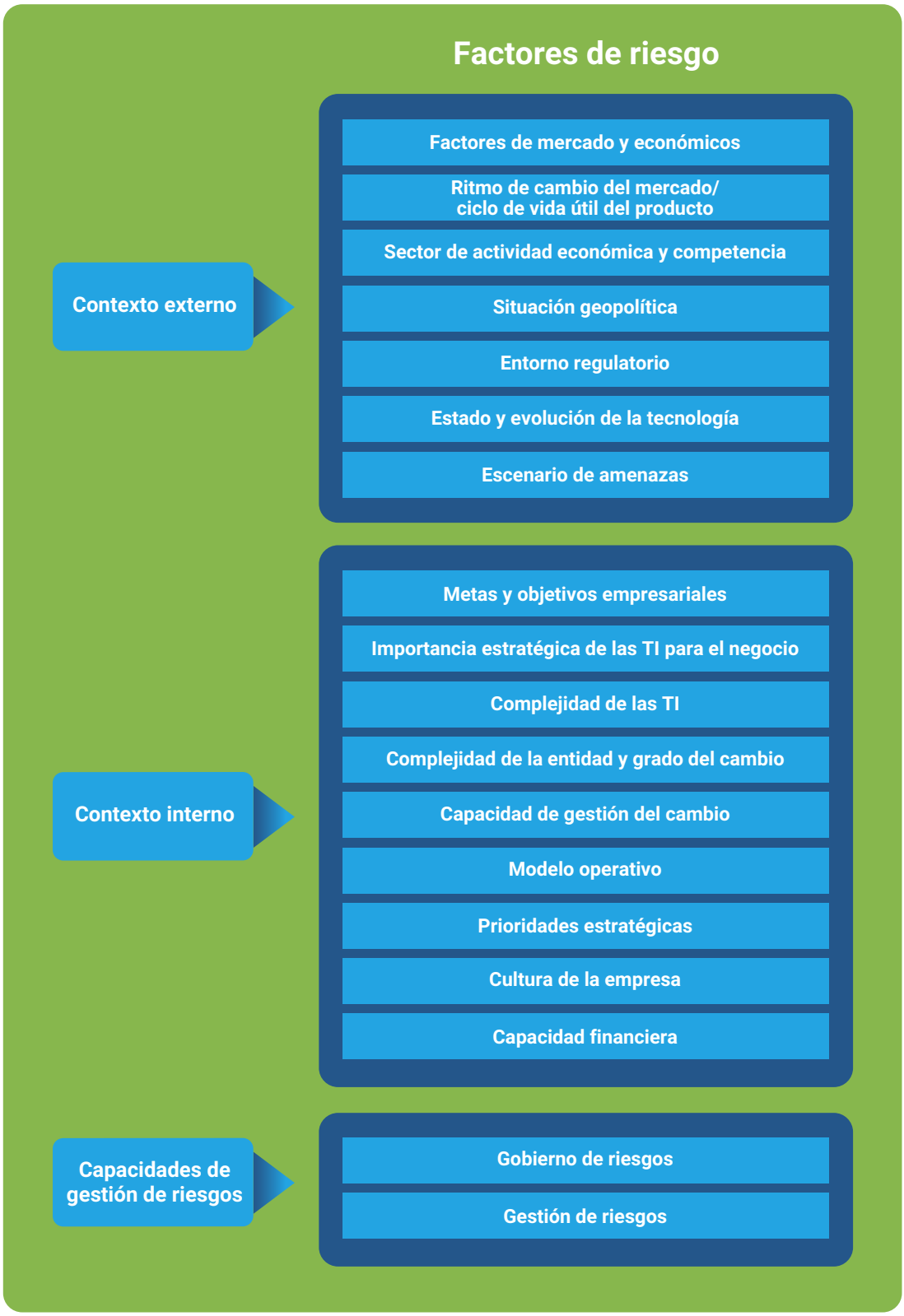
Los escenarios de riesgo pueden obtenerse a través de dos mecanismos diferentes:

- Un **enfoque de arriba hacia abajo**, en el que se utilizan la misión, la estrategia, y los objetivos del negocio como la base para la identificación y el análisis del riesgo que sea verosímil y relevante para conseguir los resultados deseados. Si los criterios del impacto están bien alineados con los verdaderos impulsores de valor de la empresa, se desarrollarán escenarios de riesgo relevantes.
- Un **enfoque de abajo hacia arriba**, que generalmente comienza con los activos, los sistemas o las aplicaciones considerados importantes para la empresa, y prosigue con el uso de una lista de amenazas o escenarios de pérdidas genéricas para definir un conjunto de escenarios más concretos y personalizados aplicados a la situación particular de la empresa. El enfoque de abajo hacia arriba se usa comúnmente en las evaluaciones de ciberamenazas y vulnerabilidades, pero puede limitar o pasar por alto el impacto real sobre el negocio si no se combina con una consideración exhaustiva del enfoque de arriba hacia abajo expuesto anteriormente.

Ambos enfoques son complementarios y deberían usarse simultáneamente. Es aquí donde una **taxonomía** de riesgo podría resultar útil. Una taxonomía de riesgo proporciona un esquema para clasificar las fuentes y las categorías del riesgo. El tránsito entre una ciberamenaza o área de preocupación y un riesgo requiere que la descripción de riesgos se descomponga en componentes sobre los que se pueda actuar. Una taxonomía de riesgo proporciona un lenguaje común para discutir y comunicar el riesgo a las partes interesadas. Los escenarios de riesgo deben ser relevantes y estar vinculados al riesgo real del negocio o de la misión.

Una vez que se ha definido el conjunto de los escenarios de riesgo, este se puede usar para el análisis de riesgos, en el que se evalúan la frecuencia y el impacto del escenario. Un componente importante de esta evaluación son los factores de riesgo. Los factores de riesgo son aquellos factores que influyen en la frecuencia y/o el impacto en el negocio o la misión de los escenarios de riesgo; pueden ser de diferentes naturalezas, y se pueden clasificar como se muestra en la **figura 5.1**:

Figura 5.1—Ejemplos de factores de riesgo



Los factores contextuales pueden ser internos o externos a la empresa, siendo la principal diferencia el grado de control que una organización tiene sobre ellos:

- Los factores contextuales externos están, en gran medida, fuera del control de la empresa. Por ejemplo, un planteamiento de gestión de riesgos maduro dedicará menos tiempo a realizar el análisis sobre la probabilidad de que se produzca una amenaza, y más tiempo a desarrollar capacidades que detectarían y contendrían más rápidamente la amenaza si esta se materializara.
- Los factores contextuales internos están, en gran medida, bajo el control de la empresa, aunque no siempre puedan ser fáciles de cambiar. Por ejemplo, las malas prácticas de concienciación de los usuarios suelen ser la causa raíz de un riesgo que se materializa y ocasiona un incidente.

Se propone la siguiente estructura para los escenarios de riesgo, basada en una revisión de las metodologías de riesgos actuales (Risk IT, COBIT 2019, FAIR, Committee of Sponsoring Organizations of the Treadway Commission [COSO] Enterprise Risk Management [ERM] 2017). La estructura recoge todos los elementos que deberían describirse para tener un escenario de riesgo completo y analizable.

La principal diferencia entre la definición de un escenario de riesgo presentado en el Marco de riesgos de TI y la estructura de escenarios de riesgo de la actualización de COBIT es la adición del componente del efecto. Este componente es autoexplicativo: describe el efecto del evento de amenaza que se materializa.

Figura 5.2—Estructura del escenario de riesgo

Fuente: ISACA, *Risk IT Framework, 2nd Edition*, USA, 2020, figura 6.2,*https://www.isaca.org/bookstore/bookstore-risk-digital/ritf2*

Los diferentes componentes de la estructura del escenario de riesgo se muestran en la **figura 5.2** y se describen de la siguiente manera:

- **Agente/Comunidad de la amenaza.**—¿Quién genera la amenaza que explota una vulnerabilidad? Los agentes pueden ser internos o externos, y pueden ser humanos o no humanos. No todos los tipos de amenaza requieren de un agente; por ejemplo, los fallos o las causas naturales podrían constituir amenazas. Los agentes se categorizan de la siguiente manera:
  - Los agentes internos están dentro de la empresa, como el personal y los contratistas.
  - Los agentes externos incluyen a las personas ajenas a la empresa, los competidores, los reguladores y el mercado.
- **Intención/Motivación** (la naturaleza del evento).—¿Es maliciosa? Si no es así, ¿es accidental o es un fallo de un proceso bien definido? ¿Es un evento natural?
- **Evento de amenaza.**—¿Es la divulgación de información confidencial, la interrupción de un sistema o de un proyecto, el robo o la destrucción? La acción también incluye el diseño ineficaz de sistemas, procesos, etc.; el uso inapropiado; los cambios en las normas y las regulaciones que vayan a tener un impacto significativo en un sistema; o la ejecución ineficaz de procesos, tales como los procedimientos de gestión de cambios, los procedimientos de adquisición o los procesos de priorización de proyectos.

- **Activo/recurso.**—Un activo es cualquier elemento que sea de valor para la empresa o que suponga una responsabilidad para la empresa, que puede verse afectado por el evento y producir un impacto en el negocio. Un recurso es cualquier cosa que ayude a lograr las metas de TI. Los activos y los recursos pueden ser idénticos; por ejemplo, el hardware de TI es un recurso importante porque todas las aplicaciones de TI lo utilizan y, al mismo tiempo, es un activo porque tiene un cierto valor para la empresa.
  Los activos pueden ser o no críticos, como muestra la diferencia entre un sitio web que presta servicio al cliente de un banco importante y el sitio web del estacionamiento local o la intranet del grupo de desarrollo de software. Los recursos críticos probablemente atraigan un mayor número de ataques o una mayor atención en caso de fallos; por lo tanto, la frecuencia de los escenarios relacionados probablemente sea mayor. Se necesita habilidad, experiencia y una comprensión completa de las dependencias para captar la diferencia entre un activo crítico y un activo no crítico.
- Los activos/recursos incluyen:
  - las personas y las habilidades;
  - las estructuras organizativas;
  - la infraestructura física, las instalaciones, los equipos, etc.;
  - la infraestructura de TI, incluyendo el hardware de los sistemas informáticos, la infraestructura de red, el middleware;
  - otros componentes de la arquitectura empresarial, incluyendo la información, y las aplicaciones.
- **Efecto**.— Este componente refleja el efecto del escenario de amenaza, generalmente una repercusión negativa.
- **Temporización**.— Es la dimensión en la que se podrían describir las siguientes cuestiones, si son relevantes para el escenario:
  - la duración del evento, como una interrupción prolongada de un servicio o un centro de datos;
  - el momento (¿El evento ocurre en un momento crítico?);
  - la detección (¿La detección es inmediata o no?);
  - el tiempo transcurrido entre el evento y el impacto (¿Hay un impacto inmediato, como un fallo de red o un período de inactividad inmediato, o un impacto retrasado, como una arquitectura de TI incorrecta con altos costes acumulados durante un período de varios años?).

Es importante ser consciente de las diferencias entre los eventos de pérdida, los eventos de amenaza, y los eventos de vulnerabilidad. Cuando se materializa un escenario de riesgo, se produce un evento de pérdida. El evento de pérdida se ha desencadenado por un evento de amenaza (tipo de amenaza más evento). La frecuencia del evento de amenaza que conduce a un evento de pérdida está influenciada por los factores de riesgo o la vulnerabilidad. La vulnerabilidad es, en general, un estado y puede aumentar/disminuir por eventos de vulnerabilidad; por ejemplo, el debilitamiento de los controles o la fortaleza de la amenaza. **Estos tres tipos de eventos no deberían combinarse en un macro "inventario de riesgos".**

Capítulo 6
Guía para la elaboración de escenarios de riesgo

6.1 Desarrollo de los escenarios de riesgo

En la práctica, se sugiere el siguiente planteamiento para elaborar escenarios de riesgo de TI:

- Usar la relación de ejemplos de escenarios genéricos de riesgo mostrados en la **figura 6.2** para definir un conjunto manejable de escenarios personalizados de riesgo para la empresa. Para determinar un conjunto manejable de escenarios, una empresa podría comenzar teniendo en cuenta escenarios que ocurren comúnmente en su sector de actividad económica o en su área de producto, escenarios que describen fuentes de amenaza que están aumentando en cantidad o en gravedad, y escenarios que involucran requisitos legales y regulatorios aplicables al negocio. Otro planteamiento podría ser la identificación de las unidades de negocio de alto riesgo y la evaluación en cada una de uno o dos procesos operativos de alto riesgo, incluyendo los componentes de TI que habilitan dicho proceso. También deberían incluirse algunas situaciones menos comunes en los escenarios.
- Realizar una validación frente a los objetivos de negocio de la entidad. ¿Los escenarios de riesgo seleccionados abordan los impactos potenciales en el logro de los objetivos empresariales de la entidad, soportando los objetivos de negocio globales de la empresa?
- Perfeccionar los escenarios seleccionados basándose en esta validación; detallarlos a un nivel que esté en consonancia con la criticidad de la entidad.
- Reducir el número de escenarios a un conjunto manejable. “Manejable” no significa una cantidad fija, sino que el número debería estar alineado con la importancia general (tamaño) y la criticidad de la unidad. No hay una regla general, pero si los escenarios se enfocan de manera razonable y realista, la empresa debería esperar una cantidad de, cuanto menos, varias docenas de escenarios.
- Conserve todos los escenarios en una lista de forma que se puedan reevaluar en la siguiente iteración, e incluirse en el análisis detallado si se hacen relevantes en ese momento.
- Incluya en los escenarios un evento sin especificar; por ejemplo, un incidente no cubierto por otros escenarios.
- Contemple la evaluación de escenarios que tengan alguna posibilidad de ocurrir simultáneamente. Con frecuencia, esto se conoce como pruebas de estrés y, en realidad, supone combinar múltiples escenarios y comprender el impacto adicional que tendría si ocurrieran conjuntamente.
- Base el análisis de escenarios no sólo en la experiencia pasada y en los eventos actualmente conocidos, sino también en las posibles circunstancias futuras.

Una vez que se ha definido el conjunto de escenarios de riesgo, éste se puede usar para el análisis de riesgos, en el que se evalúan la frecuencia y el impacto del escenario. Un componente importante que debe considerarse durante dichas evaluaciones son los factores de riesgo mostrados en la **figura 5.1**.

6.1.1 Principales problemas cuando se desarrollan y usan los escenarios de riesgo

El uso de escenarios es clave para la gestión de riesgos, y la técnica es aplicable a cualquier empresa. Cada empresa necesita elaborar un conjunto de escenarios (que contenga los componentes descritos en el Capítulo 5) como punto de partida para realizar su análisis de riesgos.

El desarrollo de un conjunto completo de escenarios significa, en teoría, que debería combinarse cada valor posible de cada componente. Debería, por tanto, evaluarse la relevancia y el realismo de cada combinación y, si se considera significativa, esta se debería incorporar al registro de riesgos. En la práctica, esto no es posible; rápidamente, se puede originar un número de escenarios de riesgo diferentes inviable. La cantidad de escenarios que hay que

desarrollar y analizar debería mantenerse en un número relativamente reducido de escenarios de riesgo relevantes para que sigan siendo manejables y significativos.

La **figura 6.1** muestra algunas de las principales áreas de atención/problemas que se deben abordar cuando se utiliza la técnica de escenarios de riesgo.

Figura 6.1—Principales problemas/áreas de atención de la técnica de escenarios de riesgo

Problema/área de atención	Guía resumida
Mantener actualizados los escenarios de riesgo y los factores de riesgo.	Los factores de riesgo y la empresa cambian con el tiempo; por lo tanto, los escenarios cambiarán con el tiempo, en el transcurso de un proyecto o con la evolución de la tecnología. Por ejemplo, es fundamental que la función de riesgo desarrolle un calendario de revisiones, y que el Director de informática (CIO) trabaje con las líneas de negocio para revisar y actualizar la relevancia e importancia de los escenarios. La frecuencia de este ejercicio depende del perfil general de riesgos de la empresa, y se debería realizar por lo menos una vez al año o cuando se producen cambios importantes.
Utilizar escenarios de riesgo genéricos como punto de partida, y desarrollar más detalles donde y cuando sea necesario.	Una técnica para que la cantidad de escenarios sea manejable es propagar un conjunto estándar de escenarios de riesgo genéricos a través de la empresa, y desarrollar escenarios más detallados y relevantes sólo para los niveles más bajos (de la entidad) cuando sea necesario y esté justificado por el perfil del riesgo. Las suposiciones hechas al agrupar o generalizar deberían entenderse bien por todos, y documentarse adecuadamente, ya que podrían ocultar ciertos escenarios o ser confusas cuando se busca una respuesta al riesgo. Por ejemplo, si la "amenaza interna" no está bien definida en un escenario, podría no estar claro si esta amenaza incluye usuarios privilegiados y no privilegiados. Las diferencias entre estos aspectos de un escenario pueden ser críticas para tratar de entender la frecuencia y el impacto de los eventos, así como las posibilidades de mitigación.
La cantidad de escenarios debería ser representativa, y reflejar la realidad y la complejidad del negocio.	La gestión de riesgos ayuda a afrontar la enorme complejidad de los entornos de TI actuales al priorizar la acción potencial de acuerdo con su valor para la reducción del riesgo. La gestión de riesgos trata de reducir la complejidad, no de generarla; por consiguiente, este es otro motivo para trabajar con un número manejable de escenarios de riesgo. En cualquier caso, el número de escenarios preservado aún debe reflejar con exactitud la realidad y la complejidad del negocio.
La taxonomía de riesgos debería reflejar la realidad y la complejidad del negocio.	Debería haber un número suficiente de escalas de escenarios de riesgo para reflejar la complejidad de la empresa y el alcance de las exposiciones a las que está sujeta la empresa. Las posibles escalas podrían ser una graduación baja, media, alta, o un índice numérico que califica la importancia del riesgo entre 0 y 5. Las escalas deberían estar alineadas en toda la empresa para garantizar una puntuación consistente.
Utilizar una estructura de escenario de riesgo genérico para simplificar los informes de riesgos.	Del mismo modo, con el fin de informar los riesgos, las entidades no deberían informar sobre todos los escenarios específicos y detallados, sino que pueden hacerlo usando la estructura del escenario de riesgo genérico. Por ejemplo, una entidad podría haber adoptado el escenario de riesgo genérico 2 de la **figura 6.2** (calidad del proyecto), traducirlo a cinco escenarios para sus proyectos principales, y posteriormente, realizar un análisis de riesgos para cada uno de los escenarios, para luego agregar o resumir los resultados e informarlos utilizando el encabezado del escenario de riesgo genérico "calidad del proyecto".

Figura 6.1—Principales problemas/áreas de atención de la técnica de escenarios de riesgo *(cont.)*

Problema/área de atención	Guía resumida
Verificar que la empresa tenga los requisitos de personal y habilidades adecuados para desarrollar escenarios de riesgo relevantes.	El desarrollo de un conjunto manejable y relevante de escenarios de riesgo requiere: • Destreza y experiencia para evitar pasar por alto los escenarios relevantes y verse atraído por escenarios muy poco realistas o irrelevantes. Si bien es importante evitar escenarios irrealistas o irrelevantes para utilizar adecuadamente los recursos limitados, se debería prestar atención a las situaciones que son infrecuentes e impredecibles, pero que podrían tener un impacto catastrófico en la empresa. • Una comprensión completa del entorno. Esto incluye el entorno de TI (p. ej., la infraestructura, las aplicaciones, las dependencias entre aplicaciones, los componentes de la infraestructura), el entorno de negocio en general, y la comprensión de cómo y qué entornos de TI respaldan el entorno de negocio para entender el impacto en el negocio. • La intervención y los puntos de vista comunes de todas las partes involucradas: la alta dirección, que tiene el poder decisorio; la dirección del negocio, que cuenta con la mejor visión sobre el impacto en el negocio; el área de TI, que sabe lo que puede ir mal con la TI; y la dirección de riesgos, que puede moderar y estructurar el debate entre las demás partes. • Normalmente el proceso de desarrollo de escenarios mejora con un planteamiento de lluvia de ideas/talleres, lo que suele requerir de la realización de una evaluación de alto nivel para reducir la cantidad de escenarios a un número manejable, pero relevante y representativo.
Usar el proceso de desarrollo de escenarios de riesgo para conseguir su aceptación.	El análisis de escenarios no es tan sólo un ejercicio analítico que involucra a los analistas de riesgos. Un importante beneficio adicional del análisis de escenarios es lograr la aceptación de las entidades de la empresa y las líneas de negocio, la gestión de riesgos, la TI, las finanzas, el cumplimiento y otras partes. La obtención de esta aceptación es la razón por la cual el análisis de escenarios debería ser un proceso facilitado cuidadosamente.
Involucrar a la primera línea de defensa en el proceso de desarrollo de escenarios.	Además de la coordinación con la dirección, se recomienda incluir en los debates a miembros seleccionados del personal que estén familiarizados con las operaciones detalladas, cuando se considere apropiado. El personal cuyo quehacer diario consiste en las operaciones detalladas suele estar más familiarizado con las vulnerabilidades de la tecnología y los procesos que pueden explotarse.
No centrarse sólo en escenarios poco comunes y extremos.	Al desarrollar escenarios, no debería centrarse sólo en los eventos de caso peor, ya que rara vez se materializan; otros incidentes menos graves ocurren más a menudo.
Deducir escenarios complejos de escenarios simples, mostrando el impacto y las dependencias.	Los escenarios simples, una vez desarrollados, deberían afinarse en escenarios más complejos, que muestren impactos en cascada y/o coincidentes, y reflejando las dependencias. Por ejemplo: • Un escenario de fallo importante del hardware se puede combinar con el escenario de un PRD fallido. • Un escenario de un fallo importante del software puede conducir a la corrupción de la base de datos y, en combinación con una gestión deficiente del respaldo de los datos, puede dar lugar a consecuencias graves, o al menos a consecuencias de una magnitud diferente a un fallo de software por sí solo. • Un escenario de un evento externo importante puede conducir a un escenario de apatía interna.

Figura 6.1—Principales problemas/áreas de atención de la técnica de escenarios de riesgo *(cont.)*

Problema/área de atención	Guía resumida
Considerar el riesgo sistémico y el contagioso.	Se debería prestar atención a los escenarios de riesgo sistémicos y/o contagiosos: • **Sistémico**: sucede algo con un socio de negocio importante, que afecta a un gran grupo de empresas dentro de un área o de un sector de actividad económica. Un ejemplo sería un sistema nacional de control de tráfico aéreo que se cae durante un período de tiempo prolongado, como seis horas, lo que afecta al tráfico aéreo a gran escala. • **Contagioso**: eventos que ocurren en varios de los socios de negocio de la empresa en un plazo muy corto. Un ejemplo sería una cámara de compensación que puede estar completamente preparada para cualquier tipo de emergencia al tener medidas de recuperación de desastres muy sofisticadas, pero cuando ocurre una catástrofe, descubre que ninguno de sus proveedores envía transacciones, y por lo tanto, queda temporalmente fuera de servicio.
Usar el desarrollo de escenarios para aumentar la concienciación sobre la detección de riesgos.	El desarrollo de escenarios también ayuda a abordar la cuestión de la detectabilidad, alejándose de una situación en la que una empresa no sabe qué es lo que no sabe. El planteamiento colaborativo para el desarrollo de escenarios ayuda a identificar el riesgo al que , hasta entonces, la empresa, no se había dado cuenta de que hacía frente (y, por lo tanto, para el que nunca habría pensado en poner en práctica alguna contramedida). Una vez que se identifica el conjunto completo de elementos de riesgo durante la generación de escenarios, el análisis de riesgos evalúa la frecuencia y el impacto de los escenarios. Las preguntas que se deben formular incluyen: • ¿La empresa detectará alguna vez que el escenario de riesgo se ha materializado? • ¿La empresa notará que algo ha salido mal para poder reaccionar adecuadamente? Generar escenarios y pensar creativamente en lo que puede salir mal aumentará automáticamente y, con suerte, dará respuestas a la cuestión de la detectabilidad. La detectabilidad de escenarios incluye dos pasos: la visibilidad y el reconocimiento. La empresa debe encontrarse en una posición en la que observe cualquier cosa que vaya mal, y necesita la capacidad de reconocer un evento observado como algo incorrecto.

La **figura 6.2** muestra ejemplos de escenarios de riesgo genéricos y específicos. Su objetivo es ayudar al profesional de riesgos a entender y predecir situaciones potenciales con el fin de desarrollar holísticamente la respuesta al riesgo adecuada.

Figura 6.2—Ejemplo de escenarios de riesgo genéricos y específicos

Categoría del escenario de riesgo		Ejemplos de escenario de riesgo genérico		Ejemplos de escenario de riesgo específico
1	**Toma de decisiones sobre inversiones de TI, definición y mantenimiento de la cartera (portfolio)**	A	Los programas seleccionados para su implementación están desalineados con la estrategia y las prioridades corporativas.	• Los programas seleccionados para su implementación están desalineados con la estrategia y las prioridades corporativas, lo que da como resultado una nueva aplicación de gestión de relaciones con el cliente (CRM) inadecuada que no soporta la estrategia de servicio al cliente.
		B	Las inversiones relacionadas con la TI no respaldan la estrategia digital de la empresa.	• La empresa cuenta con una inversión desalineada en un nuevo sistema de contabilidad que limita la disponibilidad de fondos para la inversión en la aplicación multicanal orientada al cliente.

Figura 6.2—Ejemplo de escenarios de riesgo genéricos y específicos *(cont.)*

Categoría del escenario de riesgo		Ejemplos de escenario de riesgo genérico		Ejemplos de escenario de riesgo específico
1	**Toma de decisiones sobre inversiones de TI, definición y mantenimiento de la cartera (portfolio)** *(cont.)*	C	Se selecciona un software inapropiado (coste, desempeño, características, compatibilidad, redundancia, etc.) para su adquisición e mplementación.	• Se implementa un software incompatible con los equipos de producción más antiguos para reemplazar sistemas heredados, generando pérdidas de producción y de negocio.
		D	Se selecciona una infraestructura inapropiada (coste, desempeño, características, compatibilidad, etc.) para su implementación.	• Se realiza una inversión en infraestructura en las instalaciones pese a carecer de las capacidades necesarias para su implementación y soporte satisfactorios, dando lugar a costes mayores y fallos en el servicio. • Se realiza una inversión en infraestructura en la nube que da como resultado una limitación en la disponibilidad local necesaria para soportar las metas de negocio, lo que genera fallos en la disponibilidad del servicio.
		E	Existen duplicidades o solapamientos importantes entre distintas iniciativas de inversión.	• Dos departamentos grandes de la empresa están invirtiendo mucho en nuevas aplicaciones orientadas al cliente, pero cada uno está desarrollando su propia base de datos de clientes (diferentes), causando mayores costes a la organización.
		F	Nuevos programas de inversión crean una incompatibilidad a largo plazo con la arquitectura empresarial.	• Los programas seleccionados para su implementación están desalineados con la arquitectura empresarial, dando lugar a una nueva aplicación de contabilidad inadecuada que no se integra con el entorno actual de aplicaciones, causando un aumento de los costes y fallos en el servicio.
		G	Se asignan y gestionan de manera ineficiente recursos que se encuentran bajo litigio, sin alineamiento con las prioridades del negocio.	• Se asigna a expertos técnicos en tecnologías críticas a trabajar en proyectos menos críticos en vez de en proyectos clave o de alta prioridad, provocando fallos en la entrega de productos y servicios.
		H	Se despliegan soluciones como TI en la sombra y software como servicio (SaaS) con cargo a los presupuestos departamentales, generando problemas de arquitectura a más largo plazo y un coste global de TI excesivo.	• El departamento de marketing adquiere su propio sistema de gestión de clientes basado en SaaS, lo que ocasiona costosos desarrollos adicionales de interfaces adecuadas con sistemas heredados.
		I	Se le da una atención inadecuada a futuros requisitos o solicitudes.	• Los criterios de selección de inversiones en TI no incluyen los requisitos futuros de usuario, lo que da lugar a soluciones incompletas o desalineadas con la estrategia de negocio.
		J	Los aspectos económicos de la iniciativa no se tienen en cuenta durante las decisiones de inversión.	• Los aspectos económicos de los proyectos no se utilizan de manera adecuada para la selección de inversiones, lo que implica que se descarten proyectos de alta rentabilidad o que no se abandonen proyectos con rentabilidad negativa.
2	**Gestión del ciclo de vida de los programas y proyectos**	A	La alta dirección no pone fin a los proyectos que fracasan (explosión de costes, retrasos excesivas, aumento descontrolado del alcance, cambios en las prioridades del negocio).	• Un proyecto ambicioso de larga duración para construir un nuevo sistema de recursos humanos (RR.HH.) todavía no ha proporcionado ningún resultado tangible en su intento por integrar la gestión de nómina, la gestión del tiempo y la gestión de desempeño. La empresa, a pesar de la falta de resultados, continúa (sub)financiando el proyecto durante el próximo período.
		B	Los proyectos de TI exceden los presupuestos planificados.	• Un importante proyecto para la implementación de un nuevo sistema de planificación de recursos empresariales (ERP) se acerca a un exceso de presupuesto del 100 por ciento.

Figura 6.2—Ejemplo de escenarios de riesgo genéricos y específicos *(cont.)*

Categoría del escenario de riesgo		Ejemplos de escenario de riesgo genérico		Ejemplos de escenario de riesgo específico
2	**Gestión del ciclo de vida de los programas y proyectos** *(cont.)*	C	Los proyectos de TI no cumplen con los requisitos de negocio.	• El nuevo sistema de CRM está funcionando inadmisiblemente despacio y es inestable debido a multitud de fallos, lo que provoca una tasa de disponibilidad de menos del 90 por ciento. • Durante las pruebas de aceptación, la implementación de las regulaciones de privacidad en el nuevo sistema de CRM falla en el 50 por ciento de los casos de prueba, creando una exposición por incumplimiento. • Las capacidades funcionales del nuevo sistema de CRM y la interfaz de usuario (UI) no se aceptan por los usuarios previstos, al no haberse conseguido la participación activa de todas las partes interesadas (incluyendo al patrocinador) en el ciclo de vida del programa/proyecto. • Debido un análisis de requisitos de negocio y/o a un diseño funcional incompletos, el nuevo sistema de RR.HH. está desalineado con las expectativas de los usuarios. • Debido a un proceso de pruebas inefectivo, el nuevo sistema ERP contiene muchos defectos del software e impacta en la productividad.
		D	Los proyectos de TI se entregan tarde.	• El nuevo sitio web de la empresa, incluyendo la tienda en línea, se entrega con seis meses de retraso, causando la pérdida de una oportunidad de mercado.
		E	Los usuarios no adoptan el nuevo software de aplicaciones.	• Un incorrecto análisis de requisitos da como resultado la imposibilidad de que los usuarios adopten la nueva aplicación de CRM y una pérdida de eficiencia.
		F	Se implementa un software inmaduro (usuarios pioneros, defectos del software, etc.).	• Una aplicación de negocio experimenta interrupciones del servicio debido a defectos del software.
		G	Los requisitos de seguridad se evalúan de manera inadecuada.	• La falta de consideración de los requisitos de seguridad lleva a una solución insegura para una nueva aplicación de acceso remoto, requiriendose una amplia reelaboración y retrasos.
		H	El alcance del programa/proyecto no está bien gestionado.	• Cambios frecuentes y tardíos en el alcance del programa impuestos por el propietario del sistema al desarrollador dan lugar a soluciones inconsistentes e inestables, ocasionando una amplia reelaboración y retrasos.
		I	Los KPI existentes son inadecuados para medir el logro del propósito del programa.	• La empresa no puede gestionar los proyectos correctamente porque no es consciente de su verdadero estado, lo que lleva a decisiones de proyectos tardías o incorrectas, retrasos, y sobrecostes generalizados.
3	**Coste y supervisión de TI**	A	Existe una gran dependencia y uso de soluciones ad hoc y/o creadas por los usuarios.	• La gran dependencia del empleo de informática de usuario final para satisfacer las necesidades de información importante da lugar a deficiencias en la seguridad. • La gran dependencia del empleo de informática de usuario final satisfacer para las necesidades de información importante ocasiona datos imprecisos y poco fiables. • La gran dependencia de soluciones ad hoc para satisfacer las necesidades de información importante conduce a un uso ineficiente de recursos y un coste añadido.

Figura 6.2—Ejemplo de escenarios de riesgo genéricos y específicos *(cont.)*

Categoría del escenario de riesgo		Ejemplos de escenario de riesgo genérico		Ejemplos de escenario de riesgo específico
3	**Coste y supervisión de TI** *(cont.)*	B	La gestión de cambios sobre las soluciones ad hoc es inadecuada.	• La gestión de cambios y el control de calidad inadecuados de las soluciones de usuario ad hoc dan lugar a resultados informáticos y a decisiones de negocio incorrectos (p. ej. los resultados del caso de negocio son tremendamente inexactos).
		C	Las compras relacionadas con la I&T al margen del proceso de adquisición de TI son costosas e inefectivas.	• Distintos departamentos están adquiriendo sus propias soluciones de automatización de oficina. • Distintos departamentos están suscribiendo acuerdos con diversas empresas de externalización (outsourcing) o proveedoras de servicios.
		D	Unos requisitos inadecuados dan lugar a acuerdos de nivel de servicio (ANS) inefectivos.	• Hay partes interesadas relevantes que no participaron en la fase de requisitos, lo que da como resultado requisitos y ANS incompletos.
		E	Hay falta de fondos para las inversiones relacionadas con la I&T.	• La escasez de fondos para las actualizaciones de seguridad necesarias conduce al fallo de los sistemas de TI por ciberataques. • La falta de fondos para nuevas innovaciones de I&T da como resultado una respuesta al mercado más lenta y una pérdida de ventaja competitiva.
4	**Destreza, habilidades y comportamiento de TI**	A	Hay carencia, o desajuste, de habilidades relacionadas con las TI en el área de TI (p. ej. debido a nuevas tecnologías o métodos de trabajo).	• El personal actual de TI no cuenta con las habilidades necesarias para las nuevas tecnologías (p. ej. cadena de bloques), lo que provoca curvas de aprendizaje más largas y retrasos en los proyectos. • El personal actual de desarrollo y operaciones de TI no está capacitado en las herramientas y las formas de trabajo de DevOps, provocando menos beneficios de los previstos del planteamiento DevOps.
		B	Una falta de comprensión del negocio por parte del personal de TI afecta a la entrega de servicios/calidad de los proyectos.	• Una falta de comprensión del negocio en el personal de TI afecta la calidad del nuevo sistema ERP debido a una implementación deficiente de los requisitos de usuario y a la implementación de características innecesarias.
		C	La empresa no puede contratar y retener personal de TI.	• El departamento de RR.HH. fracasa reiteradamente en la contratación de expertos en seguridad de la información suficientemente cualificados, provocando una mayor exposición y mayores costes de expertos externos. • No hay un retorno en la inversión suficiente en relación con la formación debido a la pronta salida del personal capacitado de TI (p. ej., individuos con titulaciones avanzadas de negocio).
		D	Se contratan personas con perfiles inadecuados debido a una falta de diligencia debida en el proceso de reclutamiento.	• El departamento de RR.HH. contrata empleados con falsas credenciales, lo que provoca daño a la marca a largo plazo. • La imposibilidad de realizar la diligencia debida necesaria en una nueva contratación provocó el hackeo interno de datos confidenciales.

Figura 6.2—Ejemplo de escenarios de riesgo genéricos y específicos *(cont.)*

Categoría del escenario de riesgo		Ejemplos de escenario de riesgo genérico		Ejemplos de escenario de riesgo específico
4	**Destreza, habilidades y comportamiento de TI** *(cont.)*	E	Falta formación en I&T.	• La falta de formación en I&T conduce a la salida del personal de TI. • La falta de formación relacionada con I&T provoca el aumento de los problemas de calidad en los servicios prestados. • La empresa no puede actualizar las habilidades de I&T al nivel adecuado mediante la formación.
		F	Existe una dependencia excesiva del personal clave para los servicios de I&T.	• Se pierde conocimiento interno crítico cuando el personal clave deja la organización.
		G	No existe una revisión formal del desempeño del personal.	• La falta de revisión formal del desempeño del personal de desarrollo de TI lleva a una calidad mediocre del software y a retrasos en el tiempo de entrega de las nuevas aplicaciones.
		H	Las tareas no se segregan efectivamente.	• La segregación inefectiva de las tareas para la compra de aplicaciones posibilita las transacciones fraudulentas.
		I	Existen desafíos de comunicación entre TI y los usuarios.	• Las difíciles relaciones entre TI y los usuarios conducen a soluciones deficientes y a solicitudes de usuarios que no se entienden bien.
5	**Arquitectura de empresa/TI**	A	La arquitectura empresarial es compleja e inflexible, lo que obstaculiza una mayor evolución y expansión, lo que lleva a perder oportunidades de negocio.	• Una nueva aplicación para gestión de relaciones con el cliente no puede implementarse, o se debe reducir su funcionalidad, porque la comunicación con otros sistemas internos es demasiado lenta debido a interfaces muy lentas.
		B	La empresa no adopta y explota nuevas infraestructuras, o no abandona las infraestructuras obsoletas oportunamente.	• El cableado de la infraestructura abandonada reduce la eficiencia de los sistemas de calefacción, ventilación y aire acondicionado (HVAC).
		C	La empresa no adopta la arquitectura empresarial/de TI existente cuando diseña e implementa las nuevas soluciones tecnológicas.	• El departamento de marketing decide utilizar una solución de SaaS sin consultar a los arquitectos de la empresa, dando lugar a una solución que es incompatible con los sistemas internos actuales, requiriendose la costosa elaboración de un software de interfaz adicional.
		D	La empresa no adopta y explota el nuevo software (funcionalidad, optimización, etc.) o no abandona las aplicaciones obsoletas oportunamente.	• La caída de una aplicación de contabilidad antigua y sin soporte provoca grandes pérdidas del beneficio. • El hecho de no abandonar las aplicaciones obsoletas consume tiempo y recursos innecesarios (es decir, dinero y personas).
		E	La arquitectura empresarial indocumentada da lugar a ineficiencias y duplicidades.	• El departamento de marketing decide utilizar una solución de SaaS sin consultar a los arquitectos de la empresa, dando lugar a una solución que es incompatible con los sistemas internos actuales, requiriendo la costosa elaboración de un software de interfaz adicional.

Figura 6.2—Ejemplo de escenarios de riesgo genéricos y específicos *(cont.)*

Categoría del escenario de riesgo		Ejemplos de escenario de riesgo genérico		Ejemplos de escenario de riesgo específico
5	**Arquitectura de empresa/TI** *(cont.)*	F	Hay una cantidad excesiva de excepciones a los estándares de arquitectura empresarial.	• Durante el año anterior, casi el 75 por ciento de los nuevos proyectos han solicitado (y se les han concedido) excepciones a los estándares de arquitectura empresarial. Esto hace que los estándares sean irrelevantes en la práctica, y se crearán soluciones inconsistentes y costes excesivos en el futuro.
6	**Operaciones de TI**	A	El personal de TI comete errores (durante la realización de las copias de seguridad, las actualizaciones de sistemas, el mantenimiento de sistemas, etc.).	• El personal de operaciones de TI (interno o del prestador del servicio) introduce un comando incorrecto durante la actualización de un sistema, dejando el sistema vulnerable desde el punto de vista de la seguridad.
		B	El personal de TI o los usuarios del sistema introducen información incorrecta.	• El administrador del sistema de un servidor crítico introduce información de redes incorrecta en el sistema, degradando la velocidad de la comunicación del sistema hasta niveles inaceptables.
		C	La gestión deficiente de las copias de seguridad/restauración incluye el etiquetado incorrecto o la colocación en lugar equivocado de los medios de respaldo.	• La gestión deficiente de las copias de seguridad/restauración está causando la pérdida de datos cuando los respaldos no pueden restaurarse después de un incidente de hardware. • La deficiente gestión de las copias de seguridad/restauración está causando la pérdida de datos cuando los respaldos no pueden restaurarse después de un incidente de software malicioso de petición de rescate (ransomware). • No se monitoriza correctamente el estado de la copia de seguridad y/o no se resuelven los problemas de las copias de seguridad de manera oportuna, lo que causará una pérdida de datos potencial cuando una restauración sea necesaria.
		D	La gestión de parches/ vulnerabilidades es inadecuada.	• La gestión inadecuada de parches y vulnerabilidades deja a los sistemas vulnerables a ataques o accidentes, reduciendo los niveles de servicio.
		E	La monitorización del desempeño y de las operaciones es inadecuada.	• La monitorización inadecuada de aplicaciones o sistemas puede causar que una degradación del sistema pase inadvertida durante demasiado tiempo, dando lugar a interrupciones en el servicio.
		F	La resiliencia de las instalaciones es inadecuada.	• Las interrupciones del suministro eléctrico o los sobrevoltajes, sin contar con un adecuado sistema de alimentación ininterrumpida (SAI), dañan el equipamiento informático y pueden provocar interrupciones en el servicio o pérdida de datos.
7	**Gestión de los derechos de acceso del usuario**	A	El software está alterado.	• Un gestor de operaciones de TI en un entorno de DevOps realiza diversos cambios en el software, que él considera que harán que una nueva aplicación funcione mejor, provocando inadvertidamente un error o una merma de desempeño en el sistema.
		B	Se modifica o manipula intencionalmente el software, conduciendo a datos erróneos.	• La modificación malintencionada del código fuente de la base de datos por parte de un desarrollador da lugar a datos erróneos.

Figura 6.2—Ejemplo de escenarios de riesgo genéricos y específicos *(cont.)*

Categoría del escenario de riesgo		Ejemplos de escenario de riesgo genérico		Ejemplos de escenario de riesgo específico
7	**Gestión de los derechos de acceso del usuario** *(cont.)*	C	Se modifica o manipula intencionadamente la configuración de seguridad.	• La manipulación de la configuración de seguridad del equipo de red crea importantes vulnerabilidades, permitiendo el éxito de los ataques.
		D	Se modifica o manipula intencionadamente el software, conduciendo a acciones fraudulentas.	• Un ingeniero de software realiza cambios no autorizados en un sistema de pagos para poder realizar pagos sin autorización y fraudulentos.
		E	Se modifica de manera no intencionada el software, provocando resultados inexactos.	• La modificación errónea no intencionada del código fuente de la base de datos por parte de un desarrollador inconsciente provoca pérdidas de producción y de datos.
		F	Se cometen errores no intencionados en la configuración y en la gestión de cambios.	• Los errores de configuración o de gestión de cambios podrían causar interrupciones del sistema, provocando una interrupción del servicio en las aplicaciones orientadas al cliente.
		G	Se emiten comunicaciones no intencionadas.	• Se envía un correo electrónico con información personal sensible a destinatarios erróneos, causando violaciones o reclamaciones por privacidad.
		H	Se abusa de los derechos de acceso de roles anteriores para acceder a la infraestructura de TI.	• La falta de control interno de los roles asignados conduce a derechos incorrectos de acceso de los usuarios. Los empleados pueden acceder a los datos financieros y los roban.
		I	Hay usuarios autorizados que intencionada o accidentalmente llevan a cabo acciones no autorizadas.	• Un usuario privilegiado accede a información personal privada de clientes sin ninguna razón de negocio válida, exponiendo a la empresa a una violación de la privacidad.
		J	Se comparten derechos de acceso o contraseñas con otras personas.	• Hay usuarios autorizados (privilegiados o no) que comparten sus credenciales con otros usuarios, permitiéndoles realizar acciones a las que no están autorizados y dificultando el no repudio.
		K	La gestión de cuentas privilegiadas/de emergencia es inadecuada.	• La gestión deficiente de cuentas privilegiadas da lugar a una cantidad excesiva de usuarios con privilegios, aumentando la probabilidad de acciones no autorizadas y reduciendo el no repudio.
		L	La provisión de acceso a usuarios no es efectiva.	• Los procesos de exenciones a las políticas durante un desastre no son efectivas. (En el transcurso de un desastre, algunos controles existentes podrían no ser viables. Por lo tanto, debería haber un proceso de exención para evaluar el riesgo y dar seguimiento a la exención.)
		M	La matriz de acceso no está definida o implementada.	• Una matriz de accesos mal diseñada, o implementada, podría dar lugar a usuarios con (típicamente) excesivos privilegios, dando como resultado controles de negocio sobre transacciones (p. ej. financieras) mal implementados.
		N	Surge un conflicto de interés durante la gestión de acceso de usuarios.	• La presión de la dirección de TI sobre el equipo de seguridad bajo su autoridad conduce a que se otorguen derechos de acceso excesivos a algunos usuarios.

Figura 6.2—Ejemplo de escenarios de riesgo genéricos y específicos *(cont.)*

Categoría del escenario de riesgo		Ejemplos de escenario de riesgo genérico		Ejemplos de escenario de riesgo específico
8	**Uso y adopción de software**	A	Los usuarios no adoptan el nuevo software de aplicación.	• Los usuarios rechazan, o se muestran reticentes a usar, la nueva aplicación de software debido a la falta de formación/comunicación, con lo que renuncian a las correspondientes mejoras de eficiencia.
		B	Los usuarios utilizan el nuevo software de manera ineficiente.	• A los usuarios se les provee de un nuevo sistema para gestionar las quejas de los clientes que automatiza el flujo de trabajo, pero continúan enviando en paralelo correos electrónicos directos al equipo de soporte.
		C	Surge el uso no previsto de nuevas aplicaciones de software.	• Los usuarios del negocio no están usando la nueva aplicación de software como se pretende, provocando pérdidas de productividad.
		D	Los usuarios de la empresa no pueden usar el software para lograr los resultados deseados (p. ej. no se realiza el cambio de modelo de negocio u organizacional precisado).	• Una nueva aplicación de negocio sufre una interrupción debido a la falta de familiaridad con un sistema de servidores recién instalado.
		E	Surgen fallos operativos cuando se pone en funcionamiento un nuevo software.	• No se puede acceder de forma intermitente al sitio web público de la organización después de la instalación de una actualización del software.
		F	Un software crítico de aplicación funciona mal con frecuencia.	• Una aplicación crítica orientada al cliente se vuelve muy inestable después del último cambio de software, reduciendose considerablemente la disponibilidad de la aplicación y ocasionando numerosas quejas de clientes.
		G	El software de aplicación está obsoleto (tecnología antigua, mal documentado, costoso de mantener, difícil de ampliar, no integrado a la arquitectura actual, etc.).	• Una aplicación clave de negocio es inestable debido al uso de tecnologías antiguas y sin soporte, provocando interrupciones periódicas.
		H	La empresa no puede volver a versiones anteriores del software cuando surgen problemas operativos con la nueva versión.	• Una aplicación clave de negocio está deshabilitada debido a un fallo en la nueva versión del software, y la empresa no puede volver a la versión anterior.
		I	La corrupción de una base de datos inducida por el software ocasiona la pérdida de acceso a los datos.	• Un defecto (bug) en la última versión del software da lugar a la corrupción de datos en una aplicación clave del negocio, lo que hace que la aplicación no esté disponible.
		J	Surgen problemas de integridad de la información provocados por el software.	• Un cambio en el software introduce una nueva lógica de negocio y procesamiento, pero los errores causan problemas de integridad de la información, conduciendo a decisiones de negocio equivocadas (p. ej. aprobaciones de créditos, procesamiento de pedidos de clientes).
9	**Hardware de TI**	A	Se instala una nueva infraestructura y, como resultado, los sistemas se vuelven inestables, provocando incidentes operativos (p. ej. un programa de “traiga su propio dispositivo” [BYOD]).	• Hay una interrupción de una aplicación clave del negocio por la inestabilidad de un nuevo hardware de red Cisco.

Figura 6.2—Ejemplo de escenarios de riesgo genéricos y específicos *(cont.)*

Categoría del escenario de riesgo		Ejemplos de escenario de riesgo genérico		Ejemplos de escenario de riesgo específico
9	**Hardware de TI** *(cont.)*	B	Los sistemas no pueden manejar el volumen de transacciones cuando aumenta el número de usuarios.	• Una base de datos no puede manejar el volumen de transacciones, provocando interrupciones periódicas. • Una aplicación no puede manejar el volumen de transacciones, dando lugar a tiempos de respuesta lentos.
		C	Los sistemas no pueden manejar la carga de proceso cuando se despliegan nuevas aplicaciones o iniciativas.	• Las limitaciones de capacidad de transmisión de las redes introducen retardos en las transacciones cuando se implementa el nuevo cortafuegos (firewall).
		D	Fallan los servicios públicos (p. ej. telecomunicaciones, electricidad).	• Las transacciones en línea de los consumidores se interrumpen cuando una tormenta provoca un corte en el suministro de electricidad.
		E	El hardware falla debido a sobrecalentamiento y/u otras condiciones ambientales, como la humedad.	• Las transacciones al por menor en línea se interrumpen cuando el hardware del sistema falla debido a un fallo de climatización (HVAC).
		F	El hardware falla por falta de mantenimiento preventivo.	• Un sistema de climatización (HVAC) falla por causa de un mantenimiento tardío, provocando un corte en la sala de ordenadores.
		G	Se dañan componentes del hardware, ocasionando la destrucción (parcial) de datos por personal interno.	• Un miembro del personal descontento destruye físicamente un disco duro, causando la pérdida de datos.
		H	Se pierden o divulgan medios que contienen datos sensibles (CD, memorias USB, discos portátiles, etc.).	• La información de los clientes se ve comprometida debido a que los empleados utilizan memorias USB sin autorización ni cifrado.
		I	La empresa experimenta un aumento del tiempo de resolución o retrasos en el soporte en casos de incidentes de hardware.	• Los clientes sufren retrasos prolongados en la entrega de servicios debido a caídas de un elemento hardware que ya no está soportado por el proveedor.
		J	Los componentes del hardware se configuran de forma errónea.	• Tras una actualización del sistema de almacenamiento, se configuran incorrectamente varios discos, haciendo que las aplicaciones que utilizan los datos funcionen con errores.
		K	La gestión de la puesta en marcha y la eliminación del hardware es inadecuada.	• Un procedimiento deficiente de eliminación del hardware provoca que los datos no sean destruidos antes de que el equipo sea desmantelado y eliminado de las instalaciones.
		L	La gestión del cumplimiento de la configuración del hardware es inadecuada.	• Un operador que no cumple con el procedimiento de configuración del hardware deja un nuevo equipo mal configurado, lo que provoca su explotación y genera una interrupción del servicio.
		M	Finaliza el soporte del proveedor.	• El proveedor de un sistema heredado utilizado por la empresa ha finalizado el soporte del sistema, dando lugar a una interrupción total del servicio en caso de defecto del hardware.

Figura 6.2—Ejemplo de escenarios de riesgo genéricos y específicos *(cont.)*

Categoría del escenario de riesgo		Ejemplos de escenario de riesgo genérico		Ejemplos de escenario de riesgo específico
10	**Amenazas de seguridad internas y externas (hacker, software malicioso [malware], etc.)**	A	Hay usuarios (internos) no autorizados que penetran con éxito los sistemas.	• Un usuario interno irrumpe en una aplicación clave de negocio y elimina la información de cuentas de clientes.
		B	Un ataque de denegación de servicio (DoS) provoca una interrupción del servicio.	• Un ataque de denegación de servicio distribuido (DDoS) da lugar a una degradación del desempeño de un sitio web clave del negocio.
		C	Se desfigura un sitio web.	• Un defecto en la seguridad del principal sitio web de comercialización conduce a una desfiguración del sitio web que avergüenza a la empresa.
		D	La empresa experimenta un ataque de software malicioso [malware].	• Un software malicioso [malware] infecta servidores de operaciones críticas. • Los ordenadores portátiles se infectan habitualmente con software malicioso [malware]. • La empresa se ve obligada a pagar un rescate debido a una serie de ataques de DoS.
		E	Se produce espionaje industrial.	• Una empresa o estado extranjero accede a los sistemas de la empresa y obtiene información importante y confidencial de productos y clientes, deteriorando la posición competitiva de la empresa.
		F	Se produce hacktivismo.	• Un grupo contrario a las políticas ambientales de la empresa perpetra un ataque de DDoS, dejando su sitio web fuera de servicio durante más de 24 horas.
		G	Un empleado descontento implementa una bomba de tiempo, que da lugar a la pérdida de datos.	• Un empleado descontento que implementa una bomba de tiempo de eliminación de datos elimina, y hace irrecuperable, registros de la base de datos central de información de clientes.
		H	Se roban datos de la empresa a través de un acceso no autorizado obtenido por un ataque de phishing.	• Hay empleados que usan memorias USB no autorizadas, distribuidas en el estacionamiento, lo que ocasiona pérdida de datos. • Un empleado desprevenido abre un correo electrónico de phishing, ocasionando un acceso no autorizado a los datos financieros.
		I	Un gobierno extranjero realiza ataques contra sistemas críticos.	• Un gobierno extranjero ataca sistemas críticos. • Grupos del crimen organizado se infiltran en los sistemas para realizar transacciones fraudulentas.
		J	El personal destruye el centro de datos (sabotaje, etc.).	• El personal de operaciones del centro de datos coloca una bomba en las instalaciones de acondicionamiento (HVAC).
		K	Se roba un dispositivo con datos sensibles.	• Un administrador autorizado sustrae un dispositivo con datos financieros sensibles.
		L	Los equipos de TI se dañan accidentalmente.	• El personal de limpieza daña accidentalmente el equipo del armario de red. • El personal de operaciones de TI daña accidentalmente unos bastidores de discos.
		M	Se roba un componente clave de infraestructura.	• Un miembro del personal del equipo de limpieza del centro de datos hurta el ordenador portátil de gestión del sistema de control de acceso al centro de datos, imposibilitando la entrada segura al centro de datos.
		N	El hardware (dispositivos de seguridad, etc.) se altera intencionadamente.	• Un técnico altera el sistema de reconocimiento de huella dactilar en lugares sensibles para que el sistema permita entrar a cualquiera.

Figura 6.2—Ejemplo de escenarios de riesgo genéricos y específicos *(cont.)*

Categoría del escenario de riesgo		Ejemplos de escenario de riesgo genérico		Ejemplos de escenario de riesgo específico
11	**Incidentes de terceros/ proveedores**	A	El desempeño de un subcontratista en un acuerdo de externalización (outsourcing) a largo plazo y a gran escala es inadecuado (p. ej., por causa de la falta de diligencia debida del proveedor con respecto a la viabilidad financiera, de la capacidad de entrega, y de la sostenibilidad del servicio del proveedor).	• La entrega de componentes de productos clave se interrumpe debido al colapso financiero de un proveedor externo.
		B	La empresa acepta condiciones de negocio irrazonables de proveedores de TI (p. ej. por falta de asesoramiento jurídico).	• Se producen sobrecostes debido a una mala negociación de los términos en acuerdos con proveedores de servicio TI.
		C	Los proveedores entregan servicios y soporte inadecuados, desalineados con el ANS.	• Se producen retrasos en las reparaciones del software del sitio web de comercio electrónico debido a que los proveedores de software no cumplen con los requisitos del ANS para la puntualidad y/o la calidad.
		D	Se produce un incumplimiento de los acuerdos de licenciamiento de software (uso y/o distribución de software sin licencia, etc.).	• Un proveedor de software que identifica que la empresa ha violado el acuerdo de licenciamiento de software por la distribución no permitida del software presenta una acción legal.
		E	La empresa no puede migrar a proveedores alternativos debido al exceso de confianza o a la dependencia del proveedor actual.	• Los servicios de entrega de productos se degradan debido al exceso de confianza en un único proveedor de servicio que no puede escalar para satisfacer el aumento de la demanda.
		F	Hay servicios de TI (en especial, servicios en la nube) que el negocio adquiere sin la consulta/participación del área de TI, lo que da lugar a la imposibilidad de integrar dichos servicios con los servicios internos.	• Se selecciona un proveedor de servicios en la nube que no es compatible con las aplicaciones internas.
		G	Se incurre en penalizaciones debido al incumplimiento de los ANS.	• Se presentan acciones legales contra la empresa por no haber podido cumplir con los requisitos contractuales para la entrega de servicios.
		H	El ANS no es apropiado para obtener los servicios requeridos.	• Un ANS inapropiado no describe los niveles de servicios requeridos, que, consecuentemente el proveedor externo no entrega, afectando la productividad del personal.
		I	Finaliza el servicio.	• Un proveedor de servicio desaparece tras su bancarrota, lo que lleva a una interrupción del servicio.
		J	Los proveedores de la nube interrumpen el servicio operativo.	• El proveedor de la nube que alberga la base de datos de clientes de la empresa tiene una avería operativa de sus sistemas, lo que provoca que la base de datos de clientes no esté disponible durante un día.
		K	Se produce un incumplimiento de los requisitos de seguridad.	• Un proveedor de servicios de la nube no cumple con los requisitos de seguridad contractuales, lo que lleva a una violación a la confidencialidad con consecuencias legales para la empresa.

Figura 6.2—Ejemplo de escenarios de riesgo genéricos y específicos *(cont.)*

Categoría del escenario de riesgo		Ejemplos de escenario de riesgo genérico		Ejemplos de escenario de riesgo específico
11	**Incidentes de terceros/ proveedores** *(cont.)*	L	Los proveedores de externalización no entregan los proyectos conforme a los acuerdos contractuales (cualquier combinación de presupuestos excedidos, problemas de calidad, falta de funcionalidad, entrega fuera de plazo).	• El contratista del nuevo sistema de ERP no puede hacer su entrega en el plazo acordado y probablemente lo entregará un año después.
		M	La monitorización de los ANS con proveedores externos es inadecuada.	• Debido a la falta de monitorización del desempeño de un proveedor de la nube, la degradación de los servicios y el incumplimiento de los niveles de servicio contractuales pasan inadvertidos, afectando a la productividad del personal.
		N	El proveedor de la nube pierde datos.	• El proveedor de la nube que alberga la base de datos de clientes de la empresa tiene una avería importante en sus sistemas, lo que causa una pérdida de las actualizaciones de clientes del mes anterior.
12	**Incumplimiento**	A	Se produce un incumplimiento de las regulaciones locales o internacionales (p. ej. privacidad, contabilidad, fabricación, medioambiente).	• La empresa incurre en multas elevadas y daños importantes a su marca debido a errores innecesarios contra las normas del RGPD. • Un análisis inapropiado de las regulaciones lleva al incumplimiento no intencionado y, como resultado, se incurre en multas.
		B	La empresa desconoce los posibles cambios regulatorios que podrían tener un impacto en el negocio.	• La empresa lleva a cabo un seguimiento incompleto de los cambios en las regulaciones ambientales.
		C	La empresa se enfrenta a contratiempos operativos por causa de las regulaciones.	• El regulador impide el flujo transfronterizo de datos debido a la insuficiencia de los controles.
		D	La empresa experimenta incumplimientos de los procedimientos internos.	• El personal presenta acciones legales contra la organización alegando el incumplimiento de las políticas de seguridad internas. • Hay usuarios que incumplen las políticas internas sobre la descarga de software externo, lo que conduce a la infección de los sistemas y a posteriores interrupciones del servicio.
		E	Las regulaciones transfronterizas causan obstáculos para la empresa.	• La existencia de diferentes regulaciones en los países prohíbe o inhibe la transferencia de información, generando costes adicionales y pérdidas de eficiencia.
13	**Problemas geopolíticos**	A	La empresa sufre interrupciones del servicio debido a incidentes disruptivos (p. ej. ataque físico) en locales en el extranjero.	• El centro de datos en un país extranjero es bombardeado, provocando importantes problemas en la cadena de suministros.
		B	La interferencia gubernamental y las políticas nacionales impactan en la empresa.	• La interferencia gubernamental y las políticas nacionales limitan la entrega de productos o servicios internacionales.

Figura 6.2—Ejemplo de escenarios de riesgo genéricos y específicos *(cont.)*

Categoría del escenario de riesgo		Ejemplos de escenario de riesgo genérico		Ejemplos de escenario de riesgo específico
13	**Problemas geopolíticos** *(cont.)*	C	La empresa sufre acciones específicas de grupos o agencias con patrocinio gubernamental.	• Una acción específica contra la empresa da lugar a la destrucción de infraestructuras críticas. • Acciones específicas de entidades extranjeras obtienen información confidencial de los productos, perjudicando la posición competitiva de la empresa.
14	**Acción sindical**	A	No se puede acceder a las instalaciones y los edificios debido a una huelga sindical.	• Se produce una reducción en la productividad porque los trabajadores de la planta de producción no pueden ir a trabajar por una huelga sindical.
		B	Un proveedor externo no puede prestar sus servicios debido a una huelga.	• Los técnicos externos no pueden prestar los servicios técnicos porque las instalaciones están bloqueadas por huelguistas, ocasionando la degradación del servicio.
		C	Hay personal clave que no se encuentra disponible como consecuencia de una acción sindical externa (p. ej. una huelga de transportes o servicios públicos).	• Se produce una reducción en la productividad porque el personal clave no puede ir a trabajar por una huelga de transportes.
15	**Desastres naturales**	A	Un terremoto destruye o daña infraestructuras importantes de TI.	• Un terremoto daña el centro de operaciones de TI, provocando una interrupción de los servicios de comercio en línea.
		B	Un tsunami destruye instalaciones críticas.	• Un tsunami destruye un importante centro de distribución, dando lugar a la incapacidad para cumplir con los plazos de entrega de los productos.
		C	Grandes tormentas y ciclones tropicales dañan infraestructuras críticas.	• Una gran tormenta daña la infraestructura eléctrica, provocando la indisponibilidad de las redes eléctricas que abastecen al centro de datos durante más de dos semanas.
		D	Grandes incendios forestales y/o inundaciones dañan instalaciones críticas.	• Un incendio forestal obliga al personal de un centro de datos a abandonar las instalaciones, ocasionando una interrupción prolongada del servicio. • Una inundación en las instalaciones causa daños irreparables en los equipos informáticos.
		E	Las condiciones ambientales cambiantes afectan a la empresa.	• La elevación del nivel freático inutiliza un emplazamiento crítico, haciendo necesaria su reubicación. • El incremento de las temperaturas hace que la operación de un emplazamiento crítico no sea rentable.
		F	Una pandemia afecta a las personas y a la economía.	• El personal no puede acceder a las oficinas debido a un desastre natural (p. ej. inundación o COVID-19), provocando una degradación de la eficiencia. • La pérdida permanente o prolongada de empleados clave durante una pandemia ocasiona la interrupción del servicio, vacíos de conocimiento, y una degradación de la eficiencia. • La empresa no puede adquirir recursos clave (p.ej. ancho de banda) durante la pandemia.

Figura 6.2—Ejemplo de escenarios de riesgo genéricos y específicos *(cont.)*

Categoría del escenario de riesgo		Ejemplos de escenario de riesgo genérico		Ejemplos de escenario de riesgo específico
16	**Tecnologías emergentes e innovación**	A	No se identifican nuevas e importantes tendencias tecnológicas.	• El desaprovechamiento de los avances tecnológicos provoca una pérdida de cuota de mercado.
		B	La empresa no percibe el valor y el potencial de las nuevas tecnologías (nuevas capacidades funcionales, optimización de procesos).	• La empresa incurre en costes de oportunidad importantes al no adoptar de manera oportuna una nueva plataforma de software para interactuar con clientes.
		C	La empresa sufre la adopción temprana problemática de una nueva tecnología.	• La adopción temprana de nuevas tecnologías ocasiona inconsistencias en la estabilidad y la fiabilidad, provocando interrupciones no previstas de las operaciones, solicitudes masivas de soporte y actualizaciones frecuentes, todo lo que da lugar a la degradación de la eficiencia.
		D	La empresa no puede entender o abordar el riesgo vinculado a la adopción de nuevas tecnologías (p. ej. falta de una guía de refuerzo).	• La adopción de nuevas tecnologías sin suficiente refuerzo podría exponer a la empresa a riesgos de seguridad, y ocasionar interrupciones del servicio.
		E	La tecnología emergente desaparece del mercado.	• Una nueva tecnología que ha sido adoptada anticipadamente desaparece del mercado, provocando interrupciones del servicio o costes adicionales para las tecnologías de reemplazo.
17	**Medio ambiente**	A	El equipo utilizado por la empresa no es ecológico (p. ej. consumo de energía, embalaje).	• El uso de pulverizadores de herbicidas que no son conformes con las prácticas de seguridad establecidas ocasiona daños a las especies de vida silvestre en riesgo de extinción.
		B	La empresa utiliza equipos que no cumplen con las regulaciones ambientales o las normas de consumo de energía.	• El equipo informático no cumple con las regulaciones ambientales, lo que da lugar a sanciones.
		C	El equipo utilizado por la empresa no cumple con los últimos estándares de consumo de energía.	• El consumo de energía del equipo informático de la empresa es excesivo y genera un mayor coste.
18	**Gestión de datos e información**	A	Personas no autorizadas descubren información sensible debido a la ineficiencia de la retención, el archivado o la eliminación de la información.	• La divulgación accidental de información sensible de clientes debido a la imposibilidad de cumplir con las directrices de manejo de la información (p. ej. eliminación de documentos) da lugar a procesos judiciales.
		B	Se realizan modificaciones intencionadas ilícitas o maliciosas en los datos.	• La modificación intencionada ilícita o maliciosa de datos contables da lugar a un dictamen de auditoría desfavorable. • La modificación intencionada ilícita o maliciosa de la historia clínica de un paciente da lugar a procesos judiciales.
		C	Se produce la divulgación no autorizada de información sensible a través de correos electrónicos o redes sociales.	• Un ingeniero de diseño comparte información nueva y confidencial sobre un producto en sus cuentas de redes sociales con muchos seguidores. • Un miembro del personal de RR.HH. comparte noticias confidenciales sobre despidos en sus cuentas de redes sociales, ocasionando una enorme atención de la prensa y un gran trastorno en la organización.

Figura 6.2—Ejemplo de escenarios de riesgo genéricos y específicos *(cont.)*

Categoría del escenario de riesgo		Ejemplos de escenario de riesgo genérico		Ejemplos de escenario de riesgo específico
18	**Gestión de datos e información** *(cont.)*	D	La empresa pierde propiedad Intelectual (PI) y/o sufre la exfiltración de información competitiva.	• La empresa pierde propiedad intelectual y/o su información competitiva se filtra debido a que miembros clave del equipo dejaron la organización y se llevaron información con ellos. • Un hackeo trae como resultado una pérdida de propiedad intelectual y/o la exfiltración de información competitiva.
		E	La información de la empresa es de mala calidad.	• La dirección de una organización de servicio no puede optimizar la planificación de su personal debido a la mala calidad de la utilización del personal y de la comunicación consistente.
		F	La gestión de datos maestros es inapropiada.	• Debido a la mala gestión de los datos maestros o a la deficiente arquitectura de los datos, hay múltiples instancias de los mismos datos en los sistemas de la empresa, dando lugar a una importante degradación del servicio al cliente y de la eficiencia.
		G	La clasificación de la información es inapropiada.	• Una clasificación de la información deficiente da lugar a la protección inadecuada de la información, y a la divulgación de información confidencial de marketing, menoscabando la ventaja competitiva de la empresa.

Capítulo 7
Conceptos esenciales de la respuesta al riesgo

7.1 Componentes de respuesta al riesgo

Este capítulo trata los componentes esenciales de la respuesta al riesgo. Los temas tratados aquí incluyen:

1. evitación del riesgo;
2. mitigación del riesgo;
3. compartición o transferencia del riesgo;
4. aceptación del riesgo;
5. agregación preliminar de riesgos para las acciones de respuesta;
6. selección preliminar de la respuesta al riesgo y priorización.

El propósito de establecer una respuesta al riesgo es que, tras el análisis de riesgos, el riesgo quede alineado con el apetito de riesgo definido para la empresa. En otras palabras, debe establecerse una respuesta de manera tal que el riesgo residual futuro (riesgo actual con la respuesta al riesgo definida e implementada) esté comprendido dentro de los límites de tolerancia al riesgo en la medida de lo posible (normalmente dependiendo del presupuesto disponible). También podría haber un proceso de excepción que otorgase un período de tiempo dado para implementar una respuesta al riesgo, o durante el que la dirección podría decidir aceptar cualquier riesgo, independientemente de las circunstancias.

7.1.1 Evitación del riesgo

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

- ninguna otra respuesta rentable puede lograr reducir el impacto del riesgo materializado por debajo de los umbrales definidos para las pérdidas;
- el riesgo no se puede compartir ni transferir;
- la dirección considera que el riesgo es inaceptable.

Algunos ejemplos de evitación de riesgo relacionado con la I&T podrían ser la reubicación de un centro de datos lejos de una región con peligros naturales significativos, o rehusar a participar en un proyecto muy grande cuando el caso de negocio muestra un riesgo notable de fracaso.

7.1.2 Mitigación del riesgo

Mitigación del riesgo significa que una vez que el riesgo ha sido identificado y analizado, se adoptan medidas para reducir su frecuencia y/o su impacto. Las formas más comunes de mitigar el riesgo incluyen:

- Fortalecer las prácticas generales de la gestión de riesgos. Esto puede lograrse asignando la responsabilidad de la identificación del riesgo y la gestión de riesgos a aquellos que guarden mayor proximidad con las actividades que generan riesgos significativos. Este tipo de actividad también ayuda a aumentar la concienciación del riesgo en toda la empresa.
- Integrar las actividades de concienciación del riesgo en el flujo de trabajo habitual del negocio para que pasen a ser parte del curso regular de las actividades diarias. Esto permite que el personal comprenda mejor y reconozca los comportamientos de riesgo antes de que un incidente se materialice.

- Mejorar los procesos de la gestión de riesgos y desarrollar las tolerancias relevantes que se propaguen por doquier desde la estrategia hasta el área de producción o la primera línea de la empresa.
- Automatizar, cuando sea posible, los disparadores o alertas que identificarán o indicarán cuándo se encuentran los umbrales fuera de la tolerancia.
- Introducir o fortalecer controles destinados a reducir la frecuencia o el impacto de un riesgo materializado. Algunas técnicas para conseguirlo se tratan en las siguientes secciones.

7.1.3 Compartición o transferencia del riesgo

Compartir significa reducir la frecuencia o el impacto del riesgo al transferir o compartir una parte del mismo. Las técnicas más comunes incluyen el seguro y la externalización (outsourcing). Los ejemplos incluyen la contratación de cobertura de seguros para incidentes relacionados con la TI (p. ej. recuperación de desastre) o ciberincidentes (p. ej. brechas de datos, ransomware), la externalización (outsourcing) de parte de las actividades de I&T, o compartir mitigaciones de proyectos de I&T con el proveedor a través de acuerdos a precio fijo o convenios de inversión compartida. Estas técnicas no eximen a una empresa de un riesgo, ni en sentido físico y ni en el legal, pero pueden aprovechar las habilidades de otra parte para gestionar el riesgo y reducir su impacto financiero si ocurre un evento adverso. La propiedad del riesgo siempre permanece en la empresa, incluso cuando se suscribe un acuerdo de transferencia de riesgo, compartición de riesgo, o de externalización (outsourcing).

Durante las actividades del análisis de riesgos, es importante tener presente que el riesgo inminente o de alto impacto podría tener que elevarse al nivel apropiado de la organización para que puedan adoptarse las decisiones adecuadas sobre las opciones de respuesta. Consulte la Sección 1.1.1 para obtener consideraciones adicionales para comunicar y asesorar a las partes interesadas apropiadas de la empresa que bien deben rendir cuentas de ellas, bien son sus responsables. También podría ser prudente verificar las suposiciones de evaluación y análisis, técnicas, y de matemáticas básicas o de cálculo de modelos, para garantizar que el análisis sea exacto. Las suposiciones y las técnicas tienen la misma importancia en las evaluaciones cualitativas y cuantitativas. También existe una oportunidad aquí para entender mejor la conexión entre la PML/MFL y las consideraciones de cobertura de seguros para ciertos escenarios. Podría ser aconsejable establecer un límite del seguro para cubrir la MFL, y la prima anual o la franquicia en torno a la PML.

Durante las actividades del análisis de riesgos, es importante tener presente que el riesgo inminente o de alto impacto podría tener que elevarse al nivel apropiado de la organización para que puedan adoptarse las decisiones adecuadas sobre las opciones de respuesta.

7.1.4 Aceptación del riesgo

La aceptación del riesgo significa que no se adopta ninguna medida en relación con un riesgo en particular, y la pérdida es aceptada cuando/si ocurre. Esto es diferente de ignorar del riesgo; aceptar el riesgo supone que el riesgo es conocido, es decir, la dirección ha tomado una decisión informada para aceptarlo como tal. Si una empresa adopta una postura de aceptación del riesgo, debería considerar cuidadosamente quién puede aceptar el riesgo, muy especialmente el riesgo de I&T. El riesgo de I&T debería aceptarse únicamente por la dirección del negocio (y los propietarios del proceso de negocio), en colaboración con y asesorado por el departamento de TI o la función de soporte de TI, y la aceptación debería comunicarse a las partes interesadas adecuadas, como la alta dirección y el consejo, según sea necesario y dictaminado por las políticas. La identificación o mitigación de cada riesgo podría no ser relevante o rentable. Además, deberían seguirse a lo largo del tiempo, y comunicarse, las pérdidas o los incidentes relacionados con el riesgo aceptado, y el riesgo aceptado debería reevaluarse de forma periódica ante cambios en el panorama de negocio, en las suposiciones o en otros factores.

7.1.5 Agregación preliminar del riesgo para acciones de respuesta

La agregación del riesgo es el método o proceso por el que podrían combinarse áreas de riesgo individual para su informe o tratamiento, o para obtener un perfil de riesgo integrado o un índice de riesgo. Las decisiones relacionadas con la gestión de riesgos de I&T serán más beneficiosas para la empresa si el riesgo se gestiona desde la perspectiva de una visión agregada de extremo a extremo (de la actividad de negocio) de todos los riesgos. Una visión agregada del riesgo permite hacer una revisión completa y minuciosa del apetito de riesgo y de la tolerancia al riesgo, en lugar de contar tan solo una visión aislada de elementos de riesgo individuales o parciales.

El riesgo de I&T se agrupa con frecuencia por tipo de riesgo o por el riesgo que se abordaría mediante una respuesta al riesgo similar o un tratamiento de control específico. Por ejemplo, si hay hallazgos de auditoría repetidos o deficiencias de control en el planteamiento de gestión de acceso de una organización que afectan a muchas áreas diferentes del negocio o la misión, la organización podría decidir que una iniciativa empresarial de gestión de accesos podría solucionar esta cuestión.

Hay diferentes formas de realizar la agregación del riesgo. Las consideraciones que deben contemplarse para agregar riesgos y utilizar mapas de riesgos al presentar información de riesgos incluyen:

- Asegurarse de que existe un método uniforme, consistente, acordado y comunicado para evaluar la frecuencia y el impacto de los escenarios de riesgo. Se debería utilizar este mismo método para presentar el riesgo agregado. El uso de una taxonomía consistente para describir el riesgo permite la agregación y la presentación de informes de diferentes tipos de riesgo.
- Ser cauteloso con las matemáticas, y agregar sólo los datos y los números que sean significativos. No agregar datos de diferente naturaleza (p. ej. sobre el estado de los controles o las métricas operativas de TI). Aunque por separado podrían ser indicadores de riesgo adecuados, no tienen sentido cuando no están asociados con un impacto final en el negocio.
- Centrarse en el riesgo para las actividades de negocio y sus indicadores más importantes, y evitar dedicarse a sumar cosas que son fácilmente medibles pero menos relevantes. Informar de ataques al cortafuegos (firewall) podría resultar fácil de medir, pero si hay desplegadas medidas de seguridad actualizadas, estos ataques, aunque probablemente muy frecuentes, podrían tener poco impacto en el negocio.
- No agregar información de riesgos de tal manera que se oculten detalles sobre los que se pueda actuar. Esto podría ocurrir debido al nivel de reporte organizacional de los asuntos cuya responsabilidad corresponde a un determinado nivel organizativo, y que deben ser visibles a dicho nivel; pero podrían agregase y ocultarse al siguiente nivel de autoridad, porque no se requiere ninguna acción inmediata del mismo. La causa raíz del riesgo debe ser visible para los responsables de gestionarlo. Se debe prestar atención al algoritmo de agregación que se utiliza.
- La agregación se puede realizar en múltiples dimensiones (p. ej. unidades organizativas, tipos de elementos de riesgo, procesos de negocio). El beneficio de la agregación en los procesos de negocio es que revela eslabones débiles para lograr resultados satisfactorios de negocio. A veces, para satisfacer las necesidades de la gestión de riesgos y del negocio se podrían necesitar múltiples vistas (usando una combinación de varias dimensiones).
- Agregar el riesgo a nivel empresarial, al que el riesgo puede contemplarse en combinación con todo el resto de riesgos que la empresa debe gestionar (integración con GRE). Tenga en cuenta la estructura organizativa (división geográfica, unidades de negocio, etc.) para establecer un árbol de agregación del riesgo significativo, sin perder de vista los elementos de riesgo específicos importantes.

Un beneficio de la agregación es que el riesgo para la empresa completa se hace muy visible, y la necesidad de definir una respuesta de la empresa al riesgo es más viable o justificable. Por lo tanto, la agregación permite la definición e implementación de una respuesta rentable para el riesgo actual, y que el riesgo residual se circunscriba a los niveles definidos por el apetito de riesgo.

7.1.6 Selección de la respuesta preliminar al riesgo y priorización

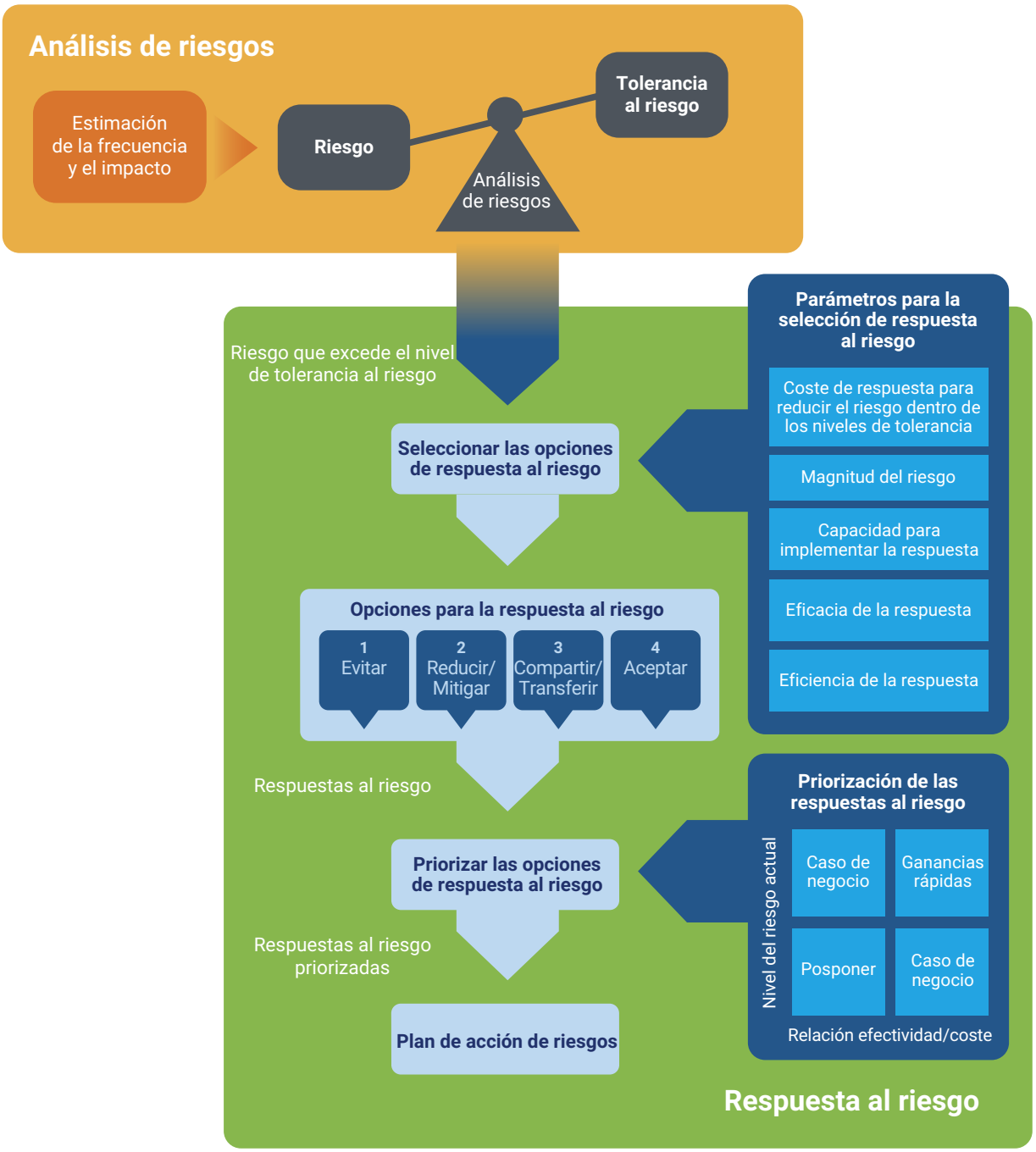
Las secciones anteriores enumeraron las opciones de respuesta al riesgo disponibles. Esta sección contiene una breve discusión sobre la selección de una respuesta adecuada (es decir, dado el riesgo en cuestión), cómo responder, y cómo elegir entre las opciones de respuesta disponibles (**figura 7.1**). Cualquier referencia a la respuesta al riesgo no debería confundirse con respuestas a incidentes o a crisis. La respuesta a un incidente podría considerarse la respuesta a un riesgo que se ha materializado, y que está causando que la empresa esté sufriendo consecuencias que están ocurriendo y que deben contenerse o desencadenar actuaciones antes de que se conviertan en una crisis. En general, la respuesta a un incidente se realiza por un equipo ad hoc o dedicado con unos requisitos de habilidades establecidos para abordar el impacto inmediato. La diferencia entre un incidente y una crisis es con frecuencia de carácter temporal; por ejemplo, ocurre un incidente y, si no se adopta ninguna medida rápidamente, el incidente podría dar lugar a una situación de crisis. Una crisis también podría estar relacionada con la magnitud de las pérdidas resultante de un riesgo materializado; por ejemplo, si el impacto de las pérdidas fue suficiente como para que una organización cese sus operaciones o sufra un contratiempo importante, eso se consideraría una crisis. Deben tenerse en cuenta los siguientes parámetros durante el proceso de respuesta al riesgo y de priorización:

- coste de la respuesta (p. ej. en el caso de transferencia de riesgo, el coste de la prima del seguro; en el caso de mitigación del riesgo, el coste de implementar, mantener y probar los controles);
- la importancia del riesgo abordado por la respuesta (es decir, su prioridad o índice en el registro de riesgos);
- la capacidad de la empresa para implementar y mantener la respuesta a lo largo del tiempo. Cuanto más madura sea la capacidad de gestión de riesgos de una empresa, mejores serán las respuestas que pueden implementarse. Cuando la empresa es bastante inmadura, se podrían utilizar algunas respuestas muy básicas, e irlas después mejorando;
- la efectividad de la respuesta (es decir, la medida en que las actividades de respuesta reducirán la frecuencia o el impacto del riesgo, en caso de materializarse);
- otras inversiones relacionadas con la I&T (la competencia permanente entre invertir en medidas de respuesta al riesgo y otras inversiones de I&T);
- otras respuestas (una respuesta podría hacer frente a varios riesgos mientras que otra no), como en el caso del riesgo que puede agregarse y abordarse con una respuesta común.

A veces, la totalidad del esfuerzo o de los recursos necesarios para dar respuesta al riesgo (p. ej. la colección de controles que deben implementarse o fortalecerse) excederá la capacidad disponible de la empresa. En este caso, se precisan decisiones sobre priorización, habilidad y experiencia organizacional. Las posibles opciones de respuesta al riesgo podrían agruparse de la siguiente manera:

- Ganancias rápidas, que son respuestas a muy corto plazo, con eficiencia temporal, y efectivas al riesgo de alto impacto.
- Obligaciones de cumplimiento para las que exista un requisito no negociable. La gestión de riesgos de incumplimiento debería realizarse junto con otras respuestas al riesgo para evitar duplicidades o solapamientos.
- Caso de negocio que debe elaborarse, con respuestas más costosas o difíciles para el riesgo de alto impacto, que requiere de un análisis minucioso y decisiones de gestión en inversiones. Las respuestas en esta categoría también podrían incluir decisiones para externalizar (outsource) la gestión del riesgo que la organización no tiene capacidad para abordar adecuadamente.
- Posponer y/o monitorizar las condiciones para determinar si los cambios en el riesgo identificado o el entorno justificarían una respuesta diferente.

Figura 7.1—Priorización y opciones de respuesta al riesgo



Fuente: ISACA, *Risk IT Framework, 2nd Edition*, USA, 2020, figura 7.1, *https://www.isaca.org/bookstore/bookstore-risk-digital/ritf2*

Los siguientes son aspectos de los criterios de priorización que merecen considerarse cuando se determina qué riesgo abordar primero, segundo, tercero, etc.:

- Centrarse en la misión y los objetivos estratégicos de la organización como punto de partida para determinar qué riesgo, de materializarse, tendría un mayor impacto en la empresa. Realizar lluvias de ideas sobre los escenarios hasta que haya un conjunto sólido de casos que sea verosímil y relevante para la empresa, la misión, el nivel de capacidad de respuesta y la dependencia de terceros.
- Determinar los productos y servicios más importantes para la empresa, y la tecnología subyacente que soporta la entrega de dichos productos o servicios. La consideración de un activo tecnológico en el contexto de la misión y la estrategia ayuda a determinar su criticidad. La criticidad de un activo es un criterio fundamental para determinar qué riesgo abordar primero.
- De la relación de servicios y productos de la empresa, elaborar un inventario de proveedores, prestadores de servicios, suministradores o terceros que les proporcionen parte o todos los recursos necesarios para entregar cada producto o servicio. La consideración de los prestadores de servicios y proveedores en el contexto de la misión y la estrategia ayuda a determinar la criticidad de los terceros y, posteriormente, a priorizar el riesgo.
- Realizar investigaciones y preguntar a expertos en el tema dentro y fuera de la organización para contribuir a determinar la probabilidad, o la verosimilitud, de que se materialice un escenario determinado. Algunas amenazas no son relevantes para la organización o la organización podría no tener la vulnerabilidad que permite que la amenaza se materialice.
- Centrarse en el riesgo con el mayor impacto potencial en la empresa. ¿Qué riesgo, si se materializase, tendría un impacto mayor en la capacidad de la organización para continuar entregando sus productos y servicios?
- Someter al dictamen de la alta dirección o del consejo de administración qué escenarios tendrían potencialmente un impacto mayor en la empresa. Sus respuestas podrían ser sorprendentes, y también proporcionar un valioso conocimiento para ayudar a refinar las declaraciones de apetito de riesgo y de tolerancia al riesgo.
- Evaluar la capacidad de la empresa para detectar y responder a un escenario determinado o a una serie de escenarios. Algunas organizaciones caen por debajo del umbral de pobreza en ciberseguridad[19] y no son capaces de responder de manera adecuada a uno o más escenarios de riesgos. Este es un riesgo real para muchas organizaciones, en especial para aquellas que continúan operando con una gran deuda técnica, y la alta dirección de la empresa debe ser consciente de ello para decidir mejor el curso de acción.

Entre los principales impulsores para la gestión de riesgos figuran la necesidad de mejorar la toma de decisiones en las empresas, la de alinear los recursos de gestión de riesgos para abordar el riesgo con un mayor impacto potencial en la empresa, y la de desarrollar las capacidades y reunir los recursos necesarios para detectar y responder al riesgo materializado.

[19] El umbral de pobreza en [ciber]seguridad es un término creado por Wendy Nather en 2013; ver Nather, W.; "The Longevity Challenge in Infosec," 4 October 2016, RSA Conference, *https://www.rsaconference.com/industry-topics/blog/the-longevity-challenge-in-infosec*.

APÉNDICE A
Recursos de riesgos

Este apéndice proporciona recursos disponibles de dominio público o provenientes de organizaciones de estándares internacionales para ayudar en el itinerario de la gestión de riesgos. Las publicaciones que son exclusivas a un sector económico individual, como el de las finanzas, están excluidas de esta publicación.

Existen diferentes taxonomías de riesgo disponibles que podrían resultar informativas:

- Una taxonomía de amenazas para la gestión compleja de riesgos[20]
- Una taxonomía de riesgos operativos de ciberseguridad Versión 2[21]
- Taxonomía de riesgos abierta[22]
- Taxonomía de riesgos OpenFAIR[23]

Algunos ejemplos de estándares y marcos que podrían ser fuentes útiles de buenas prácticas incluyen:

- *Marco de riesgos de TI*, 2ª Edición, ISACA[24]*;*
- *Gestión del riesgo empresarial: marco integrado* de COSO[25]*;*
- *Marco de evaluación de amenazas, activos y vulnerabilidades operacionalmente críticas* (OCTAVE Allegro)[26]*;*
- ISO/IEC 27005:2011 *Tecnología de la información — Técnicas de seguridad — Gestión de riesgos de seguridad de la información*[27]*;*
- ISO 31000:2009 *Gestión de riesgos — Principios y pautas*[28]*;*
- IEC 31010:2009 *Gestión de riesgos — Técnicas de evaluación de riesgos*[29]*;*
- Publicación especial del NIST 800-30 Revisión 1, *Guía para la realización de evaluaciones de riesgo*[30]*;*
- Publicación especial del NIST 800-39 *Gestión del riesgo de seguridad de la información: organización, misión y vista del sistema de información*[31].

[20] University of Cambridge, Judge Business School, "A Taxonomy of Threats for Complex Risk Management," *https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/managing-multi-threat/a-taxonomy-of-threats-for-complex-risk-management/*
[21] Cebula, J.; Popeck, M.; Young, L.; "A Taxonomy of Operational Cyber Security Risks Version 2," CMU/SEI-2014-TN-006, Software Engineering Institute, Carnegie Mellon University, 2014, *http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=91013*
[22] Papadopoulos, P.; "Open Risk Taxonomy," OpenRisk, 24 June 2015, *https://www.openrisk.eu/WhitePapers/OpenRiskWP04_061415.pdf*
[23] The Open Group, "Risk Taxonomy (O-RT), Version 2.0," 2009, *https://publications.opengroup.org/c13k*
[24] ISACA, *Risk IT Framework*, *2nd Edition*, 2020, USA, *www.isaca.org/bookstore/bookstore-risk-digital/ritf2*
[25] Committee of Sponsoring Organizations (COSO), *Enterprise Risk Management—Integrated Framework*, June 2017, *https://www.coso.org/Pages/erm.aspx*
[26] Alberts, C.J.; Behrens, S.; Pethia, R.D.; Wilson, W.R; *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework*, Version 1.0, Carnegie Mellon University Software Engineering Institute, September 1999, *https://resources.sei.cmu.edu/asset_files/TechnicalReport/1999_005_001_16769.pdf*
[27] International Organization for Standardization (ISO®), ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*, June 2011, *https://www.iso.org/standard/56742.html*
[28] ISO, ISO 31000:2009, *Risk management — Principles and guidelines*, November 2009, *https://www.iso.org/standard/43170.html*
[29] ISO, IEC 31010:2009, *Risk management — Risk assessment techniques*, November 2009, *https://www.iso.org/standard/51073.html*
[30] NIST, SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments*, September 2012, *https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final*
[31] NIST, SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011, *https://csrc.nist.gov/publications/detail/sp/800-39/final*

Esta página se dejó en blanco intencionalmente

APÉNDICE B
Glosario

TÉRMINO	DEFINICIÓN
Aceptación del riesgo	Si el riesgo está dentro del margen de tolerancia al riesgo de la empresa o si el coste de mitigar el riesgo es mayor que las pérdidas potenciales, la empresa puede asumir el riesgo y absorber las pérdidas.
Activo intangible	Un activo que no es de naturaleza física. **Notas de alcance:** Algunos ejemplos incluyen: propiedad intelectual (patentes, marcas, derechos de autor, procesos), fondo de comercio y reconocimiento de marca.
Agente de amenaza	Los métodos y las cosas utilizados para explotar una vulnerabilidad. **Notas de alcance:** Los ejemplos incluyen la determinación, la capacidad, el motivo y los recursos.
Agregación de riesgos	El proceso de integrar las evaluaciones de riesgos a nivel corporativo para obtener una visión completa del riesgo global para la empresa.
Amenaza	Cualquier cosa (por ejemplo, un objeto, una sustancia, un ser humano) que sea capaz de actuar contra un activo de manera que pueda ocasionar daños. **Notas de alcance:** Causa potencial de un incidente indeseado. (ISO/IEC 13335)
Análisis/evaluación del impacto al negocio (BIA)	Evaluar la criticidad y la sensibilidad de los activos de información. Un ejercicio que determina el impacto de perder el soporte de cualquier recurso para una empresa, establece la distribución de esas pérdidas a lo largo del tiempo, identifica los recursos mínimos necesarios para la recuperación, y prioriza la recuperación de los procesos y del sistema de soporte. **Notas de alcance:** Este proceso también incluye abordar: • la pérdida de ingresos; • los gastos inesperados; • los temas legales (cumplimiento regulatorio o contractual); • los procesos interdependientes; • la pérdida de reputación o de confianza del público.
Análisis de amenazas	Una evaluación del tipo, el alcance y la naturaleza de los eventos o las acciones que pueden ocasionar consecuencias adversas; la identificación de las amenazas que existen contra los activos de la empresa. **Notas de alcance:** El análisis de amenazas normalmente define el nivel de amenaza y la probabilidad de que ésta se materialice.

TÉRMINO	DEFINICIÓN
Análisis de riesgos	1. Un proceso mediante el que se calculan la frecuencia y la magnitud de los escenarios de riesgo de TI. 2. Los pasos iniciales de la gestión de riesgos: el análisis del valor de los activos para el negocio, la identificación de las amenazas a esos activos, y la evaluación de cuán vulnerable es cada activo a esas amenazas. **Notas de alcance:** A menudo, involucra la evaluación de la frecuencia probable de un evento en particular, así como del impacto probable de ese evento.
Análisis de vulnerabilidades	Un proceso de identificación y clasificación de las vulnerabilidades.
Apetito de riesgo	La cantidad de riesgo que, en términos generales, una entidad está dispuesta a aceptar para llevar a cabo su misión.
Autoevaluación de riesgos de control	Un método/proceso mediante el que la dirección y el personal de todos los niveles identifican y valoran colectivamente el riesgo y los controles con sus áreas de negocio. Esto podría formar parte de la orientación de un facilitador, como un auditor o un gerente de riesgo.
Compartición del riesgo	**Notas de alcance:** Ver transferencia del riesgo.
Continuidad del negocio	Prevención, mitigación y recuperación de las interrupciones. **Notas de alcance:** Los términos 'planes de reanudación de negocios', 'planes de recuperación ante desastres' y 'planes de contingencia' también se podrían utilizar en este contexto; se centran en los aspectos de recuperación de la continuidad, y por ese motivo el aspecto de la 'resiliencia' debería también tenerse en cuenta. Perspectiva de COBIT 5 y COBIT 2019
Contramedida	Cualquier proceso que reduce directamente una amenaza o vulnerabilidad.
Control	Los medios para gestionar el riesgo, incluyendo políticas, procedimientos, guías, prácticas o estructuras organizacionales que pueden ser de naturaleza administrativa, técnica, gerencial o legal CR. **Notas de alcance:** También se utiliza como sinónimo de salvaguarda o de contramedida. Ver también control interno.
Control compensatorio	Control interno que reduce el riesgo de una debilidad de control existente o potencial que de lugar en errores y omisiones.
Control correctivo	Diseñado para corregir errores, omisiones y usos e intrusiones no autorizados, una vez que se detectan.
Control de los procesos del negocio	Las políticas, los procedimientos, las prácticas y las estructuras organizativas diseñadas para proporcionar un aseguramiento razonable de que un proceso de negocio logre sus objetivos. **Notas de alcance:** Perspectiva de COBIT 5 y COBIT 2019
Control general de SI	Control general diseñado para gestionar y monitorizar el entorno de SI y que, por lo tanto, afecta a todas las actividades relacionadas con los SI.

TÉRMINO	DEFINICIÓN
Control preventivo	Un control interno que se utiliza para evitar eventos no deseados, errores y otros sucesos que una empresa haya determinado que podrían tener un efecto sustancialmente negativo en un proceso o producto final.
Controles detallados de SI	Controles sobre la adquisición, la implementación, la entrega, y el soporte a los servicios y los sistemas de SI compuestos por controles de aplicación más aquellos controles generales que no están incluidos en los controles globales.
Controles internos	Las políticas, los procedimientos, las prácticas y las estructuras organizacionales que están diseñadas para proporcionar un aseguramiento razonable de que se lograrán los objetivos de negocio, y se evitarán, o detectarán y corregirán, los eventos no deseados.
Criticidad	La importancia de un activo o una función particular para la empresa, y el impacto si ese activo o función no está disponible.
Cultura	Patrón de conductas, creencias, suposiciones, actitudes y formas de hacer las cosas. **Notas de alcance:** Perspectiva de COBIT 5 y COBIT 2019
Cultura de riesgos	Conjunto de valores y creencias compartidos que gobierna las actitudes hacia la adopción de riesgos, el cuidado y la integridad, que determina la franqueza con que se informan y discuten los riesgos y las pérdidas.
Debilidad de control	Una deficiencia en el diseño o funcionamiento de un procedimiento de control. Las debilidades de control pueden potencialmente dar como resultado que el riesgo relevante para el área de actividad no se reduzca a un nivel aceptable (el riesgo relevante amenaza el logro de los objetivos relevantes para el área de la actividad que se está examinando). Las debilidades de control pueden ser importantes cuando el diseño o el funcionamiento de uno o más procedimientos de control no reduce a un nivel relativamente bajo el riesgo de que pudiesen ocurrir errores causados por actos ilegales o irregularidades y que los procedimientos de control correspondientes no los detecten.
Descripción del riesgo	Una descripción de las condiciones actuales que podrían dar lugar a pérdidas; y una descripción de las pérdidas. Fuente: Software Engineering Institute (SEI) **Notas de alcance:** Para que un riesgo sea comprensible, debe expresarse con claridad. Dicho tratamiento debe incluir una descripción de las condiciones actuales que podrían dar lugar a pérdidas; y una descripción de las pérdidas.
Escaneo (scanning) de vulnerabilidades	Un proceso automatizado para identificar de forma proactiva las debilidades de seguridad en una red o en un sistema individual.
Escenario de riesgo	La representación tangible y evaluable del riesgo. **Notas de alcance:** Uno de los elementos clave de información necesario para identificar, analizar y responder al riesgo (objetivo de COBIT 2019 APO12)
Escenario de riesgo de TI	La descripción de un evento relacionado con TI que puede derivar en un impacto en el negocio.

TÉRMINO	DEFINICIÓN
Evaluación de riesgos	El proceso utilizado para identificar y valorar los riesgos y sus efectos potenciales. **Notas de alcance:** Las evaluaciones de riesgo se utilizan para identificar los elementos o áreas que presentan mayor exposición, vulnerabilidad o riesgo para la empresa, para su inclusión en el plan de auditoría anual de SI. Las evaluaciones de riesgo también se utilizan para gestionar la entrega de proyectos y el riesgo de los beneficios de proyectos.
Evento	Algo que sucede en un lugar y/o momento específico.
Evento de amenaza	Cualquier evento durante el que un elemento/agente de amenaza actúa contra de un activo de una manera que tiene potencial de ocasionar directamente un daño.
Evento de pérdida	Cualquier evento durante el que una amenaza de lugar a pérdidas. **Notas de alcance:** Según Jones, J.; "FAIR Taxonomy," Risk Management Insight, USA, 2008
Evento de vulnerabilidad	Cualquier evento durante el que se produzca un aumento significativo en la vulnerabilidad. Tenga en cuenta que este aumento en la vulnerabilidad puede provenir de cambios en las condiciones de control o de cambios en la capacidad/fuerza de la amenaza CR . **Notas de alcance:** De Jones, J.; "FAIR Taxonomy," Risk Management Insight, USA, 2008
Evitación del riesgo	El proceso para evitar un riesgo en forma sistemática, lo que constituye un planteamiento de gestión del riesgo.
Explotación de día cero	Una vulnerabilidad que se explota antes de que el creador o proveedor del software tenga siquiera conocimiento de su existencia.
Exposición	Pérdida potencial para un área debido a que suceda un evento adverso.
Factor de riesgo	Una condición que puede influir en la frecuencia y/o magnitud y, en última instancia, en el impacto que los eventos/escenarios relacionados con TI tienen sobre el negocio.
Frecuencia	Medida de la cantidad de eventos que ocurren durante un determinado período de tiempo.
Gestión de riesgo empresarial (GRE)	Disciplina por la cual una empresa de cualquier sector de actividad económica evalúa, controla, explota, financia y monitoriza el riesgo proveniente de todas sus fuentes con el propósito de aumentar el valor de la empresa para sus partes interesadas, a corto y largo plazo.

TÉRMINO	DEFINICIÓN
Gestión de riesgos	1. Las actividades coordinadas para dirigir y controlar una empresa con relación al riesgo. **Notas de alcance:** En el estándar internacional, el término "control" se utiliza como sinónimo de "medida". (ISO/IEC Guide 73:2002) 2. Uno de los objetivos del gobierno. Implica reconocer el riesgo; evaluar el impacto y la probabilidad de ese riesgo; y desarrollar estrategias, tales como evitar el riesgo, reducir el efecto negativo del riesgo y/o transferir el riesgo, para gestionarlo en el contexto del apetito de riesgo de la empresa. **Notas de alcance:** Perspectiva de COBIT 5
Gobierno corporativo	Sistema mediante el cual se dirigen y controlan las empresas. El consejo de administración es el responsable del gobierno de su empresa. Se compone del liderazgo, las estructuras organizativas y los procesos que garantizan que la empresa mantenga y amplíe sus estrategias y objetivos.
Impacto	Magnitud de las pérdidas resultantes de una amenaza que explota una vulnerabilidad.
Impacto en el negocio	El efecto neto, positivo o negativo, sobre la consecución de los objetivos del negocio.
Incidente de seguridad	Una serie de eventos inesperados que implican un ataque, o serie de ataques (compromiso y/o violación de la seguridad), a uno o más sitios. Un incidente de seguridad normalmente incluye una estimación de su nivel de impacto. Se define una cantidad limitada de niveles de impacto y, para cada uno, se identifican las acciones específicas requeridas y las personas que deben ser notificadas.
Incidente de TI	Cualquier evento que no forme parte de la operación habitual de un servicio que cause, o pudiese causar, una interrupción o una reducción de la calidad de ese servicio.
Incidente relacionado con TI	Un evento relacionado con la TI que causa un impacto operativo, de desarrollo y/o estratégico en el negocio.
Indicador clave de riesgo (KRI)	Un subconjunto de indicadores de riesgo que son muy relevantes y que tienen una alta probabilidad de predecir o de indicar un riesgo importante. **Notas de alcance:** Ver también Indicador de riesgo.
Indicador de riesgo	Una métrica capaz de mostrar que la empresa está expuesta, o tiene una alta probabilidad de estarlo, a un riesgo que excede el apetito de riesgo definido.
Instancia de riesgo de TI	Una combinación de condiciones de control, valor y amenaza que suponen un nivel notable de riesgo de TI.
Interrupción del negocio	Cualquier evento, sea previsto (p.ej. huelga en el servicio público) o imprevisto (p. ej. apagón) que interrumpe el curso normal de las operaciones comerciales en una empresa.
Mapa de riesgos	Una herramienta (gráfica) para clasificar y representar el riesgo por rangos definidos de frecuencia y magnitud.

TÉRMINO	DEFINICIÓN
Marco	**Notas de alcance:** Ver marco de control y marco de gobierno de TI.
Marco de control	Conjunto de controles fundamentales que facilita el cumplimiento de las responsabilidades del propietario del proceso de negocio para evitar pérdidas financieras o de información en una empresa.
Meta de negocio	La traducción de la misión de la empresa de una declaración de intenciones a objetivos de desempeño y resultados.
Mitigación del riesgo	La gestión de un riesgo mediante el uso de contramedidas y controles.
Objetivo de control	Declaración del resultado deseado o propósito que se va a lograr mediante la implementación de procedimientos de control en un proceso determinado.
Objetivo de negocio	Desarrollo adicional de las metas de negocio en objetivos tácticos y resultados deseados.
Perfil de riesgo de TI	Descripción de la totalidad del riesgo de TI (identificado) al que la empresa está expuesta.
Práctica de control	Mecanismo de control clave que contribuye al logro de los objetivos de control mediante el uso responsable de los recursos, la gestión de riesgos adecuada, y la alineación de TI con el negocio.
Probabilidad	La probabilidad de que algo suceda.
Proceso	En general, un conjunto de actividades influenciadas por las políticas y los procedimientos de la empresa que capta entradas de varias fuentes (incluyendo otros procesos), trata la información, y produce unos resultados. **Notas de alcance:** Los procesos tienen unas motivaciones de negocio claras para existir, propietarios responsables, roles y responsabilidades claros relativos a la ejecución del proceso, y los medios para medir el desempeño.
Propietario del riesgo	Persona a la que la organización ha investido de autoridad y ha asignado la rendición de cuentas para adoptar las decisiones basadas en el riesgo, y que es propietaria de las pérdidas asociadas con la materialización de un escenario de riesgo. **Notas de alcance:** El propietario del riesgo podría no ser el responsable de la implementación de su tratamiento.
Reducción del riesgo	La implementación de controles o contramedidas para reducir la probabilidad o el impacto de un riesgo hasta un nivel acorde con la tolerancia al riesgo de la organización.
Registro de riesgos de TI	Un repositorio de los atributos clave de riesgos de TI potenciales y conocidos. Entre los atributos podría figurar su nombre, descripción, propietario, frecuencia esperada/real, magnitud potencial/real, impacto en el negocio potencial/real y disposición.
Respuesta al riesgo	Evitación del riesgo, aceptación del riesgo, compartición/transferencia del riesgo, mitigación del riesgo, que conducen a una situación en la que tanto riesgo residual futuro (riesgo actual con la respuesta al riesgo definida e implementada) como sea posible (normalmente dependiendo de los presupuestos disponibles) cae dentro de los límites del apetito de riesgo.

TÉRMINO	DEFINICIÓN
Riesgo	La combinación de la probabilidad de un evento y su impacto.
Riesgo de control	Riesgo de que exista un error sustancial que el sistema de controles internos no evitaría o detectaría oportunamente (ver riesgo inherente).
Riesgo de negocio	Situación posible cuya frecuencia y magnitud de pérdidas (o ganancias) es incierta.
Riesgo de seguridad/transacción	El riesgo actual y futuro para las ganancias y el capital proveniente del fraude, del error y la incapacidad para entregar servicios o productos, de mantener una situación competitiva y de gestionar la información. **Notas de alcance:** El riesgo de seguridad se manifiesta en cada producto o servicio ofrecido, y comprende el desarrollo y la entrega del producto, el procesamiento de las transacciones, el desarrollo de los sistemas, los entornos informáticos, la complejidad de los productos y servicios, y entorno de control interno. Los productos bancarios en Internet podrían tener un grado de riesgo de seguridad alto, en especial si esas líneas de negocio no se planifican, implementan y monitorizan correctamente.
Riesgo de TI	El riesgo de negocio asociado con el uso, la propiedad, la operación, el involucramiento, la influencia y la adopción de la TI dentro de una empresa.
Riesgo inherente	Nivel o exposición al riesgo sin tener en cuenta las acciones que la dirección ha tomado o podría tomar (p. ej. implementar controles).
Riesgo reputacional	El efecto actual y futuro sobre las ganancias y el capital y el capital derivado de una opinión pública negativa. **Notas de alcance:** El riesgo reputacional afecta la capacidad de un banco para establecer nuevas relaciones o servicios, o de continuar prestando servicios a las relaciones existentes. Podría exponer al banco a litigios, pérdidas financieras o una disminución de su base de clientes. La reputación de un banco puede dañarse por causa de servicios de banca por internet que se ejecuten de forma deficiente o que, de alguna otra manera, ofenda a los clientes y al público. Un banco en Internet tiene un riesgo reputacional mayor en comparación con un banco tradicional con presencia física, porque es más fácil para sus clientes dejarlo y buscar otro banco en Internet diferente, y también debido a que no puede discutir personalmente ningún problema con el cliente.
Riesgo residual	El riesgo restante después de que la dirección ha implementado una respuesta al riesgo.
Salvaguarda	Una práctica, procedimiento o mecanismo que reduce el riesgo.
Tecnología de la información (TI)	Hardware, software, comunicaciones, y otras instalaciones utilizadas para la entrada, el almacenamiento, el proceso, la transmisión y la salida de datos en cualquiera de sus formas.

TÉRMINO	DEFINICIÓN
Tipo de evento	A efectos de la gestión de riesgos de TI, uno de los tres siguientes posibles tipos de eventos: evento de amenaza, evento de pérdida y evento de vulnerabilidad. **Notas de alcance:** Poder diferenciar de manera consistente y efectiva los diferentes tipos de eventos que contribuyen al riesgo es un elemento crítico para el desarrollo de buenas métricas relacionadas con el riesgo y de decisiones bien informadas. A menos que se reconozcan y apliquen estas diferencias de categoría, las métricas resultantes pierden significado y, como resultado, las decisiones basadas en tales métricas son mucho más propensas a tener fallos.
Tolerancia al riesgo	Nivel aceptable de desviación que la dirección está dispuesta a permitir para cualquier riesgo específico mientras la empresa persigue sus objetivos.
Transferencia del riesgo	Proceso de ceder el riesgo a otra empresa, por lo general, mediante la suscripción de una póliza de seguro o por la externalización (outsourcing) del servicio. **Notas de alcance:** También conocido como compartición del riesgo.
Tratamiento del riesgo	El proceso de selección y ejecución de medidas para modificar el riesgo (Guía ISO/IEC 73:2002).
Valoración del riesgo	El proceso por el que se compara el riesgo estimado con unos criterios de un riesgo dados para determinar la importancia del riesgo. [ISO/IEC Guide 73:2002].
Vector de amenazas	El itinerario o recorrido utilizado por el adversario para conseguir el acceso al objetivo.
Vista de la cartera (portfolio) de riesgos	1. Un método para identificar interdependencias e interconexiones entre los riesgos, así como el efecto de las respuestas al riesgo sobre múltiples tipos de riesgo. 2. Un método para calcular el impacto agregado de múltiples tipos de riesgo (p. ej. escenarios/tipos de amenazas en cascada y coincidentes, concentración/correlación de riesgos entre silos) y el efecto potencial de la respuesta al riesgo en múltiples tipos de riesgo.
Vulnerabilidad	Una debilidad en el diseño, la implementación, la operación o el control interno de un proceso que podría exponer al sistema a amenazas adversas provenientes de eventos de amenazas.