# Marco de Riesgos de TI

**Principios**

**Detalles del proceso**

**Directrices de gestión**

**Modelo de madurez**

Risk IT

BASADO EN COBIT ®

ISACA®

Serving IT Governance Professionals

**ISACA®**

Con más de 86.000 miembros en más de 160 países, ISACA® (*www.isaca.org*) es líder global como proveedor de conocimiento, certificaciones, comunidad, apoyo y educación en aseguramiento y seguridad en sistemas de información (SI), Gobierno de TI de la empresa, y riesgos y cumplimiento relacionados con TI. Fundada en 1969, ISACA patrocina conferencias internacionales, publica el *ISACA® Journal*, y desarrolla estándares internacionales en control y auditoría de sistemas de información (SI). Además administra las globalmente respetadas designaciones Certified Information Systems Auditor™ (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) y Certified in Risk and Information Systems Control™ (CRISC™).

ISACA desarrolla y actualiza continuamente el marco de los riesgos de TI ® COBIT y Val IT ™, que ayudan a los profesionales de TI y los líderes de la empresa cumplir con sus responsabilidades de gobierno y entregar valor al negocio

**Descargo de responsabilidad**

ISACA ha diseñado y creado *The Risk IT Framework* (the 'Work') principalmente como un recurso educativo para los oficiales de información (CIOs) ,la alta dirección y administración de TI.ISACA no pretende que el uso de cualquiera de los trabajos asegure un resultado satisfactorio . La publicación no debe considerarse como incluyente de cualquier procedimiento y prueba apropiado, o excluyente de otros procedimientos y pruebas que estén razonablemente dirigidos a la obtención de los mismos resultados. Para determinar la aplicabilidad de cualquier procedimiento o prueba específicos, el profesional de control debe aplicar su buen juicio profesional a las circunstancias de control específicas presentadas por el entorno particular de sistemas o de la tecnología de información.



**ISACA**

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: info@isaca.org
Web site: www.isaca.org

ISBN 978-1-60420-111-6
*The Risk IT Framework*
Printed in the United States of America

# AGRADECIMIENTOS


## ISACA desea reconocer a:

**Equipo de desarrollo**
Dirk Steuperaert, CISA, CGEIT, IT In Balance BVBA, Belgium, Chair
Steven De Haes, Ph.D., University of Antwerp Management School, Belgium
Gert du Preez, CGEIT, PricewaterhouseCoopers, Belgium
Rachel Massa, CISSP, PricewaterhouseCoopers LLP, USA
Bart Peeters, PricewaterhouseCoopers, Belgium
Steve Reznik, CISA, PricewaterhouseCoopers LLP, USA

**Grupo de tareas del riesgo de TI (2008-2009)**
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Steven Babb, CGEIT, KPMG, UK
Brian Barnier, CGEIT, ValueBridge Advisors, USA
Jack Jones, CISA, CISM, CISSP, Risk Management Insight LLC, USA
John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA
Gladys Rouissi, CISA, MComp, Commonwealth Bank of Australia, Australia
Lisa R. Young, CISA, CISSP, Carnegie Mellon University, USA

**Revisores expertos**
Mark Adler, CISA, CISM, CGEIT, CFE, CFSA, CIA, CISSP, Commercial Metals, USA
Steven Babb, CGEIT, KPMG, UK
Gary Baker, CGEIT, CA, Deloitte and Touche LLP, Canada
Dave H. Barnett, CISM, CISSP, CSDP, CSSLP, Applied Biosystems, USA
Brian Barnier, CGEIT, ValueBridge Advisors, USA
Laurence J. Best, PricewaterhouseCoopers LLP, USA
Peter R. Bitterli, CISA, CISM, Bitterli Consulting AG, Switzerland
Luis Blanco, CISA, Citibank, UK
Adrian Bowles, Ph.D., Sustainability Insights Group (SIG411), USA
Dirk Bruyndonckx, CISA, CISM, CGEIT, MCA, KPMG Advisory, Belgium
Olivia Xardel-Burtin, Grand Duchy of Luxembourg
M. Christophe Burtin, Grand Duchy of Luxembourg
Rahul Chaurasia, Student, Indian Institute of Information Technology, India
Philip De Picker, CISA, MCA, Nationale Bank van Belgie, Belgium
Roger Debreceny, Ph.D., FCPA, University of Hawaii-Manoa, USA
Heidi L. Erchinger, CISA, CISSP, System Security Solutions Inc., USA
Robert Fabian, Ph.D., I.S.P., Independent Consultant, Canada
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Shawna Flanders, CISA, CISM, ACS, PSCU Financial Services, USA
John Garms, CISM, CISSP, ISSEP, Electric-Tronics Inc., USA
Dennis Gaughan, AMR Research, USA
Yalcin Gerek, CISA, CGEIT, TAC, Turkey
Edson Gin, CISA, CFE, CIPP, SSCP, USA
Pete Goodhart, PricewaterhouseCoopers LLP, USA
Gary Hardy, CGEIT, IT Winners, South Africa
Winston Hayden, ITGS Consultants, South Africa
Jimmy Heschl, CISA, CISM, CGEIT, KPMG, Austria
Monica Jain, CGEIT, CSQA, CSSBB, USA
Jack Jones, CISA, CISM, CISSP, Risk Management Insight LLC, USA
Dharmesh Joshi, CISA, CGEIT, CA, CIA, CISSP, CIBC, Canada
Catherine I. Jourdan, PricewaterhouseCoopers LLP, USA
Kamal Khan, CISA, CISSP, MBCS, Saudi Aramco, Saudi Arabia
Marty King, CISA, CGEIT, CPA, BCBSNC, USA
Terry Kowalyk, Credit Union Deposit Guarantee Corp., Canada
Denis Labhart, Swiss Life, Switzerland
John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA
Philip Le Grand, Datum International Ltd., UK
Bjarne Lonberg, CISSP, A.P. Moller—Maersk, Denmark
Jo Lusk, CISA, Federal Government, USA
Charles Mansour, CISA, Charles Mansour Audit and Risk Service, UK
Mario Micallef, CGEIT, CPAA, FIA, Ganado & Associates, Malta
Jack Musgrove, CGEIT, CMC, BI International, USA
Paul Phillips, Barclays Bank Plc, UK
Andre Pitkowski, CGEIT, OCTAVE, APIT Informatica, Brazil
Jack M. Pullara, CISA, PricewaterhouseCoopers LLP, USA

# AGRADECIMIENTOS *(cont.)*

**Revisores expertos *(cont.)***
Felix Ramirez, CISA, CGEIT, Riebeeck Associates, USA
Gladys Rouissi, CISA, MComp, Commonwealth Bank of Australia, Australia
Daniel L. Ruggles, CISM, CGEIT, CISSP, CMC, PMP, PM Kinetics LLC, USA
Stephen J. Russell, PricewaterhouseCoopers LLP, USA
Deena Lavina Saldanha, CISA, CISM, Obegi Chemicals LLC, UAE
Mark Scherling, Canada
Gustavo Adolfo Solis Montes, Grupo Cynthus SA de CV, Mexico
John Spangenberg, SeaQuation, The Netherlands
Robert E. Stroud, CGEIT, CA Inc., USA
John Thorp, CMC, I.S.P., The Thorp Network, Canada
Lance M. Turcato, CISA, CISM, CGEIT, CPA, CITP, City of Phoenix, USA
Kenneth Tyminski, Retired, USA
E.P. van Heijningen, Ph.D., RA, ING Group, The Netherlands
Sylvain Viau, CISA, CGEIT, ISO Lead Auditor, 712iem Escadron de Communication, Canada
Greet Volders, CGEIT, Voquals NV, Belgium
Thomas M. Wagner, Marsh Risk Consulting, Canada
Owen Watkins, ACA, MBCS, Siemens, UK
Clive E. Waugh, CISSP, CEH, Intuit, USA
Amanda Xu, CISA, CISM, Indymac Bank, USA
Lisa R. Young, CISA, CISSP, Carnegie Mellon University, USA

**Consejo de administración de ISACA**
Emil D'Angelo, CISA, CISM, Bank of Tokyo Mitsubishi UFJ, USA, International President
George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control SA-NV, Belgium, Vice President
Yonosuke Harada, CISA, CISM, CGEIT, CAIS, InfoCom Research Inc., Japan, Vice President
Ria Lucas, CISA, CGEIT, Telstra Corp. Ltd., Australia, Vice President
Jose Angel Pena Ibarra, CGEIT, Alintec, Mexico, Vice President
Robert E. Stroud, CGEIT, CA Inc., USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President
Rolf von Roessing, CISA, CISM, CGEIT, KPMG Germany, Germany, Vice President
Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, KPMG LLP, UK, Past International President
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA, Director
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Director
Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Director
Jeff Spivey, CPP, PSP, Security Risk Management, USA, Trustee

**Marco del comite**
Patrick Stachtchenko, CISA, CGEIT, CA, Stachtchenko & Associes SAS, France, Chair
George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control SA-NV, Belgium, Vice President
Steven A. Babb, CGEIT, United Kingdom
Sergio Fleginsky, CISA, Akzonobel, Uruguay
John W. Lainhart, IV, CISA, CISM, CGEIT, IBM Global Business Services, USA
Mario C. Micallef, CGEIT, CPAA, FIA, Malta
Derek J. Oliver, CISA, CISM, CFE, FBCS, United Kingdom
Robert G. Parker, CISA, CA, CMC, FCA, Canada
Jo Stewart-Rattray, CISA, CISM, CGEIT, RSM Bird Cameron, Australia
Robert E. Stroud, CGEIT, CA Inc., USA
Rolf M. von Roessing, CISA, CISM, CGEIT, KPMG Germany, Germany

**Reconocimiento especial**
To the following members of the 2008-2009 IT Governance Committee who initiated the project and steered it to a successful conclusion:
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Chair
Sushil Chatterji, Edutech Enterprises, Singapore
Kyung-Tae Hwang, CISA, Dongguk University, Korea
John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA
Hugh Penri-Williams, CISA, CISM, CCSA, CIA, Glaniad 1865 Eurl, France
Gustavo Adolfo Solis Montes, CISA, CISM, Grupo Cynthus SA de CV, Mexico
Robert E. Stroud, CGEIT, CA Inc., USA
John Thorp, CMC, I.S.P., The Thorp Network Inc., Canada
Wim Van Grembergen, Ph.D., University of Antwerp Management School and IT Alignment and Governance Research Institute, Belgium

**Versión en español realizada por la Cátedra de Buen Gobierno Universidad de Deusto**
Director del Proyecto:
Manuel Ballester, PhD, IEEE, MBA,CISA, CISM, CGEIT.
Traductores:
María Heras, CISA
Gabriel Curiel, CISA
Angela Franquet
Lidia García, ITIL
Pamela Estrada

# TABLA DE CONTENIDOS

**Página en blanco intencionadamente**

# 1. RESUMEN EJECUTIVO

Este documento forma parte de la iniciativa de los Riesgos de TI de ISACA, que se dedica a ayudar a las organizaciones a gestionar los riesgos relacionados con TI. Para el desarrollo de este documento se ha consultado a un experimentado equipo de profesionales y expertos, junto con las nuevas prácticas y metodologías empleadas para la gestión eficaz de los riesgos de TI. Por tanto, RISK IT es un marco basado en un conjunto de principios y guías, procesos de negocio y directrices de gestión que se ajustan a estos principios.

El marco de los riesgos de TI, RISK IT, se complementa con COBIT, que proporciona un marco integral para el control y la gestión de las organizaciones de soluciones y servicios de TI. Aunque COBIT establece las mejores prácticas para la gestión de riesgos proporcionando un conjunto de controles para mitigar los riesgos de TI, RISK IT establece las mejores prácticas con el fin de establecer un marco para las organizaciones para identificar, gobernar y administrar los riesgos asociados a su negocio.

El marco de riesgos de TI es utilizado para ayudar a implementar el gobierno de TI, y las organizaciones que han adoptado (o están planeando adoptar) COBIT como marco de su gobierno de TI pueden utilizar RISK IT para mejorar la gestión de sus riesgos.

COBIT, propiedad de ISACA, se encarga de gestionar todas las actividades relacionadas con TI en la organización. Estos procesos tienen que tratar con eventos internos o externos a la organización. Los eventos internos pueden incluir los incidentes operacionales, los fracasos del proyecto, cambios de la estrategia de TI y las fusiones. Los eventos externos pueden incluir cambios en las condiciones del mercado, nuevos competidores, nuevas tecnologías disponibles y las nuevas regulaciones que le afectan.

Estos eventos, plantean un riesgo y una oportunidad para evaluar el mismo y generar las soluciones oportunas. La dimensión del riesgo, y cómo gestionarlo, es el tema principal de RISK IT.

Cuándo se identifican las oportunidades de cambios del negocio relacionados con TI, el Marco VAL IT describe cómo progresar y maximizar el retorno de la inversión realizada en los mismos.
El resultado de la evaluación tendrá probablemente un impacto en algunos de los procesos de TI, por lo que las flechas de la "Gestión de Riesgos" y "Gestión del Valor" se dirigen a la "Gestión de los Procesos de TI", tal y como se muestra en la **figura 1**.

Un riesgo de TI es también un riesgo del negocio, riesgos del negocio asociados con el uso, propiedad, operación, participación, la influencia y la adopción de las TI en una organización. Se compone de los eventos relacionados con TI que potencialmente podrían afectar el negocio. Este hecho puede ocurrir con una frecuencia y magnitud inciertas, y supone dificultades para alcanzar las metas y objetivos estratégicos. Los riesgos de TI pueden clasificarse de diversas maneras (véase la **figura 2**).

[1]

Figura 1 - Risk IT, Val IT y CobiT

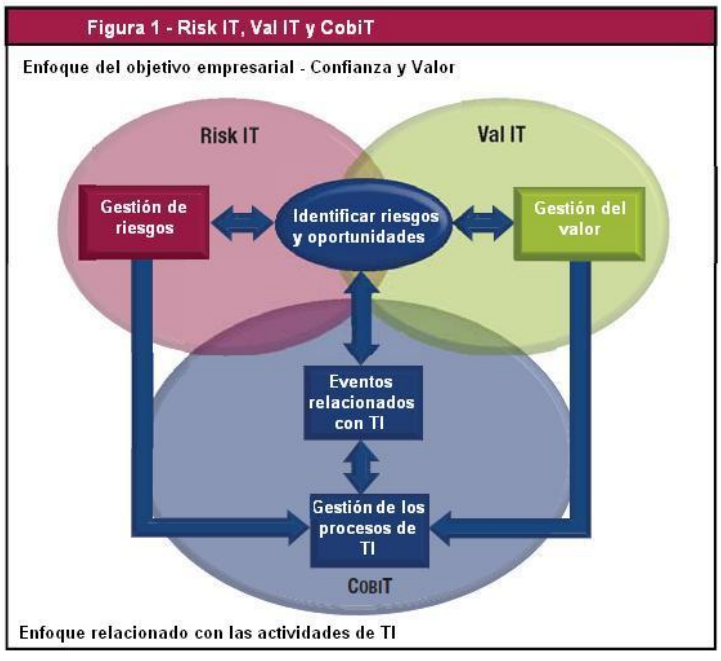
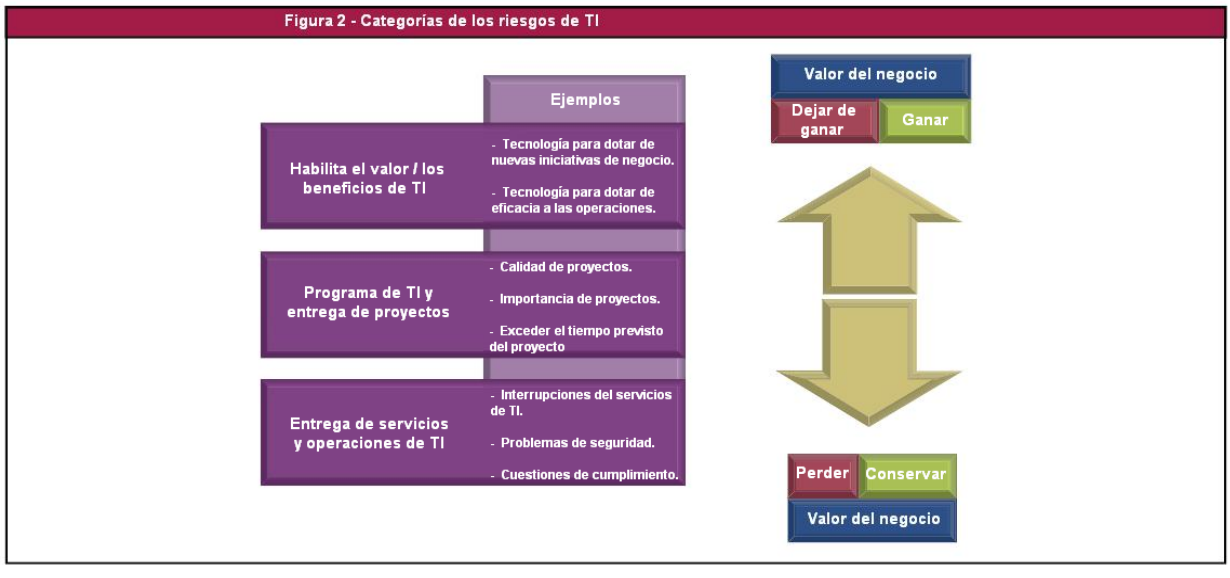



Figura 2 - Categorías de los riesgos de TI



- Beneficios / riesgos de TI - Asociados con la ausencia de las oportunidades para utilizar la tecnología, con el fin de mejorar la eficiencia o efectividad de los procesos de negocio o como un facilitador para nuevas iniciativas organizacionales.
- Programa de TI y el riesgo de ejecución de proyectos - Asociado con la contribución de las TI para soluciones de negocios nuevos o mejorados, por lo general en la forma o los proyectos y programas. Esto se vincula a la gestión de las inversiones de cartera (como se describe en el marco de VAL IT).
- Las operaciones de TI y el riesgo de la prestación de servicios - Asociado con todos los aspectos del desempeño de TI y servicios del sistema, que puede ocasionar la destrucción o la reducción de valor para la organización.

Los riesgos de TI siempre existen, sean o no detectados o reconocidos por la organización.

**La figura 2** muestra que para todas las categorías de riesgos de TI no existe un aspecto positivo equivalente. Por ejemplo:
- La prestación de servicios - Si se fortalecen las prácticas de prestación de servicios, la organización puede beneficiarse, por ejemplo, por estar preparada para absorber los volúmenes de transacciones adicionales o cuota de mercado.
- La ejecución de proyectos – La ejecución de proyectos con éxito trae funcionalidad de nuevos negocios.

Es importante mantener esta relación riesgo / beneficio en todas las decisiones relacionadas con el riesgo. Por ejemplo, las decisiones deben considerar la exposición que puede producirse si el riesgo no es tratado contra el beneficio si se trata o los posibles beneficios que pueden derivarse de las oportunidades que se toman frente a las prestaciones perdidas si las oportunidades son percibidas.

El marco de RISK IT está destinado a un público amplio, ya que la gestión de riesgos es una práctica global y un requisito estratégico en cualquier organización. El público objetivo incluye:
- Los principales ejecutivos y miembros del consejo que necesitan para establecer la dirección y seguimiento del riesgo a nivel de organización.
- Encargados de TI y de los departamentos de negocio que necesitan definir el proceso de la gestión de riesgos.
- Profesionales de la gestión de riesgos que necesitan la dirección específica en cuanto a los riesgos de TI.
- Las partes interesadas externas.

Podrá disponer de una orientación adicional en *The Risk IT Practitioner Guide* (que se resume en esta publicación, con un volumen más completo publicado por separado), en el que se incluyen ejemplos prácticos y metodologías, así como la vinculación entre RISK IT, COBIT y VAL IT.

El marco de RISK IT se basa en los principios de gestión de los riesgos organizacionales (ERM), las normas y marcos como COSO ERM[2] y AS/NZS 4360[3] (que pronto serán complementados o sustituidos por la norma ISO 31000), y provee información acerca de cómo aplicar estos principios a las TI. RISK IT aplica los conceptos generalmente aceptados de los principales estándares y marcos, así como los principales conceptos de la gestión de otros riesgos de TI, relacionados con las normas.

Sin embargo, la terminología utilizada por RISK IT, en ocasiones puede diferir de la utilizada en otras normas, así que para aquellos profesionales que están más familiarizados con las normas o marcos de gestión de riesgos, hemos proporcionado en la *Practicioner Guide* amplias comparaciones entre RISK IT y otras importantes normas de gestión de riesgos. RISK IT se diferencia de otros documentos existentes que tratan la gestión de los riesgos de TI en que se centra exclusivamente en la seguridad de TI ya que RISK IT cubre todos los riesgos de TI.

Aunque RISK IT se alinea con los principales marcos de ERM, la presencia y la aplicación de esos marcos no es requisito previo para la adopción de RISK IT. Mediante la adopción de RISK IT en las organizaciones se aplicarán automáticamente todos los principios de ERM. En el caso de que ERM esté presente de alguna forma en la organización, es importante aprovechar los puntos fuertes del programa de ERM existente ya que éste ayudará a la organización a la adopción de la gestión de riesgos, a ahorrar tiempo y dinero y a evitar los malentendidos acerca de los riesgos específicos de TI que pueden ocasionar un mayor riesgo en el negocio.

RISK IT se define y se basa en una serie de guías para la gestión eficaz de los riesgos de TI. Dichas guías se basan en los principios comúnmente aceptados en ERM, que se han aplicado en el ámbito de las TI. El modelo del proceso de los riesgos de TI está diseñado y estructurado para que las organizaciones puedan poner los principios en práctica y comparar sus resultados.

El marco de RISK IT se basa en los riesgos de TI. En otras palabras, el riesgo organizacional está relacionado con el uso de las TI. La conexión con la organización se basa en los principios en los que se construye el marco, es decir, el gobierno efectivo de la organización y gestión de los riesgos de TI, como se muestra en la **Figura 5:**

- Alinear siempre con los objetivos organizacionales.
- Alinear la gestión de las TI con el riesgo organizacional relacionado con el total de ERM.
- Balance de los costes y los beneficios de la gestión de los riesgos de TI.
- Promover la comunicación abierta y equitativa de los riesgos de TI.
- Establecer el tono correcto desde un enfoque de arriba abajo, definiendo y haciendo cumplir la responsabilidad del personal con los niveles de tolerancia aceptables y bien definidos.
- Son un proceso continuo y parte de las actividades diarias.

[2] Committee of Sponsoring Organizations (COSO) of the Treadway Commission, *Enterprise Risk Management—Integrated Framework*, USA, 2004, *www.coso.org*
[3] Standards Australia, AS/NZS 4360:2004, *Australian/New Zealand Standard for Risk Management*, Australia, 2004, *www.saiglobal.com*
[4] ISACA, *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, USA, 2008, *www.isaca.org*

Alrededor de estos bloques se ha creado, mediante la gestión de riesgos de TI, un modelo de proceso que les será familiar a los usuarios de COBIT y Val IT. Se facilitan guías sobre las actividades clave dentro de cada proceso, las responsabilidades para el proceso, los flujos de información entre los procesos y la gestión del rendimiento del proceso. El modelo se divide en tres ámbitos: gobernanza del riesgo, evaluación de riesgos y el riesgo de respuesta, cada uno con tres procesos:

- Gobierno del riesgos (GR)
  - RG1 Establecer y mantener una vista de riesgo común.
  - RG2 Integrar con ERM.
  - RG3 Tomar decisiones conscientes de los riesgos del negocio.
- Evaluación de riesgos (RE)
  - RE1 Recoger datos.
  - RE2 Analizar los riesgos.
  - RE3 Mantener perfil de riesgo.
- Respuesta de riesgos
  - RR1 Riesgo articulado
  - RR2 Manejar riesgos
  - RR3 Reaccionar a acontecimientos

La aplicación de mejores prácticas para la gestión de los riesgos de TI, como se describe en RISK IT, proporcionará beneficios tangibles de negocios, por ejemplo, un menor número de eventos inesperados y fracasos, el aumento de la calidad de la información, una mayor confianza de las partes interesadas, menos preocupaciones de carácter regulatorio y nuevas iniciativas para el negocio apoyadas por aplicaciones innovadoras.

El marco de RISK IT es parte de la cartera de productos de ISACA sobre el gobierno de TI aunque este marco se puede entender como un documento independiente, que incluye referencias a COBIT. La guía profesional expedida en apoyo a este marco hace amplia referencia a COBIT y Val IT y se recomienda que los gerentes y los profesionales puedan conocer los principales contenidos y principios de ambos marcos.

Al igual que COBIT y Val IT, RISK IT, es un marco, no una norma. Esto significa que las organizaciones pueden y deben personalizar los componentes previstos en el marco para adaptarlos a la organización y su contexto.

**Página en blanco intencionadamente**

# 2. MARCO DE RIESGOS DE TI – FINALIDAD Y DESTINATARIOS

### Riesgos de TI

Los riesgos de TI son un componente del universo de riesgos a los que está sometida una organización, como se muestra en la **figura 3**. Otros de los riesgos a los que una organización se enfrenta pueden ser riesgos estratégicos, riesgos ambientales, riesgos de mercado, riesgos de crédito, riesgos operativos y riesgos de cumplimiento. En muchas organizaciones, los riesgos relacionados con TI se consideran un componente de riesgo operativo, por ejemplo, el sector financiero en el marco de Basilea II. Sin embargo, incluso el riesgo estratégico de TI puede tener un componente financiero, especialmente en aquellas organizaciones en las que es el elemento clave de nuevas iniciativas empresariales. Lo mismo se aplica para el riesgo de crédito, donde una política pobre en cuanto a seguridad de la información se refiere, puede conducir a menores calificaciones de crédito. Por esta razón, es mejor no describir los riesgos de TI con una dependencia jerárquica en una de las categorías de riesgo, tal como se muestra en el ejemplo orientado a la industria financiera de la **figura 3**.

Figura 3 - Riesgos de TI en la jerarquía de riesgos


RISK IT es el riesgo comercial, es decir, el riesgo de los negocios asociados con el uso, la propiedad, la operación, la participación, la influencia y la adopción de las TI dentro de una organización. Se compone de eventos relacionados con IT que podrían afectar a la organización. Esto incluye tanto la frecuencia y la magnitud incierta, la creación de problemas en el cumplimiento de metas y objetivos estratégicos, así como la incertidumbre en la búsqueda de oportunidades. Los riesgos pueden clasificarse de varias formas:

- El valor de los riesgos de TI permitidos – Asociado con las oportunidades no aprovechadas para mejorar la eficiencia o efectividad de los procesos de negocio, o la capacidad de soportar nuevas iniciativas, a través del uso de la tecnología.
- Programas de TI y riesgos en las entregas de proyectos – Asociada a la contribución de IT sobre nuevas soluciones de negocio, generalmente en forma de proyectos y programas.
- Operaciones de TI y riesgos en las entregas de servicios – Asociadas con todos los aspectos relacionados con los servicios y sistemas de TI, los cuales puede producir pérdidas o reducción del valor a la organización.

Los riesgos relacionados de TI existen, independientemente de si son descubiertos o reconocidos por una organización. En este contexto es importante identificar y gestionar potencialmente los asuntos importantes de riesgo de TI, a diferencia del resto de riesgos, ya que éste puede no ser rentable.

### Propósito del marco de trabajo de riesgo de TI

La correcta gestión de los riesgos a los que está expuesta la organización es esencial para la correcta administración de cualquier organización. Casi todas las decisiones de negocio requieren que el los negocios requieren que la alta dirección o los gerentes sopesen los riesgos y los beneficios.

El uso común y general de las TI puede proporcionar importantes beneficios a una organización, pero también implica riesgos. Debido a su importancia para las organizaciones, los riesgos relacionados con TI deberían ser tratados como los demás riesgos claves organizacionales, tales como el riesgo del mercado, el riesgo de crédito y otros riesgos operativos. Dichos riesgos los podemos ubicar por debajo de la categoría más crítica de los riesgos en una organización: el hecho de no lograr los objetivos estratégicos del negocio. Si bien estos riesgos han sido incorporados a las organizaciones en los procesos de toma de decisión, muchos ejecutivos tienden a relegar los riesgos a los especialistas técnicos.

El marco de Riesgos de TI explica los riesgos y permite a los usuarios:
- Integrar la gestión de los riesgos en el ERM de la organización, esto permitirá que se tomen decisiones conscientes sobre el retorno de los riesgos.
- Tomar decisiones con conocimiento acerca de la magnitud del riesgo, el apetito de riesgo y la tolerancia al riesgo de la organización.
- Entender cómo responder a los riesgos.

En resumen, este marco permite a la organización adoptar las decisiones de riesgo apropiadas.

La práctica ha demostrado que la función de TI y los riesgos de TI a menudo no son bien comprendidos por las principales partes interesadas de una organización, entre ellos los miembros de la junta y la dirección ejecutiva. Sin embargo, estas son las personas que dependen de TI para alcanzar los objetivos estratégicos y operativos de la organización y, en consecuencia, deberían ser los 0responsables de la gestión de los riesgos. Sin una clara comprensión de la función y de los riesgos asociados a TI, los ejecutivos de alto rango no tienen un marco de referencia para priorizar y administrar los riesgos de TI.

Los riesgos de TI no son puramente una cuestión técnica. A pesar de que se necesita de expertos en la materia para entender y gestionar los aspectos de los riesgos de TI, el conocimiento sobre la gestión del negocio es lo más importante. Los gerentes del negocio han de determinar lo que se debe hacer para apoyar su negocio y establecer los objetivos de TI. Por consiguiente, son responsables de la gestión de los riesgos asociados. En RISK IT, la gestión del negocio incluye los roles o cargos corporativos, líderes del negocio y funciones de apoyo (director financiero [CFO], jefe de información [CIO], recursos humanos [HR], etc.)

El marco de RISK IT llena los huecos entre la gestión de los riesgos genéricos, como los marcos de COSO ERM y AS / NZS 4360, ISO 31000, el dominio británico ARMS5 y marcos de dominios específicos (por ejemplo, relacionados con la seguridad o en proyectos relacionados con la gestión). Proporciona de principio a fin, visión global de todos los riesgos relacionados con el uso de las TI y un tratamiento igualmente minucioso de la gestión del riesgo, desde el tono y la cultura hasta las cuestiones operativas. En resumen, el marco permitirá a las organizaciones entender y gestionar todos los tipos importantes de riesgos de TI.

El Marco provee de:

- Un marco de proceso de punta a punta para gestión de riesgos de TI correcta.
- Orientación para los profesionales, incluyendo herramientas y técnicas para entender y gestionar los riesgos concretos para las operaciones de negocio. Esto incluye una lista genérica de campo común, los panoramas relacionados con la TI potencialmente adversos del riesgo que podrían afectar la realización de los objetivos de negocio.

### El público y las partes interesadas

El público al que está dirigido el marco de RISK IT es muy amplio, ya que se ofrecen razones y beneficios para usar el marco por cada uno de los grupos en cuestión (figura 4). Todos los grupos citados en la figura 4 pueden ser considerados partes interesadas para la gestión de los riesgos de TI.

**Figura 4 - Público y Ventajas**

| Papel | Beneficios de/ Razones para usar el marco de riesgos de TI |
|---|---|
| Junta y Dirección Ejecutiva | Mejor comprensión de sus responsabilidades y funciones con respecto a la gestión de riesgos de TI. |
| Gestores de Riesgos | Asistencia con la gestión de los riesgos de TI, de acuerdo con la organización generalmente aceptados por los principios de la gestión de riesgos. |
| Administrador de los riesgos Operacionales | Marco de su vinculación con los riesgos de TI, la identificación de las pérdidas operativas o el desarrollo de los principales indicadores de riesgo. |
| Dirección de TI | Mejor comprensión de cómo identificar y gestionar los riesgos y la forma de comunicar los riesgos a la toma de decisiones de negocios |
| Directores de servicios de TI | Mejora de su punto de vista sobre los riesgos relacionados con TI, los cuales deberían encajar en el conjunto global del marco de trabajo de la gestión de riesgos de IT. |
| Administrador de la continuidad de negocio | La alineación con la organización de gestión de riesgos (desde la evaluación de riesgo es un aspecto clave de su responsabilidad) |
| Administrador de seguridad de TI | Posicionamiento de los riesgos de seguridad, entre otras categorías de riesgo de IT |
| CFOs | Obtener una mejor visión de los riesgos relacionados con TI y sus implicaciones financieras |
| Oficiales del gobierno organizacional | Asistencia con su examen y la supervisión de las responsabilidades de gobierno y otras funciones de gobierno de TI. |
| Directores ejecutivos | La comprensión y la gestión de los riesgos es uno de los muchos riesgos de negocios, todos los cuales deben ajustarse. |
| Los auditores de TI | Mejor análisis de riesgo en apoyo de los planes de auditoría e informes |
| Reguladores | Apoyo de su evaluación de las organizaciones reguladas “enfoque de gestión de riesgos de TI |
| Auditores externos | Orientación adicional sobre las tecnologías relacionadas con los niveles de riesgo cuando se crea una opinión |
| Aseguradores | Apoyo en el establecimiento de cobertura de seguro adecuada de TI y la búsqueda de un acuerdo sobre los niveles de riesgo |
| Las agencias de calificación | En colaboración con aseguradores; una referencia para evaluar objetivamente y la tarifa como una organización se ocupa de los riesgos |

### Beneficios y resultados

El marco de RISK IT aborda muchas cuestiones a las cuales las organizaciones se enfrentan hoy en día. Es notable su necesidad de:

- Una visión precisa del presente y del futuro próximo sobre los riesgos relacionados con TI en toda la organización y el éxito con el que la organización se ocupa de dichos riesgos.
- Orientación de principio a fin sobre la forma de gestionar los riesgos relacionados con TI, más allá de medidas puramente técnicas de control y de seguridad.
- Comprensión de cómo capitalizar una inversión realizada en un sistema de control interno de TI ya existente para gestionar los riesgos relacionados con TI.
- En cuanto a la evaluación y gestión de los riesgos de TI, la integración con el riesgo global y el cumplimiento de las estructuras dentro de la organización.
- Un marco/lengua común para ayudar a gestionar la relación entre los ejecutivos encargados de adoptar decisiones (o junta de los altos directivos), el director de información (CIO) y la organización de gestión del riesgo, o entre los auditores y la dirección.
- Promoción de la responsabilidad del riesgo y su aceptación en toda la organización.
- Un perfil de riesgo completo para mejor entender el riesgo y aprovechar mejor los recursos de la organización.

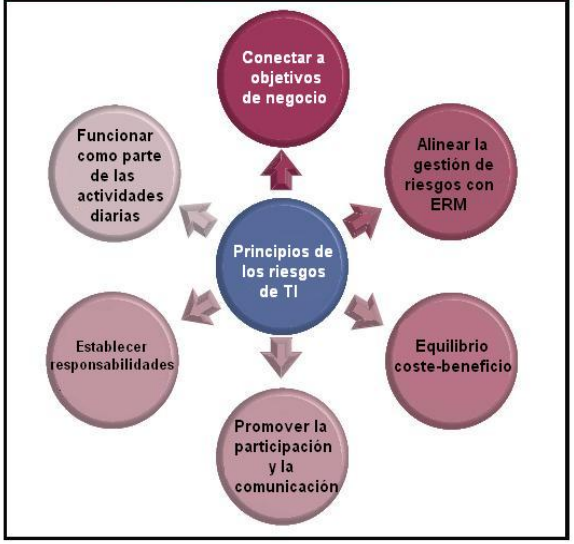
5 AIRMIC, ALARM, IRM, ‘A Risk Management Standard’, 2002, *www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf*

# 3. PRINCIPIOS DE LOS RIESGOS DE TI

RISK IT define, de manera fundamentada, una serie de guías para la gestión eficaz de los riesgos. Dichas guías son generalmente aceptadas sobre la base de los principios de la gestión del riesgo, que se han aplicado en el campo de las TI. El modelo de proceso de RISK IT está diseñado y estructurado para que las organizaciones puedan aplicar los principios en la práctica y comparar sus resultados.

El marco de RISK IT se refiere a los riesgos de TI - en pocas palabras, Los riesgos organizacionales relacionados con el uso de TI .La conexión con el negocio se fundamenta en los principios en los que se basa el marco, por ejemplo, un gobierno efectivo de la organización y la gestión eficaz de los riesgos de TI, tal y como se muestra en la **figura 5**:

Figura 5 - Principios de los riesgos de TI




- Siempre se alinea con los objetivos de la organización.
- Alinear la gestión de TI con el riesgo organizacional con ERM, por ejemplo ERM se aplica en la organización.
- Balance de los costos y beneficios de la gestión de los riesgos de TI.
- Promueve la comunicación abierta y justa de los riesgos de TI.
- Establece la definición y ejecución de las responsabilidades personales para el funcionamiento dentro de los niveles de tolerancia aceptables y bien definidos.
- ¿Es un proceso continuo y parte de las actividades diarias?

Cada uno de estos principios se examina a continuación con más detalle.

La eficaz gestión de la organización de los riesgos de TI siempre se alinea con los objetivos de la organización:

- El riesgo de TI es tratado como un riesgo de negocio, en contraposición a un tipo de riesgo, y el enfoque es integral y transversal;
- La atención se centra en los resultados del negocio. Apoya la consecución de los objetivos del negocio y los riesgos de TI se expresan en el impacto que pueden tener en el logro de los objetivos de la organización o la estrategia.
- Todo análisis de los riesgos de TI contiene una dependencia del análisis de cómo el negocio depende de la función de todas las capas subyacentes de la infraestructura de TI.
- La gestión de riesgos de TI es un instrumento de negocio, no un inhibidor. El riesgo de negocio relacionado con TI es visto desde ambos ángulos: protección contra destrucción de valor y generación de valor.

El gobierno eficaz de la organización con respecto a los riesgos de TI alinea la gestión de riesgos de relacionados con TI con el riesgo organizacional en general con ERM:

- Los objetivos de negocio y la cantidad de riesgo que la organización está dispuesta a asumir están claramente definidos.
- El proceso de toma de decisiones de la organización examina toda la gama de posibles consecuencias potenciales y oportunidades de los riesgos de TI.
- El apetito de riesgo de la entidad refleja su filosofía de gestión del riesgo e influencia en la cultura y en el tipo de funcionamiento (como se indica en el COSO Enterprise Risk Management-Integrated Framework).
- Los temas relativos a los riesgos están integrados en cada departamento de la organización, es decir, la visión del riesgo se comunica y expande a través de toda la estructura de la organización.
- Certificado de los controles suministrados.

El gobierno eficaz de la organización con respecto a los riesgos de TI equilibra los costos y beneficios de la gestión del riesgo:

- El riesgo es priorizado y dirigido en consonancia con el apetito del riesgo y la tolerancia.
- Los controles se llevarán a cabo con respecto a un determinado riesgos y en base a un análisis sobre el coste-beneficio del mismo. En pocas palabras, los controles no se implementan por el hecho de tener controles.
- Los controles existentes son aprovechados para hacer frente a múltiples riesgos o para hacer frente a los riesgos de manera más eficiente.

La dirección eficaz de los riesgos de TI promueve la comunicación abierta y justa de los riesgos de TI:

- La información abierta, exacta, oportuna y transparente sobre riesgos de TI sirve como la base para todas las decisiones relacionadas con el riesgo.
- Las tareas, principios y métodos de la gestión de riesgos se han integrado en toda la organización.
- Las conclusiones técnicas son traducidas en términos de negocio relevante y comprensible.

La gestión eficaz de los riesgos de TI establece el tono correcto definiendo y estableciendo las responsabilidades personales para el funcionamiento dentro de los niveles de tolerancia aceptables y bien definidos:

- Personas clave, p. e. personas influyentes, los dueños de negocios y el consejo de administración, se dedican a la gestión de riesgos de TI.
- Hay una asignación clara aceptación de la propiedad del riesgo, incluyendo la rendición de cuentas, haciendo la medición del rendimiento e integrando la gestión del riesgo en el sistema de recompensas. Las acciones a seguir son divulgadas desde el principio por medio de políticas, procedimientos y el correcto nivel de ejecución.
- La cultura del riesgo se promueve de manera activa, comenzando por las capas más altas. Esto ayuda a asegurar que aquellos implicados en la gestión de riesgos operacional funcionan sobre suposiciones de riesgo constantes.
- Las decisiones de riesgos se toman por personas autorizadas, con un enfoque en la gestión organizacional, que desempeña un papel clave en la gestión de los riesgos, por ejemplo, para las decisiones de inversión, la financiación de proyectos, los principales cambios de entorno de TI, evaluaciones de riesgo, y el seguimiento de los controles y pruebas.

La gestión eficaz de los riesgos promueve la mejora continua y es una parte de las actividades diarias:

- Debido a la naturaleza dinámica del riesgo, gestión de riesgos es un iterativo y perpetuo proceso en curso. Cada cambio conlleva riesgos y/o oportunidades, y la organización se prepara para ello, dando cuenta previamente a los cambios en la propia organización (fusiones y adquisiciones), en la regulación, en tecnologías de información, en el negocio, etc.
- Se presta atención a la evaluación del riesgo mediante métodos, funciones y responsabilidades, herramientas, técnicas y criterios en toda la organización.
  - -Identificación de los procesos clave y los riesgos asociados (la asignación de prioridad, que posee el perfil de riesgo)
  - -Conocimiento de los impactos en el logro de objetivos
  - -Identificación de los factores desencadenantes que indican cuándo una actualización del marco o de los componentes es necesaria.
- Las prácticas de gestión de riesgos están adecuadamente integradas en orden de prioridad y los procesos de toma de decisiones organizacionales.
- Las prácticas de gestión de riesgos son simples y fáciles de usar, y contienen las prácticas para detectar las amenazas y los riesgos potenciales, así como para prevenir y mitigar las mismas.

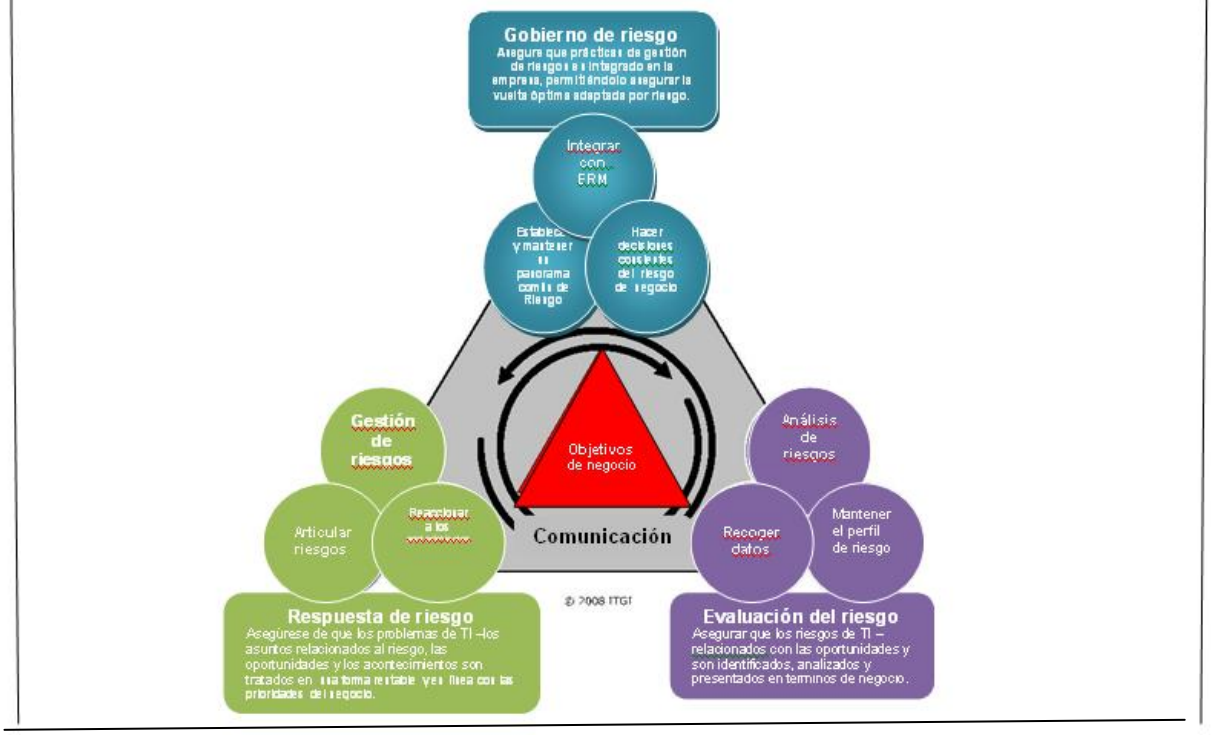
# 4. MARCO DE LOS RIESGOS DE TI

El marco de los riesgos de TI se basa en los principios establecidos en el capítulo 3 y se ha desarrollado en base a un modelo de proceso integral (figura 6).

El modelo del proceso en la gestión de riesgos fija ciertas actividades clave en una serie de procesos. Estos procesos se agrupan en tres ámbitos. El modelo del proceso resultará familiar a los usuarios de COBIT y Val IT: existen guías que ofrecen orientación sobre las actividades clave dentro de cada proceso, las responsabilidades para el proceso, los flujos de información entre los procesos y la gestión del rendimiento del proceso.

Los tres ámbitos del marco de RISK IT – Gobierno del riesgo, Evaluación del Riesgo y Respuesta ante el Riesgos – cada uno de los cuales contiene tres procesos, tal y como se muestra en la figura 6.

Figura 6 – Marco del riesgo de TI




Los siguientes capítulos contienen un número de prácticas y técnicas importantes para cada uno de los tres ámbitos del marco de RISK IT.

El modelo se explica con todos los detalles en el capítulo 11.

**Página en blanco intencionadamente**

# 5. FUNDAMENTOS DE GOBIERNO DEL RIESGO

Este capítulo trata sobre algunos de los componentes esenciales del dominio de Gobierno del Riesgo. Se discuten brevemente, ya que para más información y orientación práctica se puede consultar *The Risk IT Practitioner Guide*. Los temas relatados aquí incluyen:

- El apetito del riesgo y la tolerancia al riesgo
- Responsabilidades y rendición de cuentas sobre la gestión riesgos de TI
- Sensibilización y comunicación
- Cultura del riesgo

## Apetito de Riesgo y Tolerancia

***Definición COSO***

El Apetito del riesgo y la tolerancia son conceptos que se utilizan con frecuencia, aunque la posibilidad de malentendido es alta. Algunas personas utilizan indistintamente los dos conceptos, otros ven una clara diferencia. Las definiciones del marco de RISK IT son compatibles con las definiciones de
COSO ERM (que, a su vez, son equivalentes a las definiciones de la norma ISO 31000 en la guía 73):

- Apetito del riesgo - cantidad de riesgo que una organización u otra entidad está dispuesta a aceptar en el cumplimiento de su misión (o visión).
- Tolerancia del riesgo - La variación aceptable en relación a la consecución de un objetivo (y con frecuencia se mide mejor en las mismas unidades que las que se utiliza para medir los objetivos relacionados)

Ambos conceptos son introducidos en el modelo del proceso de riesgos de TI, en la principal gestión de prácticas RG1.2, RG1.3 y RG1.4 del proceso RG1 *Establish and maintain a common risk view*.

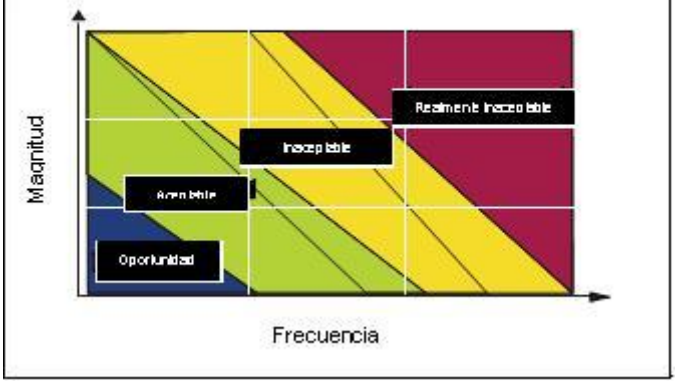
***Apetito del riesgo***

El apetito de riesgo es la cantidad de riesgo que una entidad está dispuesta a aceptar cuando se trata de alcanzar sus objetivos. Al examinar los niveles de apetito para la organización, surgen dos grandes factores importantes:

- La Capacidad Objetiva de la organización para absorber pérdida, p.e., pérdida financiera, daño de reputación
- La cultura o la predisposición a asumir riesgos-prudentes o agresivos. ¿Cuál es la cantidad de pérdida que la organización quiere aceptar llevar a cabo?

El apetito de riesgo se puede definir en la práctica en términos de combinaciones de la frecuencia y la magnitud de un riesgo.
El apetito de riesgo puede y va a ser diferente entre las organizaciones ya que no existe una norma absoluta o una norma de lo que constituye un riesgo aceptable e inaceptable

Figura 7: Mapa de Riesgo que Indica bandas del Apetito de Riesgo




El apetito por el riesgo se puede definir mediante los mapas de riesgo. Diferentes grupos de riesgo importancia se puede definir, indicado por las bandas de colores en el mapa de riesgo se muestra en la **figura 7.**

En este ejemplo se definen cuatro bandas de importancia
• Rojo - indica que realmente es un riesgo inaceptable. La organización estima que este nivel de riesgo es mucho más allá de su apetito de riesgo normal. Cualquier riesgo que se encuentren en esta banda podría desencadenar una respuesta inmediata de riesgos.

• Amarillo: indica riesgo elevado, es decir, también por encima de apetito de riesgo aceptable. La organización podría aceptarlo, como cuestión de política. Requieren mitigación u respuesta adecuada a definir dentro de los límites de tiempo determinado.

• Verde: indica un nivel aceptable normal de riesgo, normalmente con ninguna acción especial requerida, excepto el mantenimiento de los controles actuales o de otras respuestas.

• Azul -indicio de un riesgo muy bajo, donde el ahorro del costo de oportunidades se puede encontrar al disminuir el grado de control o donde las oportunidades para asumir más riesgos pueden surgir.

Este esquema de apetito de riesgo es un ejemplo. Cada organización tiene que definir sus propios niveles de apetito de riesgo y repasarlos de manera regular. Esta definición debería estar en la línea de la cultura de riesgos que la organización quiere expresar, p. ej., el riesgo contrario para arriesgar la toma o búsqueda de oportunidades. No hay ningún derecho universal correcto o erróneo, pero éste debe ser definido, bien entendido y comunicado. El apetito de riesgo y la tolerancia de riesgo deberían ser aplicados no sólo para arriesgar evaluaciones, sino que también para la toma de decisiones de riesgo de TI.

***Tolerancia al riesgo***

La tolerancia al riesgo es la desviación tolerable desde el nivel establecido por la definición del apetito de riesgo, por ejemplo, las normas o proyectos que deben realizarse dentro de los presupuestos y el tiempo, pero sobre costes del 10 por ciento del presupuesto o el 20 por ciento del tiempo son tolerados.

El apetito de riesgo y tolerancia al riesgo, la guía se aplica lo siguiente: Se aplica la siguiente orientación

- El apetito de riesgo y tolerancia al riesgo van de la mano La tolerancia de riesgos se define a nivel de organización y se refleja en las políticas establecidas por los ejecutivos, a un menor (táctico) los niveles de la organización, o en algunas entidades de la organización, las excepciones se pueden tolerar (o diferentes umbrales definidos), mientras en el nivel de la organización la exposición total no supere el apetito de riesgo establecidos. Cualquier iniciativa organizacional incluye un componente de riesgo, de modo de gestión deberían tener la posibilidad de conseguir nuevas oportunidades de riesgo. Las organizaciones en las que las políticas están labradas en piedra en lugar de "líneas en la arena" podría carecer de la agilidad y la innovación para aprovechar las oportunidades de negocio. Por el contrario, hay situaciones en que las políticas se basan en los requisitos específicos legales, reglamentarios o de la industria en los que conviene no tener la tolerancia de riesgo de incumplimiento.
- La tolerancia del riesgo se define a nivel de la organización por el consejo y claramente para comunicado todas las partes interesadas (ver el proceso de RG1 del riesgo que modelo de proceso). Un proceso debe ser en lugar de revisar y aprobar cualquier excepción a esas normas.
- • El apetito por el riesgo y la tolerancia a tiempo sobre el Cambio, de hecho, las nuevas tecnologías, nuevas estructuras organizativas, nuevas condiciones de mercado, la nueva estrategia de negocios y muchos otros factores que exigir a la organización a revisar su cartera de riesgo a intervalos regulares, y también exigir a la organización para volver a confirmar su riesgo el apetito a intervalos regulares, provocando exámenes de las políticas de riesgo. En este sentido, la organización también tiene que comprender que la mejor gestión del riesgo que tiene en su lugar, más riesgo se pueden tomar en la búsqueda de rentabilidad.
- 
- • El costo de las opciones de mitigación pueden afectar a la tolerancia al riesgo, de hecho, puede haber circunstancias donde el coste / impacto en el negocio de las opciones de mitigación de riesgos excede la capacidad de una organización / recursos, lo que obliga a mayor tolerancia para una o más condiciones de riesgo. Por ejemplo, si un reglamento dice que "los datos sensibles en reposo debe estar encriptada, sin embargo, no existe una solución de cifrado factible o el costo de la implementación de una solución tendría un gran impacto negativo, la organización puede optar por aceptar el riesgo asociado con la reglamentación de incumplimiento, que es una compensación del riesgo.

Capitulo 2 of *The Risk IT Practitioner Guide* discute el apetito del riesgo y tolerancia al riesgo en más detalle.

## Responsabilidades y rendición de cuentas sobre los riesgos de TI

En el cuadro en la figura 8 se definen una serie de funciones para la gestión del riesgo y se indica que estas funciones asumen la responsabilidad o rendición de cuentas por una o más actividades dentro de un proceso.

- La responsabilidad corresponde a aquellos que deben velar por que las actividades se han completado con éxito.
- La rendición de cuentas se aplica a quienes poseen los recursos necesarios y tener la autoridad para aprobar la ejecución y / o aceptar el resultado de una actividad específica dentro de los procesos de TI de riesgo. Esta tabla es un resumen de los cuadros detallados en el modelo de proceso.

Las funciones descritas en la tabla se aplican de manera diferente en cada organización y, por tanto, no corresponden necesariamente a las unidades de organización o funciones. Para ello, cada función ha sido descrita brevemente en el cuadro.

## Sensibilización y comunicación

La concienciación de los riesgos es de reconocer que el riesgo es una parte integral de la organización. Esto no implica que todos los riesgos que deben ser evitadas o eliminadas, sino que se entienden y conocen los riesgos de TI, problemas de riesgo sean identificables, y la organización reconoce y utiliza los medios de manejar los riesgos de TI

***Beneficios de comunicación y sensibilización***
Los beneficios de la comunicación abierta sobre los riesgos de TI incluyen:

- Contribución de la gestión ejecutiva para la comprensión de la actual exposición a los riesgos de TI, la definición de habilitación de riesgos apropiados y respuestas
- Sensibilización interna entre todas las partes interesadas de la importancia de la integración de riesgo y oportunidad en sus funciones diarias
- Transparencia para las partes interesados externas en el nivel real de riesgo y los procesos de gestión de riesgos en uso

Las consecuencias de la falta de comunicación incluyen:

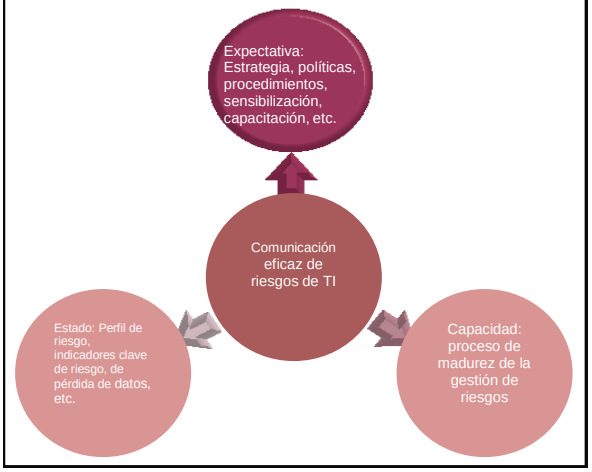
- Una falsa sensación de confianza en la parte superior en el grado de exposición real relacionados con IT, y la falta de un bien entendido sentido de la gestión de riesgos de arriba hacia abajo
- La sobre comunicación sobre el riesgo para el mundo exterior, sobre todo si está en riesgo o apenas un elevado nivel aceptable. Esto puede disuadir a posibles clientes o inversores, o generar un escrutinio innecesario de los reguladores.
- La percepción de que la organización está tratando de encubrir riesgos conocidos a los interesados

**Figura 8 -Responsabilidades y rendición de cuentas de los riesgos de TI**

| Definición de la función | | Gobierno del riesgo | | | Evaluación de riesgo | | | Respuesta de riesgo | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Función** | **Definición sugerida** | Vision común del riesgo | Integrar con ERM | Decisiones conscientes-riesgo | Recopilar datos | Análisis del riesgo | Mantener perfil del riesgo | Articular riesgo | Gestión de riesgos | Acontecimientos de riesgo |
| **Consejo** | El grupo de los más altos ejecutivos y / o no-ejecutivos de la organización que son responsables de la gestión de la organización y tener el control total de sus recursos. | ■ | ■ | | | | | | | |
| **(CEO) Director Ejecutivo** | El más alto rango oficial que se encarga de la gestión total de la organización | ■ | ■ | | | | | | ■ | |
| **(CRO) Responsable de riesgos** | Supervisa todos los aspectos de la gestión de riesgos en toda la organización. Un oficial de los riesgos, puede ser establecido para supervisar los riesgos relacionados con la TI | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| **(CIO) Responsable de TI** | El más alto funcionario de la organización que es responsable de TI para la promoción; la alineación de TI y las estrategias organizacionales y la planificación, la asignación de recursos y la gestión de la prestación de los servicios de TI, la información y el despliegue de los recursos humanos asociados. El CIO normalmente preside el consejo de gobierno que maneja la cartera. | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| **(CFO) Responsable Financiero** | El más alto funcionario de la organización que es responsable de la planificación financiera, el mantenimiento de registros, relaciones con los inversores y los riesgos financieros | ■ | | | | | | | | |
| **Comité de organización de riesgo** | El grupo de ejecutivos de la organización que son responsables de la organización a nivel de la colaboración y el consenso necesario para apoyar las actividades de gestión de riesgos y decisiones. Un consejo de los riesgos puede ser establecido para examinar los riesgos con más detalle y asesorar al comité de organización de | ■ | | ■ | | ■ | | ■ | | |
| **Gestión de organizacion** | Personas con funciones de negocio relacionadas con la gestión de (un) programa (s) | ■ | ■ | ■ | | ■ | ■ | ■ | ■ | ■ |
| **Propietario de procesos de negocio** | La persona responsable de la identificación de los requisitos del proceso, diseño y proceso de aprobación de la gestión de proceso de ejecución. En general, un proceso de negocio debe ser titular en un nivel suficientemente elevado en la organización y tener autoridad para comprometer recursos para el proceso específico de las actividades de gestión de riesgo. | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| **Funciones de control de riesgos** | Las funciones en la organización responsable de la gestión de los dominios específicos de riesgo (por ejemplo, el jefe de seguridad de la información oficial, la continuidad del negocio-plan de recuperación de desastres, la cadena de suministro, gestión de proyectos de oficina) | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| **(RH) recursos humanos** | El más alto funcionario de una organización que es responsable de la planificación y las políticas con respecto a todos los recursos humanos en esa organización. | ■ | | | | | | | | |
| **Cumplimiento y auditoría** | La función (s) en la organización responsable del cumplimiento y de auditoría | ■ | | | | | | | | ■ |

Leyenda de la tabla:
■ celda azul— El papel lleva la responsabilidad y / o la rendición de cuentas parcial para el proceso.
■ celda roja— El papel lleva la responsabilidad principal de este proceso. Sólo un papel puede ser la principal responsable de un determinado

Figura 9— Componentes de Comunicación de Riesgos de TI




***La comunicación de riesgos -¿Qué Comunicar?***
La comunicación de riesgos de TI abarca una amplia gama de flujos de información.
Los riesgos de TI se distinguen entre los siguientes tipos principales de comunicación
de riesgos de TI, como se muestra en la **Figura 9:**

- Información sobre las expectativas de la gestión del riesgo: estrategia de riesgo, políticas, procedimientos, capacitación de sensibilización, el refuerzo continuo de los principios, etc. Esta es la comunicación esencial en la estrategia general de la organización hacia los riesgos de TI, y conduce todos los esfuerzos posteriores sobre la gestión del riesgo. En él se establecen las expectativas generales de la gestión de riesgos.
- Información sobre la actual capacidad de gestionar riesgos. Este control de la información permite saber el estado del motor de la gestión de riesgos en la organización, y es un indicador clave para la buena gestión de riesgos.
- Tiene un valor predictivo de lo buena que será para la organización la gestión del riesgo y la reducción de la exposición. La información sobre la situación real con respecto al riesgo del TI. Éste incluye la información por ejemplo:

- El perfil de riesgo de la organización, p. ej. la cartera total de riesgos (identificados) a los cuales la organización está expuesta.
- KRIS para apoyar la gestión de información sobre el riesgo
- Datos de eventos de pérdida
- La Causa de origen de los eventos de pérdida
- Opciones para mitigar los riesgos (el coste y ventajas)

Para ser eficaz, la información que fluye dentro de estas tres ramas de la comunicación debe ser siempre:

- Clara – Conocida y comprendida por todas las partes interesadas
- Concisa – La información o comunicación no debe inundar a los receptores. Todas las reglas de una buena comunicación se aplican a la comunicación del riesgo.
- Útil – cualquier comunicación sobre el riesgo debe ser pertinente. La información técnica que es demasiado detallada y / o se envía a partes inadecuadas dificultan, en lugar de permitir una visión clara de riesgo.
- Oportuna – en cada riesgo existen momentos críticos desde su origen y sus posibles consecuencias. Por ejemplo, un riesgo puede originarse cuando se crea una inadecuada organización de TI, y la consecuencia es una organización ineficiente en la prestación de servicios de TI. Otro ejemplo, el punto de origen puede ser el fracaso del proyecto, y el consiguiente retraso de las iniciativas organizacionales. Mediante una oportuna comunicación se permite que las medidas que deben adoptarse en los momentos adecuados para identificar y tratar el riesgo. Que no tiene ninguna utilidad para comunicarse proyecto demora de una semana antes de la fecha límite.
- Dirigida a la audiencia correcta – La información debe ser comunicada en el nivel de agregación, adaptada para el público y permitir decisiones informadas. Por ejemplo, un agente de seguridad será informado de las necesidades de TI de datos técnicos sobre las intrusiones y los virus para implementar soluciones mientras que un comité directivo de TI no necesita este nivel de detalle, pero sí necesita otra información con el fin de decidir sobre cambios de política o de los presupuestos adicionales para tratar el mismo riesgo.
- Disponible – para conocer la base del riesgo de TI, la información relacionada debe ser conocida y comunicada a todos las Partes con una necesidad real, un registro de riesgos con todos los riesgos documentados no es información pública y debe estar debidamente protegidos contra las partes internas y externas sin necesidad de ella.

La comunicación no necesita siempre ser formal, a través de informes escritos o de mensajes. Las reuniones cara a cara oportunas entre los tenedores de apuestas son apenas medios de una comunicación importantes para la información Él-riesgo-relacionada.

***La comunicación de riesgos – Las partes interesadas***
En la tabla **la Figura 10** proporciona una visión general rápida de los canales de comunicación más importantes para la gestión del riesgo eficaz y eficiente. Intención de la tabla es proporcionar una visión general de la página principal de la comunicación sobre los flujos de los riesgos de TI que debe existir en una forma u otra en cualquier organización. Más información detallada, por ejemplo, el origen y el destino de la información, se puede encontrar en el riesgo que las descripciones del proceso, en la entrada y tablas de salida. Este cuadro se centra en la información más importante que cada interesado debe procesar.

**Figura 10—Riesgo de flujos de comunicación**

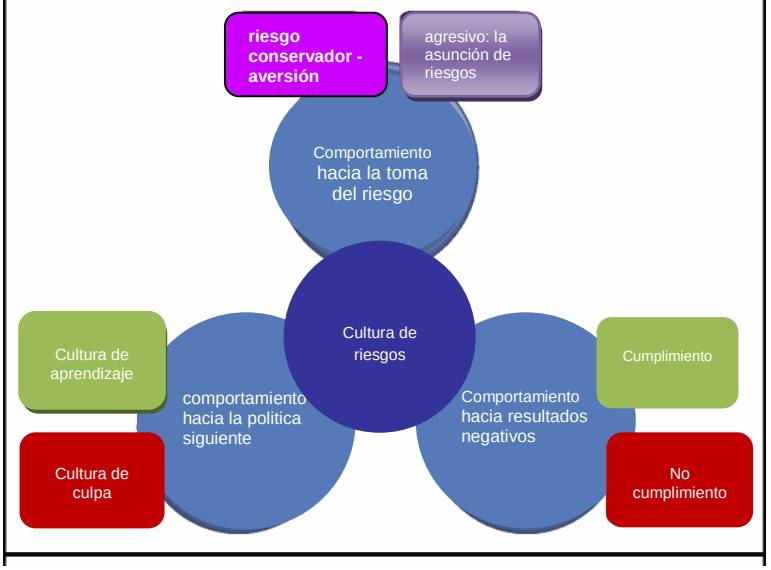
| Entrada | Partes interesadas | Salida |
|---|---|---|
| • Resumen ejecutivo de los informes de riesgo<br>• Exposición de corriente de riesgo / perfil<br>• KRIs | La dirección ejecutiva y de consejo | • Apetito del riesgo organizacional<br>• Objetivos claves de rendimiento<br>• Los riesgos gráficos RACI<br>• Políticas de riesgo,<br>• expresando la tolerancia de la gestión de riesgos<br>• Expectativas de conciencia de riesgo<br>• Cultura de riesgo |
| • Plan alcance y dirección de riesgos de TI<br>• Registro de riesgos de TI<br>• Resultados de análisis de riesgos<br>• Integrado / informe agregado de riesgos de TI<br>• KRIs<br>• Solicitud de análisis de riesgo | CRO y comité de riesgo de organización | • Apetito del riesgo organizacional<br>• la exposición a riesgos residuales<br>• Información de riesgo operacional : exposiciones residuales |
| • Apetito organizacional de los riesgos de TI<br>• Plan alcance y dirección de riesgos de TI<br>• Objetivos claves de rendimiento<br>• Los riesgos gráficos RACI<br>• Metodología de evaluación de riesgos de TI<br>• Registro de riesgos de TI | CIO Responsable de Informática | • la exposición a riesgos residuales<br>• Información de riesgo operacional<br>• Impacto de los riesgos de TI sobre las organizaciones y las unidades de negocio afectadas<br>• Los cambios en curso a los factores de riesgo (amenazas) |
| • Objetivos clave de rendimiento | CFO Director Financiero | • información financiera con respecto a TI y los programas / proyectos (presupuesto, real, tendencias, etc.) |
| • Alcance y dirección de riesgos de TI<br>• Planes para la organización en curso y la comunicación de riesgos de TI<br>• Cultura de riesgo<br>• Impacto de los riesgos de TI sobre las organizaciones y las unidades de negocio afectadas<br>• Los cambios en curso a los factores de riesgo | Gestión organizacional y propietarios de los procesos de negocio | • Control y supervisión de cumplimiento<br>• Solicitud de análisis de riesgo |
| • Objetivos clave de rendimiento<br>• Plan de acción riesgos de TI<br>• Metodología de evaluación de riesgos de TI<br>• Registro de riesgos de TI<br>• Cultura de riesgo | La administración de TI (incluyendo la seguridad, la gestión de los servicios) | • la exposición a riesgos residuales |
| • Objetivos clave de rendimiento<br>• Los riesgos gráficos RACI<br>• Plan y dirección de riesgos de TI<br>• Control y supervisión de cumplimiento | Cumplimiento y auditoría | • Conclusiones de la auditoría |
| • Objetivos clave de rendimiento<br>• Acción del plan de riesgos de TI<br>• Metodología de evaluación de riesgos de TI<br>• Registro de riesgos de TI<br>• Resultados de Auditoría | Funciones de control de riesgos | • Requisitos para los controles y presentación de Informes<br>• Resumen de conclusiones sobre el riesgo |
| • Expectativas de conciencia de riesgo<br>• Cultura de riesgo | Recursos humanos (HR) | • Los riesgos potenciales<br>• Apoyo sobre iniciativas de conciencia de riesgo |
| • Control y supervisión de cumplimiento | Auditores externos | • Conclusiones de la auditoría |
| • La opinión pública, la legislación<br>• Riesgo informe resumen ejecutivo<br>• En general, todas las comunicaciones destinados a la junta directiva y la dirección ejecutiva | Reguladores | • Requisitos para la presentación de informes y controles<br>• Resumen de conclusiones sobre el riesgo |
| • Resumen Ejecutivo los informes de riesgo | Inversores | • Niveles de riesgo de tolerancia para su cartera de inversiones |
| • Resumen de los informes de riesgo, incluyendo riesgo residual, el riesgo para los principales activos, controles de niveles de madurez, las conclusiones de la auditoría | Asegurador | • La cobertura del seguro (la propiedad, interrupción de negocios, D & O) |
| • Expectativas de conciencia de riesgo<br>• Cultura de riesgo | Todos los empleados | • Asuntos potenciales de los riesgos de TI |

## Cultura de Riesgos

La gestión de riesgos consiste en ayudar a las organizaciones a asumir mayores riesgos en la búsqueda de la rentabilidad. Una cultura de riesgos asumidos ofrece un entorno en el que los componentes de riesgo se discuten abiertamente, y los niveles de riesgo aceptables se entienden y se mantienen. La cultura de riesgos aceptables comienza en la parte superior, con la junta y los ejecutivos de negocios que establece la dirección, comunicando el riesgo de toma de decisiones aceptables y premiando la cultura de aprendizaje en la gestión eficaz del riesgo. El conocimiento del riesgo también implica que todos los niveles dentro de una organización son conscientes de cómo y por qué para responder a los eventos adversos de TI.

La cultura del riesgo es un concepto que no es fácil de describir. Se compone de una serie de comportamientos, como se muestra en la **figura 11.**

Figura 11—Elementos de la cultura de riesgo




La cultura del riesgo incluye:

- El comportamiento hacia la toma del riesgo - ¿Cuál es el
- grado de riesgo que siente la organización que puede asumir
- y qué riesgos está dispuesta a tomar?
- El comportamiento hacia la política siguiente - ¿En qué
- medida la gente va a aceptar y / o cumplir con la política?
- El comportamiento hacia resultados negativos – ¿Cómo la organización se ocupa de los resultados negativos, es decir, acontecimientos de pérdida u oportunidades perdidas? ¿Aprenderá ellos de esto y tratarán de adaptarse, o se culpará sin tratar la causa de origen?

Algunos de los síntomas de una cultura inadecuada del riesgo o problemáticos son:

- La desalineación entre el actual apetito de riesgo y las políticas traducidas, La verdadera posición de la dirección hacia el riesgo puede ser razonablemente
- agresivos y la asunción de riesgos, mientras que las políticas que se crean reflejan una actitud mucho más estricta.
- La existencia de una "Cultura de culpa". Este tipo de cultura debe por todos los medios ser evitada, ya que este es el inhibidor la comunicación relevante y eficaz. En una cultura de culpa, las unidades de negocio tienden a señalar con el dedo a los proyectos de TI, cuando no son entregados a tiempo o no cumplen las expectativas. Al hacerlo, no se dan cuenta de cómo la participación de la unidad de negocio desde el principio afecta el éxito del proyecto. En casos extremos, la unidad de negocio puede asignar la culpa de la incapacidad de satisfacer las expectativas. El 'juego de la culpa "sólo perjudica la comunicación efectiva a través de las unidades, alimentando aún más las demoras. El liderazgo ejecutivo debe identificar y controlar rápidamente una cultura de la culpa si la colaboración se debe fomentar en toda la organización.

# 6. FUNDAMENTOS DE LA EVALUACIÓN DE RIESGOS

En este capítulo, unos pocos componentes esenciales del dominio de evaluación de riesgos se discuten brevemente. Más información y orientación práctica se puede encontrar en *The Risk IT Practitioner Guide*. Los temas discutidos aquí incluyen:

- Descripción del impacto de la organización
- Escenarios de riesgo

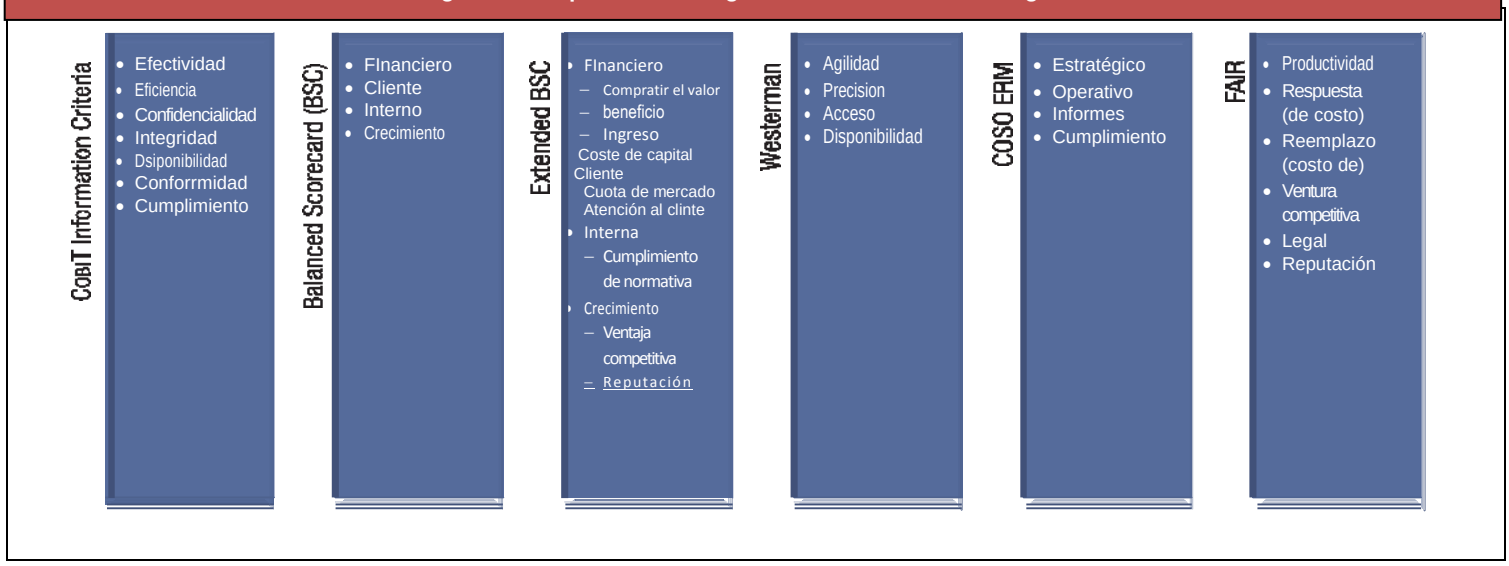
## Descripción del impacto de la organización

La evaluación significativa de riesgos de TI y el riesgo - de decisiones basadas en los riesgos de TI requieren ser expresadas en términos inequívocos y claros relevantes de negocios. La gestión efectiva del riesgo requiere de la comprensión mutua entre TI y el negocio sobre el que el riesgo debe ser gestionado y por qué. Todas las partes interesadas deben tener la capacidad de comprender y expresar cómo los eventos adversos pueden afectar a los objetivos de negocio. Esto significa que:

- Una persona de TI debe comprender como – Los fallos relacionados o acontecimientos relacionados con TI pueden afectar a los objetivos de la organización y causar perdida directa o indirecta a la organización
- Una persona de negocios deben entender cómo – Los Fallos o eventos relacionados con TI pueden afectar a los servicios y procesos clave.

El vínculo entre la TI y el impacto de escenarios de riesgo organizacional fundamental debe ser establecido para comprender los efectos de los eventos adversos. Varias técnicas y opciones existen que pueden ayudar a la organización para describirlo en términos de riesgos de negocios. El marco de riesgos de TI requiere riesgos para la traducir o expresado en términos pertinentes con la organización, pero no prescribe ningún método único. Algunos métodos disponibles se muestran en la **figura12** y se discuten brevemente en lo que resta de esta sección. Para más detalles sobre los métodos descritos en la **figura 12** y orientación sobre cómo aplicarlas en la práctica se incluyen en la Guía Profesional de riesgos de TI.

**Figura 12 - Expresando Riesgos de TI en términos de negocio**




***Criterios de información COBIT (requisitos de información de negocios)***
Los criterios de información de COBIT permite la expresión de los aspectos comerciales relacionados con el uso de TI. Expresan una condición para que la información (en el sentido más amplio), según lo previsto través de TI, debe ajustarse para que sea beneficiosa para la organización.

El impa cto en el negocio de cualquier TI – eventos, relacionados se encuentra en la consecuencia de no alcanzar los criterios de información. Mediante la descripción de impacto en estos términos, esto sigue siendo una especie de técnica intermedia, no una descripción completa del impacto de negocios, por ejemplo, el impacto sobre los clientes o en términos financieros.

***Los objetivos de negocios Cobit y el balanced scorecard***
Otra técnica se basa en el concepto de "objetivos de negocio", introducida en COBIT. De hecho, el riesgo de negocio se encuentra en cualquier combinación de los objetivos de negocio que no se alcance. Los objetivos de negocio COBIT se estructuran de acuerdo con la tarjeta de puntuación equilibrada Clásicas (BSC) perspectivas: los clientes, financieros, internos y el crecimiento.

***Criterios extendidos BSC***
Una variante del método descrito en la sección anterior, COBIT Objetivos de Negocios y Balanced Scorecard, va un paso más allá, vinculando las dimensiones del BSC a un conjunto más limitado de criterios tangibles. El conjunto de los criterios descritos en la **Figura 12** se puede utilizar de forma selectiva, y el usuario debe ser consciente de que todavía existen relaciones de causa-efecto, en este cuadro (por ejemplo, la satisfacción de los clientes puede afectar la ventaja competitiva y / o participación de mercado). Por lo general un subconjunto de estos criterios se utilizan para expresar el riesgo en términos de negocio.

***Westerman 4 'A'-un enfoque alternativo para expresar el impacto de la organización***
Un cuarto medio de expresión de los riesgos de TI en términos de negocio se basa en el 4A framework[6], que define el riesgo como el potencial de participación de un acontecimiento imprevisto para amenazar cualquiera de los cuatro objetivos de las organizaciones relacionadas entre sí:
- Agilidad - Dispone de la capacidad de cambiar con gestionados costo y la velocidad.
- Precisión - Provee adecuada, información puntual y completa que cumple con los requisitos de gestión, personal, clientes, proveedores y reguladores
- Acceso - Garantizar el acceso adecuado a datos y sistemas, de modo que las personas indicadas tengan el acceso que ellos necesitan y las no indicadas no lo tengan.
- Disponibilidad - mantener los sistemas (y los procesos de su negocio) en funcionamiento, y las interrupciones recuperarse.

***COSO ERM***
COSO *Enterprise Risk Management—Integrated Framework* las listas de los siguientes criterios:
- Estrategia - Alto- nivel de objetivos, alineados con y apoyando la misión de la organización. Los objetivos estratégicos reflejan la opción de la dirección en cuanto a como la organización procurará crear el valor para sus partes interesadas
- Operaciones: Estos se refieren a la eficacia y eficiencia de las operaciones de la organización, incluidos los objetivos de rendimiento y la rentabilidad y la protección contra la pérdida de los recursos.
- Informes: Estos se refieren a la fiabilidad de la información. Estos incluyen la presentación de informes internos y externos y podrá financieros implican y la información no financiera
- Cumplimento - se refieren a la adhesión de las leyes y reglamentos

***Conveniente***
El método de seguridad es conveniente -se orienta en origen, pero los criterios del impacto se aplican a todos los riesgos relacionados con TI.

## Escenarios de riesgos de TI

Uno de los desafíos para la gestión de riesgos de TI debe identificar los riesgos importantes y relevantes entre todo lo que posiblemente puede relacionarse con TI, considerando la presencia y dependencia de TI en el negocio. Una de las técnicas para vencer este desafío es el desarrollo y el empleo de argumentos de riesgo, Es un enfoque básico para lograr el realismo, visión, compromiso organizacional, mejorar el análisis y la estructura de la compleja cuestión de los riesgos de TI

Una vez que se desarrollan estos escenarios, que se utilizan durante el análisis de riesgo, donde la frecuencia de la situación realmente está sucediendo y los impactos comerciales son estimaciones.

**La Figura 13** muestra que los escenarios de riesgo se pueden derivar a través de dos mecanismos diferentes:
- Un enfoque de arriba abajo, en el que se parte de los objetivos generales y se realiza un análisis de los escenarios de riesgos de TI más relevantes y probables que impacten len os objetivos de negocio. Si los criterios de impacto están bien alineados con los controladores de valor real de la organización, los escenarios de riesgo relevantes se desarrollarán.
- Un enfoque de abajo arriba, en el que se utiliza una lista de escenarios genérico para definir un conjunto de escenarios más concretos y personalizados, aplicados a la situación de la organización individual

Los enfoques son complementarios y deben ser utilizados simultáneamente. De hecho, los escenarios de riesgo deben ser pertinentes y deben estar vinculados con el riesgo real de negocio. Por otra parte, utilizar un conjunto de escenarios de riesgo genérico ayuda a asegurar que no se pasan por alto los riesgos y proporciona una visión más amplia y completa sobre los riesgos de TI.

Una vez que el conjunto de escenarios de riesgo se define, puede ser utilizado para el análisis de riesgos, donde se evalúa la frecuencia y el impacto del escenario. Un componente importante de esta evaluación son los factores de riesgo, como se muestra en la **figura 13.**

Los factores de riesgo son aquellos factores que influyen en la frecuencia y / o impacto en el negocio de los escenarios de riesgo, ya que pueden ser de diferente naturaleza, y se pueden clasificar en dos categorías principales:
- Factores ambientales: estos se pueden dividir en factores internos y externos, diferenciándose en el grado de control que una organización tiene sobre ellos:
  - Factores internos del medio ambiente están, en gran medida, bajo el control de la organización, aunque no siempre sea fácil de cambiar.
  - Factores externos del medio ambiente están, en gran medida, fuera del control de la organización.

- Capacidades - Lo buena que es una organización en las actividades relacionadas con TI. Pueden distinguirse según los tres marcos principales de ISACA:
  - Capacidades de gestión de riesgos de TI-¿En qué medida es la organización madura en el desempeño de la gestión del riesgo de los procesos definidos en el marco de RISK IT?
  - Capacidades de TI-¿Cuán buena es la organización realizando los procesos de TI definidos en COBIT?

[6]Westerman, G.; R. Hunter; 'IT Risk—Turning Business Threats Into Competitive Advantage', Harvard Business School Press, USA, 2007

-Capacidades de negocio relacionadas con TI (o gestión de valor) - ¿Cómo se alinean las actividades de gestión de valor de la organización con las expresadas en los procesos de Val IT?

Los factores de riesgo también se pueden interpretar como factores causales de la situación que se ha materializado, como vulnerabilidades o debilidades. Estos son términos que a menudo se utilizan en otros marcos de gestión de riesgos.

**Figura 13 - Desarrollo de escenarios de riesgo de TI**

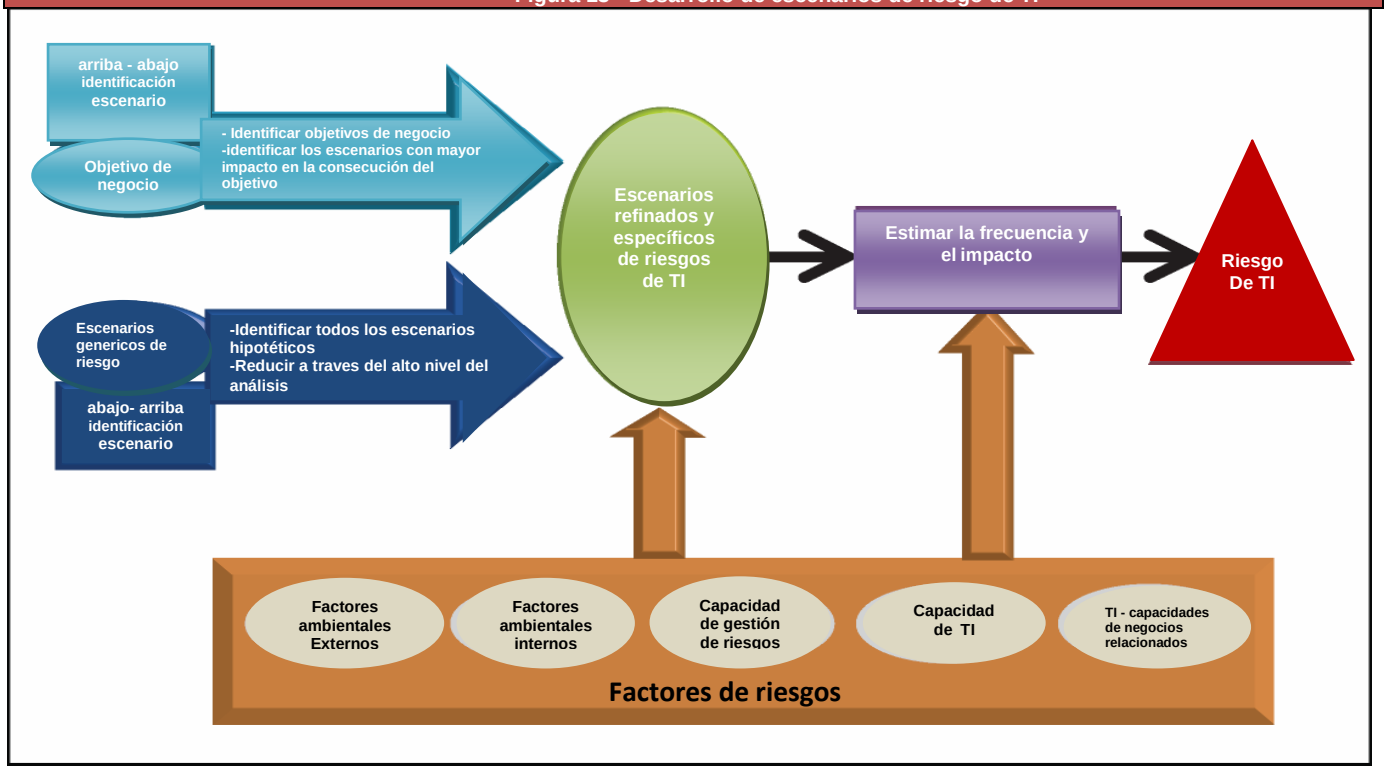



**Figura 14 – Componentes de escenario de riesgo**

Un escenario de riesgo es la descripción de un evento relacionado con TI que puede conducir a un impacto en el negocio. Para que los escenarios de riesgo sean completos y se puedan utilizar en análisis de riesgos, deben contener los siguientes componentes, que se muestran en la **Figura 14:**

- Actor que genera la amenaza - Los actores pueden ser internos o externos y puede ser humano o no humano:
  – Los actores internos están dentro de la organización, por ejemplo, personal, contratistas.
  – Los agentes externos son extraños, competidores, reguladores y el mercado.

No todo tipo de amenaza exige un actor, por ejemplo, fallas o causas naturales.

- Tipo de amenaza - La naturaleza del evento. ¿Es malintencionado? Si no ¿es accidental? o ¿Es un fracaso de un proceso bien definido? ¿Es un evento natural (fuerza mayor)?
- Evento - Un escenario siempre tiene un evento. ¿Es una revelación (de la información confidencial), la interrupción (de un sistema, un proyecto), la modificación, robo, destrucción, etc.? También incluye el diseño ineficaz (de los sistemas, procesos, etc.), la ejecución ineficaz de los procesos (por ejemplo, cambiar los procedimientos de gestión, los procedimientos de adquisición, los procesos de priorización de proyectos), (impacto de la regulación) y el uso inadecuado.
- Activo - recurso sobre el cual el escenario actúa - Un activo es cualquier objeto de valor de la organización que puede ser afectado por un evento y crear un impacto en el negocio. Un recurso es cualquier cosa que ayude a lograr los objetivos de TI. Los bienes y recursos pueden ser idénticos, por ejemplo, los equipos informáticos son un recurso importante porque todas las aplicaciones de IT los utilizan y son un activo porque tienen un valor a la organización. Activos / recursos incluyen:
  – La gente y la organización
  – Los procesos de TI, por ejemplo, el modelo como COBIT o Val de los procesos de TI, o de los procesos de negocio
  – La infraestructura física, por ejemplo, instalaciones, equipos
  – La infraestructura de TI, incluyendo el hardware de computación, infraestructura de red, middleware
  – Los demás componentes de la arquitectura de la organización, incluyendo:
- Información
- Aplicaciones

El activo puede ser crítico o no, p. ejemplo, un sitio web cliente de un banco principal comparado al sitio web del garaje local o la intranet del grupo de desarrollo de software. Los recursos críticos probablemente atraerán un mayor número de ataques o mayor atención en caso de fallo, de ahí que la frecuencia de los escenarios relacionados probablemente sea mayor. Se necesita habilidad, experiencia y profundo conocimiento de las dependencias para entender la diferencia entre un activo crítico y un activo crítico.

- Planificación del tiempo, que podría definir lo siguiente, si es relevante para el escenario:
  -La duración del evento (corte de energía prolongado de un servicio o centro de datos)
  -El tiempo (¿Ocurre el acontecimiento en un momento crítico?)
  -Tiempo transcurrido entre el evento y la consecuencia. ¿Hay una consecuencia inmediata, por ejemplo, insuficiencia de la red?
  -¿Tiempo de inactividad de inmediato, o una consecuencia retardada, por ejemplo, mala arquitectura de TI con los altos costos acumulados durante un lapso de tiempo de varios años?.

La estructura del escenario de riesgo se diferencia por los eventos de pérdida (la generación de eventos de los efectos negativos), la vulnerabilidad de los eventos (acontecimientos que contribuyen a la magnitud o frecuencia de eventos de pérdida que ocurren), y eventos de amenaza (circunstancias o eventos que pueden desencadenar eventos de pérdida). Es importante no confundir estos riesgos o incluirlos en una lista de grandes riesgos.

*The Risk IT Practitioner Guide* contiene una amplia orientación sobre cómo construir conjuntos pertinentes y manejables de escenarios de riesgos de TI, e incluye una lista de ejemplos de escenarios de riesgo.

# 7. FUNDAMENTOS DE LA RESPUESTA DE RIESGO

En este capítulo, algunos componentes esenciales del dominio de respuesta a los riesgos se discuten brevemente. Más información y orientación práctica se puede encontrar en *The Risk TI Practitioner Guide.* Los temas discutidos aquí incluyen:

- RIESGO
- Definición de respuesta de riesgo y priorización

## Principales indicadores de riesgo

Los indicadores de riesgos métricos son capaces de demostrar que la empresa está sujeta a, o tiene una alta probabilidad de, estar sometida a un riesgo que excede del apetito de riesgo definido. Son específicos para cada empresa y su selección depende de una serie de parámetros en el entorno interno y externo, tales como el tamaño y la complejidad de la empresa, si se trata de operar en un mercado altamente regulado y su objetivo de estrategia. La identificación de indicadores de riesgo debe tener en cuenta los siguientes pasos (entre otros):

• Considerar las distintas partes interesadas en la empresa. Los indicadores de riesgos deben no sólo centrarse en las operaciones o en la parte estratégica de riesgo. Pueden y deben ser identificados para todas las partes interesadas. La participación de los interesados adecuados en la selección de indicadores de riesgo también deberá garantizar una mayor aportación y adecuación de los mismos.

• Hacer una selección equilibrada de indicadores del riesgo, cubriendo Indicadores de los resultados (indicando el riesgo después de que hayan ocurrido los hechos), Indicadores principales (lo que indica que las capacidades están en el lugar apropiado para evitar que se produzcan acontecimientos) y las tendencias (análisis de indicadores en el tiempo o la correlación de los indicadores para obtener información)

• Asegurar que los indicadores seleccionados detallen el origen de la causa de los eventos (indicación del origen y no solo los síntomas)

Una empresa puede desarrollar un amplio conjunto de métricas para servir como indicadores de riesgo, sin embargo, no es posible o factible sostener un conjunto completo de indicadores como indicadores clave de riesgo (RISK). Los RISK se distinguen por ser de gran relevancia, por poseer una alta probabilidad de predecir o por que indican un riesgo importante. Los criterios para seleccionar RISK incluyen:

- Impacto: los indicadores de riesgo con alto impacto comercial son más propensos a ser RISK.
- Esfuerzo para aplicar, medir y reportar: Los indicadores diferentes que son equivalentes en la sensibilidad, el criterio debe ser la facilidad.
- Fiabilidad: el indicador debe poseer una alta correlación con el riesgo y ser un buen vaticinador o medida de resultado.
- Sensibilidad: el indicador debe ser representativo para el riesgo y capaz de indicar con precisión las diferencias en el riesgo.

Para ilustrar la diferencia entre la fiabilidad y la sensibilidad en la lista anterior, si tomamos como ejemplo un detector de humo, fiabilidad significa que el detector de humo hará sonar una alarma cada vez que haya humo. Sensibilidad significa que el detector de humo suena cuando se alcanza un determinado umbral de densidad de humo.

El juego completo de RISK también debe equilibrar los indicadores de los riesgos y causas fundamentales así como el impacto comercial.

La selección de un conjunto adecuado de RISK proporcionará los siguientes beneficios a la empresa:

- Proporcionar una alerta temprana (con mira al futuro): Señal de que un alto riesgo está surgiendo para permitir a la administración adoptar medidas proactivas (antes de que el riesgo se convierte en una pérdida).
- Proporcionar una opinión retrospectiva sobre los acontecimientos de riesgo que han ocurrido, permitiendo respuestas de riesgo y la gestión de su mejora.
- Facilitar la documentación y el análisis de las tendencias.
- Proporcionar indicadores a la empresa del apetito de riesgo y la tolerancia a través de la configuración métrica (es decir, los umbrales de KRI).
- Aumentar la probabilidad de lograr los objetivos estratégicos de la empresa.
- Ayudar continuamente a la optimización de la gestión del riesgo y del entorno.

Algunos desafíos comunes que surgen en la definición de RISK son:

- RISK. Los riesgos específicos no están vinculados.
- RISK son a menudo incompletos o inexactos en la especificación, es decir, demasiados genéricos.
- Existe una falta de alineación entre el riesgo, la descripción KRI y la métrica KRI.
- Hay demasiados RISK.
- Son difíciles de medir.
- Es difícil agregar, comparar e interpretar RISK de manera sistemática a nivel empresarial.

Del mismo modo que el ambiente interno y externo de la empresa está cambiando constantemente, el ambiente de riesgo es también altamente dinámico y el sistema de RISK necesita ser cambiado periódicamente. Cada KRI está relacionada con el apetito de riesgo y la tolerancia para que los niveles de activación se puedan definir, lo que permitirá a los interesados tomar las medidas adecuadas en el momento oportuno.

## Definición y priorización de la respuesta del riesgo

El objetivo de definir una respuesta al riesgo es llevar el riesgo al mismo nivel que el apetito de riesgo definido para la empresa después del análisis de riesgo. En otras palabras, una respuesta tiene que ser definida tal que el futuro riesgo residual (respuesta de riesgo definida y puesta en práctica) es, tanto como sea posible (por lo general dependerá de los recursos económicos disponible), dentro de los límites de tolerancia de riesgo.

***Evitar riesgos***
Evitar significa salir de las actividades o de las condiciones que dan lugar a riesgo. Evitar riesgos se aplica cuando no hay otra respuesta adecuada. Este es el caso cuando:

- No hay ninguna otra respuesta rentable que puede tener éxito en la reducción de la frecuencia y de la magnitud por debajo de los umbrales definidos para el apetito del riesgo.
- El riesgo no puede ser compartido o transferido.
- El riesgo se juzga inaceptable por la administración.

Algunos ejemplos relacionados con la cobertura de riesgos de TI pueden incluir la reubicación de un centro de datos fuera de una región con importantes peligros naturales, o negarse a participar en un proyecto muy grande, cuando el caso de negocio muestra un notable riesgo de fracaso.

***Reducción de Riesgos / Mitigación***
La reducción significa, que medidas están tomadas para detectar el riesgo, seguido por la acción para reducir la frecuencia y/o el impacto de un riesgo. Las maneras más comunes de respuesta al riesgo incluyen:

- Fortalecimiento global de la gestión de las prácticas de riesgos de TI, es decir, aplicación de la suficiente madurez de la gestión de riesgos y los Procesos que deben definirse como el riesgo marco de TI.
- Introducción de una serie de medidas de control intentando reducir las frecuencias de un suceso de consecuencias adversas y / o el impacto empresarial de un evento, en caso de que suceda. Esto se discute en el resto de esta sección.

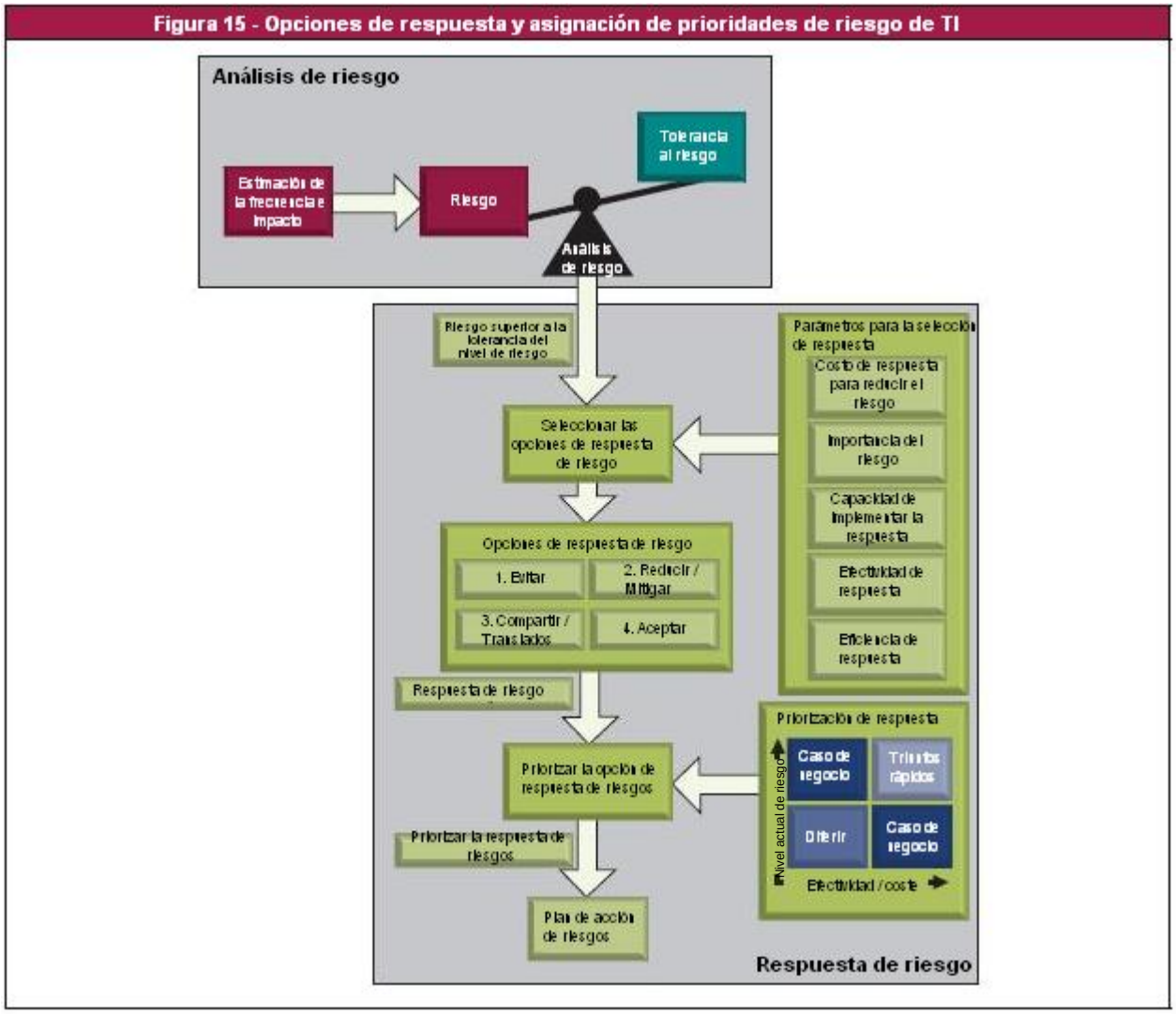
***Riesgo Compartido / Transferencia***
Compartir significa reducir la frecuencia de riesgo o impacto mediante la transferencia o distribución de una parte del riesgo. Las técnicas más comunes son los seguros y la subcontratación.
Los ejemplos incluyen tener un seguro para los incidentes relacionados con las TI, la subcontratación de parte de las actividades de TI, o establecer un proyecto de riesgo de TI compartido con el proveedor a través de acuerdos de precios fijos o acuerdos de inversión compartida. Tanto en un sentido físico y jurídico estas técnicas no alivian una empresa de un riesgo, pero puede afectar la capacidad de la otra parte en la gestión del riesgo y reducir las consecuencias económicas si se produce un evento adverso.

***Aceptación del riesgo***
Aceptación significa que no se tomen medidas relativas con un riesgo particular, y la pérdida es aceptada cuando y si se produce. Esto es diferente de ignorar el riesgo, aceptar el riesgo supone que el riesgo es conocido, es decir, una decisión informada se ha aceptado por la dirección. Si una empresa adopta una postura de aceptación de riesgo, se debe considerar cuidadosamente quién puede asumir el riesgo, más aún con los riesgos de TI. Los riesgos de TI deben ser aceptados por la dirección de la empresa (y los propietarios de procesos de negocio) con la colaboración y el apoyo de TI, y la aceptación debe ser comunicada a la Junta. Si un riesgo particular es evaluado por ser extremadamente raro, pero muy importante (catastrófico) y los enfoques para reducirla son prohibitivos, la administración puede decidir aceptarlo.

*The Risk TI Practitioner Guide* (capitulo 6) incluye ejemplos de respuesta a los riesgos y ofrece una orientación más detallada sobre cómo seleccionar y dar prioridad a la respuesta de riesgo. Específicamente para la reducción de riesgos, COBIT y VAL IT contienen un conjunto amplio de medidas de control, y el *The Risk TI Practitioner Guide* ofrece orientación sobre los diferentes riesgos que pueden reducirse utilizando estos marcos (capítulo 8).

La respuesta al riesgo y los procesos de priorización son representados en la **figura 15**

**Figura 15 - Opciones de respuesta y asignación de prioridades de riesgo de TI**




## Selección y priorización de respuesta de riesgo

Las cuatro secciones anteriores enumeran las opciones de respuesta al riesgo disponibles. El siguiente es un breve debate sobre la selección de una respuesta adecuada, es decir, dado el riesgo, cómo responder y cómo elegir entre las opciones de respuesta disponibles. Los siguientes parámetros deben tenerse en cuenta en este proceso:

- Respuesta del coste, por ejemplo, en el caso de la transferencia del riesgo, el coste de la prima del seguro; en el caso de mitigación de riesgo, el coste (gasto de capital, salarios, consultoría) para aplicar medidas de control.
- Importancia del riesgo dirigido por la respuesta, por ejemplo, su posición en el mapa de riesgos (que refleja la frecuencia y la magnitud de los niveles combinados).
- Capacidad de la empresa para aplicar la respuesta, cuando la empresa tiene la madurez suficiente en sus procesos de gestión de riesgos, pueden llevarse a cabo las respuestas mas sofisticadas, cuando la empresa tiene un nivel bajo de madurez, algunas respuestas básicas, pueden ser mejores.
- Eficacia de la respuesta, es decir, la medida de la respuesta reducirá la frecuencia y el impacto del riesgo.
- La eficiencia de la respuesta, es decir, por beneficios prometidos por la respuesta.

El esfuerzo para la mitigación de la respuesta, compartir/transferencia, por ejemplo, la colección de controles que necesita ser implementada o reforzada, excederá los recursos disponibles. En este caso, se requiere establecer prioridad.
Usando el mismo criterio para la respuesta de selección de riesgo, la respuesta al riesgo se puede ubicar en un cuadrante, ofreciendo tres posibles opciones:

- Triunfos rápidos -muy eficientes y eficaces en las respuestas al riesgo alto.
- Caso de negocio efectuado -más costoso en respuestas complicadas a un alto riesgo, eficiente y eficaz en las respuestas a un menor riesgo, en ambos se requiere un análisis cuidadoso y decisiones de gestión de las inversiones. El enfoque del marco de VAL IT se puede aplicar aquí.
- Aplazamiento - costosas respuestas a menores riesgos.

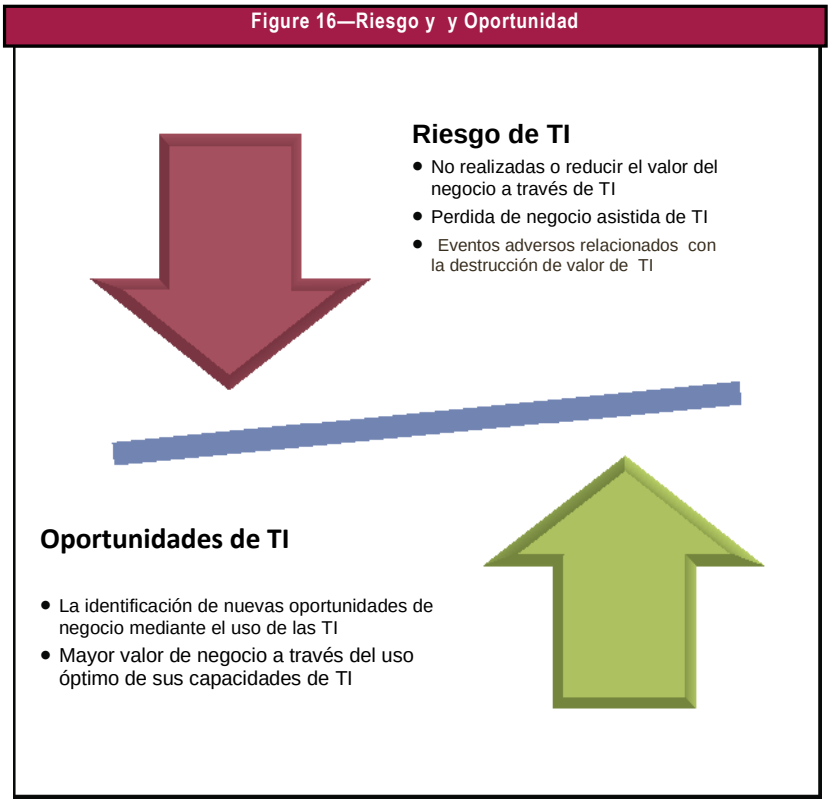
Por esta razón, la organización tiene que seleccionar y priorizar las respuestas al riesgo, utilizando los siguientes criterios:

- El coste de la respuesta, por ejemplo, en el caso de la transferencia del riesgo, el costo de la prima del seguro; en el caso de mitigación de riesgo, el costo (gasto de capital, salarios, consultoría) para aplicar medidas de control
- Importancia del riesgo dirigido por la respuesta, por ejemplo**;** su posición en el mapa de riesgos (que refleja la frecuencia y la magnitud de los niveles combinados).
- Capacidad de la organización para aplicar la respuesta**,**
- La efectividad de la respuesta, es decir, que la medida de la respuesta reducirá el impacto y la frecuencia de eventos adversos.
- La eficiencia de la respuesta, es decir, la relativa por beneficios prometidos por la respuesta en comparación con:
  - Otras inversiones relacionadas de TI (investigando medidas en respuesta del riesgo) siempre compite con otras inversiones de TI (o no de TI).
  - Otras respuestas (una respuesta puede estar dirigida a riesgos severos mientras otras no)

# 8. RIESGOS y OPORTUNIDADES DE GESTIÓN USANDO COBIT, VAL IT y RIESGOS DE TI

En un día típico en una organización típica, las actividades de TI, los procesos de TI están organizados y desplegados. Se producen eventos en varias áreas: las opciones tecnológicas deben ser evaluadas, las reparaciones en caso de incidentes operacionales deben ser aplicadas, los problemas de software deben ser abordados y las solicitudes deben ser respondidas. Cada uno de estos eventos lleva aparejado riesgo y oportunidad.
El riesgo refleja la combinación de la frecuencia de los hechos ocurridos y el impacto que tienen estos acontecimientos sobre la organización. El riesgo potencial para los acontecimientos y sus consecuencias contiene las oportunidades de beneficio (al revés) o de amenazas para el éxito (negativo). Riesgo y oportunidad van juntas, de hecho, para proporcionar valor de negocio a los interesados, las empresas deben participar en diversas actividades e iniciativas (oportunidades), todos conllevan grado de incertidumbre y, por tanto, de riesgo. Gestión del riesgo y de la oportunidad es una actividad estratégica clave para el éxito de la organización.
TI pueden jugar varios roles en relación riesgo-oportunidad (**Figura 16):**

**Figure 16—Riesgo y y Oportunidad**




- **Valor Permitido-Las nuevas iniciativas empresariales** casi siempre dependen de alguna participación de TI:
  - Habilitando proyectos de TI de éxito que apoyan las nuevas iniciativas y, así, la creación de valor.
  - La aplicación de nuevas tecnologías o el uso de nueva tecnología de forma innovadora que permitan nuevas iniciativas empresariales y la creación de valor.
- **Valor inhibidor - El reverso de lo anterior** aplica cómo:
  - TI- permitió que los proyectos de negocios o inversiones, a menudo, no produzcan los resultados esperados, por lo que el valor no se entrega.
- La organización puede fallar para identificar o capturar oportunidades de nuevas iniciativas empresariales derivadas de la nueva tecnología.

Destrucción de valor, algunos eventos de TI, especialmente en las operaciones de TI, pueden causar leves o graves trastornos operativos a la empresa, por ejemplo, el sistema o interrupciones de la red de corta duración o ampliado; la pérdida, la divulgación o la corrupción de la información.
Inversión de la declaración anterior, la capacidad para hacer un cambio de negocio y poner en práctica la mejora de los procesos de negocios impulsada por el programa de TI y soluciones de proyecto, junto con el sistema fiable, flexible y sensible de TI (en funcionamiento) la capacitación puede permitir a la empresa crecer más rápido o tomar nuevas iniciativas empresariales. Esto equivale a coches más rápidos y con mejores resultados que necesitan mejores frenos. Capacidades y controles eficaces para que las empresas puedan evitar riesgos (protección de valor) y tomar riesgos (creación de valor).

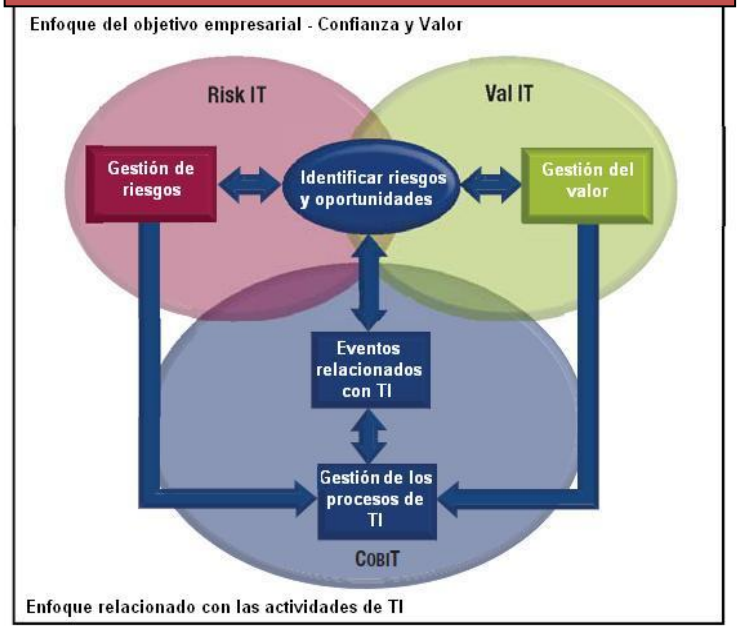
- ¿Cómo puede una empresa hacer frente a esto en la práctica? Lo ideal sería que la empresa tomara consciencia de los riesgos y de la oportunidad que supone la evaluación y el control de todas las iniciativas que requieren la participación de TI. Por ejemplo:
- Cuando se propone una importante inversión en infraestructura de TI, ya sea como una iniciativa proactiva o de reacción la empresa debe considerar todos los siguientes elementos en la toma de decisiones:

- Beneficios en la reducción del riesgo de la nueva iniciativa.
  - Los riesgos asociados con la inversión (por ejemplo, el riesgo del proyecto).
  - Los beneficios comerciales resultantes de la posesión de la nueva infraestructura de TI y las oportunidades.
  - Cuando surge una nueva tecnología, la empresa debe considerar lo siguiente al determinar si conviene o no adoptar la tecnología:
  - Impacto de la adopción de la tecnología (de apoyo, fiabilidad, facilidad de integración).
  - Los riesgos asociados con la operación de la nueva tecnología (por ejemplo, seguridad, fiabilidad)
  - Consecuencias (por ejemplo, la obsolescencia, quedar muy por detrás de los competidores), de no adoptar la nueva tecnología.
  - Los beneficios comerciales de la nueva tecnología (por ejemplo, la habilitación de nuevas iniciativas empresariales, el logro de la eficacia y la eficiencia)

Después de que la empresa realice su evaluación inicial de los riesgos y / o de oportunidades, es necesario determinar la forma de tratarlos. Aquí, los tres Marcos de ISACA (COBIT, VAL IT y riesgos de TI) se complementan entre sí y proporcionan una orientación práctica (**figura 1**).

Los procesos de COBIT debe gestionar todas las actividades Relacionadas con la TI en la organización.
Estos procesos tienen que tratar eventos internos o externos a la organización. Los acontecimientos internos pueden incluir los incidentes operacionales, los fracasos del proyecto, cambia completode estrategia TI y las fusiones.
Los acontecimientos externos pueden incluir cambios en las condiciones el mercado, nuevos competidores, nuevas tecnologías disponibles y nuevas regulaciones que le afectan.
Todos estos hechos constituyen un riesgo y / o la oportunidad y necesidad de ser evaluados y desarrollar respuestas.
La dimensión del riesgo, y cómo manejarlo, es el tema principal del marco de riesgos.
Cuando las oportunidades por el cambio de negocios se identifican, VAL IT es el que mejor describe cómo progresar y maximizar el retorno sobre la inversión.
El resultado de la evaluación, probablemente tendrá un impacto en algunos de los procesos de TI y / o en la entrada a los procesos de TI, por lo que las flechas de la «Gestión del Valor de Administración de Riesgos" y "las cajas se dirigen de nuevo al área de gestión de procesos de TI " en la **figura 1**.
Algunas personas consideran la dicotomía riesgo–oportunidad como «asumir mayor riesgo y el acaparamiento de las oportunidades potenciales". Esto puede ser una descripción adecuada del apetito de riesgo global que la organización ha definido para sí misma, sin embargo, cabe señalar que puede suponer más riesgo por ejemplo, seguir adelante sin un plan completo de continuidad del negocio, puede ahorrar dinero a corto plazo, pero también puede dificultar el crecimiento de la empresa en una etapa posterior.
Un buen método de análisis de riesgo incluye los componentes descritos anteriormente y la identificación de las opciones a realizar.
Aplicar una buena gestión de riesgos y prácticas de gestión de valor permite tomar decisiones con conocimiento de causa.

Figura1. Posicionamiento de Cobit, Val IT y Risk IT

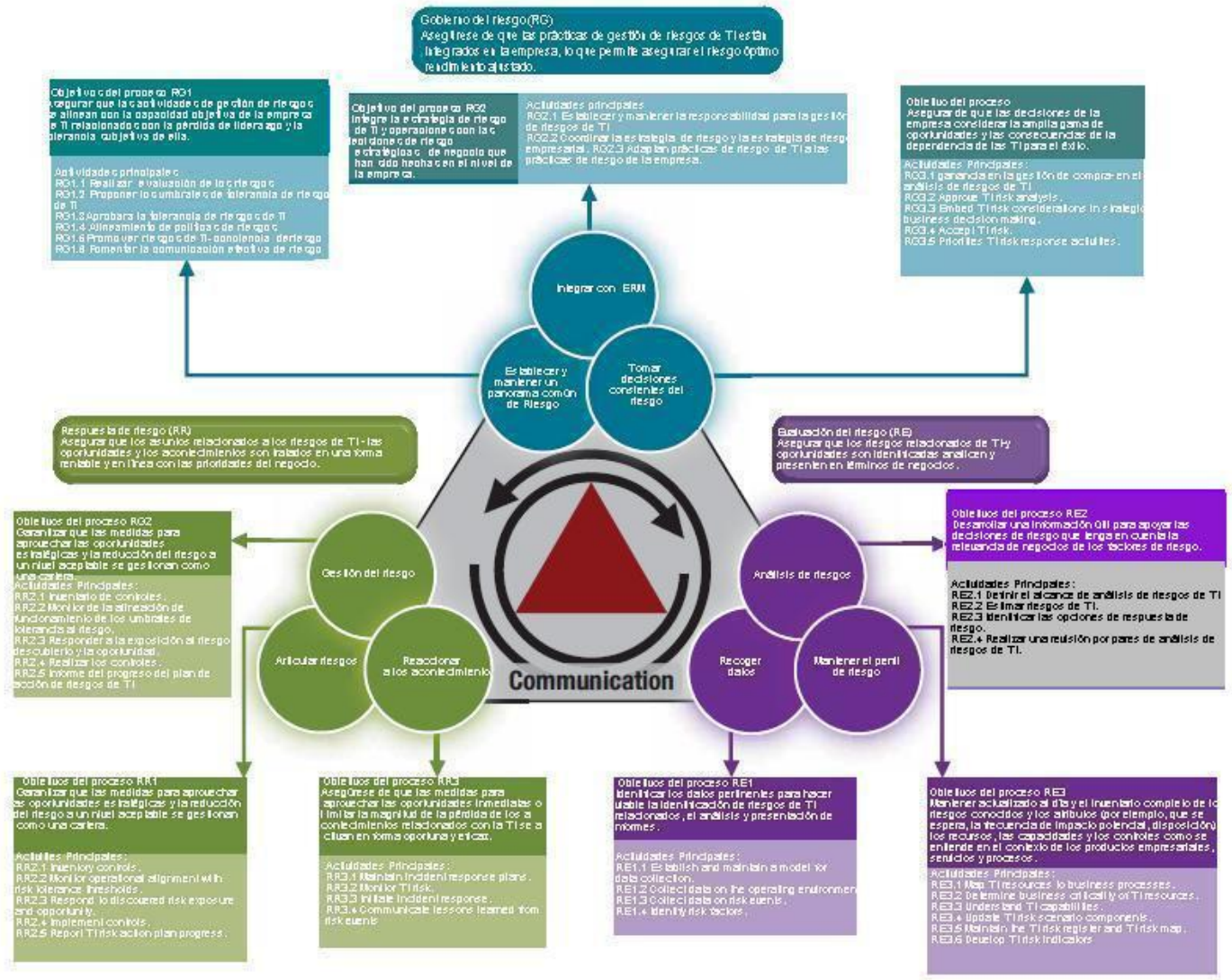


# 9. PANORAMA DEL PROCESO DEL MODELO DEL MARCO DE RIESGOS DE TI

La **figura 17** muestra un panorama general del riesgo de TI como proceso modelo. Para cada uno de los tres ámbitos, se destacó el objetivo de dominio y de sus tres procesos. Para cada uno de los nueve procesos, figuran el objetivo del proceso y las actividades principales.

# 9. PANORAMA DEL PROCESO DEL MODELO DEL MARCO DE RIESGOS DE TI

**Figura 17 - Proceso general del modelo de riesgos de TI**



**Página en blanco intencionadamente**

# 10. GESTIÓN DEL RIESGO EN LA PRÁCTICA —VISIÓN GENERAL DE LA GUÍA PROFESIONAL

*The Risk TI Practitioner Guide* complements *The Risk TI Framework*. La guía profesional ofrece ejemplos de las técnicas posibles y una orientación más detallada sobre cómo abordar, desde una base práctica los conceptos tratados en los capítulos anteriores y en el modelo de proceso detallado. Algunos de los conceptos y técnicas tratados en más detalle en la guía incluyen:

- Escenarios de la construcción de escenarios, basados en un conjunto genérico de los riesgos de TI.
- Construcción de un mapa de riesgos con las técnicas de describir la incidencia y la frecuencia de los escenarios.
- Construyendo criterios de Impacto con importancia en el negocio.
- Definición de RISK.
- Utilizando COBIT y VAL IT para mitigar el riesgo, la relación entre el riesgo y COBIT y VAL IT objetivos de control y prácticas claves de gestión.

La figura 18 muestra un panorama general de los riesgos. La Guía Profesional y mapas de los dominios y los procesos del riesgo y los modelos de proceso a los que se pueden aplicar:

- RG1 Establecer y mantener una visión común
- RG2 integrarse con ERM
- RG3 Hacer decisiones conscientes de riesgo de negocio
- RE1 Recopilar datos
- RE2 Análisis de riesgo
- RE3 Mantener el perfil del riesgo
- RR1 Articular riesgo
- RR2 gestionar el riesgo
- RR3 Reaccionar a eventos

**Figura 18— Guía profesional general de los riesgos de TI**

| Sección | Subsección | Procesos de dominio del Marco de Referencia de Riesgos | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | RG1 | RG2 | RG3 | RE1 | RE2 | RE3 | RR | RR2 | RR |
| 1. Definición de un universo de riesgos y ámbito de gestión de riesgo. | | RG1 | RG2 | RG3 | | RE2 | RE3 | | RR2 | |
| 2. Apetito de riesgo y tolerancia al riesgo | | RG1 | | | | | | | | |
| 3.Conciencia del riesgo, Comunicación y presentación de informes | Conciencia del riesgo, Comunicación | RG1 | RG2 | RG3 | RE1 | RE2 | RE3 | RR1 | RR2 | RR3 |
| | Principales indicadores del riesgo y presentación de informes | | | | | | RE3 | RR1 | RR2 | |
| | Perfil del riesgo | | | | | | RE3 | | | |
| | Agregación de riesgos | RG1 | RG2 | RG3 | | | | RR1 | | |
| | Cultura de riesgos | RG1 | RG2 | | | | | | | |
| 4. Expresando y describiendo el riesgo | Introducción | RG1 | RG2 | | | RE2 | | RR1 | | |
| | Expresando su impacto en términos de negocios | RG1 | RG2 | | | RE2 | | RR1 | | |
| | Describiendo Riesgo-Expresando Frecuencia | RG1 | | | | RE2 | | RR1 | | |
| | Describiendo Riesgo-Expresando Impacto | RG1 | | | | RE2 | | RR1 | | |
| | Mapeando los objetivos de negocios de COBIT con otros criterios de impacto | RG1 | RG2 | | | | | | | |
| | Mapa de Riesgos | RG1 | | | | | RE3 | RR1 | | |
| | Registro de Riesgos | | | | | | RE3 | | | |
| 5. Escenarios de riesgo | Explicación de los escenarios de riesgo | RG1 | | | | RE2 | RE3 | | | |
| | Ejemplo de escenarios de riesgo | | | | | RE2 | | | | |
| | Capacidad de Factores de Riesgo en el Proceso de Análisis de Riesgo | RG1 | | | RE1 | RE2 | RE3 | | | |
| | Factores de Riesgo Ambiental en el Proceso de Análisis de Riesgo | RG1 | | | RE1 | RE2 | | | | |
| Riesgo de respuesta y asignación de prioridades | | | | RG3 | | | | | RR2 | RR3 |
| 7.Un flujo de trabajo de Análisis de Riesgo | | | | | RE1 | RE2 | RE3 | RR1 | | |
| 8. Mitigación de Riesgos de TI Uso de COBIT y VAL IT | | | | | | RE2 | | RE1 | RR2 | RR3 |

**Página en blanco intencionadamente**

# 11. PANORAMA DEL MODELO DE PROCESO DEL MARCO DE RIESGO DE TI

Esta sección proporciona una visión general de los nueve procesos de negocio a través de riesgos de TI de los tres ámbitos: gobernanza del riesgo, evaluación de riesgos y el riesgo de respuesta. Las directrices de gestión incluyen metas y mediciones en diferentes niveles y gráficos RACI (responsable, obligado a dar cuenta, consultado e informado). Para permitir las comparaciones y puntos de referencia, se presenta un modelo de madurez para cada dominio, proporcionando una escala de medición incremental de cero a cinco años. En el nivel 0, “no existe”, la empresa aún no ha adoptado aún las más básicas prácticas de gestión de riesgos de TI. En el nivel 5, “optimizado”, la empresa es capaz de cuantificar el valor de la gestión de riesgos de manera madura, la evaluación de riesgos y la capacidad de respuesta de riesgos y tiene los medios para mejorar de manera continuada y optimizar.

## Las descripciones detalladas de procesos

**Componentes del proceso**
Un proceso efectivo es un conjunto fiable y repetitivo de las actividades y los controles para realizar una tarea determinada. Los procesos de entrada de una o varias fuentes (incluyendo otros procesos) deben manipular la entrada, utilizar los recursos de acuerdo a las políticas y producir una salida (incluida la salida de otros procesos). Los procesos deben tener claras razones empresariales para los propietarios de cuentas, funciones y responsabilidades claras en torno a la ejecución de cada actividad clave y los medios para llevar a cabo y medir el rendimiento.

**Prácticas de Gestión**
Las prácticas de gestión son las características necesarias para que los procesos tengan éxito. En riesgo, las prácticas de gestión apoyan directamente las actividades principales. Las secciones del proceso proporcionan los detalles de una agrupación de las prácticas de gestión para cada actividad clave. (Este enfoque es diferente de COBIT y VAL IT, que especifican las actividades que están relacionadas pero distintas de las prácticas de gestión.) Las prácticas de gestión del riesgo no deben ser consideradas como una metodología. Sin embargo, proporcionan un marco que las empresas pueden utilizar para evaluar sus prácticas actuales, determinar dónde hay áreas de mejora y las iniciativas de guía para hacer la mejora. Cada empresa debe tener en cuenta sus propias políticas, el apetito de riesgo y el ambiente al seleccionar las prácticas de gestión que mejor se aplican a esa empresa.

**Entradas y salidas**
Los nueve procesos de riesgo de TI, aunque se enumeran de forma secuencial, están relacionados entre sí de manera compleja. Para ilustrar cómo el intercambio de información y los procesos dependen unos de otros, las entradas y salidas se definen en la práctica de gestión / nivel de actividad (figura 19). (Este enfoque es diferente de COBIT y VAL IT, que modelan entradas y salidas a nivel de proceso). Las entradas sugieren que la información de una actividad de riesgo de TI necesita de otras actividades y procesos para tener éxito. Al mismo tiempo, las actividades de riesgo de TI deben generar información (resultados) para apoyar al gobierno de TI y el riesgo de las actividades empresariales y procesos de gestión (por ejemplo, COBIT, VAL IT y procesos de negocios externos).El riesgo ilustrativo TI de entradas y salidas no debería ser considerado como una lista exhaustiva, ya que flujos adicionales de la información podrían ser definidos dependiendo del ambiente de una organización particular y el marco de proceso.

Los vínculos principales entre los procesos de negocio y COBIT son a través de los siguientes procesos de TI de COBIT:
- P01 Definir un plan estratégico de TI
- P02 Definir la arquitectura de información
- P04 Definir los procesos de TI la organización y sus relaciones
- P05 Dirección de inversión TI
- P06 Dirección de comunicación objetiva y direcciones
- P09 Evaluar y administrar riesgos de TI
- DS2 Administrar servicios de terceros
- DS8 Administrar servicios de apoyo e incidentes
- DS1O Administrar Problemas.
- ME1 Monitorear y evaluar el desempeño de TI.
- ME2. Monitorear y evaluar el centro interno
- ME3. Garantizar el cumplimiento regulatorio.
- ME4 Proveer el Gobierno de TI

Los principales vínculos entre el Val de TI y riesgos de TI son a través de los siguientes procesos de negocio:
- VG1 Establecer un liderazgo informado y comprometido
- VG3 Definir características de cartera.
- VG5 Establecer una supervisión de gobernanza eficaz.
- PM4 Evaluar y seleccionar programas para financiar.
- IM1 Desarrollar y evaluar el programa del diseño inicial de negocio.
- IM2 Comprender los candidatos y las opciones del programa de ejecución.
- IM5.Desarrollar el caso de negocio detallado del programa candidato
- IM9 Supervisar e informar sobre el programa.

Además, *The Risk TI Practitioner Guide* establece un vínculo entre los escenarios de riesgo genéricos y prácticas de gestión y los controles dentro de los procesos COBIT y VAL IT .

Figura 19-Ejemplo de las entradas y salidas (RE2.3)

| De | Entradas |
|---|---|
| RG1 .3 | Umbrales de tolerancia de los riesgos de TI |
| RG3.4, RR3.4 | Requisitos de la respuesta de Riesgo |
| RE2.1 | Alcance del análisis de riesgo |
| RE2.2 | Resultados del análisis de escenarios |
| RE3.5 | Perfil del riesgo de TI |
| RR1 .1, RR1 .4, RR2.2 | temas y oportunidades de los riesgos de TI |
| RR1 .2, RR2.2 | Huecos de control y excepción de políticas |
| RR2.1 | Riesgos y control de referencia |
| VAL IT PM4 | Los programas de inversión aprobados |
| COBIT PO5 | Los presupuestos de TI |
| COBIT PO10 | Directrices de gestión de proyectos |
| COBIT ME2 | Informe sobre la eficacia de los controles de TI |
| | Presupuesto operante |

| Para | Salidas |
|---|---|
| RE2.4, RR1,1 | Resultado del análisis de riesgo |

* Input from/output to outside Risk IT, Val IT and COBIT

***Gestión de directrices***

Las directrices de gestión de riesgos de TI ofrecen sugerencias que las empresas pueden utilizar para implementar procesos de gestión de riesgos de TI y las prácticas en su entorno. Las directrices pueden ayudar con respuestas a preguntas típicas de gestión tales como:

- ¿Cómo los procesos de gestión de riesgos de TI y las actividades se interrelacionan?
- ¿Cuáles son las principales actividades que deben llevarse a cabo o mejorar?
- ¿Qué funciones y responsabilidades deben definirse para el éxito de procesos de gestión de riesgos de TI?
- ¿Cómo se mide y se comparan los procesos de gestión de riesgos de TI en la empresa?
- ¿Cuáles son los indicadores de buen desempeño?

Para cada proceso de riesgos de TI proporcionar las directrices:

- Entradas y salidas (incrustado en detalle el proceso, como se ha descrito anteriormente).
- Funciones y responsabilidades.
- Objetivos y métrica.

***Roles y responsabilidades- Gráfico RACI***

Un Gráfico RACI (**figura 20)** indica los roles para cada actividad clave definidos como un grupo de apoyo a las prácticas de gestión de la tabla de riesgos de TI procesos asociados. Los RACI se definen:

- Responsable (R)-Los que deben garantizar las actividades se completan con éxito.
- Responsable (A)-Los que poseen los recursos necesarios y tienen la autoridad para aprobar la ejecución y / o aceptar el resultado de una actividad.
- Consulta (C)-Los que se solicitan opiniones sobre una actividad (comunicación bidireccional)
- Informado (I)-Los que se mantenga al día sobre el progreso de una actividad (de un modo de comunicación)

Un cuadro es siempre de riesgo para cada proceso de TI.

**Figura 20-Ejemplo de l cuadro RACI (RE2)**

**Cuadro RACI** **Funciones**

**Actividades principales**

| | Board | CEO | CRO | CIO | CFO | Enterprise Risk Committee | Business Management | Business Process Owner | Risk Control Functions | HR | Compliance and Audit |
|---|---|---|---|---|---|---|---|---|---|---|---|
| RE2.1. Definir el alcance de los riesgos de TI | | I | R | C | I | C | A | R | C | | C |
| RE2.2.Estimar riesgos de TI | | I | R | C | C | I | A/R | R | R | | C |
| RE.2.3 Identificar las opciones de respuesta de riesgo. | | | C | C | C | R | A | R | R | | I |
| RE2.4 Realizar una revisión por pares de análisis de riesgos de TI. | | | A/R | | | | I | | I | | I |

A **RACI** chart identifies who is **R**esponsible, **A**ccountable,

La siguiente Figura 21 enumera funciones RACI (estos también aparecen en la **figura 8**).

Las

**La Figura 21- Definición del papel**

| Papeles | Sugerir Definición |
|---|---|
| Consejo | Los más altos ejecutivos y / o no-ejecutivos de la empresa que son responsables de la gestión de la organización y tienen el control total de los recursos |
| (CEO) Director Ejecutivo | El más alto rango oficial, que se encarga de la gestión total de la organización |
| (CRO) Jefe Oficial de Riesgo | Supervisa todos los aspectos de la gestión de riesgos en toda la empresa. Un oficial de los riesgos, puede ser establecido para supervisar los riesgos relacionados con la TI |
| (CIO) Jefe Oficial de Información | El más alto funcionario de la empresa que es responsable de TI para la promoción; la alineación de TI y las estrategias empresariales y la planificación, la asignación de recursos y la gestión de la prestación de los servicios de TI, la información y el despliegue de los recursos humanos asociados. El CIO normalmente preside el consejo de gobierno que maneja la cartera. |
| (CFO) Jefe Oficial de Financiero | El más alto funcionario de la empresa que es responsable de la planificación financiera, el mantenimiento de registros, relaciones con los inversores y los riesgos financieros |
| Comité de Riesgos | Los ejecutivos de la empresa que son responsables de la empresa a nivel de la colaboración y consenso necesario para apoyar las actividades de gestión de riesgos y decisiones. Un consejo de riesgos puede ser establecido para examinar los riesgos con más detalle y asesorar al comité de riesgos. |
| Gestión empresarial | Personas con funciones de negocio relacionadas con la gestión de un programa(s) |
| Propietario de procesos de negocio | La persona responsable de la identificación de los requisitos del proceso, diseño y proceso de aprobación de la gestión de proceso de ejecución. En general, un proceso de negocio debe ser titular en un nivel suficientemente elevado en la empresa y tener autoridad para comprometer recursos para el proceso específico de las actividades de gestión de riesgo. |
| Funciones de control de riesgos. | Las funciones en la empresa responsable de la gestión de los dominios específicos de riesgo (por ejemplo, el jefe de seguridad de la información oficial, la continuidad del negocio-plan de recuperación de desastres, la cadena de suministro, gestión de proyectos de oficina) |
| (RH) Recursos Humanos | El más alto funcionario de una empresa que es responsable de la planificación y las políticas con respecto a todos los recursos humanos en esa empresa. |
| Cumplimiento y Auditoría | La función (es) en la empresa responsable del cumplimiento y de auditoría |

**figuras 8** y **21**, aunque que no pretenden representar un organigrama o estructura, muestran las interrelaciones entre las funciones propuestas.

La asignación efectiva de R, A, C e I variará entre empresas en función de su modelo organizativo y de otros factores. Determinados requisitos reglamentarios pueden asignar responsabilidades a las funciones específicas, por ejemplo, la normativa bancaria puede asignar responsabilidad a las juntas para determinadas actividades que de otro modo podrían no recibir un alto nivel de atención, o los reglamentos del mercado financiero pueden asignar determinadas actividades a una empresa en cuestiones de continuidad. Para cada actividad clave, lo ideal sería que una sola persona fuera Responsable (aquí referido a asignar un A).
A quien se les asigna un A debe tener la autoridad y recursos suficientes para patrocinar la actividad. Una o más personas pueden ser Responsable (aquí referido a R) dependiendo de la actividad del ámbito de aplicación. Las funciones a las que no se haya asignado un R, A, C o I para una determinada actividad normalmente no están directamente involucrados o afectados por el rendimiento de la actividad. Las tareas de riesgo que son de carácter genérico y sugerencias constituyen ejemplos solamente.

Los siguientes supuestos fueron hechos desarrollando el gráfico RACI en el Riesgo de TI:

- Una gobernanza eficaz de gestión de riesgos en todas las disciplinas (incluyendo el riesgo de crédito, riesgo de tipo de interés, riesgo de liquidez y riesgo operativo) depende en gran medida de la capacidad de madurez de las tres líneas de defensa del modelo. Las tres líneas de defensa modelo distinguen entre las funciones de la propiedad y la gestión de los riesgos, funciones de supervisión de riesgos y proporcionan funciones de aseguramiento independientes. Como tal, el riesgo que segrega la función de auditoría de la CRO y las funciones de control de riesgos. Este enfoque es diferente de COBIT y VAL IT, que representan el cumplimiento, la auditoría, el riesgo y la seguridad como una sola función.
- El CIO no hace informe para ningún otro CRO, como el CFO, pero en cambio informa directamente al CEO. Si no es la cuestión, entonces las designaciones RACI se diferenciarán.
- El CIO ha subordinado toda la administración de TI y las funciones de presentación de informes que puede y, por lo tanto, el control y la respuesta para todos ellos.
- El CRO ha subordinado todas las funciones de riesgos, por ejemplo, un riesgo de TI y el cumplimiento de una empresa o grupo de análisis de riesgos del grupo, la presentación de informes a él / ella y puede, por lo tanto, el control y la respuesta para todos ellos.
- Debido a la dotación de personal y presupuesto, en la práctica algunas funciones puede ser necesario asignarlas de manera multifuncional (una persona, varias funciones).

***Objetivos y Métricas***
Los riesgos de TI presentan una cascada de arriba hacia abajo, de las metas y las cifras de todo el dominio, el proceso y los niveles de actividad. Definir objetivos de lo que la empresa espera, mientras que las cifras reales o potenciales proporcionan medidas de resultado. Los objetivos de dominio son alcanzados por la interacción de procesos, cada uno de los cuales tienen distintos objetivos de proceso que, a su vez, dependen de los objetivos de actividad. Las métricas pueden ser indicadores de retraso, que proporcionan una medida de lo que realmente se ha hecho o logrado, o indicadores, que proporcionan una medida de lo que potencialmente se puede lograr. Las métricas por sí solas no son un remedio, sino que son un punto de partida, ligado a la madurez de la empresa. Tomados en conjunto, las metas y los indicadores pueden proporcionar elementos básicos puntuar una empresa. (Es importante señalar que en el riesgo el objetivo de la actividad objetivo es sinónimo del nombre de la actividad.)

**La figura 22** contiene un ejemplo de un cuadro de métricas y de objetivo.

7 ISACA, *IT Control Objectives for Basel II, The Importance of Governance and Risk Management for Compliance*, USA, 2007, p. 56-57, *www.isaca.org*

| Figura 22 - Ejemplo de objetivos y el cuadro Métrica (RE2) | | |
|---|---|---|
| **Objetivos de la actividad** | **Objetivo de Proceso** | **Objetivo del dominio** |
| • Definir el ámbito del análisis de riesgos de TI.<br>• Estimar los riesgos de TI.<br>• Identificar las opciones de respuesta de riesgo.<br>• Realice una revisión por pares de los resultados de los análisis de riesgos de TI. | • Desarrollar una información útil para apoyar las decisiones de riesgo que tengan en cuenta la pertinencia de negocios de los factores de riesgo (por ejemplo, las amenazas, las vulnerabilidades, el valor, la responsabilidad). | • Asegurar que los riesgos relacionados con la TI y las oportunidades que se identifiquen, analicen y presenten en términos de negocio. |
| **Actividad métrica** | **Métrica de Proceso** | **Métrica de dominio** |
| • El porcentaje del análisis de tiempo son justificados por la experiencia posterior o pruebas (la exactitud).<br>• El porcentaje de tiempo de revisión inter pares no encuentra lógica importante, errores de cálculo o incompleto (defendible).<br>• El Porcentaje de evaluaciones en tiempos paralelos sobre mismos argumentos realizados por analistas diferentes consiguen mismos resultados (consistencia).<br>• El Porcentaje de análisis de tiempos, son realizados por analistas entrenados (el nivel más alto métrico relacionado con la exactitud, defendible y la consistencia).<br>• Un "índice de satisfacción", sobre el análisis de los riesgos derivados de la presentación de informes (por ejemplo, el porcentaje de satisfacción de las respuestas a la encuesta de ejecutivos de empresas con respecto a la legibilidad, la utilidad y la exactitud de los informes de análisis de riesgos). | • El porcentaje de los riesgos para el cual la frecuencia probable de presencia (acontecimiento) y la magnitud probable del impacto de negocio es medida dentro del alcance.<br>• El porcentaje de activos altamente clasificados, los objetivos y los recursos examinados para conocer el efecto de los controles operacionales.<br>• El porcentaje de análisis de riesgo sometidos a revisión por pares antes de ser enviado a la dirección.<br>• Proporción de pérdidas acumulativas reales a magnitud de pérdida esperada. | • El impacto acumulativo de las empresas de TI y los incidentes relacionados con eventos no identificados por los procesos de evaluación de riesgo. |

***Modelos de madurez***

El consejo y la dirección ejecutiva necesitan considerar la eficacia de sus organizaciones que están en riesgo, y la gestión de TI debe ser capaz de responder a estas cuestiones conexas:

- ¿Qué están haciendo nuestros compañeros de la organización para gestionar los riesgos de TI y cómo estamos en relación con ellos?
- ¿Cuáles son las mejores prácticas en la gestión de riesgos de TI y cómo los hemos puesto con respecto a estas prácticas?
- A partir de estas comparaciones, ¿estamos haciendo lo suficiente?
- ¿Cómo hace la empresa para identificar lo que tenemos que hacer para alcanzar el nivel de la gestión de riesgos de TI que busca?

Puede ser difícil obtener respuestas significativas a estas preguntas. La dirección busca constantemente la evaluación comparativa y herramientas de auto evaluación en respuesta a la necesidad de saber qué hacer para lograr los mejores resultados. Uno de estos instrumentos es el modelo de madurez, que pueden permitir a la organización la misma tasa con menos nivel de madurez (con inexistentes o no estructurados procesos) a las más maduras (de haber aprobado y optimizar el uso de mejores prácticas).

Los modelos de madurez son útiles para identificar un número limitado de niveles. Un número mayor haría al sistema difícil de usar y sugeriría una precisión que no es justificable. En general, el propósito es identificar a las empresas que están en favor de ciertas actividades y sugerir la manera de establecer prioridades para las mejoras.

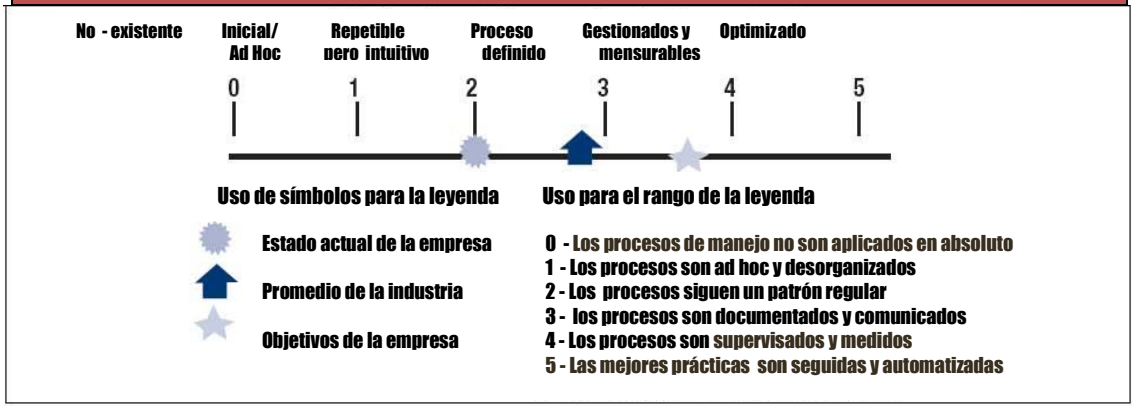
Los niveles de madurez de los riesgos de TI son diseñados como los perfiles en el que una organización puede identificar los síntomas o las descripciones de sus actuales y posibles futuros estados. Cada empresa tendrá que reconocer que muchos de sus procesos se encuentran en diferentes niveles de madurez, por ejemplo, algunos procesos pueden estar en el nivel 1, algunas en nivel 3 y otros en el nivel 4. De esta manera, los modelos de madurez están diseñados para que la dirección pueda centrarse en áreas clave que requieren la atención más que en tratar de obtener que todos los procesos se estabilicen en un nivel antes de pasar al siguiente.

Utilizando los modelos de madurez de riesgo, la Dirección puede identificar:

- El rendimiento actual de la organización; donde está hoy la organización.
- El objetivo de la organización para su mejoría; donde la organización quiere estar (por ejemplo, el apetito de riesgo, estilo de gestión, capacidad de respuesta de riesgo y / o progresión de una opinión de todos los peligros).

Hacer que los resultados sean fácilmente utilizables en la gestión de información; en los que debería presentarse como un medio para apoyar el caso de los planes futuros para mejorar el gobierno del riesgo, evaluación y respuesta a un método de presentación gráfica, podría ser necesario siempre (**figura 23**).

La figura 23 - Modelo de madurez




Para cada dominio de riesgos de TI, tanto de alto nivel y las versiones del modelo de madurez se prestan. Las versiones se construyen en torno a los siguientes atributos, cada uno de los cuales evolucionan a través de los niveles:

- Conocimiento y comunicación
- Responsabilidad y rendición de cuentas
- La fijación y medición de objetivos
- Políticas, normas y procedimientos
- Conocimientos y experiencia
- Herramientas y la automatización

El modelo de madurez de gestión de las escalas puede ayudar a entender que existen deficiencias y establecer objetivos para cuando es necesario. El más adecuado nivel de madurez de la empresa se verá influido por la empresa, los objetivos de negocio, el entorno operativo y las prácticas de la industria. En concreto, el nivel de madurez de gestión de riesgos de TI dependerá de lo que la empresa depende de las TI, su sofisticación tecnológica y, lo más importante, el futuro de su papel ejecutivo y prever la gestión de la tecnología de la información.

**Página en blanco intencionadamente**

# 12. MARCO DE RIESGOS DE TI

Este capítulo presenta el marco en sí y contiene lo siguiente:

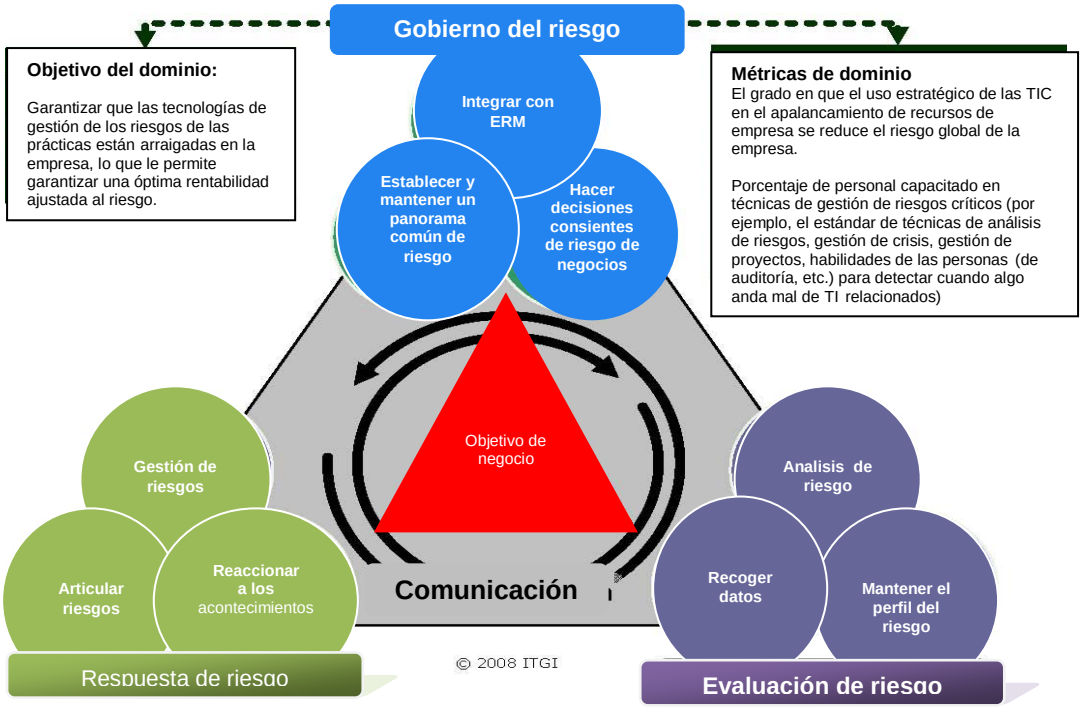
- Dominio; nivel de información:
  - Visión general del dominio. Una gráfica visión general del dominio dentro del marco de los reflejos del objetivo(s) y métrica(s) del dominio (**figuras 24,30 y 36**).
  - Modelo de Madurez; alto nivel y opiniones detalladas.
- Proceso; nivel de información:
  - Visión general del proceso; Un gráfico general del proceso en el marco, destacando el objetivo del proceso y las principales actividades (Las **figuras 25, 26, 27, 31, 32, 33, 37, 38 y 39**).
  - Detalle del proceso; las prácticas de gestión de claves, con entradas y salidas.
  - Las directrices de gestión; los gráficos RACI, las metas y los indicadores.

El marco de riesgos de TI consiste de:

- Dominio; Gobierno del riesgo (RG).
  - RG1 Establecer y mantener una visión común de riesgo.
  - RG2 Intégrese con la Gestión de riesgos de la empresa (ERM).
  - RG3 Hacer decisiones conscientes del riesgo de negocio.
- Domino; Evaluación de riesgo (RE)
  - RE1 Recoger datos.
  - RE2 Analizar los riesgos.
  - RE3 Mantener el Perfil de riesgo.
- Dominio; Respuesta de riesgo (RR)
  - RR1 Articular el riesgo.
  - RR2 Gestión de riesgos.
  - RR3 Reaccionar a los eventos.

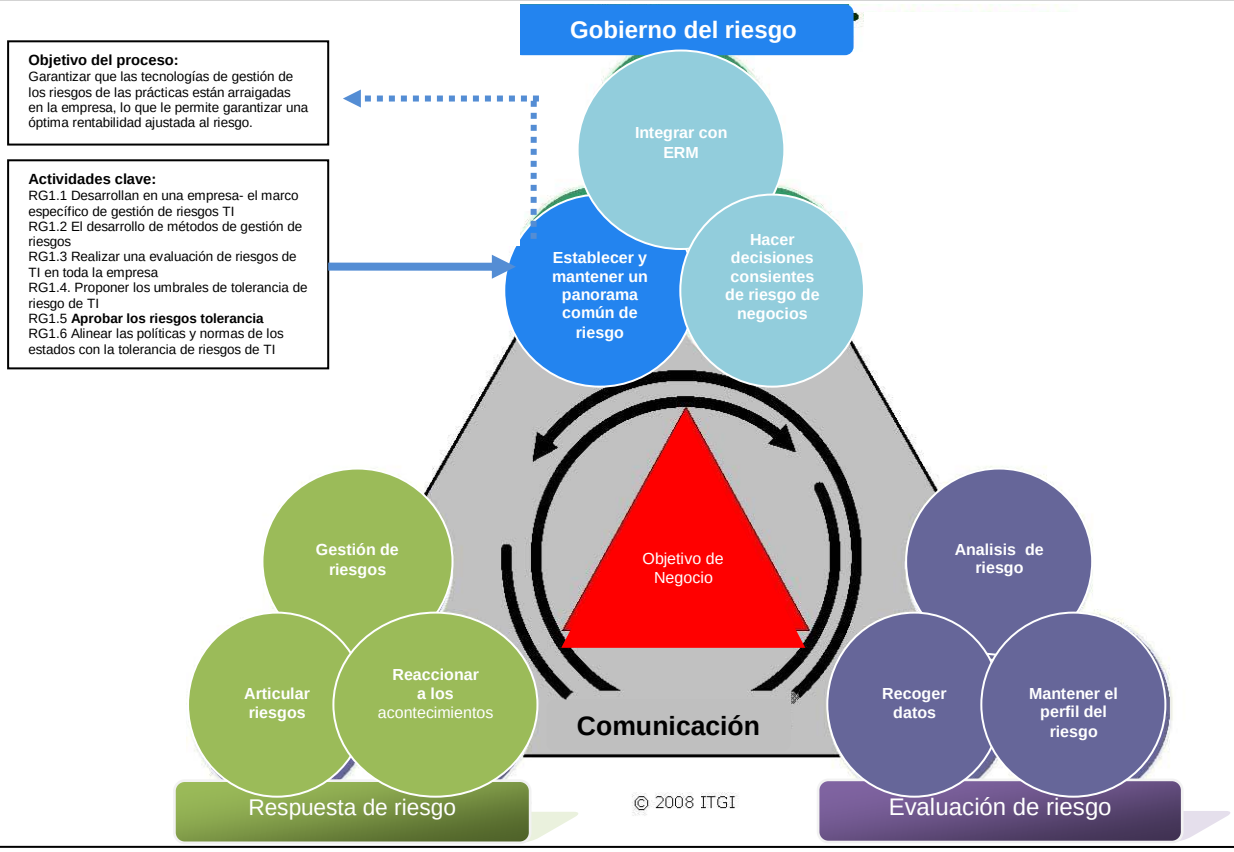
## Visión general del dominio — Gobierno del riesgo (RG)

**Figura 24—Dominio del Gobierno del riesgo**




## Visión general del proceso

**Figura 25 Establecer y mantener el la visión común del riesgo**



## DETALLE DEL PROCESO

### RG1 Establece y Mantiene una Visión de Riesgo Común

Asegurar que las actividades de gestión de riesgos se alinean con la capacidad objetiva de la empresa de TI relacionados con la pérdida de liderazgo y la tolerancia subjetiva de ella.

***RG1.1 Desarrolla en una empresa el marco específico de gestión de riesgos TI***
Se deben patrocinar talleres con la dirección empresarial para discutir la ampliación de los riesgos. La empresa debe estar dispuesta a aceptar la realización de sus objetivos (apetito por el riesgo). Los administradores de TI ayudan a las empresas a comprender el riesgo en el contexto de situaciones que afectan a su negocio y los objetivos, por ejemplo, que son lo más importante en su vida cotidiana (ventas, costes, satisfacción de los clientes, dinero en efectivo). Es necesarios dar de arriba abajo un vistazo a los servicios empresariales y procesos e identificar los principales puntos de soporte de TI. Identificar dónde se genera el valor y donde debe ser protegido y sostenido. Identificar eventos relacionados con la TI y las condiciones que pueden poner en peligro el valor que afectan el rendimiento empresarial y la ejecución de las actividades críticas de negocio dentro de unos límites aceptables, o afectar de otro modo los objetivos de la empresa (por ejemplo, el negocio, regulatorios, jurídicos, los contratos, la tecnología, socio comercial, recursos humanos, otros aspectos operativos). Se debe hacer un Mapa de ellos a una jerarquía de negocios impulsado por las categorías de riesgo (por ejemplo, TI / beneficio de habilitación de valor,
programa y la ejecución de proyectos, operaciones de TI y la prestación de servicios) y subcategorías (TI dominios de riesgo) derivado de escenarios de alto nivel de riesgos de TI. Romper los riesgos de TI por líneas de negocio, producto, servicio y proceso. Identificar posibles riesgos en cascada y los tipos de amenazas y analizar la causa-efecto probable de la concentración de riesgos y correlación. Entender cómo las capacidades de TI contribuyen a la capacidad de la empresa para añadir valor y soportar la pérdida. Comparar la percepción de la gerencia de la importancia de las capacidades de TI a su estado actual. Considere cómo las estrategias de TI, las iniciativas de cambio y las exigencias externas (por ejemplo, la regulación, contratos, estándares de la industria) pueden afectar el perfil de riesgo. Identificar donde se concentran las zonas de riesgo, los escenarios, las dependencias, los factores de riesgo y medidas de riesgo que requieren atención de la administración y posteriormente analizar y desarrollar.

| Para | Entrada |
|---|---|
| RG2.2 | La estrategia de gestión integrada de riesgos |
| RG2.3 | Los métodos de gestión integrada de riesgos |
| RE1 .4 | Factores de riesgo |
| RE3.3 | Evaluación de las capacidades de TI |
| RE3.4 | Componente del escenario de riesgos de TI |
| RE3.5 | Perfil de los riesgos de TI |
| RR1 .3 | Resultados de la evaluación independiente en el contexto de TI |
| Val IT PM1 | Objetivos de retroalimentación y estrategias de TI |
| Val IT IM7 | Cartera de servicios |
| COBIT PO1 | Plan estratégico de TI, los planes tácticos de TI, IT cartera de proyectos, la cartera de servicios de TI, la estrategia de externalización de TI, la estrategia de adquisición de TI |
| COBIT PO4 | Los propietarios del sistema documentado, organización y relaciones |
| COBIT ME3 | Catálogo de los requisitos legales y reglamentarios relacionados con la prestación de servicios de TI, el informe sobre el cumplimiento de las actividades de TI externos con los requisitos legales y reglamentarios |
| COBIT ME4 | El apetito de las empresas para los riesgos de TI, dirección estratégica para las empresas de TI |
| * | La estrategia empresarial, objetivos, metas, el universo de riesgo, el apetito de riesgo, marco de gestión de riesgos, requisitos legales y reglamentarios de asignaciones |

| De | Salida |
|---|---|
| RG1 .2, RG1 .3, RG1 .4, RE2.1, * | Clave del negocio y objetivos de TI, factores de riesgo importantes |
| RG1 .2, RG1 .3, RG1 .4, RG1 .5, RG2.1, RG2.2, RE2.1, RR2.1 | Áreas de enfoque de riesgo |
| RG1 .2, RG1 .3, RG1 .4, RG1 .5, RG2.2, RG3.3, RE2.1, RE3.1, RE3.4 | Escenarios de alto nivel de riesgo |
| RG1 .2, RG1 .3, RG1 .4, RG2.2, RG3.3, RE2.1, RE3.1, RE3.4; Val IT VG1; COBIT PO1, PO9, DS1 | Los principales servicios y el apoyo a los procesos de negocio y los sistemas |
| RG1 .2, RG1 .3, RG1 .4, RG1 .5, RE2.1, RE3.2, RE3.4 | Establecimiento de prioridades de los inventarios de riesgos y el impacto de las categorías |
| RE2.1 | Solicitud de análisis de riesgos |
| RE3.2 | Activo/recurso de importancia (nivel macro) |

* Input from/output to outside Risk IT, Val IT and COBIT

***RG1.2 Proponer los umbrales de tolerancia de riesgo de TI.***
Establecer la cantidad de riesgos relacionados con TI. Una línea de negocio, producto, servicio, proceso, etc., está dispuesto a tomar una serie de riesgos para cumplir con sus objetivos (el apetito de riesgo). Límites expresos en medidas similares a los objetivos de negocio subyacentes y contra los impactos de negocio aceptables e inaceptables. Considere cualquier compensación que sea necesaria para alcanzar los objetivos clave en el contexto de la relación riesgo / retorno. Proponer los límites y medidas en el contexto de su relación beneficio / valor de la implantación, las operaciones de TI de los programas y la ejecución de proyectos, TI y prestación de servicios en múltiples horizontes de tiempo (por ejemplo, de inmediato, a corto plazo, largo plazo).

| Para | Entrada |
|---|---|
| RG1.1 | Negocios claves y objetivos de TI,los prinicpales factores de riesgo, áreas de enfoque de riesgo, escenarios de riesgo de alto nivel, los servicios esenciales y el apoyo a los procesos de negocio y sistemas, los inventarios de prioridad de riesgo y el impacto de las categorías |
| RG1.3 | Umbrales de tolerancia de los riesgos de TI (aprobado) |
| COBIT me4 | Apetito de la empresa para los riesgo de TI, La dirección estratégica de la empresa para TI |
| * | Umbrales de la tolerancia del riesgo de negocio |

| De | Salida |
|---|---|
| RG1.3, | Umbrales de tolerancia de los riesgos de TI(propuestos) |

* Input from/output to outside Risk IT, Val IT and COBIT

***RG1.3 aprobar la tolerancia al riesgo.***
Propone evaluar los umbrales de tolerancia al riesgo frente a un riesgo aceptable de la empresa y los niveles de oportunidad. Tomar en cuenta los resultados de la evaluación de riesgos de TI de la empresa y las compensaciones necesarias para alcanzar los objetivos clave en el contexto de la relación riesgo / retorno. Tenga en cuenta los posibles efectos de la concentración de riesgos de TI y de correlación entre las líneas de negocio, productos, servicios y procesos. Determinar si alguna unidad de los umbrales de tolerancia específicos deberían aplicarse a todas las líneas de negocio. Definir los tipos de eventos (internos o externos) y los cambios en los entornos de negocios o tecnologías que puedan requerir una modificación de la TI tolerancia al riesgo. Aprobar los riesgos de TI umbrales de tolerancia.

| Para | Entrada |
|---|---|
| RG1.1 | Negocios claves y objetivos de TI, factores de riesgo, áreas de enfoque de riesgo, escenarios de riesgo de alto nivel, los servicios esenciales y el apoyo a los procesos de negocio y sistemas, los inventarios de prioridad de riesgo y el impacto de las categorías |
| RG1.2 | Umbrales de tolerancia de los riesgos de TI(propuestos |
| COBIT me4 | Apetito de la empresa para los riesgo de TI, La dirección estratégica de la empresa para TI |
| * | Umbrales de la tolerancia del riesgo de negocio |

| De | Salida |
|---|---|
| RG1.2, RG1.4, RG1.5, RG1.6, RG2.4, RG2.5, RG3.3, RG3.4, RG3.5, RE2.2, RE2.3, RE3.2, RE3.5, RE3.6, RR1.3, RR2.1, RR2.2, RR3.2, RR3.4; Val IT VG3; COBIT PO9; * | Umbrales de tolerancia de los riesgos de TI |

* Input from/output to outside Risk IT, Val IT and COBIT

***RG1.4 Alinear la política de riesgos de TI.***
Codificar el apetito por el riesgo y la tolerancia en la política en todos los niveles de la empresa. Reconocer que el riesgo es inherente a los objetivos de la empresa y documentar cuánto riesgo se desea y se deja en la consecución de esos objetivos. Los principios de gestión de documentos de riesgo, áreas de enfoque de riesgo y las medidas clave. Ajustar la política de TI del riesgo basada en cambios de las condiciones de riesgo y las amenazas emergentes. Alinear la política de funcionamiento y normas de los estados con la tolerancia de riesgo. Realizar revisiones periódicas de la política operativa y normas contra la política de riesgos de TI y la tolerancia. Donde existen lagunas, se deben establecer los objetivos fijando las fechas basándose en los límites admisibles de tiempo de exposición al riesgo y los recursos necesarios. En su caso, proponer ajustes a la tolerancia al riesgo en vez de modificar la política establecida y eficaz funcionamiento y normas.

| Para | Entrada |
|---|---|
| RG1.1 | Negocios claves y objetivos de TI,los prinicpales factores de riesgo, áreas de enfoque de riesgo, escenarios de riesgo de alto nivel, los servicios esenciales y el apoyo a los procesos de negocio y sistemas, los inventarios de prioridad de riesgo y el impacto de las categorías |
| RG1 .3 | Umbrales de tolerancia de los riesgos de TI |
| RG2.1 | Los propietarios del dominio de riesgos de TI, las metas de desempeño, incentivos y recompensas, las funciones integradas y responsabilidades para la gestión del riesgo y de supervisión |
| RG2.2 | La estrategia de gestión integrada de riesgos |
| RE1 .4 | Los factores de riesgo, las amenazas emergentes. |
| RE3.5 | Perfil de riesgo |
| RR1 .1, RR1 .4, RR2.2 | Temas y oportunidades de los riesgos de TI |
| RR1 .2 | Estado de informes de cumplimiento |
| COBIT PO3 | Los estándares tecnológicos |
| COBIT PO6 | Politicas de TI |
| COBIT ME4 | Apetito de la empresa para los riesgo de TI, La dirección estratégica de la empresa para TI |
| * | Umbrales de la tolerancia del riesgo de negocio |

| De | Salida |
|---|---|
| RG1.5, RG1.6, RG2.1, RG2.2, RG2.4, RG2.5, RG3.1, RR1.3, RR2.1; Val IT VG5; COBIT PO6; * | Politicas de riesgo de TI |
| RG1.5, RG1.6; COBIT PO3, PO4, PO6, PO7, * | TI - relacionados con las políticas y normas (actualizaciones) |

* Input from/output to outside Risk IT, Val IT and COBIT

***RG1.5 Promover los riesgos de TI – cultura consciente.***
Sobre la base de una comprensión de la cultura actual de riesgos, capacitar a la empresa para identificar proactivamente los riesgos de TI, las oportunidades y los impactos potenciales de negocio. Aliente a los empleados para hacer frente a los riesgos de TI cuestiones antes de grave escalada es necesario. De negocios de trenes y el personal de TI sobre las amenazas, los impactos y las respuestas previstas de la empresa de eventos de riesgo específicos. Comunicar el "por qué usted debe cuidar" mensaje de áreas de enfoque de riesgo, y explicar cómo tomar el riesgo de acciones conscientes de las situaciones no especificadas en las políticas. Caminar a través de escenarios para las zonas no reguladas directamente por la política, y reforzar las expectativas para la comprensión de la dirección política general y el uso de su buen juicio. Demostrar una actitud que fomenta el debate y la aceptación de la cantidad apropiada de riesgo. Sea positivo acerca de la promoción de una cultura de riesgo adecuada para las TI y en consonancia con la cultura del riesgo empresarial consciente.

| Para | Entrada |
|---|---|
| RG1.1 | Negocios claves y objetivos de TI,los prinicpales factores de riesgo, áreas de enfoque de riesgo, escenarios de riesgo de alto nivel, los servicios esenciales y el apoyo a los procesos de negocio y sistemas, los inventarios de prioridad de riesgo y el impacto de las categorías |
| RG1 .3 | Umbrales de tolerancia de los riesgos de TI |
| RG1.4 | Politicas de riesgo de TI, relacionados con las políticas y normas de TI (actualizaciones) |
| RG2.1 | Los objetivos de rendimiento, incentivos y recompensas, las funciones integradas y responsabilidades para la gestión del riesgo y la supervisión |
| RG2.3 | Los métodos de gestión integrada de riesgos |
| RE3.4 | Componentes del escenario de riesgos de TI |
| RR1 .2 | Cumplimiento del estado de los informes |
| * | Cultura de los resultados de riesgo de la encuesta, los datos sobre la adhesión a la política y las normas, los datos sobre los umbrales de tolerancia al riesgo frente a la política frente a las operaciones |

| De | Salida |
|---|---|
| RE1.2 | Los parámetros de rendimiento de cambio cultural hacia la conciencia de los riesgos |
| COBIT PO6 | Directrices de gestión de riesgos de TI |
| COBIT DS7 | Las necesidades de formación específicas para la gestión de riesgos |

* Input from/output to outside Risk IT, Val IT and COBIT

***RG1.6 Promover una comunicación efectiva de los riesgos de TI***
Establecer y mantener un plan de comunicación de riesgos que cubra la política de riesgos de TI, responsabilidades, rendición de cuentas y el paisaje de riesgo (por ejemplo, las amenazas, los controles, los impactos, las causas profundas, las decisiones de negocios). Filtros de características en el plan de lo que es claro, conciso, útil y dirigido a la audiencia correcta. Realizar una comunicación frecuente y regular entre la dirección TI y el mando de negocio en cuanto al estado de publicación de riesgo de TI, preocupaciones (intereses) y exposiciones. Base el negocio y comunicaciones de dirección TI sobre un acercamiento predefinido con los objetivos siguientes:

- Alinear la comunicación de los riesgos de TI con los términos de riesgo empresarial.
- Priorizar constantemente los asuntos de riesgos de TI de manera que alinee con la empresa la definición de riesgo empresarial.
- Expresar los riesgos de TI en la estrategia comercial y términos operativos.
- Comunicar claramente cómo adversos los acontecimientos relacionados con TI que pueden afectar los objetivos de la empresa (por ejemplo, los objetivos de negocio / de puntuación equilibrada, la 4AS, COSO ERM objetivo Categorías).
- Permite que los altos directivos y ejecutivos de TI comprendan, en cantidades reales, el importe de los riesgos para ayudar a dirigir los recursos para responder a los riesgos de TI en consonancia con el apetito y la tolerancia.

| Para | Entradas |
|---|---|
| RG1 .3 | Umbrales de tolerancia de los riesgos de TI |
| RG1.4 | Alinear la política de riesgos de TI. |
| RG2.1 | Alcance del analisis de riesgo |
| RG2.3 | Los métodos de riesgos de gestión integrada |
| RR1 .1, RR1 .4, RR2.2 | Asuntos y oportunidades de los riesgos de TI |
| RR2.5 | Brechas de control y excepcion de póliticas |
| RR3.4 | Riesgos y control de referencia |
| COBIT PO4 | Documentos propios del sistema,organización y relación de TI |

| De | Salidas |
|---|---|
| RE2.4, RR1,1 | Resultado del analisis de |
| All, * | Comunicaión de riesgos |

## DIRECTRICES DE GESTIÓN — RG1

**Cuadro RACI** **Funciones**

**Actividades principales**

| | Board | CEO | CRO | CIO | CFO | Enterprise Risk Committee | Business Management | Business Process Owner | Risk Control Functions | HR | Compliance and Audit |
|---|---|---|---|---|---|---|---|---|---|---|---|
| RG1.1 Realizar la evaluación de la organización de riesgos de TI | I | A | R | R | C | I | R | C | R | C | C |
| RG1.2 Proponer los umbrales de tolerancia de riesgo de TI. | I | I | C | R | C | I | A | C | C | | C |
| RG 1.3 Aprobar la tolerancia al riesgo. | A | C | C | C | C | R | C | C | C | C | C |
| RG1.4 Alinear la política de riesgos de TI. | C | A | R | R | R | C | R | R | R | R | C |
| RG1.5 Promover los riesgos de TI – cultura consciente. | A | R | R | R | R | R | R | R | R | R | R |
| RG1.6 6 Promover una comunicación efectiva de los riesgos de TI | R | R | R | R | R | R | A | R | R | R | R |

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

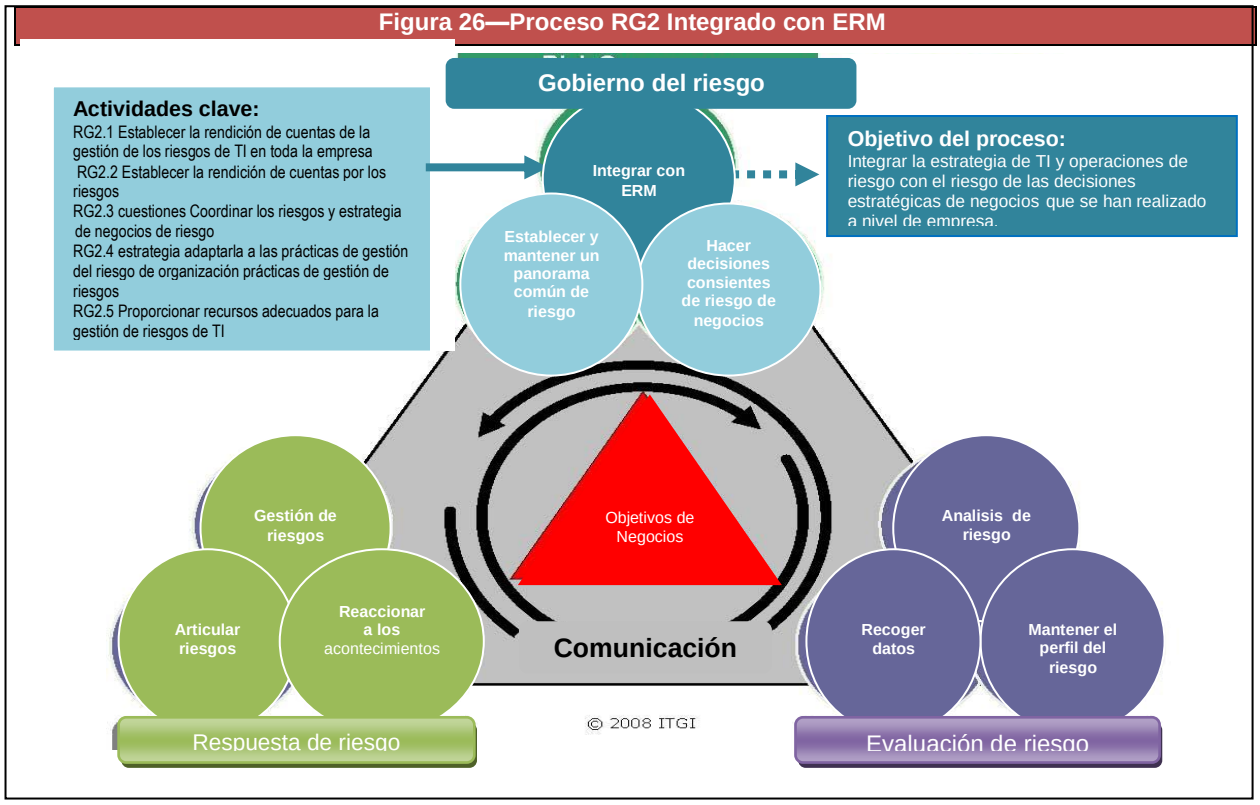
[8] Westerman, *op cit*

**Objetivos y métricas – RG1**

| Objetivos de la actividad | Objetivo de Proceso | Objetivo RG |
|---|---|---|
| • Realizar la evaluación empresarial de riesgos de TI<br>• Proponer los umbrales de tolerancia de riesgo de TI.<br>• Aprobar la tolerancia al riesgo.<br>• Alinear la política de riesgos de TI.<br>• Promover los riesgos de TI – Cultura consciente.<br>• Promover una comuncación efectiva de los riesgos de TI | • Garantizar que la gestión del riesgo alinea las actividades de la empresa con el objetivo de capacidad de TI relacionados con la pérdida del liderazgo y la tolerancia subjetiva de la misma. | • Garantizar que las prácticas de gestión de riesgos de TI están integrados en la empresa, permitiendo a la empresa para garantizar una óptima rentabilidad ajustada al riesgo. |
| Actividad métrica | Métrica de Proceso | Métrica de RG |
| • Frecuencia de evaluación de los riesgos de TI de la empresa<br>• Número de evaluaciones de riesgos de TI fuera del ciclo de toda la empresa<br>•El nivel de participación ejecutiva en evaluaciones de riesgo de TI por toda la empresa (p.ej., atienda en persona, envíe un subordinado, reciba el informe)<br>• Existencia de una política de riesgos de TI<br>• Número de políticas alineadas a la cuál la audiencia prevista ha firmado la adhesión<br>• Porcentaje de empleados capacitados en responsabilidades de gestión de riesgos de TI<br>• Número de comunicaciones que establecen y refuerzan la política de gestión de riesgos y expectativas<br>• Cobertura de la empresa por parte de comunicación al respecto la política de riesgo de TI | • Número de nivel ejecutivo conoce la tolerancia al riesgo violación no son sometidas a medidas disciplinarias (ejecución de la política)<br>• El número de acontecimientos de TI-relacionados con el impacto de negocio en el cual un fracaso de intensificarse era un factor en la presencia(el acontecimiento) de acontecimiento y/o la magnitud de pérdida (por ejemplo, el gestor de riesgos no sabía o no había una alteración en la capacidad de escalar culturales)<br>• Número de políticas en vigor con una o más declaraciones contradictorias relacionadas con una tolerancia al riesgo (la alineación de TI con políticas de tolerancia)<br>•Número de cuestiones de los riesgos que exceden la tolerancia al riesgo | • El grado al cual el empleo estratégico de TI en recursos de apalancamiento de la empresa reduce el riesgo total de la empresa<br>•Porcentaje de personal capacitado en técnicas de gestión de riesgos críticos (por ejemplo, el estándar de técnicas de análisis de riesgos, gestión de crisis, gestión de proyectos, habilidades de las personas [de auditoría, etc] para detectar cuando algo relacionados con la TI está mal) |

## Visión general del proceso

**Figura 26—Proceso RG2 Integrado con ERM**



## DETALLES DE PROCESO

### RG2 Integrar con ERM

Integrar la estrategia de riesgos de TI y las operaciones con el negocio de las decisiones estratégicas del riesgo que se han hecho a nivel de empresa.

***RG2.1 Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa***
Especificar a los responsables y encargados de la gestión de los riesgos TI de la organización. Para el ejecutivo de nivel superior con la responsabilidad general de los riesgos, establecer una expectativa de rendimiento, de incorporar la conciencia de riesgo en la cultura dominante. Establecer la medición del desempeño y procesos de presentación de informes con los niveles apropiados de reconocimiento, aprobación, incentivos y sanciones. Asegurar que hay estructuras en su lugar (por ejemplo, el comité de empresa de riesgo, los riesgos del consejo, comité de estrategia de TI, funcionarios de riesgos) la participación de la empresa con la tecnología de gestión de riesgos y decisiones día a día las operaciones. Crear una distinción entre las funciones de las unidades de negocio (que poseen y administran el riesgo en el día a día), las funciones de control de riesgos (que ofrecen experto en la materia de evaluación y asesoramiento), y la auditoría interna (que proporcionan garantía independiente). Identificar los directores de empresa con autoridad para abordar cuestiones de los riesgos de TI a través de ella, beneficios y la habilitación de valor, los programas y la ejecución de proyectos y operaciones de TI y prestación de servicios. Establezca expectativas para estos administradores de las políticas de normas, controles y el cumplimiento de las actividades de vigilancia (por ejemplo, el establecimiento y seguimiento de RISK). Establecer y evaluar los objetivos de rendimiento basados en el riesgo-retorno de toma de decisiones conscientes (por ejemplo, la capacidad de los administradores para integrar y equilibrar la gestión del rendimiento con la gestión del riesgo a través de su ámbito de autoridad). Asignar funciones específicas para la gestión de los riesgos de TI por dominios (por ejemplo, la capacidad del sistema, la dotación de personal de TI, es la selección de programas). Asignar a cada dominio un nivel de criticidad en función del riesgo / recompensa. Cuando sea necesario, asignar responsabilidades adicionales de gestión de riesgo (por ejemplo, sistemas específicos) a niveles inferiores y requisitos externos.

| Para | Entrada |
|---|---|
| RG1.1 | Enfoque de areas de riesgo |
| RG1.4 | Politicas de riesgo de TI, |
| RG2.2 | Alcance de la gestión de riesgos de TI |
| RG3.4, RR3.4 | Los requisitos de respuesta de Riesgo |
| RR1 .1, RR1 .4, RR2.2 | Oportunidades y asuntos de riesgos de TI |
| Val IT VG1 | El compromiso del liderazgo |
| Val IT VG2 | funciones de negocio, las responsabilidades, la rendición de cuentas |
| COBIT PO4 | Los propietarios del sistema documentado, organización y relaciones |
| COBIT PO7 | Funciones y responsabilidades |

| De | Salida |
|---|---|
| RG1 .4, RR2.1 | Dominio de los propietarios de riesgos de TI |
| RG1 .4, RG1 .5, RG1 .6, RG2.5; COBIT PO4, PO7; * | Los objetivos de rendimiento, incentivos y recompensas, las funciones integradas y responsabilidades para la gestión del riesgo y la supervisión |
| RG2.2, RG2.5, RG3.3, RR2.4, RR2.5, RR3.1; Val IT PM4; COBIT PO4, PO9, AI6, ME1, ME2 | Plan de acción de los riesgos de TI |
| RG2.4, RE3.1; COBIT PO4, PO7; * | Funciones y responsabilidades |

* Input from/output to outside Risk IT, Val IT and COBIT

***RG2.2 Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial.***
Relaciona como la gestión de riesgos de TI se define en el contexto de la protección y el mantenimiento de un proceso de negocio o actividad empresarial. Adoptar y adaptar su marco empresarial existente para el riesgo empresarial. Integrar los aspectos específicos de TI en un enfoque empresarial. Entender los objetivos de riesgo de la empresa y los objetivos y la mezcla de cuestiones de los riesgos que afectan a las empresas y las limitaciones de recursos. Determinar cómo la gestión de riesgos debe ser abordada en el contexto del universo de riesgos de la empresa y otros tipos de riesgos de la empresa. Definir el papel del departamento de TI en las actividades de gestión del riesgo operativo basado en el grado de dependencia del negocio en TI y la infraestructura física relacionada con la satisfacción en el logro de objetivos financieros, operativos y de clientes. Coordinar las actividades de evaluación de riesgo y realizar informes integrados. Coordinar el riesgo y asuntos de clasificación; escalas de clasificación de riesgo (por ejemplo, la frecuencia, magnitud, impacto en el negocio); categorías de control (por ejemplo, predicción, detección, corrección) y las jerarquías basadas en el riesgo para las políticas, normas y procedimientos de operación. Cuando sea posible, emplear principios del MTC y las opiniones de riesgo (por ejemplo, vista actuarial, vista de la cartera, los sistemas de vista de predicción). Determinar cuándo y cómo ciertos puntos de vista del riesgo de la empresa se van a utilizar para los riesgos de TI. Acomodación de la empresa, las necesidades de rendimiento único y externo.

| Para | Entrada |
|---|---|
| RG1.1 | Enfoque de areas de riesgo,los servicios principales ya apoyo a la empresa de procesos y sistemas,alto nivel de escenario de riesgos |
| RG1.4 | Politicas de riesgo de TI, |
| RG2.1, RG2.3, RR2.3, RR3.4 | Plan de accion de riesgos de TI |
| RR1 .2 | Entradas para la presentación de informes integrados de riesgo empresarial |
| RR1 .1, RR1 .4, RR2.2 | Oportunidades y asuntos de riesgos de TI |
| RR2.2 | Los requisitos de control |
| RR3.1 | Los planes de respuesta a incidentes |
| RR3.4 | Mejoras de los procesos |
| COBIT PO9 | Directrices de gestión relacionadoscon riesgos de TI |
| COBIT ME4 | El apetito de las empresas para los riesgos de TI, dirección estratégica para las empresas de TI |
| * | La estrategia empresarial, objetivos, metas, el universo de riesgo, el apetito de riesgo y de gestión de riesgos |

* Input from/output to outside Risk IT, Val IT and COBIT

| De | Salida |
|---|---|
| RG1 .1, RG1 .4, RG2.3, RG3.4, RE1.1, RE2.1, RR1 .1, RR2.1, RR2.2, RR3.2, COBIT PO9 | La estrategia de gestión integrada de riesgos |
| RG2.1, RG2.3, RG2.4, RG2.5, COBIT PO6 | Alcance de gestión de riesgos de TI |
| RG2.5, RG3.3, RR2.4, RR2.5, RR3.1; Val IT PM4; COBIT PO4, PO9, AI6, ME1, ME2 | Plan de accion de riesgos de TI |
| RE3.2, RE3.4 | Establecimiento de prioridades de los inventarios de riesgos y el impacto de las categorías |
| RR1 .2 | Requisitos de información integrada de riesgos |
| COBIT PO1; * | Prioridades y estrategia de negocios integrada |
| * | Cambios a la estrategia de la empresa de riesgo |

* Input from/output to outside Risk IT, Val IT and COBIT

***RG2.3 Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa.***
Organizar los riesgos de TI existentes. Los métodos de gestión son los encargados de: 1) entender el contexto de negocio de TI (por ejemplo, la actividad de negocios de TI, análisis de la dependencia, análisis de escenarios), 2) identificar los riesgos de TI (por ejemplo, modelo de datos, vías de escalada), 3) regular los riesgos de TI (por ejemplo, la empresa de riesgos de TI, procedimientos de evaluación, modelos de decisión basados en el riesgo) y 4) gestionar los riesgos de TI (por ejemplo, seleccione el RISK adecuado para el desempeño empresarial, adecuar los objetivos y definir los procedimientos de escalada). Entender las expectativas de la empresa de gestión de riesgos, actividades y métodos que son relevantes para TI (por ejemplo, la gerencia, la comunicación y la formación, cómo el riesgo se identifica y mide, cómo se evalúan los controles, qué información se proporciona a quién, cómo es el apetito de riesgo establecido y acordado). Identificar las lagunas específicas de gestión de riesgos de TI, las prácticas que deben ser actualizadas o creadas para satisfacer las expectativas de MTC. Del mismo modo, identificar las actividades de los riesgos institucionales que se deberían añadir o actualizar para tener plenamente en cuenta los riesgos de TI. Identificar otras funciones que se hagan o que haya que hacer en apoyo de los objetivos de la empresa y la gestión de riesgos de TI. Dar prioridad a los esfuerzos de la pista para cerrar las brechas entre los riesgos de TI y del MTC y mejorar la eficacia y la eficiencia (por ejemplo, optimizar controles, agilizar la evaluación de riesgos, coordinar RISK, escalada de desencadenantes e integrar los informes).

| Para | Entrada |
|---|---|
| RG2.2 | Estrategia de gestión integrada de riesgos, ámbito de aplicación de gestión de riesgos |
| RG3.1 | Enfoque de los asuntos del analisis de riesgos de TI |
| RR2.2 | Prinicipales indircadores de riesgos de TI y la escalada de los desencadenantes |
| RR3.4 | Mejoras del proceso |

| De | Salida |
|---|---|
| RG1 .1, RG1 .5, RG1 .6, RG3.1, RE2.1, RE2.2, RE3.2, RR3.2, RR3.4 | Los metodos de gestión integrada de riesgos |
| RG2.2, RG2.5, RG3.3, RR2.4, RR2.5, RR3.1; Val IT PM4; COBIT PO4, PO9, AI6, ME1, ME2 | Plan de acción de riesgos |
| * | Las actualizaciones de las actividades de ERM, proceso integrado de gestión de problemas y de la plataforma compartida por las diversas funciones de |
| * Input from/output to outside | Risk IT, Val IT and COBIT |

***RG2.4 Proporcionar recursos adecuados para la gestión de riesgos.***
Identificar necesidades de recursos para la gestión de riesgos en el negocio y el nivel de TI y en el contexto de la competencia, cuestiones de los riesgos de negocios, las limitaciones de recursos y objetivos. Asignar los fondos necesarios para llenar las lagunas y la posición de la empresa para aprovechar las oportunidades. Establecer el riesgo / recompensa de comercio externo en relación con los objetivos de la organización (por ejemplo, asignar recursos más o menos sobre la base de la criticidad de los datos dentro de un enfoque escalonado para la seguridad de la información). Considerar:
• Personas y habilidades (Como especificar los conocimientos de gestión del riesgo de los administradores y el personal de desarrollo y mantenimiento).
• Los procesos y procedimientos documentados para la gestión de los riesgos de TI.
• Sistemas de información y base de datos para cuestiones de gestión de TI.
• Presupuesto y otros recursos para la respuesta específica de actividades de riesgo.
• Expectativas de los reguladores y los auditores externos.

| Para | Entrada |
|---|---|
| RG1 .3 | Umbrales de tolerancia de los riegos de TI |
| RG1 .4 | Politicas de riesgo de TI |
| RG2.1 | Funciones responsabilidades |
| RG2.2 | Alcance de la gestión de riesgos de TI |

| De | Salida |
|---|---|
| COBIT PO4, PO7; * | Requisitos de los recursos de la gestión de riesgos de TI, funciones y responsabilidades, descripción de puestos, las habilidades de la matriz, las relaciones |
| * Input from/output to outside | Risk IT, Val IT and COBIT |

***RG2.5 Garantizar el aseguramiento independiente sobre la gestión de riesgos***
Supervisar los riesgos de TI, establecer planes de acción y obtener garantías sobre el desempeño de las principales prácticas de gestión de riesgos de TI y si el riesgo se gestiona de acuerdo con el apetito de riesgo y la tolerancia.

| Para | Entradas |
|---|---|
| RG1.3 | Umbrales de tolerancia de los riesgos de TI |
| RG1.4 | Alinear la política de riesgos de TI. |
| RG2.1, RG2.2, RG2.3, RR2.3, RR3.4 | Plan de acción de riesgos deTI |
| RG2.1 | Rendimiento de los objetivos, incentivos y recompensas, las funciones integradas y responsabilidades para la gestión del riesgo y la supervisión |
| RG2.2 | Alcance del analisis de riesgo |
| RG3.4 | Aceptación docuemnteda del riesgo |
| RR1.2 | Estado del cumplimiento de los informes, los insumos para la presentación de informes integrados de riesgo empresarial |
| RR2.1 | Base de contro y riesgos |
| RR2.5 | Procesos del plan de acción de riesgos de TI/ desviaciones |
| RR3.4 | Mejoras del proceso |
| COBIT ME4 | El apetito de las empresas para los riesgos de TI, dirección estratégica para las empresas de TI |

| De | Salidas |
|---|---|
| * | Información del consejo |

## Directrices de gestión – RG2

**Cuadro RACI** **Funciones**

**Actividades principales**

| | Board | CEO | CRO | CIO | CFO | Enterprise Risk Committee | Business Management | Business Process Owner | Risk Control Functions | HR | Compliance and Audit |
|---|---|---|---|---|---|---|---|---|---|---|---|
| RG2.1 Establecer la rendición de cuentas en toda la empresa para la gestión de los riesgos. | A | R | R | R | R | I | I | I | C | C | C |
| RG2.2 Determinar la responsabilidad para asuntos de riesgos de TI. | A | R | C | R | C | C | R | C | C | C | I |
| RG2.3 Coordinar la estrategia de riesgo de TI y estrategia de riesgo del negocio. | | | C | A/R | C | I | C | C | R | C | C |
| RG2.4 Adaptar las prácticas de gestión de riesgos de TI a las prácticas organizativas de gestión de riesgos. | A | R | C | R | | I | C | R | C | C | |
| RG2.5 Proporcionar recursos adecuados para la gestión de riesgos de TI | A/R | C | C | C | C | C | C | C | C | C | C |

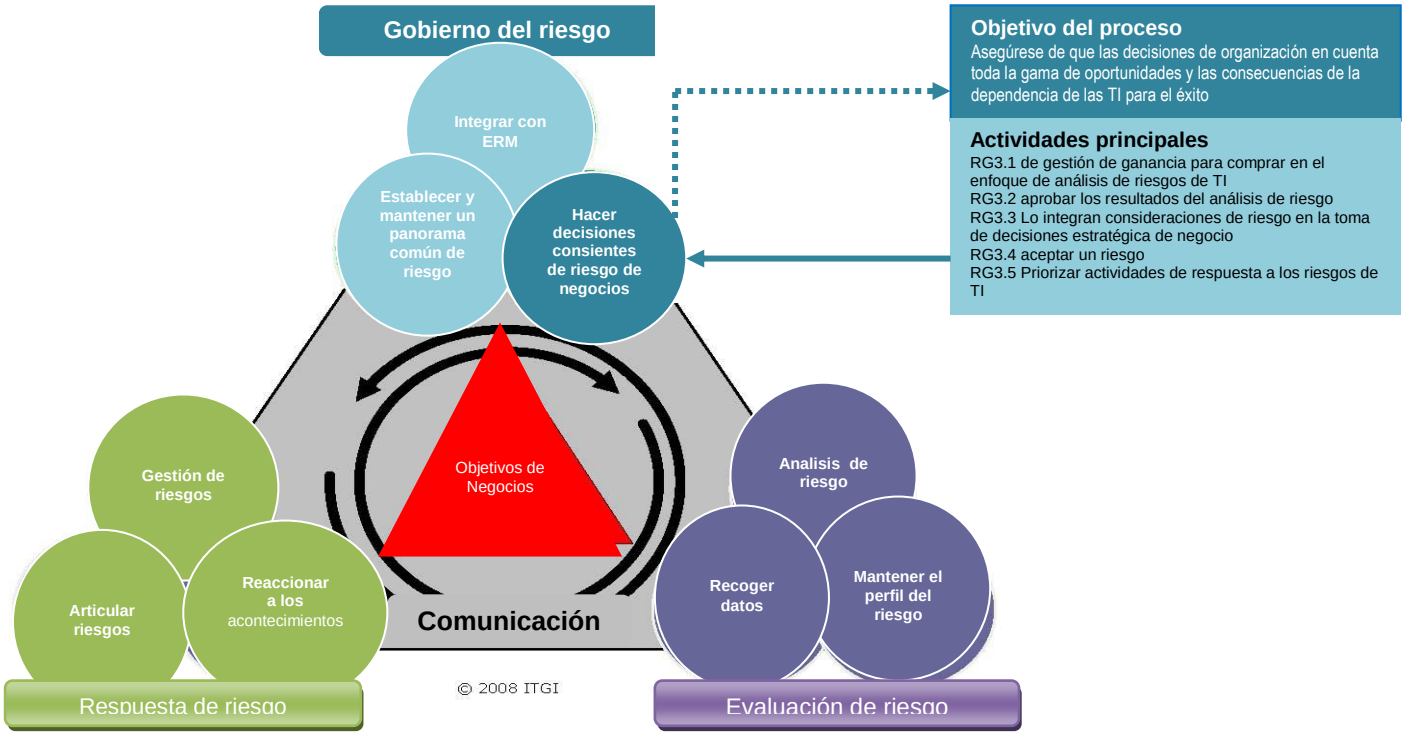
A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

***Métricas y objetivos – RG2***

| Objetivos de la actividad | Objetivos del proceso | Objetivo RG |
|---|---|---|
| • Establecer y mantener la rendición de cuentas para la gestión de riesgos.<br>• Establecer la responsabilidad para los problemas del riesgo de TI.<br>• Coordinar la estrategia del riesgo de TI y la estrategia del riesgo empresarial.<br>• Adaptar las prácticas de gestión de riesgos de TI a las prácticas de gestión de riesgos de organización.<br>• Proporcionar recursos adecuados para la gestión de riesgos de TI.<br>• Proporcionar garantías independientes sobre la gestión de riesgos de TI. | • Integrar la estrategia del riesgo TI y las operaciones con el negocio de las decisiones estratégicas del riesgo que se han hecho a nivel de empresa. | • Asegurar de que las prácticas de gestión de riesgos de TI están integradas en la empresa, permitiendo a la empresa garantizar el óptimo rendimiento de riesgo ajustado. |
| Actividad métrica | Métrica del proceso | Métricas RG |
| • Porcentaje de empleados cuyos parámetros de rendimiento y premios reflejan los objetivos de la gestión de riesgos.<br>• Una alineación de puntuación correspondiente a RACI con respecto a la clasificación de las acciones a tomar (por ejemplo, el porcentaje de riesgos más importantes de TI relacionados con la rendición de cuentas aceptada por la empresa y el personal de TI).<br>• Número diferente de informes de riesgo presentados a la Junta; extensión de integración de la información sobre los riesgos de TI.<br>• Grado de perfección de la estrategia de gestión integrada de riesgos<br>• Porcentaje de la estrategia de gestión integrada de riesgos con el apoyo de los métodos definidos aplicables a los riesgos de TI<br>• Porcentaje de estructuras informáticas de gestión de riesgos y actividades puestas en marcha frente a lo previsto<br>• Porcentaje de las prácticas de los riesgos de TI adaptadas a las expectativas de la organización de ERM.<br>• Porcentaje de los planes de gestión de acción del riesgo TI aprobados para la ejecución.<br>• Porcentaje de las actividades básicas del ERM, con la integración de consideraciones de riesgos de TI.<br>• Número de diferentes procesos de gestión de cuestiones y las plataformas<br>• Porcentaje de Líneas de Negocio Con los presupuestos asignados base de la importancia de riesgo (por ejemplo, por los resultados de la evaluación de riesgo),<br>• Número de posiciones abiertas en el personal de gestión de riesgos. | • Porcentaje de ejecutivos y gerentes de empresas que han recibido formación sobre la dependencia de la empresa y sobre el uso de las TI, el riesgo asociado, la estrategia y marco de los riesgos de TI.<br>• Porcentaje de los gastos de la gestión de riesgos operacionales que tienen una directa trazabilidad a la estrategia de negocio de riesgo.<br>• Porcentaje de los proyectos empresariales que consideran los riesgos de TI.<br>• Porcentaje de las actividades básicas del ERM que consideran los riesgos de TI.<br>• Frecuencia de los riesgos de TI como un tema del programa para el comité ejecutivo.<br>• Medida de alineación de Objetivos comunes a través de ERM y gestión de riesgos TI<br>• Porcentaje de los controles que se ponen a prueba varias veces (por ejemplo, unidades de negocio, de riesgo y las funciones de control a continuación, la auditoría interna)<br>• Número de resultados por separado dentro de las evaluaciones de riesgo de una entidad que no puede agregar | • El grado en que el uso estratégico de las TI en la movilización de recursos de la empresa reduce el riesgo de la empresa en general.<br>• Porcentaje de personal capacitado en técnicas de gestión de riesgo crítico (por ejemplo, técnicas de análisis de riesgo estándar, gestión de crisis, gestión de proyectos, habilidades de las personas [de auditoría, etc.] para detectar cuando algo relacionado con las TI está fuera de lugar). |

## Visión general del proceso

**Figura 27—Proceso RG3 Toma de riesgos - decisiones conscientes de las empresas**



## DETALLES DEL PROCESO

### RG3 Toma de decisiones consciente del riesgo de negocio

Asegurar que las decisiones de la organización cuentan con una amplia gama de oportunidades y las consecuencias de la dependencia de la TI para el éxito.

***RG3.1 Ganancia de la gestión de compra - para el enfoque de análisis de riesgos.***
Formación de gestión en la toma de decisiones sobre el enfoque del proyecto de análisis de riesgos de TI. Ilustrar cómo de los resultados de los análisis de riesgo se pueden beneficiar las grandes decisiones. Describir cuál es el nivel de calidad que se debe esperar de la toma de decisiones, cómo interpretar los informes de análisis de riesgos, las definiciones de los términos clave (por ejemplo, las probabilidades de riesgo, el grado de error, los factores de riesgo), las limitaciones de las mediciones y estimaciones basadas en datos incompletos. Identificar las brechas con las expectativas de riesgo empresarial.

| Para | Entrada |
|---|---|
| RG1 .4 | Politicas de riesgos de TI |
| RG2.3 | Los métodos de gestión integrada de riesgos |

| De | Salida |
|---|---|
| RG2.3 | Enfoque de cuestiones del analisi del riesgo |

***RG3.2Aprobar el análisis de riesgos de TI***
Determinar si el informe de análisis de riesgos proporciona información suficiente para comprender los riesgos y para evaluar los riesgos de las opciones de respuesta. Observe sus limitaciones para las decisiones actuales. Aprobar los resultados de los análisis de riesgo.

| Para | Entrada |
|---|---|
| RR1.1 | Análisis y resultados de riesgos |

| De | Salida |
|---|---|
| RG3.3, RG3.4, RG3.5 | Aprobar el informe de análisis de riesgos, las limitaciones de análisis de riesgos |
| RR1 .1 | Deficiencias en el análisis de riesgos |

***RG3.3 Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio.***
Se debe ser proactivo en la búsqueda los factores de riesgo de TI antes de la toma de decisiones de negocios para llevar información útil donde se están tomando dichas decisiones. Ejemplos de información incluyen el riesgo y niveles de desempeño dentro de la cartera de aplicaciones informáticas en comparación con el valor de los procesos de negocio que soportan o las oportunidades para reequilibrar la cartera de empresas basadas en el riesgo, el retorno y cambios previstos en el entorno de TI. Ayuda a la gestión empresarial teniendo en cuenta el efecto que los riesgos de TI y la capacidad existente de gestión de riesgos (controles, capacidades, recursos) tendrán sobre las decisiones empresariales y las decisiones de negocios. El efecto que puede tener en la exposición al riesgo de TI. Los riesgos de TI en la capacidad de gestión a futuro. Gestionar que las empresas comprendan los riesgos de TI basados en las opiniones diversas de cartera (por ejemplo, las empresas unidad, producto, proceso) y valorar el peso del impacto que la propuesta de inversiones en TI tendrán sobre el perfil de riesgo global de la empresa (aumento o reducción del riesgo). Como condición para la aprobación de las decisiones empresariales el coste y oportunidades deben sopesarse con una neta estimada que cambiará según el riesgo de exposición de TI.

| Para | Entrada |
|---|---|
| RG1 .1 | Los principales servicios y el apoyo a los procesos de negocio y sistemas de escenarios de riesgo de alto nivel |
| RG1 .3 | Umbrales de tolerancia de riesgos de TI |
| RG2.1, RG2.2, RG2.3, RR2.3, RR3.4 | Plan de acción de riesgos de TI |
| RG3.2 | Aprobar el informe de análisis de riesgos, las limitaciones de análisis de riesgos |
| RE3.3 | Evaluación de las capacidades de TI |
| RE3.5 | Perfil de los riesgos de TI |
| RR1 .1 | Pérdida o aumento de las probabilidades y los rangos, las opciones de respuesta de riesgo, costo / beneficio expectativas |
| RR1 .1, RR1 .4, RR2.2 | Temas y oprtunidades de riesgosde TI |
| RR1 .3 | Resultados de la evaluación independiente de TI en el contexto |
| COBIT PO1 | Plan estratégico de TI, los planes tácticos de TI, IT cartera de proyectos, la cartera de servicios de TI, la estrategia de externalización de TI, la estrategia de adquisición de TI |
| * | Decisiones pendientes de negocio |

*Entradas/Salidas a Risk IT, Val IT y COBIT

| De | Salida |
|---|---|
| RE2.1 | Solicitud de análisis de riesgos |
| RE3.5 | Cambio del pefil de riesgos |
| RR2.3, Val IT IM5 | El coste del ciclo vital económico y el beneficio total |
| Val IT VG1 | Elementos de riesgo que deben incluirse en el valor del proceso de gestión |
| Val IT IM1 | Los riesgos relacionados con las oportunidades |

***RG3.4 Aceptar los riesgos de TI.***
Usando los umbrales de tolerancia de riesgos como una guía, decidir si acepta el nivel de riesgo de exposición restante. Considere pertinentes la información de los informes de análisis de riesgo como la probabilidad de pérdida y de intervalos de tiempo, las opciones de respuesta ante el riesgo, costo / beneficio de las expectativas y el efecto potencial de la agregación de riesgos. Discuta con los propietarios afectados de procesos de negocio y juntos analicen las relaciones riesgo-rendimiento y determine donde pasar el presupuesto de riesgo de los riesgos "conocidos" para permitir la aceptación del riesgo desconocido. Obtener un acuerdo comercial sobre el riesgo de aceptación o de no aceptación y de adecuada respuesta de los requisitos de riesgo. Documentar cómo el riesgo se consideró en la decisión y la razón de ser de cualquier excepción a la tolerancia al riesgo (por ejemplo, gran oportunidad de negocio estratégico). Garantizar que las decisiones de aceptación del riesgo y los requisitos de respuesta al riesgo se comunican a través de líneas de organización de conformidad con el riesgo establecido de las empresas, las políticas de gobierno corporativo y los procedimientos.

| Para | Entrada |
|---|---|
| RG1 .3 | Umbrales de tolerancia de riesgos de TI |
| RG2.2 | Estrategia entregada de gestión de riesgos |
| RG3.2 | Aprobar el informe de análisis de riesgos, las limitaciones de análisis de riesgos |
| RE3.5 | Perfil de los riesgos de TI |
| RR1 .1 | Pérdida o aumento de las probabilidades y los rangos, las opciones de respuesta de riesgo, costo / beneficio expectativas |
| RR1 .1, RR1 .4, RR2.2 | Temas y oprtunidades de riesgosde TI |
| RR1 .2, RR2.2 | Resultados de la evaluación independiente de TI en el contexto |
| RR1 .3 | Plan estratégico de TI, los planes tácticos de TI, IT cartera de proyectos, la cartera de servicios de TI, la estrategia de externalización de TI, la estrategia de adquisición de TI |
| RR2.2 | La agregación de datos de riesgo |

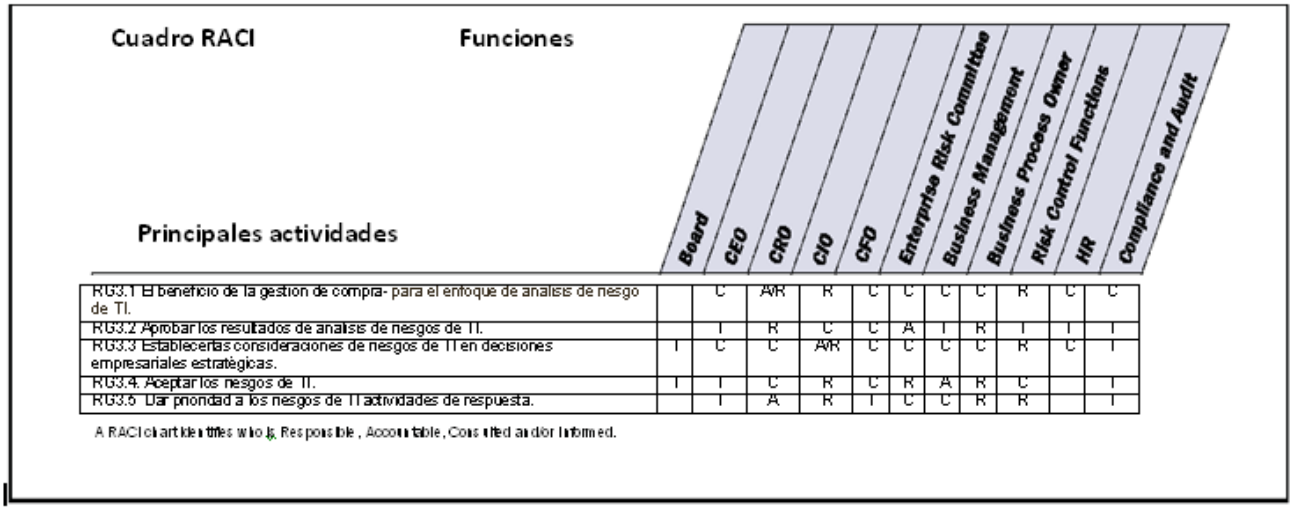
| De | Salida |
|---|---|
| RG2.1, RE2.3, RR2.1, RR2.3, RR2.4 | Los requisitos de respuesta de Riesgo |
| RG2.5, RE3.5, RE3.6 | Aceptación documentada de riesgo |
| RE2.1 | Solicitud de análisis de riesgos |
| RE3.5 | Cambio del pefil de riesgos |

***RG3.5 Priorizar actividades de respuesta de riesgos de TI.***
Examinar la cartera de actividades de respuesta al riesgo para identificar los que tienen un mayor impacto probable sobre la reducción del riesgo global. Cuantificar la reducción prevista en general en la frecuencia y magnitud a través de la aplicación de los controles, la capacidad y los recursos. Hacer hincapié en proyectos específicos con mayores probabilidades (relativas) de:
• Reducir las concentraciones de riesgo (por ejemplo, las mejoras a la arquitectura, la separación de las unidades operativas y sistemas)
• Implementar controles que tratan directamente los múltiples tipos de riesgos
• Implementar controles que mejoren la eficacia del proceso y evitar la toma de riesgos excesivos
Registrar los fundamentos, limitaciones y cómo la decisión está impulsando cambios en la política pública, los controles operativos, capacidades, el despliegue de recursos y planes de comunicación. Cuando proceda, registre la razón de que se sobrepase o caiga por debajo de apetito del riesgo y la tolerancia.

| Para | Entrada |
|---|---|
| RG1 .3 | Umbrales de tolerancia de riesgos de TI |
| RG3.2 | Aprobar el informe de análisis de riesgos, las limitaciones de análisis de riesgos Aprobar el informe de análisis de riesgos, las limitaciones de análisis de riesgos |
| RE3.5 | Perfil de los riesgos de TI |
| RR1 .1 | Pérdida o aumento de las probabilidades y los rangos, las opciones de respuesta de riesgo, costo / beneficio expectativas |
| RR1 .1, RR1 .4, RR2.2 | Temas y oprtunidades de riesgosde TI |
| RR1 .3 | Resultados de la evaluación independiente de TI en el contexto, los acontecimientos de la vulnerabilidad |
| Val IT VG3 | Criterios de evaluación de inversiones |
| Val IT IM2 | La comprensión total de los programas de candidatos incluidos los cursos de acción alternativos |
| COBIT PO5 | Presupuesto de TI |
| * | Presupuesto de funcionamiento |

| De | Salida |
|---|---|
| RE2.1 | Los requisitos de respuesta de Riesgo |
| RE3.5 | Cambios del perfil de riesgos de TI |
| RE3.5,RR2.3 | Prioridad de respuesta de riesgos (eliminación del riesgo) |
| RR2.3; Val IT PM4 (si es un caso de negocios completo está ya hecho), IM1 (si es un caso de negocios todavía tiene que ser hecho) | Prestaciones de gestión de riesgo asignado a la cartera de TI |

**Directrices de gestión-RG3**



**Cuadro RACI** **Funciones**

**Principales actividades**

| | Board | CEO | CRO | CIO | CFO | Enterprise Risk Committee | Business Management | Business Process Owner | Risk Control Functions | HR | Compliance and Audit |
|---|---|---|---|---|---|---|---|---|---|---|---|
| RG3.1 El beneficio de la gestión de compra- para el enfoque de análisis de riesgo de TI. | | C | A/R | R | C | C | C | C | R | C | C |
| RG3.2 Aprobar los resultados de análisis de riesgos de TI. | | I | R | C | C | A | I | R | I | I | I |
| RG3.3 Establecer las consideraciones de riesgos de TI en decisiones empresariales estratégicas. | I | C | C | A/R | C | C | C | C | R | C | I |
| RG3.4. Aceptar los riesgos de TI. | I | I | C | R | C | R | A | R | C | | I |
| RG3.5 Dar prioridad a los riesgos de TI actividades de respuesta. | | I | A | R | I | C | C | R | R | | I |

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

**Métricas y Objetivos**

| Objetivos de la actividad | Objetivos del proceso | Objetivos RG |
|---|---|---|
| • El beneficio de la gestión de compra- para el enfoque de análisis de riesgo de TI.<br>• Aprobar los resultados de análisis de riesgos de TI.<br>• Establecer las consideraciones de riesgos de TI en decisiones empresariales estratégicas<br>• Aceptar los riesgos de TI.<br>• Dar prioridad a los riesgos de TI actividades de respuesta. | • Asegurar que las decisiones de organización consideran la gama completa de oportunidades y consecuencias derivadas de la dependencia de las TI para el éxito | • Asegúrese de que las prácticas de gestión de riesgos de TI están integradas en la empresa, permitiendo a la empresa obtener rentabilidad ajustada al riesgo óptimo. |
| **Actividades Métricas** | **Métricas del Proceso** | **Métricas RG** |
| • Porcentaje de decisiones de negocio que debería haber considerado los riesgos de TI, pero no lo hicieron.<br>• Eventos / pérdidas derivadas de la decisión de aceptación de riesgo, incluyendo pérdidas de oportunidad<br>• Porcentaje de aceptación de riesgo con un conjunto completo de documentación de apoyo.<br>• Número de actividades de respuesta de prioridad de riesgo.<br>• El porcentaje de los asuntos de riesgos de TI para los que se registra la reducción esperada en la frecuencia y la magnitud. | • Valor de los proyectos fallidos debido a problemas no identificados durante el proceso de decisión (por ejemplo, ¿el riesgo se presenta en el registro de riesgo? ¿fue estimado correctamente? ¿Existe seguimiento?)<br>• Número de decisiones claves de gestión realizadas sin la disponibilidad de un informe de análisis de riesgo pertinentes<br>• Porcentaje de las decisiones (o indecisión) que conduce a la pérdida de TI relacionados con reconsiderar las lecciones aprendidas<br>• El tiempo de ciclo desde el descubrimiento de una deficiencia de control (por ejemplo, el evento de la vulnerabilidad) a una decisión de aceptación de riesgo<br>• El tiempo de ciclo desde las excepciones de orden a una decisión sobre su disposición. | • El grado en que el uso estratégico de las TI en la movilización de recursos de la empresa reduce el riesgo de la empresa en general.<br>• Porcentaje de la posición de la gestión de riesgos cubiertos con personal capacitado en técnicas de gestión de riesgo crítico (por ejemplo, técnicas de análisis de riesgo estándar, gestión de crisis, gestión de proyectos, habilidades de las personas [de auditoría, etc.] para detectar cuando algo no anda bien relacionado con las TI) |

## MODELOS DE MADUREZ DE DOMINIO (RG)
## ALTO NIVEL

**0 No existe cuando**
La organización no ha reconocido la necesidad de considerar el impacto en el negocio de los riesgos de TI. Las decisiones que implican la asunción de riesgos de TI tienden a basarse en la falta de información o información incorrecta. No hay conciencia de los requisitos externos para la gestión de riesgos de TI y la integración con la gestión de riesgos empresariales.

**1 Inicial cuando**
Hay un nuevo concepto de que el riesgo de TI es importante y debe ser gestionado, pero es visto como un problema técnico y la empresa considera principalmente la desventaja de los riesgos de TI. Los criterios de identificación de riesgo de TI varían ampliamente en toda la organización y en la organización de TI. De forma predeterminada TI es responsable de la gestión de problemas, la disponibilidad, el acceso al sistema, etc. El apetito por el riesgo y la tolerancia sólo se consideran en las evaluaciones de riesgos episódicos. Las políticas de empresa y las normas, que son mínimas en la mayoría de casos, pueden estar incompletas y / o reflejan sólo las exigencias externas y la falta de razones justificables y los mecanismos de observancia. Las habilidades de gestión de riesgos de TI pueden existir sobre una base *ad hoc* pero no son desarrolladas activamente. Los inventarios *ad hoc* centrados en el control se encuentran dispersos a través de aplicaciones de escritorio.

**2 Repetibles cuando**
Hay una conciencia de la necesidad de controlar activamente los riesgos de TI, pero la atención se centra en el cumplimiento técnico sin previsión del valor añadido. Hay líderes emergentes para la gestión de riesgos de TI dentro de los departamentos quienes asumen la responsabilidad y suelen ser considerados responsables, incluso si no hay un acuerdo formal. La tolerancia del riesgo se establece a nivel local y puede ser difícil de agregar. Las inversiones están centradas en cuestiones de riesgo específico, dentro de los departamentos funcionales y de negocio (por ejemplo, seguridad, continuidad del negocio, operaciones). Hay necesidad de orientación de la junta directiva para la gestión de riesgos. Requisitos de formación mínimos, que incluyen una toma de conciencia de los riesgos de TI para zonas de riesgos críticos de la empresa. Existen inventarios funcionales y departamentales de TI sobre cuestiones de riesgo.

**3 Definidos cuando**
La gestión de riesgos se ve como una cuestión empresarial y tanto las desventajas como las ventajas de los riesgos de TI son reconocidas. Hay un líder designado para los riesgos de TI en toda la empresa, este líder está comprometido con el Comité de Riesgos de la empresa, donde los riesgos de TI están al alcance y son discutidos. La empresa entiende cómo se integra a nivel mundial o a vista de cartera, la perspectiva de riesgo. La tolerancia al riesgo de la empresa se deriva de la tolerancia local y las actividades de gestión de riesgos de TI están siendo alineadas en toda la empresa. Las categorías de riesgo formales han sido identificadas y descritas en términos claros. La formación sobre sensibilización de riesgos incluye las situaciones y escenarios más allá de políticas específicas y de las estructuras y un lenguaje común para la comunicación de riesgos. Existen requisitos definidos para un inventario centralizado de los problemas de riesgo. Herramientas de flujo de trabajo se utilizan para incrementar los temas de riesgo y las decisiones en el desarrollo del trabajo. .

**4 Gestionados cuando**
La gestión de riesgos se ve como un facilitador de negocios y se entienden tanto la baja como el alza de los riesgos de TI. El líder designado para los riesgos de TI en toda la organización está plenamente comprometido con el comité de riesgo de la empresa que espera que sus opiniones aporten valor en la toma de decisiones. El papel del departamento de TI en la gestión del riesgo operacional y la gestión del riesgo empresarial más amplio está bien entendido. El Consejo define el apetito de riesgo y la tolerancia para todos los departamentos, incluidos los riesgos de TI. Las políticas de empresa y las normas reflejan la tolerancia al riesgo empresarial. Se planifican prudentemente los escenarios de riesgo considerando los riesgos de TI en toda la empresa. Las principales decisiones de riesgo se toman considerando plenamente la probabilidad de pérdida y de recompensa. Las necesidades de competencias se actualizan rutinariamente para todos los ámbitos, la competencia está garantizada para toda la gestión de riesgo de TI de gestiones de flujos de trabajo y el seguimiento de las actividades críticas y de los controles.

**5 Optimizado cuando**
Los altos ejecutivos consideran en sus decisiones todos los aspectos de riesgos de TI. El líder del riesgo se considera un asesor de confianza durante el diseño e implementación de operaciones. El departamento de TI es un actor importante en la línea de los esfuerzos empresariales de riesgo operacional y los esfuerzos globales de la empresa en relación a los riesgos. Los objetivos estratégicos se basan en un entendimiento a nivel ejecutivo de TI de las amenazas de negocios relacionados, los escenarios de riesgo y la competitividad de las oportunidades. Las políticas de empresa y las normas siguen reflejando la tolerancia al riesgo empresarial mientras aumenta la eficiencia. La empresa exige formalmente la mejora continua de la gestión de las capacidades de los riesgos de TI basada en objetivos claramente definidos de personal y de organización. Existe seguimiento en tiempo real de los eventos y excepciones de control al igual que la automatización de la gestión de la política.

| FIGURA 28 - (RG) Modelo detallado par de Madurez | | | |
|---|---|---|---|
| | **Conocimiento y comunicación** | **Responsabilidad y Rendición de Cuentas** | **Fijación y medición de objetivos** |
| 0 | La empresa no ha reconocido la necesidad de considerar el impacto en el negocio de los riesgos de TI. Las decisiones que implican la asunción de riesgos de TI carecen de información creíble. No hay conciencia de los requisitos externos para la gestión de riesgos y la integración con ERM. . | | |
| 1 | La empresa no ha reconocido la necesidad de considerar el impacto en el negocio de los riesgos de TI. Las decisiones que implican la asunción de riesgos de TI tienden a basarse en la falta de información o información incorrecta. No hay conciencia de los requisitos externos para la gestión de riesgos y la integración con la gestión de riesgos empresariales. | Por defecto, TI es el responsable de la gestión de problemas, la disponibilidad, el acceso al sistema, etc. La propiedad de los riesgos de TI en el contexto de los servicios y procesos de negocio no está definida. No hay ninguna consideración de la responsabilidad empresarial y la responsabilidad de una gestión proactiva de riesgos de TI. No existe ninguna vinculación a una medición del desempeño individual y el programa de recompensa. No hay ninguna expectativa de negocios de valor de la inclusión de los ejecutivos de TI en las decisiones de riesgo. | El apetito de riesgo y la tolerancia son considerados sólo durante evaluaciones de riesgo esporádicas. Las inversiones son enfocadas según las exigencias impuestas desde fuera y expectativas. La obligación de reportar está orientado al cumplimiento y la nueva mediación de cuestiones están identificadas por grupos de aseguramiento y terceros externos. |
| 2 | Hay conocimiento de la necesidad de controlar activamente los riesgos de TI, pero la atención se centra en el cumplimiento técnico sin previsión de valor añadido. Existe compresión de TI basándose en riesgo / recompensa. Los altos directivos y ejecutivos de TI están desarrollando un lenguaje común para los riesgos de TI, pero los riesgos de TI a través de los departamentos puede verse afectada por la competencia, unidad de negocio o la función de un lenguaje de riesgo específicos. | Hay líderes emergentes de los riesgos de TI de gestión dentro de los departamentos que asumen responsabilidad y por lo general son considerados responsables, incluso si esto no es un acuerdo formal. La Carta del Comité de Riesgos de TI cubre el riesgo pero hay una representación mínima.<br><br>Los objetivos de rendimiento están vinculados a reuniones externas de los requisitos de información y a minimizar las conclusiones negativas. Los roles están definidos y sólo contienen parcialmente coincidencias (por ejemplo, se superpone la evaluación de riesgos con la respuesta del riesgo y son los facultados para prescribir tanto soluciones locales de TI como para expresar opiniones).<br><br>Hay confusión sobre la responsabilidad de la integración de la gestión de riesgos de TI con las operaciones y del MTC. Cuando hay problemas tiende a existir cultura de búsqueda de culpable. | La tolerancia al riesgo se establece a nivel local y puede ser difícil encontrarla agregada. Las inversiones se centran en cuestiones de riesgo específicas, por ejemplo en departamentos funcionales y de negocio (seguridad, continuidad de negocio, operaciones). La presentación de informes suele ser manual y habitualmente las actividades de gestión de riesgos de TI está dirigida a la gestión de TI local. |
| 3 | Personal de TI en general, comprende cómo las fallas de TI relacionadas con los objetivos de la empresa o eventos de impacto causan pérdida directa o indirecta a la empresa, mientras que los hombres de negocios en general, comprenden cómo las fallas o eventos pueden afectar a los servicios y procesos clave. La gestión de riesgos se ve como una cuestión empresarial y tanto la baja y al alza de los riesgos de TI están reconocidos. Los riesgos de TI, las estrategias y los planes son comunicados por la gerencia. Las discusiones sobre los riesgos de TI se basan en un lenguaje definido / taxonomía. La información sobre los riesgos y oportunidades se comparten. | Hay un líder designado para los riesgos de TI en toda la empresa que forma parte del comité de empresa de riesgo donde el riesgo es discutido. La organización entiende cómo se integra en la empresa la perspectiva del riesgo a escala. El líder de riesgos de TI tiene una relación fuerte con el CFO y es consultado regularmente durante la gestión de carteras y presupuesto de actividades. El líder de riesgo de TI tiene el cargo suficiente para impugnar eficazmente las decisiones empresariales que involucren a los riesgos de TI. Las funciones de los riesgos de TI están claramente definidas y tienen un mínimo solapamiento. El proceso de responsabilidad y rendición de cuentas y la definición de los dueños del proceso han sido identificados. Las medidas de ejecución están vinculadas a proporcionar valor de negocio, además de cumplir con los requisitos externos. | La tolerancia al riesgo de empresa se deriva de la tolerancia local y las actividades de gestión de riesgos de TI se están alineando en la empresa. Las inversiones se están haciendo contra los problemas de riesgo comunes a pesar de que no puede abordar la causa fundamental en todos los casos. El apetito por el riesgo y la tolerancia se aplica durante el diseño del sistema, la aplicación y el estado de equilibrio y durante los grandes cambios de organización. La presentación de informes periódicos de los resultados de la gestión de riesgos de TI proceso está dirigido a la gestión de TI. |

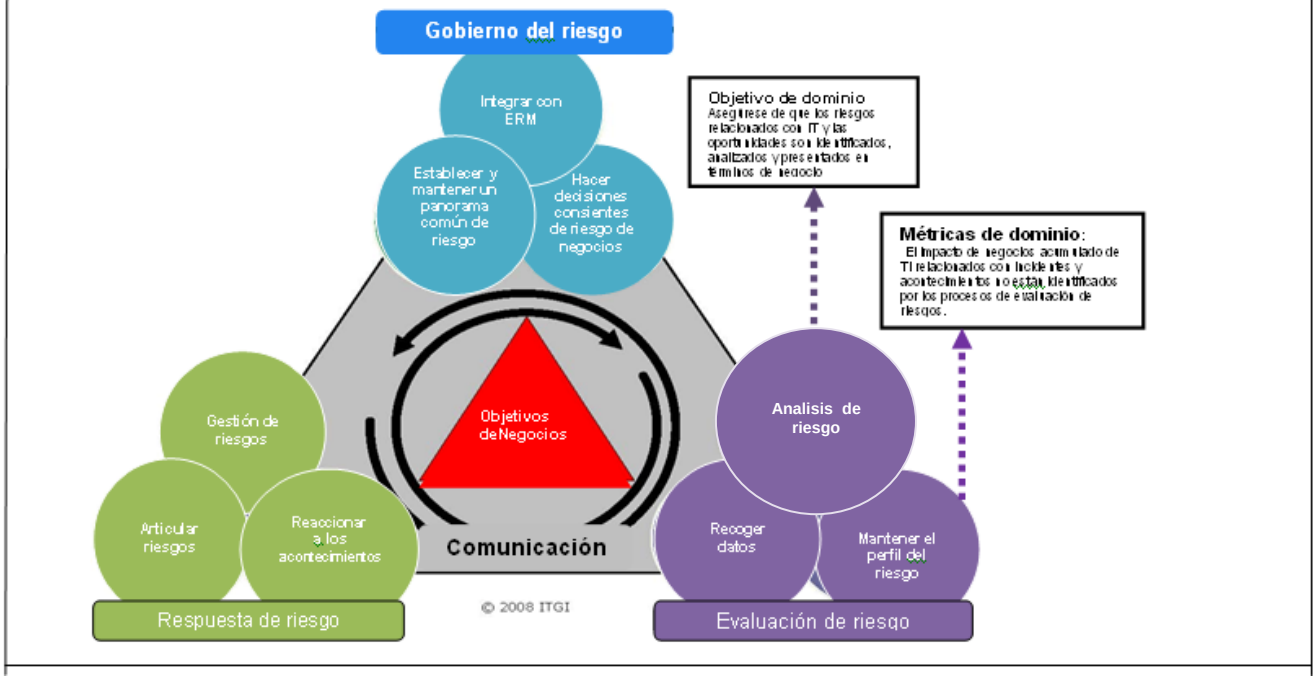
| FIGURA 28 - (RG) Modelo detallado par de Madurez | | | |
|---|---|---|---|
| 4 | La cultura de riesgo es analizada e informada. La empresa entiende el concepto riesgo / recompensa. La gestión de riesgos se ve como un facilitador de negocios y se entienden tanto la baja como el alza de los riesgos de TI.<br><br>El lenguaje informático de riesgo hablado por los altos ejecutivos se mezcla con el lenguaje y la alineación del riesgo empresarial. Los debates sobre los riesgos de TI son una parte normal en la toma de decisiones ejecutivas. | El líder designado para los riesgos de TI en toda la empresa está plenamente comprometido con el comité de riesgo de la empresa y espera que sus opiniones se tomen en cuenta en la toma de decisiones.<br><br>Se entiende bien el papel más amplio del departamento de TI en la gestión del riesgo operacional y la gestión del riesgo empresarial. La gestión integrada de riesgos, está integrado en la planificación estratégica y operaciones de negocios.<br><br>Todos los problemas de TI de riesgo identificados tienen un titular designado, y la responsabilidad y la rendición de cuentas son aceptadas. La alta dirección empresarial y la gestión de TI en conjunto, determinan el nivel aceptable de riesgo que la empresa va a tolerar. Se establece una cultura de recompensa que motiva la acción positiva. | El Consejo define el apetito de riesgo y la tolerancia para todos los departamentos, incluidos los riesgos de TI. La tolerancia del riesgo puede ser refinado por la empresa o del comité de riesgos de TI. Las visitas a la cartera de riesgo son dinámicas y la tolerancia de riesgo se evalúa basándose en diferentes puntos de vista. Las mejores decisiones de inversión son resultado de la visibilidad en toda la empresa en los costes, riesgos y beneficios de los problemas y recompensas.<br><br>Las oportunidades asociadas al riesgo forman parte de los resultados esperados del plan del riesgo.<br><br>Las inversiones se equilibran con una vista de la cartera de riesgo y abordan la causa raíz. La presentación de informes periódicos de los resultados de negocio relacionados con la gestión de riesgos se hace a la gestión empresarial. |
| 5 | La gama completa de estrategias de respuesta de riesgo es aplicado de manera integral y, cuando sea plenamente justificado, costo-eficacia de los controles de mitigar la exposición al riesgo en forma continua.<br>La documentación de proceso es desarrollada a procesos laborales automatizados. Los procesos, la política y procedimientos son estandarizados e integrados para permitir de punta a punta la respuesta de riesgo y la mejora. | El líder del riesgo se considera un asesor de confianza durante el diseño e implementación de operaciones. El patrocinio del Ejecutivo es fuerte y el discurso de la gerencia ha incorporado la gestión de riesgos integrados en la cultura de empresa. Funciones y responsabilidades por procesos, con equipos interdisciplinarios de colaboración. Rendición de cuentas sobre la gestión de riesgos para ayudar a lograr los objetivos están incrustados en todos los procesos, funciones de apoyo, líneas de negocio y áreas geográficas.<br><br>El departamento de TI es un actor importante en los esfuerzos de la línea de negocio respecto al riesgo operativo y riesgo de los esfuerzos de la empresa de manera más amplia. | Los objetivos estratégicos se basan en un nivel ejecutivo de entendimiento de las amenazas de negocios relacionados de la empresa con TI, los escenarios de riesgo y las oportunidades competitivas.<br><br>La empresa cuenta con análisis de negocios sólida para las medidas de la eficacia de la gestión de la incertidumbre y aprovechamiento de las oportunidades de riesgo. |

| FIGURA 29 - (RG) Modelo detallado par de Madurez Parte 2 | | | |
|---|---|---|---|
| | **Políticas, normas y procedimientos** | **Habilidades y experiencia** | **Herramientas y automatización** |
| 0 | | | |
| 1 | Las políticas de empresa y las normas, que son mínimas en el mejor de los casos, pueden ser incompletas y / o reflejan sólo las exigencias externas y le faltan razones defendibles y mecanismos de aplicación. Existen los procedimientos mínimos para la gestión de riesgos. Las políticas y normas no se mantienen al día con respecto a la evolución de negocios, la tecnología o los escenarios de amenazas. | La capacidad de gestión de riesgos de TI pueden existir sobre una base *ad hoc* pero no están desarrolladas activamente. Los gestores de riesgos de empresa y la falta de propietarios de procesos de negocio de TI dificultan la comprensión de riesgo. El personal de TI carece de una comprensión de los efectos comerciales de los riesgos de TI. | El control *ad hoc* de inventarios se encuentra disperso a través de aplicaciones de escritorio. Políticas y normas existentes en múltiples formatos. No hay flujo de trabajo en torno a los incidentes y las decisiones de riesgo. |
| 2 | Hay un consejo designado para emitir las directrices sobre la gestión de riesgos. Las políticas y normas se establecen para departamentos funcionales y de negocio y no se alinean con la junta general de orientación y el apetito de riesgo de negocio. | Los requisitos de formación son mínimos e incluyen una toma de conciencia de los riesgos de TI. Se identifican las zonas de riesgo crítico para la empresa. Formación sobre el riesgo se centra en la política y un lenguaje de riesgo. La formación en gestión de riesgo se presenta en respuesta a las necesidades en lugar de basarse en un plan acordado. Se produce la formación informal en el trabajo. | Existen funciones de TI e inventarios departamentales específicos sobre las cuestiones de riesgo. Los elementos clave de las decisiones de riesgo se registran en las aplicaciones de escritorio. Pueden existir algunas herramientas de gestión de riesgos a nivel de escritorio pero no un enfoque coordinado. Los beneficios esperados de las herramientas son insuficientes. |

| FIGURA 29 - (RG) Modelo detallado par de Madurez Parte 2 | | | |
|---|---|---|---|
| | **Políticas, normas y procedimientos** | **Habilidades y experiencia** | **Herramientas y automatización** |
| 3 | Categorías de riesgo formales han sido identificadas y descritas en términos claros. Las políticas de empresa y las normas reflejan el apetito de riesgo global del negocio. La política de riesgos de plantilla se basa en la Junta de orientación. Las cuestiones importantes se dirigen a la administración superior. El proceso, las políticas y procedimientos están definidos y documentados para todas las principales actividades de gestión de riesgos de TI. Las excepciones son resueltas de una manera formal. | Las necesidades de competencias están definidas y documentadas para todas las áreas de riesgo empresarial y los riesgos de TI incluyen los conceptos. La formación sobre sensibilización de riesgos incluye las situaciones y escenarios más allá de políticas específicas y de las estructuras y un lenguaje común para la comunicación de riesgos. Los gestores de riesgos de empresa y los propietarios de procesos de negocio reciben formación en TI, por ejemplo, las TI para los ejecutivos de finanzas. El personal de TI recibe una formación sobre las actividades de negocios, productos, el riesgo empresarial en general, que compiten temas de riesgo y dependencia de negocio en TI. Se desarrolla plan de formación. | Las exigencias son definidas en un inventario consolidado de cuestiones de riesgo. Los instrumentos de proceso laboral son usados para intensificar cuestiones de riesgo y decisiones de pista. Los instrumentos de recogida de datos pueden distinguirse entre múltiples tipos de acontecimientos. |
| 4 | Las políticas de empresa y las normas reflejan la tolerancia al riesgo empresarial. Los escenarios de riesgo consideran los riesgos de TI en la empresa. Las principales decisiones de riesgo toman en cuenta la probabilidad de pérdida y recompensa. Se adoptan y se siguen normas para el desarrollo y mantenimiento de los procesos de gestión integrada de riesgos y procedimientos. | Los requisitos de habilidad son rutinariamente actualizados para todos los ámbitos, la competencia está garantizada para todas las áreas de gestión de riesgos y se fomenta la certificación de los empleados. La formación sobre el riesgo es global e incluye juegos de rol y en cascada y tipos de amenazas y escenarios de coincidencia. Las técnicas de formación cruzada se aplican en función del plan de formación y se fomenta el intercambio de conocimientos. Todos los internos expertos en gestión de riesgos de TI están involucrados y la eficacia del plan de formación se evalúa. | Estas herramientas permiten la gestión del riesgo de cartera de la empresa, la automatización de flujos de trabajo de gestión de riesgos de TI, y el seguimiento de las actividades críticas y los controles. Las herramientas estándar están desplegadas de tal manera que se integra la gestión de riesgos con el MTC. |
| 5 | Las políticas de empresa y las normas siguen reflejando la tolerancia al riesgo empresarial y aumentan la eficiencia (por ejemplo, que se actualicen dinámicamente, que contengan detalles de situaciones de alto riesgo y la flexibilidad para las situaciones de menor riesgo). La gestión de riesgos se integra plenamente en los procesos de gestión de riesgos empresariales y las estructuras, actividades, líneas de negocio, productos y las iniciativas (por ejemplo, nuevas asociaciones, proveedores de servicios, fusiones, adquisiciones). Todas las decisiones de riesgo son siempre sobre la base de las probabilidades de pérdida y de recompensa. La auditoría interna, el cumplimiento, control y gestión del riesgo de TI están altamente integrados y coordinados e informados. | La organización exige formalmente la mejora continua de los riesgos de TI y la capacidad de gestión basada en objetivos claramente definidos personal y de organización. La formación y educación para soporte de TI comprende las mejores prácticas de gestión de riesgos externos y la utilización de los principales conceptos de vanguardia y las técnicas. El intercambio de conocimientos forma parte de la cultura empresarial, basada en el conocimiento y los sistemas que se están instalando. Los expertos externos y líderes de la industria se utilizan para la orientación. | Está establecida la supervisión en tiempo real de acontecimientos y excepciones de control. La dirección de política está automatizada. Los instrumentos automatizados permiten el apoyo de los procesos de gestión de riesgos de punta a punta. Los instrumentos son usados para apoyar la mejora del proceso de gestión de riesgos. |

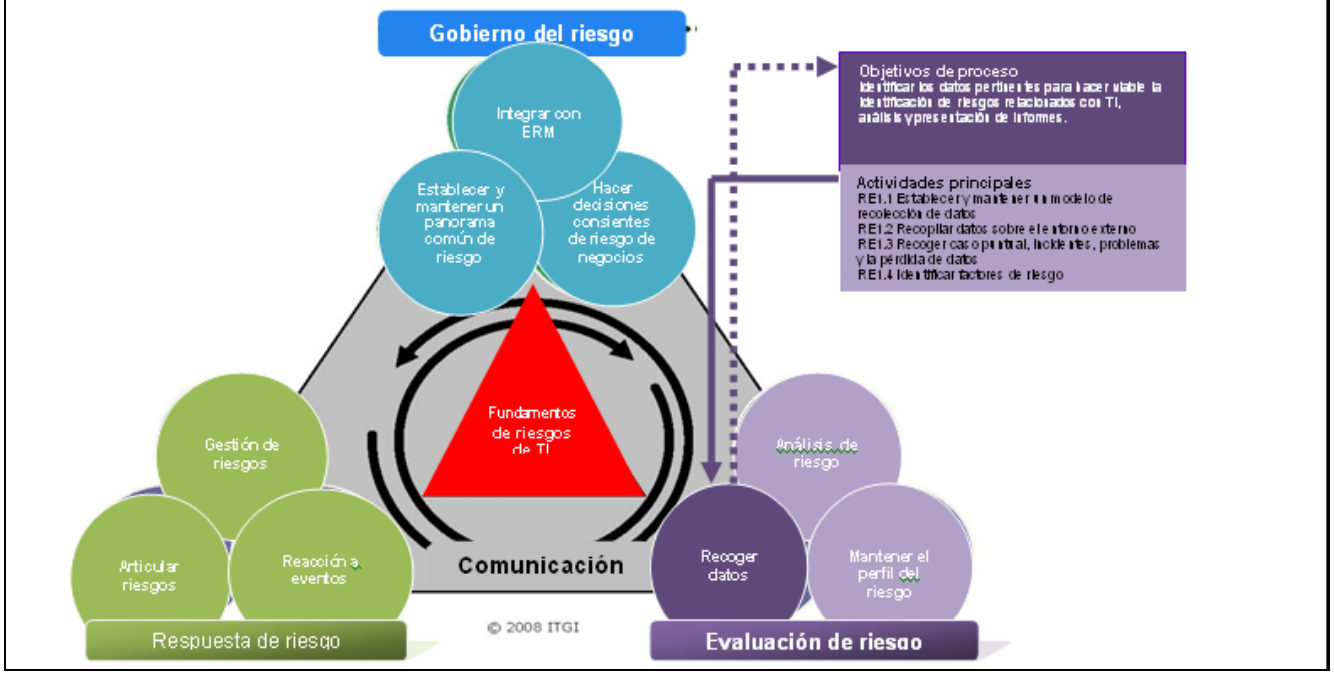
## VISIÓN GENERAL DEL DOMINIO

Figura 30—Evaluación del dominio de riesgo




## VISIÓN GENERAL DEL PROCESO

Figura 31—Proceso RE1 Recopilación de datos



## DETALLE DEL PROCESO

### RE1.Recopilar datos

Identificar los datos pertinentes para hacer viable la identificación de riesgos de TI relacionados, el análisis y presentación de informes.

***RE1.1 Establecer y mantener un modelo para la recolección de datos.***
Establecer y mantener un modelo para la recogida, clasificación y análisis de datos de TI de riesgo. Acomodar múltiples tipos de eventos (p. e., el evento de la amenaza, el evento de la vulnerabilidad, el evento de pérdida) y varias categorías de riesgos de TI (p. e., acontecimientos de amenaza, acontecimientos de vulnerabilidad, acontecimientos de pérdida). Incluye filtros y puntos de vista para ayudar a determinar los factores de riesgo específicos de cómo puede afectar el riesgo (p. e., la frecuencia, magnitud, impacto en el negocio). El modelo debe apoyar la medición y evaluación de los atributos de riesgo (por ejemplo, la disponibilidad) a través de los dominios y los riesgos de TI proporcionar datos útiles para el establecimiento de incentivos para una cultura de conciencia de riesgo.

| Para | Entrada |
|---|---|
| RG2.2 | La estrategia de gestión integrada de riesgos. |
| * | Técnicas y políticas de riesgo operativo, la pérdida de información y políticas de la escalada, las obligaciones de la organización en torno a la pérdida y el evento de presentación de informes |

| De | salida |
|---|---|
| RE1 .2, RE1 .3, Val IT VG5 | Modelo para la recopilación de datos |

* Input from/output to outside Risk IT, Val IT and COBIT

***RE1.2 Recopilar datos sobre el entorno externo***
El modelo de recopilación de datos debe dar registro de datos sobre el entorno operativo de la empresa que podría desempeñar un papel importante en la gestión de las TI. Consultar las fuentes dentro de la empresa, el departamento legal, el de auditoría, el de cumplimiento y la Oficina del CIO. Cubrir las principales fuentes de ingresos, los sistemas externos, la responsabilidad del producto, el panorama normativo, la competencia en la industria, las nuevas tendencias en la alineación de los competidores con puntos de referencia fundamentales, la madurez relativa de los principales negocios y capacidades de TI y los problemas geopolíticos. Encuesta y organización de los datos históricos, los riesgos de TI y la experiencia de la pérdida de colegas de la industria a través de la industria basada en los registros de eventos, bases de datos y los acuerdos de la industria para la divulgación de eventos comunes (por ejemplo, la banca debe establecer acuerdos sectoriales en materia de divulgación de los acontecimientos de fraude generalizado).

| Para | Entrada |
|---|---|
| RG1 .5 | Los parámetros de rendimiento de cambio cultural hacia la conciencia de los riesgos |
| RE1 .1 | Modelo para la recopilación de datos |
| RE3.3 | Evaluación de las capacidades de TI |
| COBIT DS1 0 | Los registros de problemas, problemas conocidos, errores conocidos y soluciones |
| COBIT ME1 | Las tendencias de riesgo y sucesos históricos |
| * | Evaluación de las capacidades empresariales, inteligencia de negocios, evento de riesgo entidad externa y la pérdida de datos, las asignaciones legales y reglamentarias |

| De | salida |
|---|---|
| RE1 .4, RE2.2, RE3.4, RE3.5, RE3.6, RR3.1, RR3.4 | Datos sobre el entorno operativo, histórico riesgos de TI y la pérdida de datos |

* Input from/output to outside Risk IT, Val IT and COBIT

***RE1.3 Recopilar datos sobre eventos de riesgo.***
El modelo de recogida de datos debe dar registro de datos sobre eventos de riesgo que han provocado o pueden provocar impactos en IT / beneficio de habilitación de valor, los programas y la ejecución de proyectos y / o operaciones de TI y prestación de servicios. Captura de datos relevantes de las cuestiones relacionadas, incidentes, problemas e investigaciones.

| Para | Entrada |
|---|---|
| RE1 .1 | Modelo para la recopilación de datos |
| RR3.3 | Adoptar acciones de respuesta a incidentes |
| RR3.4 | Causa raíz de los incidentes |
| COBIT PO10 | Informe del rendimiento del proyecto |
| COBIT DS2 | Informe del rendimiento del proceso, riesgos del proveedor |
| COBIT DS4 | Resultados de pruebas de contingencia, informes del rendimiento del proceso |
| COBIT DS5 | Amenazas y vulnerabilidades de la seguridad |
| COBIT DS8 | informes de incidentes |
| COBIT DS9 | Informes sobre el rendimiento del proceso |
| COBIT DS1 0 | Los registros de problemas, problemas conocidos, errores conocidos y soluciones alternativas |
| COBIT ME1 | Las tendencias de riesgo y sucesos históricos |

| De | salida |
|---|---|
| RE1 .4, RE2.2, RE3.4, RE3.5, RE3.6, RR3.1, RR3.4 | problemas y pérdida de datos en tiempo real, análisis de causa raíz y la pérdida de las tendencias |

* Input from/output to outside Risk IT, Val IT and COBIT

***RE1.4 Identificar factores de riesgo***
Para las empresas pertinentes para eventos similares, organizar los datos recogidos y poner de relieve los factores contribuyentes. Determinar qué condiciones específicas existían o no existían cuando se registraron los eventos de riesgo y cómo las condiciones pueden haber afectado la frecuencia de eventos y la magnitud de la pérdida. Determinar los factores comunes que contribuyen a través de varios eventos. Realizar eventos periódicos y análisis de los factores de riesgo para identificar cuestiones nuevas o incipientes de riesgo y de obtener una comprensión de los factores de riesgo asociados internos y externos.

| Para | Entrada |
|---|---|
| RE1 .2 | Datos sobre el entorno operativo, histórico riesgos de TI y la pérdida de datos |
| RE1 .3 | problemas y pérdida de datos en tiempo real, análisis de causa raíz y la pérdida de las tendencias |

| De | salida |
|---|---|
| RG1.1, RG1.4, RE2.1, RE2.2, RE3.4, RE3.5, RE3.6, RR3.4 | Factores de riesgo |
| RG1.4, RE2.1, RE2.2, RE3.4, RE3.5, RE3.6, RR1.4, RR3.1, RR3.4 | Amenazas emergentes |

## Directrices de gestión – RE1

**Cuadro RACI** **Funciones**

**Actividades Principales**

| | Board | CEO | CRO | CIO | CFO | Enterprise Risk Committee | Business Management | Business Process Owner | Risk Control Functions | HR | Compliance and Audit |
|---|---|---|---|---|---|---|---|---|---|---|---|
| RE1.1. Establecer y mantener un modelo para la recolección de datos. | I | I | A/R | C | C | C | C | C | C | | C |
| RE1.2 Recopilar datos sobre el entorno externo | | I | A/R | C | I | I | C | I | I | I | C |
| RE1.3 Recoger caso puntual, incidentes, problemas y pérdida de datos. | | I | A | R | C | I | | C | C | | I |
| RG3.4. Identificar los riesgos de TI. | | | A | R | I | I | C | C | R | C | C |

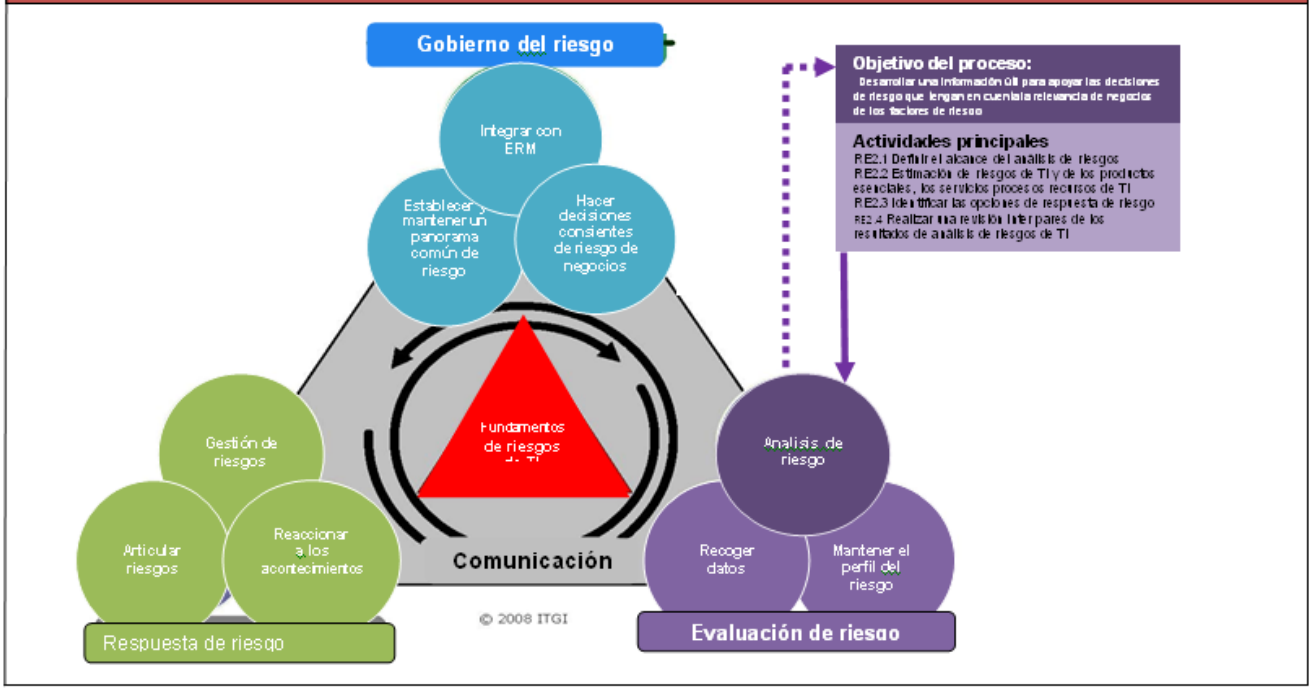
A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

**Métricas y Objetivos- RE1**

| Objetivos de la actividad | Objetivos del proceso | Objetivos RE |
|---|---|---|
| • Establecer y mantener un modelo para la recolección de datos.<br>• Recopilar datos sobre el entorno externo.<br>• Recoger caso puntual, incidentes, problemas y pérdida de datos.<br>• Identificar los riesgos de TI. | • Identificar los datos pertinentes para hacer viable la identificación de riesgos de TI relacionados, el análisis y presentación de informes. | • Asegurar que TI- los riesgos relacionados y las oportunidades- son identificados, analizados y presentados en términos de negocio. |
| **Actividades Métricas** | **Métricas del Proceso** | **Métricas RE** |
| • Existencia de un modelo de recopilación de datos definido y documentado relacionado con el riesgo.<br>• Número de fuentes utilizadas para la recopilación de datos.<br>• Integridad de los datos de eventos en contra de las normas establecidas (por ejemplo, los activos afectados, los datos de impacto, la comunidad de amenazas, acciones). Esto incluye tanto los datos de eventos discretos (por ejemplo, el control de «sí» o «no») y los datos continuos (por ejemplo, la secuencia de datos en curso sobre el tiempo de respuesta del servidor).<br>• Número de elementos de datos para los que los factores han sido identificados<br>• Integridad de los datos históricos a través de las clases de la parte superior de los riesgos de TI. | • Número de acontecimientos de pérdida con características claves no capturadas en alguna forma de depósito<br>• Grado en que apoya la recogida de datos de informes de tendencias y análisis de escenarios<br>• El grado de visibilidad y reconocimiento en el estado de control previsto por la recogida de datos<br>• El grado de visibilidad y reconocimiento en el panorama de las amenazas previstas por la recogida de datos. | • El impacto acumulativo de negocios de TI incidentes y eventos relacionados no identificados por los procesos de evaluación de riesgo. |

**Visión general del dominio**

Figura 32—Proceso RE2 Análisis de riesgo



## DETALLE DEL PROCESO

### RE 2. Análisis de riesgos

Desarrollar una información útil para apoyar las decisiones de riesgo que tenga en cuenta la importancia de factores de riesgo de negocios.

***RE2.1 Definir Alcance del Análisis de Riesgos***

Decidir sobre la amplitud y la profundidad de las expectativas de los esfuerzos de análisis de riesgos. Considere la posibilidad de una amplia gama de opciones adicionales, que incluyen:

- Requisito de la toma de decisiones estratégicas (por ejemplo, nuevos productos y servicios, nuevo entorno operativo, la externalización, nuevos requerimientos normativos).
- Empresas cuyos resultados de la evaluación de riesgos den zonas de riesgo residual fuera de los umbrales de tolerancia de gestión necesitan un examen más detenido de las operaciones en curso (por ejemplo, la línea de negocio, producto, servicios y procesos - de forma individual o en combinación).
- Mapa de los factores de riesgo pertinentes y la criticidad de los activos de empresas consideradas en el estudio / recursos y factores desencadenantes.
- Objetivo para el valor óptimo del análisis de riesgos.
- Esfuerzos para favorecer el alcance sobre la base de los procesos productivos y productos de la empresa (por ejemplo, la generación de ingresos, atención al cliente, calidad) sobre las estructuras internas que no estén directamente relacionados con los resultados de negocio (por ejemplo, los tipos de hardware, lugares, organizaciones funcionales).
- Establecer el ámbito de aplicación de análisis de riesgos después de un examen de la criticidad de negocios, el costo de la medición contra el valor esperado de la información y reducción de la incertidumbre, y todos los requisitos reglamentarios generales

| Para | Entrada |
|---|---|
| RG1 .1 | Principales negocios y objetivos de TI, factores de riesgo, áreas de enfoque de riesgo, escenarios de riesgo de alto nivel, los servicios esenciales y el apoyo a los procesos de negocio y sistemas, los inventarios de prioridad de riesgo y el impacto de las categorías |
| RG1 .1, RG3.3, RG3.4, RG3.5, RR1 .3, RR1 .4, RR2.2, RR3.1, RR3.4; * | Solicitud de análisis de riesgos |
| RG2.2 | La estrategia de gestión integrada de riesgos |
| RG2.3 | Los métodos de gestión integrada de riesgos |
| RE1 .4 | Los factores de riesgo, las amenazas emergentes, |
| RE3.2 | Activo / criticidad de los recursos |
| RE3.5 | Perfil de riesgos de TI |
| RR1 .1, RR1 .4, RR2.2 | Oportunidades y riesgos de TI |
| COBIT ME3 | Catálogo de los requisitos legales y reglamentarios relacionados con la prestación de servicios de TI, el informe sobre el cumplimiento de las actividades de TI externos con los requisitos legales y reglamentarios |

| De | salida |
|---|---|
| RE2.2, RE2.3, RE2.4 | Alcance del analisis de riesgos |

* Input from/output to outside Risk IT, Val IT and COBIT

***RE2.2 Estimación de riesgos de TI***
A través del alcance del análisis de riesgos de TI, la estimación de la frecuencia probable y la magnitud probable de la pérdida o ganancia asociada con los riesgos de TI deben aplicarse como escenarios de la influencia de los factores de riesgo. La estimación de la cantidad máxima de los daños que pudiera sufrir (por ejemplo, una pérdida del peor caso, cuando convergen los factores de riesgo específicos) o la oportunidad que se podrían obtener. Considerar la posibilidad de escenarios compuestos de cascada y / o tipos de amenaza coincidente (por ejemplo, una amenaza externa más una interna de accidente). Basado en los escenarios más importantes, desarrollar las expectativas de los controles específicos, capacidad de detección y medidas de respuesta. Evaluar los controles operativos conocidos y sus probables efectos sobre la frecuencia y la magnitud probable y los factores de riesgo aplicables. Estimación de los niveles de riesgo residual de la exposición y comparar con la tolerancia de riesgo aceptable para identificar los riesgos que pueden requerir una respuesta de riesgo.

| Para | Entrada |
|---|---|
| RG1 .3 | Umbrales de tolerancia de riesgos de TI |
| RG2.3 | Los métodos de gestión integrada de riesgos |
| RE1 .2 | Datos sobre el entorno operativo, histórico riesgos de TI y la pérdida de datos |
| RE1 .3 | problemas y pérdida de datos en tiempo real, análisis de causa raíz y la pérdida de las tendencias |
| RE1 .4 | Los factores de riesgo, las amenazas emergentes, |
| RE2.1 | Alcance del analisis de riesgos |
| RE3.2 | Activo / criticidad de los recursos |
| RE3.3 | Evaluación de las capacidades de TI |
| RE3.4 | Componentes del escenario de riesgos de TI |
| RE3.5 | Perfil de riesgos de TI |
| RR1 .3 | Resultados de la evaluación independiente de TI en el contexto, los acontecimientos de la vulnerabilidad |
| RR2.1 | Base de control y riesgos |
| COBIT PO6 | Marco de control de las empresas de TI |
| COBIT ME2 | Informe sobre la eficacia de los controles de TI |

| De | Salida |
|---|---|
| RE2.3 | Resulatdo del analisis de riesgo |

***RE2.3 Identificar las opciones de respuesta de riesgo.***
Examine la gama de opciones de respuesta de riesgo, tal como aceptar, explotar, mitigar, transferir o evitar. Documento de la justificación de cada uno. Especificar los requerimientos de alto nivel para los proyectos o programas que, basados en la tolerancia de riesgo, mitiguen el riesgo a niveles aceptables o reducir los controles existentes, identificar los costos, beneficios y la responsabilidad de la ejecución del proyecto. Desarrollar los requisitos y las expectativas de los controles de materiales en los puntos más adecuados o cuando se espera que se va a desarrollar para dar visibilidad significativa.

| Para | Entrada |
|---|---|
| RG1 .3 | Umbrales de tolerancia de riesgos de TI |
| RG3.4, RR3.4 | Los requisitos de respuesta de riesgo |
| RE2.1 | Alcance del analisis de riesgo |
| RE2.2 | Resultados de análisis de escenarios |
| RE3.5 | Perfil del riesgo de TI |
| RR1 .1, RR1 .4, RR2.2 | Oportunidades y temas de riesgos de TI |
| RR1 .2, RR2.2 | Deficiencias de control y excepciones de orden |
| RR2.1 | riesgos y control de referencia |
| Val IT PM4 | Los programas de inversión aprobados los presupuestos de TI |
| COBIT PO5 | Directrices de gestión de proyectos |
| COBIT PO10 | Informe sobre la eficacia de los controles de TI |
| COBIT ME2 | Informe sobre la eficacia de los controles de TI |
| * | Presupuesto de funcionamiento |

| De | Salida |
|---|---|
| RE2.4,RR1.1 | Resultados del analisis de riesgos |

* Input from/output to outside Risk IT, Val IT and COBIT

***RE2.4 Realizar una revisión por pares de los resultados de análisis de riesgos de TI.***
Identificar necesidades de recursos para la gestión de riesgos en el negocio y el nivel de TI y en el contexto de la competencia las cuestiones relativas a los riesgos de negocios, las limitaciones de recursos y objetivos. Asignar los fondos necesarios para llenar las lagunas y la posición de la empresa para aprovechar las oportunidades. Establecer el riesgo/recompensa de comercio externo en relación con los objetivos de la organización (por ejemplo, asignar más o menos recursos sobre la base de la criticidad de los datos dentro de un enfoque escalonado para la seguridad de la información). Considere lo siguiente
:

| Para | Entrada |
|---|---|
| RE2.1 | Alcance del analisis de riesgo |
| RE2.3 | Resusltado del analisis de riesgo |

| De | Salida |
|---|---|
| RR1.1 | archivos - revisar las recomendaciones |

## Directrices de gestión – RE2

**Cuadro RACI** **Funciones**

**Principales actividades**

| | Board | CEO | CRO | CIO | CFO | Enterprise Risk Committee | Business Management | Business Process Owner | Risk Control Functions | HR | Compliance and Audit |
|---|---|---|---|---|---|---|---|---|---|---|---|
| RE2.1. Definir el alcance de análisis de riesgos de Ti | | I | R | C | I | C | A | R | C | | C |
| RE2.2 Estimación de riesgos de TI y de los productos esenciales, los servicios procesos recursos de TI | | I | R | C | C | I | A/R | R | R | | C |
| RE2.3 Identificar las opciones de respuesta de riesgo. | | | | C | C | R | A | R | R | | I |
| RE2.4 Realizar una revisión por pares de los resultados de análisis de riesgos de TI | | | A/R | | | | I | | I | | |

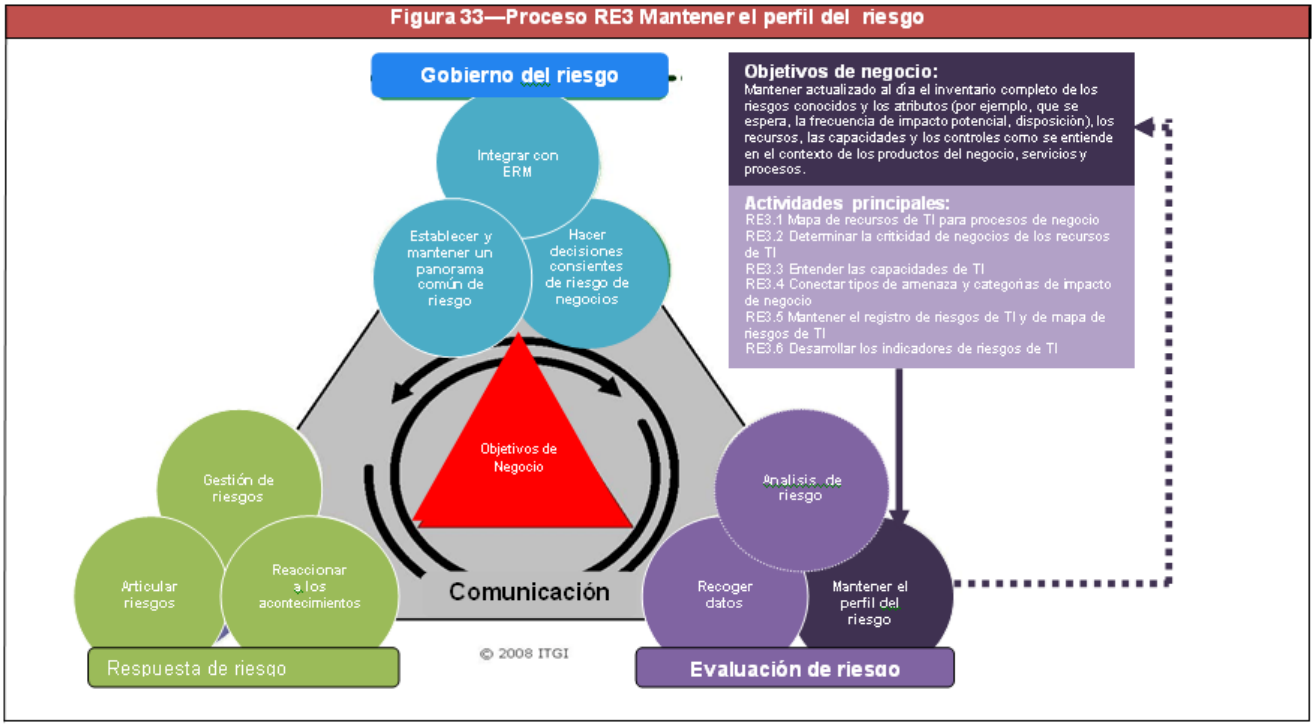
Un gráfico RACI identifica quién es responsable, de consulta y / o informado.

### Métricas y Objetivos

| Objetivos de la actividad | Dominio del proceso | Objetivo del dominio |
|---|---|---|
| • Definir el alcance de análisis de riesgos de TI<br>• Estimación de riesgos de TI y de los productos esenciales, los servicios procesos recursos de TI.<br>• Identificar las opciones de respuesta de riesgo.<br>• Realizar una revisión por pares de los resultados de análisis de riesgos de TI. | • Desarrollar una información útil para apoyar las decisiones de riesgo que tengan en cuenta la relevancia de negocios de los factores de riesgo y responsabilidad. | • Asegurar que los riesgos de TI relacionan las oportunidades y son identificados, analizados y presentados en términos de negocio. |
| **Actividades Métricas** | **Métricas del Proceso** | **Métricas del dominio** |
| • Porcentaje de tiempo de análisis fundamentado en la experiencia posterior o en pruebas (precisión).<br>• Porcentaje de tiempo de revisión por pares no encuentra ningún cálculo lógico, importante o errores incompleto (defendibles)<br>• Porcentaje de tiempo de las evaluaciones paralelas en los mismos escenarios realizados por diferentes analistas deben obtener los mismos resultados (la coherencia)<br>• El Porcentaje de análisis de tiempo es realizado por analistas entrenados (el nivel más alto métrico relacionado con la exactitud, defendible y consistencia).<br>• Un índice de satisfacción "sobre el análisis de riesgo de presentación de informes" (por ejemplo, el porcentaje de respuestas de la encuesta de satisfacción favorable de los ejecutivos de negocios en relación con la legibilidad, la utilidad y exactitud de los informes de análisis de riesgos). | • Porcentaje de los riesgos para los que la frecuencia probable de ocurrencia y la magnitud probable del impacto en las empresas se miden en el ámbito de<br>• Porcentaje de los activos de alto rango, los objetivos y los recursos de revisión para el efecto de los controles operativos conocidos<br>• Porcentaje del análisis de riesgo sometidos a revisión por pares antes de ser enviado a dirección<br>• Proporción acumulada de las pérdidas reales de la magnitud de las pérdidas esperadas. | • El impacto acumulativo de negocios de TI incidentes y eventos relacionados no identificados por los procesos de evaluación de riesgo. |

**Visión general del dominio**

Figura 33—Proceso RE3 Mantener el perfil del riesgo



## DETALLE DEL PROCESO

### RE3. Mantener el perfil de riesgos

Mantener actualizado el inventario completo de los riesgos conocidos y los atributos (por ejemplo, que se espera, la frecuencia de impacto potencial, disposición), los recursos, las capacidades y los controles como se entiende en el contexto de los productos empresariales, servicios y procesos.

***RE3.1. Mapa de recursos de TI para procesos de negocio***
Inventario de los procesos de negocio, apoyando a las personas, aplicaciones, infraestructura, instalaciones, registros manuales críticos, vendedores, proveedores y subcontratistas. Comprender la dependencia de las actividades clave del negocio en los procesos de TI de gestión de servicios y recursos de TI de la infraestructura (por ejemplo, aplicaciones, middleware, servidores, almacenamiento, redes e instalaciones físicas).

| Para | Entrada |
|---|---|
| RG1 .1 | Los principales servicios y el apoyo a los procesos de negocio y sistemas de escenarios de riesgo de alto nivel |
| RG2.1; COBIT PO7 | Responsabiidades y funciones |
| RE3.3 | Capacidad del mapa de TI |
| COBIT DS9 | Configuración de TI / detalles de los activos |
| * | Plan de continuidad de negocio |

| De | Salida |
|---|---|
| RE3.2 | Activos / inventario de los recursos |
| RE3.2, RE3.3, RE3.4; COBIT PO5, DS1 | Mapas del servicio |

* Input from/output to outside Risk IT, Val IT and COBIT

***RE3.2 Determinar la criticidad de negocios de los recursos de TI.***
Determinar qué servicios de TI y recursos de infraestructura de TI son necesarios para mantener el funcionamiento de los servicios y procesos clave de negocios. Análisis de las dependencias y los eslabones débiles en la "pila completa", es decir, de la capa de arriba abajo, a las instalaciones físicas. Conseguir el consenso de negocio y liderazgo en la empresa más valorada de la información y la tecnología relacionada con los activos (por ejemplo, los utilizados para gestionar las operaciones de negocio, proporcionando capacidades, generación de capital, proporcionar una ventaja competitiva, proteger a la empresa de la rotación de personal y gestión de las intenciones y las decisiones de la dirección ejecutiva).

| Para | Entrada |
|---|---|
| RG1 .1 | Activo / a la criticidad de los recursos (macro nivel) |
| RG1 .1, RG2.2 | Establecimiento de prioridades de los inventarios de riesgos y el impacto de las categorías |
| RG1 .3 | Umbrales de tolerancia de TI |
| RG2.3 | Los métodos de gestión integrada de riesgos |
| RE3.1 | Activos de inventario de recursos, servicio de mapas. |
| COBIT PO2 | La arquitectura de información, asignan clasificaciones de datos, procedimientos y herramientas de clasificación |
| COBIT DS1 | Actualización cartera de servicios de TI |
| COBIT DS4 | La criticidad de artículos de configuración, incidentes y los umbrales de los desastres, plan de continuidad de TI |
| COBIT ME1 | Las tendencias de riesgo y sucesos históricos |
| * | La criticidad de los servicios y procesos de negocio |

| De | Salida |
|---|---|
| RE2.1, RE2.2, RE3.3, RE3.4, RR2.2, RR3.2; Val IT IM5; COBIT DS8, DS10, DS13 | Activo / criticidad de los recursos |

* Input from/output to outside Risk IT, Val IT and COBIT

***RE3.3 Entender las capacidades de TI***
Inventario de TI y evaluar la capacidad del proceso, las habilidades y el conocimiento de personas, y los resultados del desempeño de todo el espectro de los riesgos de TI (por ejemplo, IT / beneficio de habilitación de valor, los programas y la ejecución de proyectos, operaciones y prestación de servicios).
Determinar dónde la ejecución del proceso normal puede o no proporcionar los controles correctos y la capacidad de adquirir riesgo aceptable (por ejemplo, no tener suficiente capacidad de ejecución de proyectos de TI en áreas técnicas específicas, pero con un fuerte programa de gestión de TI y la capacidad de contratación externa, por lo tanto, se subcontratan en algunos casos). Identificar donde la reducción de la variabilidad del resultado del proceso puede contribuir a una estructura más robusta de control interno, mejorar el rendimiento de TI y de negocios, y explotar / aprovechar las oportunidades.

| Para | Entrada |
|---|---|
| RE3.1 | Servicio de mapas |
| RE3.2 | Activos / inventario de los recursos |
| COBIT DS1 | Acuerdos de nivel de servicio (SLA), las mediciones de nivel de servicios |
| COBIT DS1, DS8 | Informes sobre la ejecución del proceso |

| De | Salida |
|---|---|
| RG1 .1, RG3.3, RE1 .2, RE2.2, RE3.1, RE3.4, RE3.5, RR1 .4, RR2.1 | Evaluacion de capacidades de TI |

***RE3.4 Actualización de los componentes des escenario de riesgos de TI***
Revisión de la colección de atributos y valores y, a través de ella, los componentes de escenario de riesgo (por ejemplo, el actor, el tipo de amenaza, de eventos, de activos de recursos, tiempo) y sus conexiones inherentes a las categorías de impacto en el negocio. Ajustar entradas basadas en los cambios de las condiciones de riesgo y amenazas emergentes para la prestación de TI / habilitación de valor, los programas y la ejecución de proyectos y operaciones de TI y prestación de servicios. Actualización de la distribución y rangos basados en / a la criticidad de los recursos de activos, los datos sobre el entorno operativo, los datos de eventos de riesgo (por ejemplo, análisis de causa raíz y las tendencias de la pérdida real de problemas y la pérdida de datos), los datos históricos de riesgos de TI y los efectos potenciales de los factores de riesgo (por ejemplo, cómo pueden influir en la frecuencia y / o magnitud de los riesgos de TI escenarios y sus efectos potenciales de negocio). Tipos de enlace de eventos para la categoría de riesgo y las categorías de impacto en el negocio. Tipos de eventos globales por categoría, sector de negocio y áreas funcionales. Como mínimo, la actualización de componentes de TI escenario de riesgo en respuesta a cualquier cambio interno o externo significativo, y examinar anualmente

| Para | Entrada |
|---|---|
| RG1 .1 | Los principales servicios y el apoyo a los procesos de negocio y sistemas de escenarios de riesgo de alto nivel |
| RG1 .1, RG2.2 | Establecimiento de prioridades de los inventarios de riesgos y el impacto de las categorías |
| RE1 .2 | Datos sobre el entorno operativo, histórico riesgos de TI y la pérdida de datos |
| RE1 .3 | Tiempo real-de problemas y la pérdida de datos, análisis de causa raíz y las tendencias de pérdida, las amenazas emergentes |
| RE1 .4 | Los factores de riesgo, las amenazas emergentes, |
| RE3.1 | mapa de servicio |
| RE3.2 | Ranking en relación y clasificación de los activos de riesgo |
| RE3.3 | Evaluación de las capacidades de TI |
| COBIT PO2 | La arquitectura de información, asignan clasificaciones de datos, procedimientos y herramientas de clasificación |

| De | Salida |
|---|---|
| RG1 .1, RG1 .5, RE2.2, RE3.5 | Componentes del escenario de riesgos |

***RE3.5 Mantener los riesgos de TI y mapa de registro de riesgos de TI.***

Capturar el perfil de riesgo de instrumentos tales como los riesgos de TI y mapa de registro de riesgos de TI. Construir el perfil de riesgo a través de los resultados de la evaluación de riesgos empresariales de TI, los componentes de situación de riesgo, caso de riesgo de recopilación de datos, el análisis independiente de TI en curso y resultados de la evaluación de riesgos. Para las personas en los riesgos de TI de las inscripciones, actualización de los atributos clave , tales como nombre, descripción, el titular, que se espera / frecuencia real y potencial / magnitud real de los escenarios asociados, el potencial y repercusiones reales de negocios, y la disposición (por ejemplo, aceptó, transferido, mitigar, evitar).Para el mapa de riesgos de TI y sus refinamientos actualizar las calificaciones de cada dimensión (por ejemplo, la frecuencia, magnitud, impacto en el negocio, el costo para hacer frente de acuerdo con la tolerancia aceptable). Como mínimo, actualizar el mapa de riesgos de TI en respuesta a cualquier cambio interno o externo significativo, y examinar anualmente.

| Para | Entrada |
|---|---|
| RG1 .3 | Umbrales de tolerancia de riesgos de TI |
| RG3.3, RG3.4, RG3.5, RR1.1, RR1.3 | Cambios del perfil de riesgos de TI |
| RG3.4 | Aceptar la documentacion de riesgo |
| RG3.5 | Prioridad de respuesta de riesgos (eliminación del riesgo) |
| RE1 .2 | Datos sobre el entorno operativo, histórico riesgos de TI y la pérdida de datos |
| RE1 .3 | Tiempo real-de problemas y la pérdida de datos, análisis de causa raíz y las tendencias de pérdida, las amenazas emergentes |
| RE1 .4 | Los factores de riesgo, las amenazas emergentes, |
| RE3.3 | Evaluación de las capacidades de TI |
| RE3.4 | Componentes de los escenarios de riesgo |
| RR1 .1 | Informe del analisis de riesgo |
| RR1 .3 | Resultados de la evaluación independiente de TI en el contexto, los acontecimientos de la vulnerabilidad. |
| RR2.1 | Base de control y riesgos |
| RR2.5 | Progreso del pan de acción de riesgos de TI / desviaciones |

| De | Salida |
|---|---|
| RG1.1, RG1 .4, RG3.3, RG3.4, RG3.5, RE2.1, RE2.2, RE2.3, RE3.6, RR1 .3 RR2.1, RR2.2; COBIT PO9 | Perfil del riesgo |
| RR2.1 | Actualizar el control de referncia y los riesgos |

***RE3.6 Diseñar y comunicar los indicadores de riesgo de TI.***

Las métricas de diseño o indicadores que pueden apuntar a los acontecimientos relacionados con la TI y los incidentes que pueden afectar significativamente el negocio. Base de los indicadores en un modelo que lo compromete la exposición y la capacidad en la gestión de riesgos. Estos deben reflejar el riesgo real, de lo contrario, un indicador puede ser "verde" pero el riesgo real aún puede ser grave. Hacer hincapié en indicadores revisables que avisen a los administradores cuando la exposición es superior a los umbrales de riesgo aceptable en todo el entorno operativo. Proporcionar a la dirección una comprensión de los indicadores de riesgo de utilidad: lo que son, lo que cubren, desde la infraestructura a través de una visión estratégica y las acciones a tomar si se han disparado (por ejemplo, actualizar el perfil de riesgo, ajustar las actividades de respuesta de riesgo). Revisar periódicamente RISK en uso por la administración y se recomienda que se ajuste a las cambiantes condiciones internas y externas.

| Para | Entrada |
|---|---|
| RG1 .3 | Umbrales de tolerancia de riesgos de TI |
| RG3.4 | Componentes de los escenarios de riesgo |
| RE1 .2 | Datos sobre el entorno operativo, histórico riesgos de TI y la pérdida de datos |
| RE1 .3 | Tiempo real-de problemas y la pérdida de datos, análisis de causa raíz y las tendencias de pérdida, las amenazas emergentes |
| RE1 .4 | Los factores de riesgo, las amenazas emergentes, |
| RE3.5 | Perfil de riesgos de TI |
| RR2.2 | Revisar periódicamente KRIS en uso por la administración, y recomienda que se ajuste a las cambiantes condiciones internas y externas. |
| RR3.4 | causa raíz de los incidentes |

| De | Salida |
|---|---|
| RR2.2 | Indicadores de riesgos de TI, Recomendaciones KRI |

DIRECTRICES DE GESTIÓN –RE3

Cuadro RACI

Funciones

Actividades Clave

| | Board | CEO | CRO | CIO | CFO | Enterprise Risk Committee | Business Management | Business Process Owner | Risk Control Functions | HR | Compliance and Audit |
|---|---|---|---|---|---|---|---|---|---|---|---|
| RE3.1. Mapa de recursos de TI para procesos de negocio. | | | I | R | | | A | R | C | | I |
| RE3.2 Determinar la criticidad de negocios de los recursos de TI. | | C | | R | | C | A | R | | | I |
| RE3.3 Entender la capacidad de TI | | | C | A/R | | | | C | C | | I |
| RE3.4 Conectar los tipos y categorías de amenaza de impacto en el negocio. | | | C | R | I | C | C | A | R | | C |
| RE3.5 Mantener el registro de riesgos de TI y de mapa de riesgos de TI. | | I | A | R | I | I | I | R/C | C | | I |
| RE3.6 Desarrollar indicadores de riesgos de TI | | | A | I | | | R | C | R | C | C |

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

**Métricas y Objetivos**

| Objetivos de la actividad | Objetivos del proceso | Objetivo RE |
|---|---|---|
| • Mapa de recursos de TI para procesos de negocio.<br>• Determinar la criticidad de negocios de los recursos de TI.<br>• Entender las capacidades de TI.<br>• Conectar los tipos y categorías de amenaza de impacto del negocio.<br>• Mantener el registro de riesgos de TI y de mapa de riesgos de TI.<br>• Desarrollar indicadores de riesgos de TI | • Mantener actualizado al día el inventario completo de los riesgos conocidos y los atributos (por ejemplo, que se espera, la frecuencia de impacto potencial, disposición), los recursos, las capacidades y los controles como se entiendan en el contexto de los productos del negocio, servicios y procesos. | • Asegurar que los riesgos de TI se relacionan con oportunidades y son identificados, analizados y presentados en términos de negocio. |
| **Actividades Métricas** | **Métricas del Proceso** | **Métricas RE** |
| • Porcentaje de las actividades clave del negocio con un vínculo de dependencia para el apoyo a los recursos de TI y de los recursos de infraestructura de TI<br>• Porcentaje de los elementos críticos de la cartera cubierta de TI provocado por el riesgo y los umbrales<br>• Frecuencia de las actualizaciones a los componentes de TI escenario de riesgo.<br>• Número de eventos importantes de cambio interno o externo no revisados para el impacto en los riesgos de TI de los componentes de escenario.<br>• Numero de acontecimientos importantes internos o externos de cambio no revisado para el impacto en el mapa de riesgos de TI<br>• Número de eventos realizados con impacto en el negocio que no se detectan por un mecanismo de activación. | • Número de resultados de análisis de riesgo aprobados y todavía no incorporados en el perfil de riesgo<br>• Porcentaje de servicios de la empresa críticos no cubiertos por el análisis de riesgo.<br>• Integridad de atributos y valores a través de ella los componentes de escenario de riesgo<br>• Integridad de los datos de los atributos clave de riesgo a través del registro de riesgos de TI | • El impacto acumulativo de negocios de TI: incidentes y eventos relacionados no identificados por los procesos de evaluación de riesgo |

## MODELOS DE MADUREZ DE DOMINIO (RE)
## ALTO - NIVEL

**0 No existe cuando**
La empresa no ha reconocido la necesidad de entender cómo los eventos relacionados con TI y las condiciones (factores de riesgo) pueden afectar su rendimiento. Una carencia completa de datos fuerza a asumir aspectos clave del entorno de riesgo durante la toma de decisiones y operaciones en curso. No hay conocimientos de los requisitos externos para evaluar los riesgos de TI.

**1 Inicial cuando**
El reconocimiento de la necesidad de la evaluación del riesgo está surgiendo, sin embargo, existe una mínima comprensión del entorno empresarial y los eventos asociados a fin de que las amenazas puedan afectar el desempeño. Por defecto, es responsable de la evaluación de riesgos. La información actual sobre los riesgos de TI y las opciones de mitigación se deducen de la evaluación episódica. Cualquier recopilación de datos y métodos de análisis son ad hoc y puede ser impulsada por el cumplimiento. Las habilidades de análisis de riesgos de TI pueden existir sobre una base ad hoc, pero no están desarrollando activamente.

**2 Repetibles cuando**
Peor caso – La pérdida de los escenarios son el enfoque de los debates, aunque los principales factores de estos escenarios pueden no ser entendidas. Los individuos asumen la responsabilidad tanto de la evaluación de riesgos y respuesta a los riesgos. Algunos de los análisis de riesgo previstos se producen, pero los profesionales de las principales hipótesis sobre los factores que contribuyen al riesgo. El análisis de dependencia y análisis de escenarios son ad hoc y se concentran en un número limitado de actividades empresariales. Requisitos de formación mínimos son identificados para las áreas críticas de la recopilación de datos, análisis de riesgos y perfiles de riesgo. Funcionales y de TI de silos enfoques de análisis de riesgo específicos y las herramientas existen, pero se basan en las soluciones desarrolladas por las personas clave

**3 Definidos cuando**
Hay una comprensión de los fundamentos de riesgo emergentes. Las diferencias entre las TI y los riesgos relacionados con la oportunidad y el apetito de riesgo global están siendo reconocidos. La responsabilidad y rendición de cuentas de las prácticas fundamentales de la evaluación de riesgo se definen y los dueños del proceso han sido identificados. La capacidad está en el lugar para evaluar los riesgos de TI en una empresa a nivel de todo junto con los tipos de riesgo. El análisis de dependencia y los procedimientos de análisis de escenarios se definen y se realiza a través de actividades múltiples, las líneas de negocio y productos. Necesidades de competencias definidos y documentados para todas las áreas de riesgo empresarial, con plena consideración de la recopilación de datos, análisis de riesgos y perfiles. Instrumentos de recolección de datos generalmente se adhieren a los estándares definidos y se distinguen entre los acontecimientos de amenaza, los acontecimientos de vulnerabilidad y acontecimientos de pérdida.

**4 Gestionados cuando**
El análisis del riesgo ha sido aceptado como una forma de comprender mejor la resistencia de la empresa y estar mejor preparados para alcanzar los objetivos estratégicos. Todos los tipos de riesgos tienen un titular designado, y la alta dirección empresarial y la gestión de TI en conjunto, determinan la pertinencia de negocios de los factores de riesgo. La evaluación de la eficiencia y eficacia de los riesgos son medidos y comunicados y relacionados con los objetivos de negocio y el plan estratégico de TI. Las excepciones de evaluación del riesgo se observó por la gestión y análisis de causa raíz está siendo normalizado. Todos los resultados de análisis de riesgos están sujetos a revisión por pares formal, y la causa raíz de los problemas de calidad se investiga. La empresa se ocupa del desarrollo a más largo plazo las necesidades de personal con alto potencial en la evaluación de riesgos y las técnicas relacionadas. Herramientas de análisis de riesgo se aplicará con arreglo a un plan estándar, y algunos se han integrado con otras herramientas relacionadas.

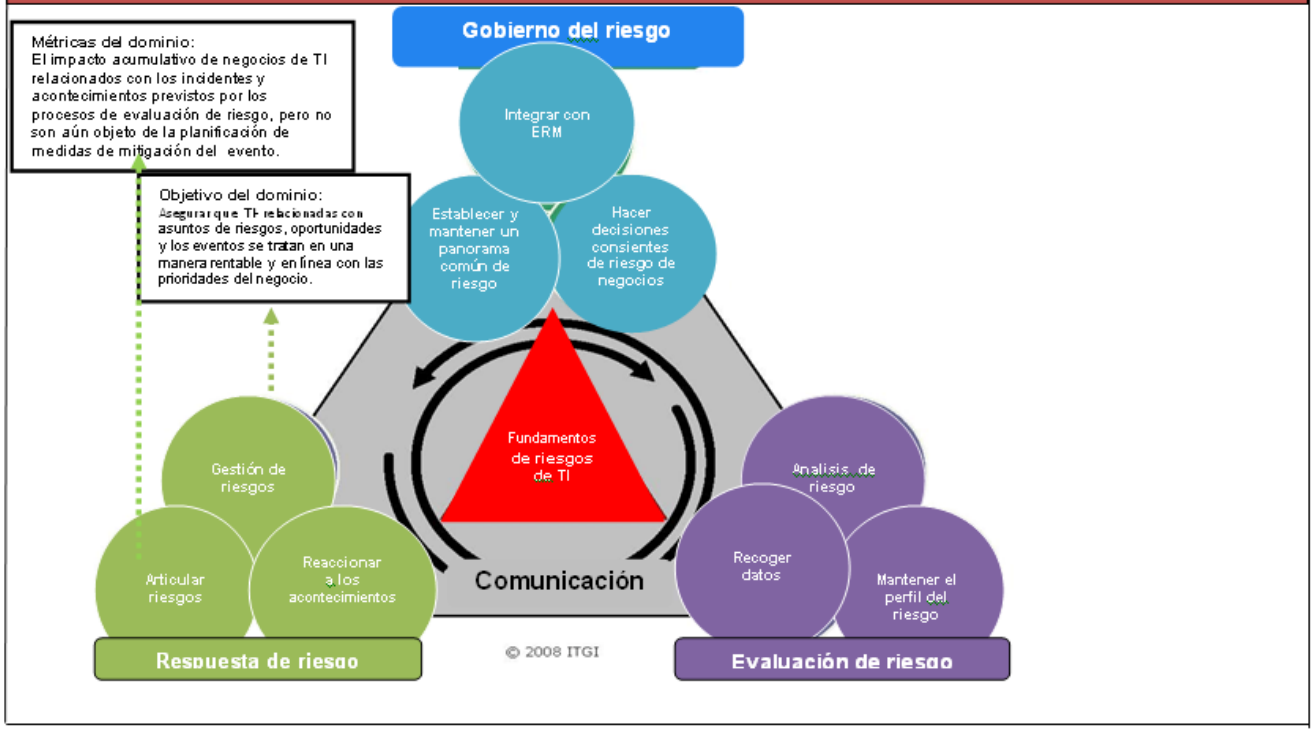
**5 Optimizado cuando**
Los responsables de las decisiones disfrutan de la transparencia en los riesgos de TI y disponer de la mejor información posible acerca de las probabilidades de pérdida, riesgos y oportunidades emergentes. El factor decisivo de los riesgos reales de las operaciones reales se comunicarán con fuerza en toda la empresa. Los empleados en todos los niveles asuman la responsabilidad directa para determinar la pertinencia de negocios de los factores de riesgo. La empresa mantiene un equilibrio óptimo entre los métodos cualitativos y cuantitativos que las decisiones de apoyo en la gestión de la incertidumbre y aprovechar las oportunidades de riesgo. Las actividades de evaluación de riesgos se basan en un conjunto amplio y profundo de los riesgos de TI escenarios que integrar todas las actividades de negocios, líneas de negocio, productos y tipos conocidos de riesgo. La empresa exige formalmente la mejora continua de la recogida de datos, análisis de riesgos y perfiles de competencias. Las herramientas automatizadas permiten extremo-a-fin, el apoyo y la mejora de los esfuerzos de evaluación de riesgos.

| Figura 34 - Modelo detallado de Madurez Parte 1 | | | |
|---|---|---|---|
| | **Conocimiento y comunicación** | **Responsabilidad y Rendición de Cuentas** | **Fijación y medición de objetivos** |
| 0 | La empresa no reconoce la necesidad de entender como TI-acontecimientos relacionados y condiciones (factores de riesgo) puede afectar su funcionamiento. Una carencia completa de datos fuerza suposiciones sobre los aspectos claves del ambiente de riesgo durante la toma de decisiones y operaciones en curso. No hay ninguna conciencia de exigencias externas para evaluar el riesgo de TI. | | |
| 1 | El reconocimiento de la necesidad de la evaluación del riesgo está surgiendo, sin embargo, existe una mínima comprensión del entorno empresarial y los acontecimientos asociados a fin de que las amenazas pueden afectar el desempeño<br><br>Hay una realimentación mínima a las personas responsables de las decisiones respecto a las decisiones de riesgo tienen efecto sobre la condición de riesgo y la condición de negocios. La identificación y el análisis de los riesgos de TI se basa en "corazonadas" en lugar de en el contexto de las actividades comerciales y pueden ser percibidos como la producción de infundadas las peores situaciones | Por defecto, es el responsable de la evaluación de riesgo. N la medición del desempeño y el programa de recompensa para respaldar la responsabilidad individual para identificar cuánto riesgo existe. | Información actual sobre los riesgos de TI y las opciones de mitigación se deducen de las evaluaciones de episodios |
| 2 | Peor caso – La pérdida de los escenarios son el enfoque de los debates,, aunque los principales factores de los escenarios no se puede entender<br><br>Alguna retroalimentación es proporcionada a quienes toman las decisiones en relación con el efecto que las decisiones de riesgo tienen la condición de negocios. Hay taxonomías localizado utilizado como base para la discusión de conceptos de análisis de riesgos de TI. | Los individuos asumen la responsabilidad tanto de la evaluación de riesgos y respuesta a los riesgos.<br><br>Hay confusión sobre responsabilidades de evaluación de riesgo por toda la empresa. Cuando los problemas ocurren, una cultura de culpa tiende a existir. | Algunos análisis de riesgo previsto se produce, pero los profesionales que las principales hipótesis sobre los factores que contribuyen al riesgo.<br><br>Algunas metas para la recogida de datos y el análisis se producen, pero no es un seguimiento con los indicadores clave. |
| 3 | Hay una comprensión de los fundamentos de riesgos emergentes. Brechas entre las TI y los riesgos relacionados con la oportunidad y el apetito de riesgo global están siendo reconocidos.<br><br>Las discusiones de los análisis de riesgos están basados en un lenguaje definido / taxonomía. Los responsables de las decisiones proporcionan retroalimentación cualitativa regulares sobre el efecto que las decisiones han de riesgo relacionados con la condición de negocios. Información a nivel de empresa sobre las prácticas de análisis de riesgos y problemas es compartida. | La responsabilidad y la rendición de cuentas de las prácticas fundamentales de la evaluación de riesgo son definidas y los dueños del proceso han sido identificados. El propietario del proceso es poco probable que tenga plena autoridad para ejercer las responsabilidades.<br>La descripción del puesto de trabajo considera la responsabilidad de la evaluación del riesgo. | La capacidad está en el lugar para evaluar los riesgos de TI en una empresa a nivel de todo junto con los tipos de riesgo<br><br>La información de riesgos y las opciones de mitigación se basan en los procedimientos definidos y satisfacer las necesidades básicas de los tomadores de decisiones.<br><br>Presentación de informes periódicos de los resultados de la evaluación de riesgos de TI proceso está dirigido a la administración de TI.<br><br>La medición de los procesos de evaluación de riesgos se desprende, pero no es coherente. |
| 4 | El análisis del riesgo ha sido aceptado como una forma de comprender mejor la resistencia de la empresa y estar mejor preparados para alcanzar los objetivos estratégicos. Identificación de riesgos y metodologías de análisis de productos estructurados de múltiples escenarios de riesgo que son bien comprendidos por la dirección y los profesionales.<br><br>Las discusiones del análisis de riesgo se basan en las condiciones establecidas. Estimación razonable de las probabilidades de pérdida y de las opciones de mitigación están disponibles para todos los interesados. Los tomadores de decisiones recibir información cuantitativa periódica sobre el efecto que las decisiones han de riesgo relacionados con la condición de negocios. Datos de riesgo de empresa se ajustan a un modelo estándar y son ampliamente compartidos. | Todos los tipos de riesgos tienen un titular designado, y la alta dirección empresarial y la gestión de TI en conjunto, determinan la pertinencia de negocios de los factores de riesgo. De evaluación de riesgos de respuesta responsabilidad y rendición de cuentas son aceptadas y de trabajo de una manera que permite a un propietario de proceso para cumplir plenamente sus responsabilidades. Una cultura de la recompensa está en el lugar que motiva a la acción positiva. | Información sobre los riesgos de TI y las opciones de mitigación se basan en métodos cuantitativos y anticipar las necesidades de los tomadores de decisiones. Management es capaz de controlar el perfil de riesgo.<br><br>La eficiencia y la eficacia de evaluación de los riesgos se miden y se comuniquen y vinculados a los objetivos de negocio y el plan estratégico de TI. Excepciones de evaluación de riesgo se observó por la gestión y análisis de causa raíz está siendo normalizado.<br><br>Los grados aceptables de error o inconsistencia en el análisis de riesgo bien son establecidos.<br><br>La dirección de empresas recibe el informe regular de los resultados de negocio relacionados con la evaluación de riesgo de TI. |
| 5 | Los responsables de las decisiones disfrutan de la transparencia en los riesgos de TI y disponen de la mejor información posible acerca de las probabilidades de pérdida, riesgos y oportunidades emergentes.<br><br>Los responsables de los riesgos reales de las operaciones reales se comunicarán con fuerza en toda la empresa. | Los empleados en todos los niveles asumen la responsabilidad directa para determinar la pertinencia de los factores de riesgo del negocio, por ejemplo, las amenazas, vulnerabilidades, el valor, la responsabilidad | La empresa mantiene un equilibrio óptimo entre los métodos cualitativos y cuantitativos que las decisiones de apoyo en la gestión de la incertidumbre y aprovechar las oportunidades de riesgo. |

| Figura 35 –RE Modelo detallado de Madurez Parte 2 | | | |
|---|---|---|---|
| | **Políticas, normas y procedimientos** | **Habilidades y experiencia** | **Herramientas y automatización** |
| 0 | | | |
| 1 | Cualquier recopilación de datos y métodos de análisis son ad hoc y pueden ser impulsadas por el cumplimiento .La evaluación de los riesgos no pueden incluir todos los componentes de riesgo. | Las habilidades de análisis de riesgos de TI puedan existir sobre una base ad hoc, pero no están desarrollando activamente. Gestores de riesgos de empresa y los propietarios de la falta de procesos de negocio de TI comprensión de evaluación de riesgos. El personal de TI carecen de las habilidades para determinar la pertinencia de negocios de los factores de riesgo.<br><br>Los empleados desean mejorar la recopilación de datos, El análisis de perfiles y competencias, pero ningún inventario de habilidades de evaluación de riesgo existe ni es un modelo de competencias establecido para la documentación de futuros requisitos de formación. | Los departamentos y funciones mantienen sus propias listas de comprobación informales para el análisis de riesgo dentro de sus silos. |
| 2 | El análisis de dependencia y análisis de escenarios son ad hoc y se concentran en un número limitado de actividades empresariales.<br><br>La recopilación de datos, análisis y métodos de perfiles se utilizan, pero falta organización podrá elementos clave y pueden variar a través de la empresa y la TI. Es difícil normalizar los datos a través de la empresa. | Los requisitos mínimos de formación son identificados para las áreas críticas de la recopilación de datos, análisis de riesgos y perfiles de riesgo.<br><br>La capacidad del análisis de riesgo es proporcionada en respuesta a las necesidades, más bien sobre la base de un plan acordado, y de formación informal en el trabajo se produce. | Funcionales y silos de TI - enfoques de análisis de riesgos específicos y las herramientas existen pero se basan en las soluciones desarrolladas por los individuos clave.<br><br>Los datos recogidos en apoyo de los análisis de riesgo se registran en las aplicaciones de escritorio. Sin embargo, la diferencia mínima entre los eventos se hace la amenaza, la vulnerabilidad de los acontecimientos y eventos de pérdida. |
| 3 | Las metodologías de evaluación de riesgos son aceptadas por la dirección. El análisis de dependencia y los procedimientos de análisis de escenarios se definen y se realiza a través de actividades múltiples, las líneas de negocio y productos.<br><br>El análisis de riesgo toma un enfoque probabilística y considera la frecuencia de las amenazas, la vulnerabilidad y la magnitud de la pérdida. Ámbito de aplicación de análisis de riesgo incluye regularmente los sistemas existentes y sistemas en el diseño y desarrollo. La mayoría de los resultados de análisis de riesgo se sometan a revisión por pares formales | Las necesidades de las competencias son definidas y documentadas para todas las áreas de riesgo empresarial, con plena consideración de la recopilación de datos, análisis de riesgos y perfiles. Formación para la evaluación de riesgos incluye las técnicas más allá de la política de mínimos y herramientas comunes para determinar la pertinencia de negocios de los factores de riesgo. Los gestores de riesgos de empresa y los propietarios de procesos de negocio orientados recibir la formación en análisis de riesgos.<br><br>Las necesidades de competencias definidos y documentados para todas las áreas de evaluación de riesgos. Un plan de capacitación formal para la evaluación del riesgo se ha desarrollado. Se dispone de datos sobre el movimiento de las habilidades de evaluación crítica de riesgo y las competencias. | Las herramientas de recolección de datos generalmente se adhieren a los estándares definidos y distinguir entre los actos de amenazas, la vulnerabilidad de los acontecimientos y eventos de pérdida.<br><br>Algunos instrumentos centralizados con los criterios de evaluación estandarizados de frecuencia, impacto y la eficacia de control son en el lugar.<br><br>Los prototipos de flujo de trabajo se han establecido para integrar las probabilidades de riesgo en los procedimientos de decisión |
| 4 | La recopilación de datos, el análisis de la dependencia y los procedimientos de análisis de escenarios se definen y se realiza a través de múltiples tipos de riesgos, actividades de negocios, líneas de negocio y de los productos<br><br>Todos los resultados de análisis de riesgos están sujetos a revisión por pares formal y la causa raíz de los problemas de calidad se investiga. | Los requisitos de habilidad son rutinariamente actualizados para todas las áreas de evaluación de riesgos, la competencia está garantizada para todas las áreas críticas y apoyan la certificación.<br><br>La empresa está dirigiendo el desarrollo a más largo plazo las necesidades de personal con alto potencial en la evaluación de riesgos y las técnicas relacionadas<br><br>Madurar las técnicas de análisis deformación del riesgo se aplicarán de acuerdo con el plan de formación, y se fomenta el intercambio de conocimientos. Todos los expertos en la evaluación interna están involucrados, y la eficacia del plan de formación se evalúa. | Las herramientas de análisis de riesgo son puestas en práctica según un plan estandartizado, y unos han sido integrados con otros instrumentos relacionados.<br><br>Las herramientas de evaluación de riesgos son utilizadas en las principales áreas para automatizar las actividades esenciales en apoyo de la recopilación de datos, análisis de riesgos y perfiles. |
| 5 | Las actividades de evaluación de riesgos se basan en un conjunto amplio y profundo de los riesgos de TI escenarios que integrar todas las actividades de negocios, líneas de negocio, productos y tipos conocidos de riesgo.<br><br>La causa principal de riesgo es siempre entendido y siempre se utiliza como base para las decisiones de respuesta a los riesgos.<br><br>La revisión de par de resultados de análisis de riesgo y de otras prácticas de evaluación de riesgo claves es sujeta al análisis de causa de origen riguroso, y las acciones siempre son tomadas para mejorar los resultados. | La empresa exige formalmente la mejora continua de la recopilación de datos, El análisis de riesgos y perfiles de competencias, sobre la base de definir claramente los objetivos personales y organizacionales. | Datos en tiempo real son recogidos sobre acontecimientos de amenaza, acontecimientos de vulnerabilidad, acontecimientos de pérdida y descubrimiento de factores de riesgo.<br><br>Los instrumentos automatizados permiten de punta a punta el apoyo y la mejora de esfuerzos de evaluación de riesgo. |

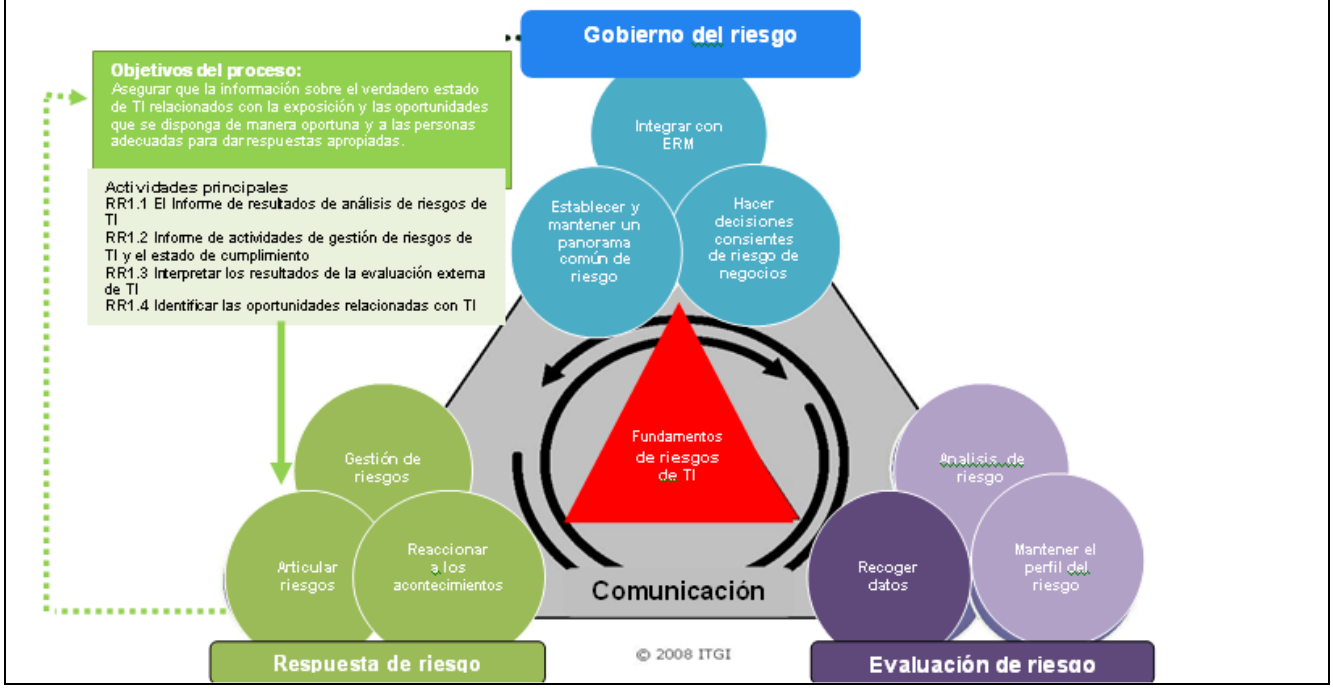
## Visión general del dominio

Figura 36—Dominio de respuesta de riesgo




## Visión general del proceso

Figura 37—Proceso RR1 Articular riesgos



**DETALLE DEL PROCESO**

## RR1 Articular riesgos

Asegurar que la información sobre el verdadero estado de TI relacionados con la exposición y las oportunidades se disponga de manera oportuna y sea accesible a las personas adecuadas para dar respuestas apropiadas.

***RR1.1 Informe de los resultados de análisis de riesgos de TI.***
El informe de resultados de los análisis de riesgos en los términos y formatos útiles para apoyar las decisiones de negocio. Coordinar la actividad de análisis de riesgo adicionales, es requerido por los tomadores de decisiones (por ejemplo, el rechazo de informe, el ajuste de alcance). Comunicar claramente el riesgo de un contexto de retorno. Siempre que sea posible, incluir las probabilidades de pérdida y / o ganancia, rangos y niveles de confianza que permitan la gestión de equilibrar el riesgo-retorno. Identificar los impactos negativos de los acontecimientos y situaciones, que debe conducir las decisiones de respuesta y el impacto positivo de los acontecimientos y situaciones, que representan oportunidades de manejo debe canalizar de nuevo la estrategia y el proceso de fijación de objetivos. Los responsables políticos deben comprender os escenarios del peor caso y más probable, la exposición debida diligencia, y la reputación importante, las consideraciones legales o reglamentarias. Incluyen los siguientes:
• Componentes clave de riesgo (ejemplo, frecuencia, magnitud, impacto).
• Estimar la magnitud probable de la perdida o la futura ganancia probable
• Calcular el potencial de pérdida / ganancia y la más probable pérdida / ganancia escenario (S) (por ejemplo, una frecuencia probable pérdida de entre tres y cinco veces por año, y de una magnitud probable pérdida de entre 50.000 dólares EE.UU. y 100.000 dólares, con un 90 por ciento de confianza).
• Información adicional pertinente de apoyo a las conclusiones y recomendaciones de los análisis

| Para | Entrada |
|---|---|
| RG2.2 | estrategia de gestión integrada de riesgos. |
| RG3.2 | Deficiencia del análisis de riesgos |
| RE2.3 | Resultado del análisis de riesgos |
| RE2.4 | Revisión por los pares recomendaciones |

| De | Salida |
|---|---|
| RG1.4,RG1.6, RG2.1, RG2.2, RG3.3, RG3.4, RG3.5, RE2.1, RE2.3, RR1 .2, RR2.3, RR3.1 | Asuntos y oportunidades de los riesgos |
| RG3.2,RE3.5,RR1.3, RR1.4,RR2.2, RR3.1, RR3.4 | Informe del análisis de riesgos |
| RG3.3, RG3.4, RG3.5 | Pérdida o aumento de las probabilidades y los rangos, las opciones de respuesta de riesgo, costo / beneficio expectativas |
| RE3.5 | Cambios de perfil de riesgos de TI |
| Val IT IM2 | Oportunidad de caso de negocio |

***RR1.2 Informe de actividades de gestión de riesgos de TI y el estado de cumplimiento.***
Conocer el riesgo de presentación de informes de las necesidades de las diversas partes interesadas por ejemplo, Junta, Comité de Riesgos, las funciones de control de riesgos y la gestión de la unidad de negocio. Para asegurar una información estratégica y eficiente de los riesgos de TI y las cuestiones de estado, aplicar los principios de pertinencia, eficiencia, puntualidad y precisión. Incluye control del rendimiento, problemas y deficiencias, el estado de rehabilitación, eventos e incidentes, y sus impactos en el perfil de riesgo. Incluyan la realización de los procesos de gestión de riesgos. Proveer aportaciones para la presentación de informes de la empresa integrada.

| Para | Entrada |
|---|---|
| RG2.2 | Requisitos de información integrada de riesgos |
| RR1 .1, RR1 .4, RR2.2 | Temas y oportunidades de los riesgos de TI |
| RR2.2 | Principales indicadores de riesgos de TI y escalada de los desencadenantes, agregación de datos de riesgo |
| COBIT PO9 | Los informes de riesgos |
| COBIT DS8 | Los informes de incidentes |
| COBIT DS1 3 | Tickets de incidentes, registro de los errores, los informes del rendimiento de los procesos |
| COBIT ME2 | Informe sobre la eficacia de los controles de TI |
| COBIT ME3 | Catálogo de los requisitos legales y reglamentarios relacionados con la prestación de servicios de TI, el informe sobre el cumplimiento de las actividades de TI externos con los requisitos legales y reglamentarios |

| De | salida |
|---|---|
| RG1 .4, RG1 .5, RG2.5; COBIT ME1, ME2 | Estado del cumplimiento de los informes |
| RG2.2, RG2.5; * | Entradas para la presentación de informes integrados del riesgo empresarial |
| RG3.4,RE2.3, RR2.1,RR2.2, RR2.3,RR32; COBIT PO9, ME1, ME2 | Deficiencias de control y excepciones de orden |

***RR1.3 Interpretar resultados de la evaluación independiente de TI.***
Revisar los resultados y conclusiones específicas del objetivo de terceros, la auditoría interna, control de calidad, la auto-evaluación de actividades, etc. Mapa para el perfil de riesgo y el riesgo y el control de línea de base, al considerar la tolerancia de riesgos establecidos. Tome las lagunas y las exposiciones frente a la empresa para su orientar el objetivo o la necesidad de análisis de riesgo. Ayudar a los negocios a entender los planes de acción correctiva y cómo afectará al perfil de riesgo global. Identificar oportunidades para la integración con los esfuerzos de rehabilitación y otras actividades de gestión de riesgos en curso.

| Para | Entrada |
|---|---|
| RG1 .3 | Umbrales de tolerancia de riesgos de TI |
| RG1 .4 | Politicas de riesgos de TI |
| RE3.5 | Perfil de riesgos de TI |
| RR1 .1 | Informe y analisis de riesgos |
| RR2.1 | Riesgo y control de referencia |
| COBIT AI7 | Supervisión de control interno |
| COBIT ME2 | Informe sobre la eficacia de los controles de TI |
| * | Los informes de auditoría externa, funciones de supervisión, auditoría interna, control de calidad, riesgo y autoevaluación de control |

| De | Salida |
|---|---|
| RG1 .1, RG3.3, RG3.4, RG3.5, RE2.2, RE3.5 | Resultados de la evaluación independiente de TI en el contexto |
| RG3.4, RG3.5, RE2.2, RE3.5, RR2.3 | Eventos de vulnerabilidad |
| RE2.1 | Solicitud de análisis de riesgo |
| RE3.5 | Cambios del analisis de riesgos de TI |

* Input from/output to outside Risk IT, Val IT and COBIT

***RR1.4 Identificar TI – Oportunidades relacionadas.***
Sobre una base recurrente, considerar los respectivos niveles del riesgo de TI para procesos de la empresa específicos a la capacidad de prevención de siniestros de TI, Unidades de negocio, productos, etcétera. En las zonas con riesgo relativo y la paridad de la capacidad de riesgo (es decir, lo que indica la capacidad de asumir más riesgo), Identificar oportunidades relacionados con la TI que podría permitir a la zona a aceptar un mayor riesgo y mejorar el crecimiento y el retorno.

Buscar oportunidades donde las TI puedan ser utilizadas:
• Apalancamiento empresarial - los recursos de toda la empresa en la creación de ventaja competitiva (por ejemplo, utilizar la información existente en formas nuevas, humanos y aprovechar mejor los recursos empresariales)
• Reducir gastos de coordinación de la empresa
• Explotar las economías de escala y ámbito de aplicación de determinados recursos estratégicos comunes a varias líneas de negocio
• Aproveche las diferencias estructurales con los competidores
• Coordinar las actividades entre las unidades de negocio o en la cadena de valor

| Para | Entrada |
|---|---|
| RE1 .4 | Amenazas emergentes |
| RE3.3 | Evaluación de las capacidades de TI |
| RR1 .1 | Informe del analisis de riesgos |
| RR2.1 | Oportunidades de reducción de Control |
| RR3.2 | Alerta de evento de riesgo |

| De | Salida |
|---|---|
| RG1.4,RG1.6,RG2.1, RG2.2,RG3.3, RG3.4, RG3.5, RE2.1, RE2.3, RR1 .2, RR2.3, RR3.1 | Asuntos y opOrtunidades de riesgos de TI |
| RE2.1 | Solicitud de análisis de riesgo |

* Input from/output to outside Risk IT, Val IT and COBIT

## Directrices de gestión - RR1

**Cuadro RACI** **Funciones**

**Actividades Clave**

| | Board | CEO | CRO | CIO | CFO | Enterprise Risk Committee | Business Management | Business Process Owner | Risk Control Functions | HR | Compliance and Audit |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **RR1.1** Comunicar los resultados del análisis de riesgos de TI. | | I | R | C | C | C | A | R | R | C | I |
| **RR1.2** Informar las actividades de gestión de riesgos y el estado de la conformidad. | I | I | C | R | I | A | I | I | I | I | C |
| **RR1.3** Interpretar los resultados de la evaluación independiente de TI. | I | I | A/R | R | I | I | I | | C | I | C |
| **RR1.4** Identificar las oportunidades relacionadas con TI. | | I | I | R | I | I | A | R | R | I | I |

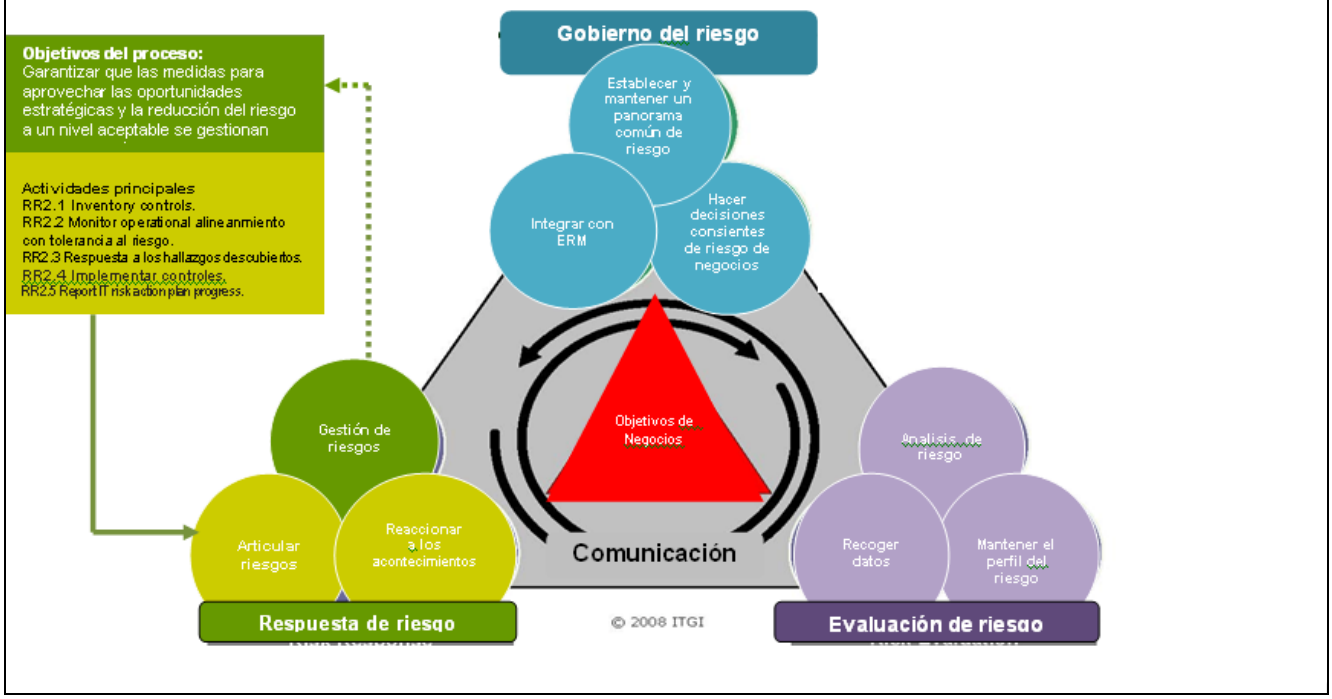
A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

### Métricas y Objetivos

| Objetivos de la actividad | Objetivos del proceso | Objetivo RR |
|---|---|---|
| • Comunicar los resultados del análisis de riesgos de TI.<br>• Informar las actividades de gestión de riesgos y el estado de la conformidad.<br>• Interpretar los resultados de la evaluación independiente de TI.<br>• Identificar las oportunidades relacionadas con TI. | • Asegurar de que la información sobre el verdadero estado de TI- relacionados con la exposición y las oportunidades que se disponga de manera oportuna y a las personas adecuadas para dar respuestas apropiadas. | • Asegurar que las TI - relacionan asuntos de riesgos, las oportunidades y los acontecimientos son tratados en una forma rentable y en línea con las prioridades del negocio |
| **Actividades Métricas** | **Métricas del Proceso** | **Métricas RR** |
| • Porcentaje de informes de análisis de riesgos aceptados en la entrega inicial<br>• Porcentaje de los informes de la gestión de riesgos del tiempo de funcionamiento<br>• La frecuencia de presentación de informes de gestión de la actividad de riesgo<br>• Número de TI- eventos relacionados con el impacto del negocio no se informó previamente como los riesgos de TI / Numero de TI<br>• Número de asuntos de riesgos TI identificados por las partes fuera aún no se ha interpretado y se asigna en el perfil de riesgo | • Porcentaje de las cuestiones de riesgo inadecuadamente distribuidas demasiado alto o demasiado bajo en la jerarquía de la organización (y en consecuencia envió hacia arriba o hacia abajo en la cadena de mando de la decisión)<br>• El número de eventos relacionados con IT con impacto en el negocio no se informó anteriormente como los riesgos de TI<br>• Porcentaje de activos de TI críticos cubiertos por las actividades de vigilancia (detección)<br>• Puntualidad de los informes sobre los riesgos de TI en relación a la amenaza o la pérdida de espera para el próximo evento<br>• Potencial de impacto en el negocio de las exposiciones (según lo acordado por la dirección) descubierto por los grupos de seguros | • El impacto acumulativo de negocio de TI relacionados con los incidentes y acontecimientos previstos por los procesos de evaluación de riesgo, pero no son aún objeto de la planificación de medidas de mitigación o de eventos |

## Visión general del proceso

Figura 38—Gestión de riesgo del proceso RR2



## DETALLE DEL PROCESO

### RR2 Gestión de los riesgos de TI

Garantizar que las medidas para aprovechar las oportunidades estratégicas y la reducción del riesgo a un nivel aceptable se gestionan como una cartera.

***RR2.1 Controles del inventario***
A través de las zonas de riesgo de enfoque, los controles de inventario en el lugar de gestionar el riesgo y permitir que los riesgos que deben adoptarse en consonancia con el apetito de riesgo y la tolerancia. Clasifica a los controles (por ejemplo, predicativo, preventivo, de detección, corrección) y un mapa específico para los riesgos de TI y los agregados de las declaraciones de los riesgos de TI. Desarrollar pruebas para el diseño de control y pruebas de la eficacia del control de funcionamiento. Identificar los procedimientos y la tecnología utilizada para supervisar el funcionamiento de los controles (por ejemplo, el seguimiento de los controles cuando se trate o la automatización de los procesos de supervisión de la empresa). Partición de los controles operativos en las siguientes categorías: controles desplegados en línea con las expectativas que no conocen las deficiencias de funcionamiento, los controles desplegados en línea con las expectativas con las deficiencias de funcionamiento conocidos, y controles desplegadas más allá de las expectativas sin deficiencias operativos más conocidos. Esta tercera categoría de los controles no pueden justificarse, y podría indicar la posibilidad de reducción de costes, manteniendo el mismo nivel de riesgo.

| Para | Entrada |
|---|---|
| RG1 .1 | Áreas de enfoque de riesgo |
| RG1 .3 | Umbrales de tolerancia de riesgos |
| RG1 .4 | Política de riesgos |
| RG2.1 | IT risk doman owners |
| RG2.2 | Gestión de estrategia integrada de riesgos |
| RG3.4, RR3.4 | Requisitos de respuesta de Riesgo |
| RE3.3 | Evaluación de las capacidades de TI |
| RE3.5 | Perfil de riesgo de TI |
| RE3.5, RR2.4 | Actualizar los riesgos y control de línea base |
| RR1 .2, RR2.2 | Deficiencias de control y excepciones de orden |
| COBIT PO6 | Control del marco de la empresa de TI |
| COBIT AI7 | Supervisión de control interno |
| COBIT ME2 | Informe sobre la eficacia de los controles de TI |
| COBIT ME3 | Catálogo de los requisitos legales y reglamentarios relacionados con la prestación de servicios de TI, el informe sobre el cumplimiento de las actividades de TI externos con los requisitos legales y reglamentarios |
| * | Requisitos legales y reglamentarios de asignaciones |

| De | Salida |
|---|---|
| RG2.5, RE2.2, RE2.3, RE3.5, RR1 .3, RR2.2, RR3.4; COBIT PO6 | Riesgo y control de referencia |
| RR1 .4 | Control y reducción de oportunidades |

* Input from/output to outside Risk IT, Val IT and COBIT

***RR2.2 Supervisar la alineación operacional de los umbrales de tolerancia al riesgo.***
Garantizar que cada línea de negocio, acepta la rendición de cuentas para operar dentro de su entidad, los niveles de tolerancia de la cartera y para incrustar instrumentos de supervisión en los procesos operativos clave. Monitorizar el rendimiento y la eficacia de control, medida y la variación de los umbrales de los objetivos. Obtener el compromiso de la dirección sobre los indicadores que funcionarán como KRIS. Poniendo en práctica a KRIS, umbrales de juego y puntos de control (p.e. semanalmente, diariamente, continuamente), y configurar donde enviar notificaciones (p.e., la dirección de línea, la dirección, la revisión de cuentas interna) para que los implicados puedan responder o ajustar sus proyectos. Integre datos KRI en el reportaje de indicador de funcionamiento en curso. Asegúrese de que hay un examen detallado de las zonas de riesgo residual fuera de los umbrales de tolerancia (por ejemplo, solicitud del análisis de riesgo).

| Para | Entrada |
|---|---|
| RG1 .3 | Umbrales de tolerancia de riesgos de TI |
| RG2.2 | La estrategia de gestión integrada de riesgos |
| RE3.2 | Activo / criticidad de los recursos |
| RE3.5 | Perfil de riesgos de TI |
| RE3.6 | Indicadores de riesgos de TI,recomendaciones KRI |
| RR1 .1 | Informe del analisis de riesgos |
| RR1 .2 | Deficiencias de control y excepciones de orden |
| RR2.1 | Riesgo y control de referencia |
| RR3.2 | Alerta de evento de riesgo |
| * | Cultura de riesgo resultados de la encuesta, los datos sobre la adhesión a la política y las normas,datos sobre los umbrales de tolerancia al riesgo frente a la política frente a las operaciones |

| De | Salida |
|---|---|
| RG1.4,RG1.6,RG2.1, RG2.2,RG3.3,RG3.4, RG3.5,RE2.1,RE2.3, RR1.2,RR2.3,RR3.1 | Asuntos y oportunidades de riesgos de TI |
| RG2.2; * | Los requisitos de control |
| RG2.3, RE3.6, RR1.2, RR2.3, RR3.2 | Principales indicadores de riesgos de TI y escaladas desencadentes |
| RG3.4, RE2.3, RR2.1, RR2.3, RR3.2; COBIT PO9, ME1, ME2 | Deficiencias de control y excepciones de orden |
| RG3.4, RR1.2; COBIT PO9 | agregación de datos de riesgo |
| RE2.1 | Solicitud de análisis de riesgos |

* Input from/output to outside Risk IT, Val IT and COBIT

***RR2.3Responder a la exposición al riesgo descubierto y la oportunidad.***
Hacer hincapié en los proyectos que se espera reducir el potencial de la frecuencia y la magnitud de los eventos adversos y pérdidas y el equilibrio con los proyectos que permitan el aprovechamiento de oportunidades estratégicas de negocio. Mantener costo / beneficio de los debates sobre la contribución de los controles nuevos o ya existentes que operan dentro de la tolerancia hacia el riesgo para los objetivos específicos. Candidatos Seleccione los controles de TI basada en amenazas concretas, el grado de exposición al riesgo, la pérdida probable y los requisitos obligatorios especificados en los estándares de TI. Monitorear los cambios en el negocio de perfiles de riesgo operativo subyacente y ajustar las clasificaciones de los proyectos de respuesta de riesgos .

| Para | Entrada |
|---|---|
| RG3.3 | Vida económica completa- coste del ciclo y los beneficios |
| RG3.4, RR3.4 | Requisitos de respuesta de Riesgo |
| RG3.5 | Prestaciones de gestión de riesgo asignado a la cartera de TI, prioridad respuesta a los riesgos (disposición del riesgo) |
| RR1 .1, RR1 .4, RR2.2 | Asuntos y oportunidades de riesgos de TI |
| RR1 .2, RR2.2 | Deficiencias de control y excepciones de orden |
| RR1 .3 | Eventos de vulnerabilidad |
| RR2.2 | Principales indicadores de riesgos de TI y escaladas desencadenantes |
| Val IT IM5 | Plan del programa |
| COBIT PO1 | Plan estratégico de TI, los planes tácticos de TI, IT cartera de proyectos, la cartera de servicios de TI, la estrategia de externalización de TI, la estrategia de adquisición de TI |
| COBIT PO2 | La arquitectura de información, asignan clasificaciones de datos, procedimientos y herramientas de clasificación |
| COBIT PO3 | Oportunidades de la tecnología |
| COBIT PO5 | Los presupuestos de TI |
| * | Arquitectura empresarial hoja de ruta o plan empresarial,perfill de riesgos operativo empresarial |

| De | Salida |
|---|---|
| RG2.2, RG2.5, RG3.3, RR2.4, RR2.5, RR3.1; Val IT PM4; COBIT PO4, PO9, AI6, ME1, ME2 | Plan de acción de los riesgos de TI |
| Val IT IM1; COBIT PO9 | Definición de respuesta a los riesgos de TI |

* Input from/output to outside Risk IT, Val IT and COBIT

***RR2.4 Implementar los controles***
Tomar las medidas necesarias para garantizar el despliegue eficaz de los nuevos controles y ajustes de los controles existentes. Comunicarse con los actores principales al inicio del proceso. Antes de confiar en el control, realizar pruebas piloto y los datos de evaluación de desempeño para verificar la operación contra el diseño. Mapa de los controles operativos nuevos y actualizados a los mecanismos de control que permitan medir el rendimiento de control en el tiempo y las medidas de gestión del sistema cuando sea necesario. Identificar y capacitar al personal sobre los nuevos procedimientos que se despliegan.

| Para | Entrada |
|---|---|
| RG2.1, RG2.2, RG2.3, RR2.3, RR3.4 | Plan de acción de los riesgos de TI |
| RG3.4, RR3.4 | Requisitos de respuesta de Riesgo |

| De | Salida |
|---|---|
| RR2.1 | Actualizar la base de control y los riesgos |
| RR3.2 | Supervisión del rendimiento de los requisitos de control |
| COBIT DS7 | Requisitos de entrenamiento específicos de la gestión de riesgos de TI |

***RR2.5 Informe del progreso del plan de acción de riesgos de TI***
Supervisar el plan de acción de riesgos de TI a todos los niveles para garantizar la eficacia de las medidas necesarias y determinar si la aceptación de riesgo residual fue obtenida. Asegurar de que las acciones cometidas son de propiedad del dueño del proceso afectada (s) y las desviaciones son reportados a la alta dirección.

| Para | Entrada |
|---|---|
| RG2.1, RG2.2, RG2.3, RR2.3, RR3.4 | Plan de acción de los riesgos de TI |
| RR3.1 | Los planes de respuesta a incidentes |

| De | Salida |
|---|---|
| RG1.6, RG2.5, RE3.5, RR3.1 | Progreso del plan de actuación del riesgo de TI /desviaciones |

* Input from/output to outside Risk IT, Val IT and COBIT

### Directrices de gestión – RR2

**Cuadro RACI** **Funciones**

**Actividades Clave**

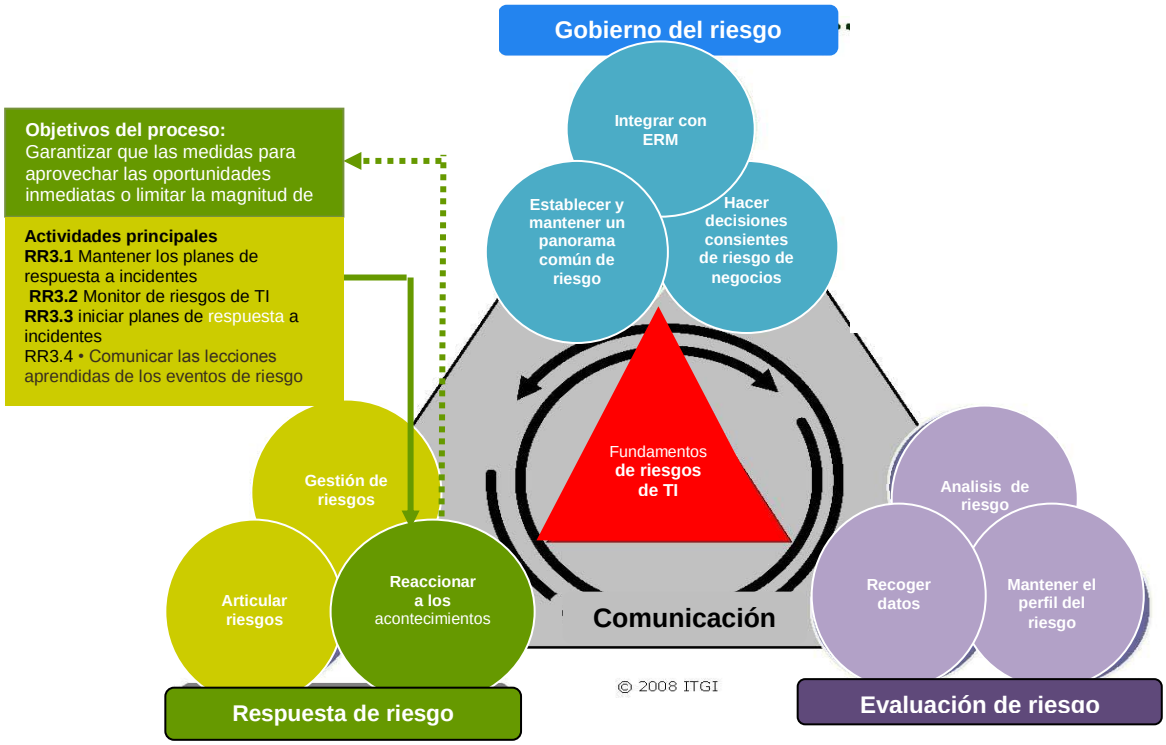
| | Board | CEO | CRO | CIO | CFO | Enterprise Risk Committee | Business Management | Business Process Owner | Risk Control Functions | HR | Compliance and Audit |
|---|---|---|---|---|---|---|---|---|---|---|---|
| RR2.1 Controles de inventario | | I | A/R | C | I | I | C | C | R | | C |
| RR2.2 Supervisar la alineación de funcionamiento de los umbrales de tolerancia al riesgo. | | | C | C | | I | A | R | R | | C |
| RR2.3 Responder a la exposición al riesgo descubierto y la oportunidad. | I | A | C | R | C | I | R | C | C | C | |
| RR2.4 Implementar los controles. | I | A | C | R | C | I | R | C | C | C | I |
| RR2.5 Informar sobre el progreso del plan de acción de los riesgos de TI | I | I | I | R | I | I | I | A | R | I | I |

A RACI chart identiies who isResponsible,Accountable,Consumed,Consulted and/or Informed.

## Métricas y objetivos

| Objetivos de la actividad | Objetivos del proceso | Objetivo RR |
|---|---|---|
| • Controles de inventario<br>• Supervisar la alineación de funcionamiento de los umbrales de tolerancia al riesgo.<br>• Responder a la exposición al riesgo descubierto y la oportunidad.<br>• Implementar los controles<br>• Informar sobre el progreso del plan de acción de los riesgos de TI | • Asegurar de que las medidas para aprovechar las oportunidades estratégicas y la reducción de los riesgos de TI a un nivel aceptable se gestionan como una cartera. | • Asegurar que las TI - relacionan asuntos de riesgos, las oportunidades y los acontecimientos son tratados en una forma rentable y en línea con las prioridades del negocio |
| **Actividades Métricas** | **Métricas del Proceso** | **Métricas RR** |
| • Existencia de un riesgo y control básico para su uso en la vigilancia<br>• Porcentaje de los umbrales de tolerancia al riesgo integrado en el riesgo y el control de línea base<br>• El porcentaje de controles que están directamente relacionados con el mantenimiento de la tolerancia al riesgo definidos<br>• El porcentaje de los riesgos de TI se definen las cuestiones de más tolerancia al riesgo de que los planes de acción se han establecido (alternativamente, el porcentaje de los planes de mitigación que no han sido desarrollados<br>• Número necesario de KRIs que se apliquen plenamente (por ejemplo, los umbrales y los puntos de control establecidos, las notificaciones configurado)<br>• Cantidad de datos KRI Integrado en el indicador de rendimiento de informes en curso<br>• Número y valor de las perdidas de TI relacionados con las oportunidades de | • Satisfacción del titular de riesgo en relación con los resultados de proyectos de mitigación<br>• Porcentaje de reducción del riesgo de los planes ejecutados en el tiempo (por decisión de la dirección, la fecha prevista)<br>• Porcentaje inaceptado de los asuntos de riesgos de TI sin el plan de acción desarrollado Porcentaje inaceptado de los asuntos de riesgos de TI con el plan de acción desarrollado<br><br>• Monto de inversión dedicado a los esfuerzos de mitigación de riesgo que luego se cancela<br>• Número de revisiones pendientes de áreas de riesgo residual fuera de umbrales de la tolerancia | • El impacto acumulativo de negocios de TI relacionados con los incidentes y acontecimientos previstos por los procesos de evaluación de riesgo, pero no son aún objeto de la planificación de medidas de mitigación o de eventos. |

**Figura 39—E l proceso RRE Reacciona a los acontecimientos**



## DETALLE DEL PROCESO

### RR3.Reacción a los acontecimientos

Asegurar que las medidas para aprovechar las oportunidades inmediatas o limitar la magnitud de la pérdida de los acontecimientos relacionados con la TI se activan en forma oportuna y eficaz.

***RR3.1 Mantener los planes de respuesta a incidentes.***
Preparar para la materialización de amenazas a través de planes que el documento de medidas específicas a tomar cuando se produce un evento de riesgo operacional, de desarrollo y / o impacto en el negocio estratégico (es decir, incidente relacionado), o ya ha causado un impacto en el negocio. Mantener una comunicación abierta sobre la aceptación de riesgos, actividades de gestión de riesgos y técnicas del análisis y los resultados disponibles para ayudar con la preparación del plan. En el desarrollo de planes de acción, considere cuánto tiempo la empresa puede estar expuesto y por cuánto tiempo puede tardar en recuperarse. Basados en los efectos conocidos o potenciales, definir las vías de escalada en toda la empresa, desde la gestión en línea a los comités ejecutivos. Compruebe que los planes de respuesta a incidentes de procesos altamente críticos son los adecuados.

| Para | Entrada |
|---|---|
| RG2.1, RG2.2, RG2.3, RR2.3, RR3.4 | Plan de acción de riesgos de TI |
| RE1 .2 | Datos sobre el entorno operativo, histórico riesgos de TI y la pérdida de datos |
| RE1 .3 | Tiempo- real de problemas y la pérdida de datos, análisis de causa raíz y las tendencias de pérdida, las amenazas emergentes, |
| RE1 .4 | Amenazas emergentes |
| RR1 .1 | Informe del análisis de riesgos |
| RR1 .1, RR1 .4, RR2.2 | Asuntos y oportunidades de los riesgos de TI |
| RR2.5 | Informar sobre el progreso del plan de acción de los riesgos de TI / desviaciones |

| De | Salida |
|---|---|
| RG2.2, RR2.5, RR3.2, RR3.3, RR3.4; COBIT PO4, PO8, PO9, AI6, DS5, DS10, ME1, ME2 | Los planes de respuesta a incidentes |
| RE2.1 | Solicitud de análisis de riesgos |
| COBIT DS4 | La disponibilidad, la continuidad y la especificación de la recuperación |

***RR3.2 Supervisión de riesgos de TI***
Supervisar el ambiente. Cuando un límite de control ha sido violada, o bien aumentan con el paso siguiente o confirmar que la medida está de vuelta dentro de unos límites. Categorizar los incidentes (por ejemplo, pérdida de negocio, violación de la política, el fracaso del sistema, el fraude, la demanda), y comparar las exposiciones reales contra los umbrales aceptables. Comunicar los impactos comerciales a los tomadores de decisiones. Continúe con la unidad de acción y los resultados deseados. Garantizar la política se sigue y que hay una clara responsabilidad por las acciones de seguimiento.

| Para | Entrada |
|---|---|
| RG1 .3 | Umbrales de tolerancia de riesgos de TI |
| RG2.2 | Estrategia de gestión integrada de riesgos |
| RG2.3 | Metodos de gestión integrada de riesgos |
| RE3.2 | Activos criticidad de recursos |
| RR1 .2, RR2.2 | Deficiencias de control y excepciones de orden |
| RR2.2 | Principales indicadores de riesgos de TI y escaladas desencadenantes |
| RR2.4 | Requisitos de vigilancia de control de rendimiento |
| RR3.1 | Los planes de respuesta a incidentes |
| COBIT DS5 | Las amenazas de seguridad y vulnerabilidades |
| COBIT DS1 3 | Resguardo de incidentes, los registros de errores, los informes de rendimiento de los procesos |

| De | Salida |
|---|---|
| RR1 .4, RR2.2, RR3.3 | Alerta de evento de riesgo |

***RR3.3 Iniciar planes de respuesta a incidentes.***
Adoptar medidas para minimizar el impacto de un incidente en el progreso. Identifique la categoría de los hechos y seguir los pasos en el plan de respuesta. Informar a todas las partes interesadas y afectadas que un incidente que está ocurriendo. Identificar la cantidad de tiempo necesario para llevar a cabo el plan y hacer los ajustes que sean necesarios, para la situación a la mano. Asegurarse de tomar la acción correcta.

| Para | Entrada |
|---|---|
| RR3.1 | Los planes de respuesta a incidentes |
| RR3.2 | Alerta de evento de riesgo |

| De | Salida |
|---|---|
| RE1 .3, RR3.4 | Acciones de respuesta adoptadas a incidentes |
| COBIT DS8 | Resguardo de incidentes |

***RR3.4 Comunicar las lecciones aprendidas de eventos de riesgo.***
Examinar los últimos acontecimientos adversos y pérdidas. Determinar si hubo una falla derivados de la falta de conciencia, la capacidad o la motivación. De Investigación de la causa raíz de los acontecimientos históricos similares adversos o pérdidas y la eficacia relativa de las medidas adoptadas entonces y ahora. Determinar el alcance de los problemas subyacentes (por ejemplo, un problema sistémico grave contra un caso aislado que pueda ser manejada a través de la formación del personal o una mayor documentación de los procedimientos). Para las operaciones de TI y los incidentes relacionados con la prestación de servicios de TI ofertas de servicios y niveles de servicio (por ejemplo, defectos, reparación), la integración con la oficina de servicio de TI y el proceso de respuesta a incidentes y el proceso de gestión de problemas de TI para identificar y corregir la causa subyacente. La identidad de la causa raíz del problema beneficio / valor y la habilitación de programas y proyectos de incidentes de entrega mediante la comunicación abierta a través de negocios y funciones de TI. Solicitar análisis de riesgo adicionales como sea necesario. Comunicar causa, los requisitos adicionales de respuesta de riesgos y mejora de los procesos de riesgo para los procesos de gobierno y toma de decisiones adecuadas.

| Para | Entrada |
|---|---|
| RG1 .3 | Umbrales de tolerancia de riesgos de TI |
| RG2.3 | Estrategia de gestión integrada de riesgos |
| RE1 .2 | Datos sobre el entorno operativo, histórico riesgos de TI y la pérdida de datos |
| RE1 .3 | Tiempo- real de problemas y la pérdida de datos, análisis de causa raíz y las tendencias de pérdida, las amenazas emergentes, |
| RE1 .4 | Factores de riesgo, amenazas emergentes |
| RR1 .1 | Informe del análisis de riesgos |
| RR2.1 | Riesgos, y línea base de control |
| RR3.1 | Los planes de respuesta a incidentes |
| RR3.3 | Tomar acciones de respuesta a incidentes |
| COBIT DS8 | Informe de incidentes |
| COBIT DS1 0 | Registros de problemas, problemas conocidos, errores conocidos y soluciones |

| De | Salida |
|---|---|
| RG1 .6, RE1 .3, RE3.6 | Causa raíz de los incidentes |
| RG2.1, RE2.3, RR2.1, RR2.3, RR2.4 | Requisitos de respuesta de Riesgo |
| RG2.2, RG2.3, RG2.5 | Mejoras de proceso |
| RG2.2,RG2.5,RG3.3, RR2.4,RR2.5,RR3.1; Val IT PM4; COBIT PO4, PO9, AI6, ME1, ME2 | Plan de acción de riesgos de TI |
| RE2.1 | Solicitud de análisis de riesgos |
| COBIT PO4 | Mejoras del marco del proceso |

## Directrices de gestión – RR3

**Cuadro RACI** **Funciones**

**Actividades Clave**

| | Board | CEO | CRO | CIO | CFO | Enterprise Risk Committee | Business Management | Business Process Owner | Risk Control Functions | HR | Compliance and Audit |
|---|---|---|---|---|---|---|---|---|---|---|---|
| RR3.1. Mantener los planes de respuesta a incidentes. | I | I | I | R | C | I | I | A | R | C | I |
| RR3.2 Supervisar los riesgos de TI. | | | C | I | I | I | I | A | R | C | R |
| RR3.3 Iniciar planes de respuesta a incidentes | I | I | I | I | I | I | R | A | R | C | I |
| RR3.4 **Comunicar las lecciones aprendidas de eventos de riesgo.** | I | I | A/R | R | C | I | C | C | R | C | I |

A RACI chart identiies who isResponsible,Accountable,Consumed,Consulted and/or Informed.

### Métricas y objetivos – RR3

| Objetivos de la actividad | Objetivos del proceso | Objetivo RE |
|---|---|---|
| • Mantener los planes de respuesta a incidentes.<br>• Supervisar los riesgos de TI.<br>• Iniciar planes de respuesta a incidentes<br>• comunicar las lecciones aprendidas de los eventos de riesgo, | • Asegurar que las medidas para aprovechar las oportunidades inmediatas o limitar la magnitud de la pérdida de los acontecimientos relacionados con la TI se activan en forma oportuna y eficaz. | • Asegurar que TI- asuntos relacionados a los riesgos, las oportunidades y los acontecimientos son tratados en una forma rentable y en línea con las prioridades del negocio. |
| **Actividades Métricas** | **Métricas del Proceso** | **Métricas RE** |
| • Porcentaje de los planes de respuesta a incidentes más allá de su próxima fecha de revisión necesaria<br>• Número de Planes de Respuesta a incidentes con los problemas sin resolver de Calidad<br>• Porcentaje de los incidentes con impacto en las empresas que no están sujetos a un examen post-mortem | • Número de eventos con impacto en las empresas debido a retraso en la ejecución de planes de respuesta de incidentes<br>• Número de planes de respuesta a incidentes sin un dueño responsable<br>• Oportunidad de promulgar proyectos de respuesta de incidente<br>• Porcentaje de los planes de respuesta a incidentes con una o más cuestiones pendientes con respecto a su calidad y / o difusión | • El impacto acumulativo de negocios de TI - incidentes y eventos relacionados no identificados por los procesos de evaluación de riesgo |

## MODELO DE MADUREZ DE DOMINIO (RR)
### ALTO NIVEL

**0 No existente cuando**
La organización no ha reconocido la necesidad de administrar las cuestiones de riesgos y las exposiciones al negocio y sus operaciones. No hay procesos de crisis de comunicación que estén en su lugar. Seguimiento de control interno no existe. No hay conciencia de los requisitos externos para implementar los controles, capacidades y recursos para limitar la frecuencia y el impacto (magnitud de la pérdida) de los acontecimientos relacionados con las TI.

**1Inicial cuando**
El reconocimiento de la necesidad de una respuesta de riesgo está surgiendo, pero es visto como limitado a evitar riesgos, para cumplir con los requisitos de cumplimiento y transferencia a través de seguros. Hay conciencia individual mínima de las amenazas y de qué hacer en caso de que se materialicen. Existe una responsabilidad mínima para garantizar que las medidas razonables de respuesta de riesgos están en el lugar y reflejan el ambiente de amenaza y los valores de los activos. Eventos de TI relacionados y condiciones que podrían afectar el día a día las operaciones en ocasiones se discuten en las reuniones de gestión, pero las respuestas de riesgo específicos no se consideran. Los controles de TI existen, pero se basan en requisitos de cumplimiento, varían ampliamente en relación al riesgo y operar en silos aislados.
La falta de habilidades y competencias para la respuesta de riesgo puede obligar a la empresa a aceptar el riesgo más allá de los niveles de tolerancia, cuando las propuestas de valor son particularmente convincentes.

**2 Repetible cuando**
Hay conciencia individual de las amenazas y los puntos de contacto para la dirección cuando se materialicen. La respuesta en cuestiones de riesgos de TI son comunicadas por la gestión pero las discusiones de respuesta de riesgo de TI pueden verse afectadas por la competencia por un lenguaje de unidad de negocio de riesgo específicos. Hay un líder emergente para la respuesta de riesgo de TI asume la responsabilidad para mitigar los riesgos y ayudar a gestionar el impacto de los acontecimientos. Deficiencias de control pueden ser identificados, pero no se remedian en forma oportuna. Los procesos de reducción del riesgo están comenzando a ponerse en práctica cuando se detecten problemas de TI de riesgo. Requisitos de formación mínimos son identificados para las áreas críticas de la articulación de riesgos, mitigación y gestión de crisis. Existen enfoques comunes para el uso de herramientas de mitigación y respuesta de riesgos pero se basan en las soluciones desarrolladas por los individuos clave.

**3 Definida cuando**
A través de la organización hay comprensión individual del impacto de las amenazas de negocio y las acciones específicas a tomar en caso de que se materialicen las amenazas de negocio. Responsabilidad y rendición de cuentas para las prácticas de respuesta clave de riesgo se definen y los dueños del proceso han sido identificados. Las deficiencias de control son identificadas y remediadas de manera oportuna. Una empresa en toda la política de respuesta a los riesgos define cuándo y cómo responder a los riesgos. Las descripciones de trabajo incluyen las expectativas de respuesta a los riesgos. Los empleados son capacitados periódicamente en amenazas relacionadas de TI, los escenarios de riesgo, y los controles pertinentes a sus funciones y responsabilidades. El plan se ha definido para su uso y normalización de las herramientas para automatizar las actividades de reducción del riesgo, como el aprovisionamiento de usuarios.

**4 Gestionado cuando**
Hay ambos comprensión individual y organizativa de todos los requisitos para responder a los riesgos. La alta dirección empresarial y la gestión de TI en conjunto, determinan si una condición de riesgo es superior a las tolerancias definidas de riesgo. Una cultura de la recompensa está en el lugar motivando a la acción positiva. La eficiencia y la eficacia de la respuesta a los riesgos son medidos y comunicados, y vinculado a los objetivos de negocio y el plan estratégico de TI. Todos los aspectos del proceso de respuesta de los riesgos se documentan y son cuantitativamente gestionados. Los requisitos de habilidad son rutinariamente actualizados para todas las zonas de riesgo de respuesta, incluyendo la articulación de riesgos, mitigación de riesgos, reaccionando a los acontecimientos y aprovechando oportunidades. Las herramientas se utilizan en las principales zonas para permitir la gestión del riesgo de cartera de la empresa y supervisar los controles críticos, las capacidades y recursos.

**5 Optimizado cuando**
No es a la vez individuales y empresariales comprensión de todos los requisitos para hacer frente al riesgo. Las respuestas a los riesgos reales a las operaciones reales se comunicarán vigorosamente en toda la empresa. La organización colabora en conjunto con entidades externas para responder a las cuestiones comunes y la pandemia de riesgo. La empresa mide la eficacia de los esfuerzos de respuesta a los riesgos tanto a nivel interno y en colaboración con entidades externas. La gama completa de estrategias de respuesta de riesgo es aplicado de manera integral y, cuando sea plenamente justificado, controles costo-eficacia mitigan la exposición al riesgo en forma continua. La empresa exige formalmente la mejora continua de las capacidades de respuesta de riesgos (por ejemplo, la articulación de riesgo, la mitigación, la gestión de crisis) sobre la base de definir claramente los objetivos personales y de organización. La empresa emplea tecnologías avanzadas de respuesta de riesgos para inteligentemente asumir riesgos adicionales y aprovechar las oportunidades competitivas.

| Figura 40- RR Modelo detallado de Madurez la Parte 1 | | | |
|---|---|---|---|
| | **Conocimiento y comunicación** | **Responsabilidad y Rendición de Cuentas** | **Fijación y medición de objetivos** |
| 0 | La organización no ha reconocido la necesidad de administrar los riesgos y las exposiciones a las cuestiones del negocio y sus operaciones. No hay procesos de crisis de comunicación están en su lugar. No existe seguimiento del control interno. No hay conciencia de los requisitos externos para implementar los controles, capacidades y recursos para limitar la frecuencia y el impacto (magnitud de la pérdida) de TI eventos relacionados. | | |
| 1 | El reconocimiento de la necesidad de una respuesta del riesgo está surgiendo, pero es visto como limitado a evitar riesgos, para cumplir con los requisitos de cumplimiento y transferencia a través de seguros. No hay conciencia individual mínima de las amenazas y qué hacer en caso de que se materialicen.<br>Hay una comunicación mínima en torno a la detección y respuesta a los acontecimientos y las respuestas de riesgo de acuerdo con las prioridades del negocio. | Existe una responsabilidad mínima para garantizar que las medidas razonables de respuesta de riesgos en el lugar y reflejan el ambiente de amenaza y los valores de los activos.<br><br>Los individuos asumen la responsabilidad tanto de la evaluación de riesgos y la respuesta a los riesgos. | TI-los eventos relacionados y las condiciones que podrían afectar el día a día las operaciones en ocasiones se discuten en las reuniones de gestión de riesgo específico, pero las respuestas no son considerados. Deficiencias de control se discuten en un modo reactivo y son difíciles de definir.<br>La Gestión de la información mínima que existe para ayudar a detectar los eventos de una manera oportuna y comparar las respuestas con las prioridades del negocio. |
| 2 | Existe una creciente conciencia de la necesidad de responder a los riesgos, como lo demuestra la introducción de estrategias de prevención más allá, como la reducción, el intercambio o la aceptación en el contexto de apetito por el riesgo y la tolerancia. No es la conciencia individual de las amenazas y los puntos de contacto para la dirección cuando se materialicen.<br>Las respuestas de riesgo de asuntos de TI son comunicados por la gerencia, pero los riesgos de TI responden a discusiones quizá afectadas por la competencia unidad de negocio de idiomas de riesgo específicos. | Hay un líder emergente para la respuesta de riesgo de TI que asume la responsabilidad de mitigar el riesgo y ayudar a manejar el impacto de acontecimientos. El líder por lo general es imputado la responsabilidad, incluso si esto formalmente no es estado de acuerdo.<br><br>En general, hay confusión acerca de la responsabilidad de la respuesta de riesgo. Cuando hay problemas, una cultura de la culpa tiende a existir. | El control de las deficiencias pueden ser identificados, pero que no se rehabiliten en forma oportuna.<br>Algunos objetivos establecen la respuesta de riesgo se produce, pero no puede centrarse en el riesgo real para las operaciones reales. |
| 3 | Los ejecutivos de negocios de TI pueden explicar sus tres principales problemas de TI de riesgo (es decir, combinaciones de control, el valor y las condiciones de amenaza que imponer un nivel significativo de riesgo) y las medidas que están tomando en respuesta, en consonancia con el apetito de riesgo y la tolerancia.<br><br>A través de la empresa es la comprensión individual de la empresa-que afectan las amenazas y las acciones específicas a tomar en caso de amenaza de la materialización del negocio. Los empleados son conscientes de su responsabilidad para las actividades de control. Hay una comprensión común de la necesidad de adoptar medidas de respuesta de riesgo.<br><br>Los riesgos de TI y los planes de las estrategias son comunicados por la gerencia. Los riesgos de TI debates de respuesta se basan en un lenguaje definido / taxonomía. Escala de empresa información sobre la respuesta de riesgo es compartido. | La responsabilidad y la rendición de cuentas para prácticas de respuesta de riesgo claves son definidas y tratan a propietarios han sido identificados. El propietario de proceso improbablemente tiene la autoridad completa para ejercer sus/sus responsabilidades.<br>Las descripciones de trabajo consideran responsabilidades de respuesta de riesgo.<br><br>Las descripciones del trabajo considera las responsabilidades de respuesta del riesgo. | Las carencias de control son identificadas y mediadas de nuevo en una manera oportuna.<br>La tolerancia inaceptable y la mitigación son relatadas al gerente apropiado.<br><br>El Apetito por el riesgo y la tolerancia se aplican durante el desarrollo de las TI de mitigación de riesgos y planes de acción del evento.<br><br>Presentación de informes periódicos de los resultados de respuesta de TI riesgo proceso está dirigido a la administración de TI. |
| 4 | La dirección es asesorada sobre los cambios en la empresa y el ambiente de TI que podrían<br>Afectar significativamente los escenarios de riesgo de TI Hay Conocimiento tanto individual como organizativo de todos los requisitos para responder a los riesgos.<br><br>Los debates respuesta a los riesgos se basan en los términos definidos. Respuesta de la empresa de información sobre riesgos se ajusta a un modelo estándar y es ampliamente compartida. | La alta dirección empresarial y la gestión de TI en conjunto, determinan si una condición de riesgo superior a definir las tolerancias de riesgo. De reducción del riesgo y la responsabilidad de respuesta y la rendición de cuentas son aceptadas y de trabajo de una manera que permite a un propietario de proceso para cumplir plenamente sus responsabilidades. Una cultura de la recompensa está en el lugar que motiva a la acción positiva. | La eficiencia y la eficacia de la respuesta a los riesgos se miden y se comunique, y vinculado a los objetivos de negocio y el plan estratégico de TI<br>El efecto de funcionamiento de las actividades de control se evalúa de forma periódica y el proceso está bien documentado.<br><br>Presentación de informes periódicos que se haga a la gestión empresarial de los resultados de negocio relacionados con TI proceso de respuesta a los riesgos. |

| Figura 40- RR Modelo detallado de Madurez la Parte 1 (cont.) | | | |
|---|---|---|---|
| 5 | La organización extendida es muy consciente de todos los requisitos y las estrategias y planes en marcha para hacer frente al riesgo<br><br>Las respuestas a los riesgos reales a las operaciones reales se comunicarán con fuerza en toda la empresa. | Los empleados en todos los niveles asuman la responsabilidad organización colabora en conjunto con entidades externas para responder a las cuestiones comunes y la pandemia de riesgo. | La organización mide la eficacia de los esfuerzos de respuesta a los riesgos tanto a nivel interno y en colaboración con entidades externas. |

| Figura 41- RR Modelo detallado de Madurez la Parte 2 | | | |
|---|---|---|---|
| | **Políticas, normas y procedimientos** | **Habilidades y experiencia** | **Herramientas y automatización** |
| **0** | | | |
| **1** | Los controles de TI existen, pero se basan en requisitos de cumplimiento, varían ampliamente en relación con los riesgos y operar en silos aislados. | Una falta de habilidades y competencias para la respuesta de riesgo puede obligar a la empresa a aceptar el riesgo más allá de los niveles de tolerancia, cuando las propuestas de valor son particularmente convincentes.<br>La articulación de riesgo de IT, la mitigación y la capacidad de gestión de crisis pueden existir en los silos, pero no están desarrollando activamente. Los gestores de riesgos de empresa y los propietarios de la falta de procesos de negocio de TI comprender la respuesta de riesgo. El personal de TI carecen de la gestión de proyectos y habilidades de gestión de crisis crítico para los programas de mitigación de riesgos y minimizar el impacto de los eventos de riesgo.<br>Los empleados desean habilidades de respuesta de riesgo mejoradas, pero ningún inventario de estas habilidades existe, ni está allí un modelo de capacidad establecido para documentar futuras exigencias de habilidad.. | Las herramientas técnicas de seguridad se implementan de manera fortuita, que generalmente no es relacionado con el riesgo, el impacto y efectividad de costes.<br><br>Algún control de inventario céntrico y herramientas de registro de incidentes pueden existir, se basa en el uso de aplicaciones de escritorio estándar. |
| **2** | Los procesos de reducción del riesgo están comenzando a ponerse en práctica cuando se detecten problemas de TI de riesgo. | Los requisitos mínimos de formación son identificados para las áreas críticas de la articulación de riesgos, mitigación y gestión de crisis.<br>La capacitación en respuesta a los riesgos es en respuesta a las necesidades tácticas, más que sobre la base de un plan acordado, y de formación informal se produce en el trabajo. | Los accesos comunes al empleo de mitigación de riesgo e instrumentos de respuesta existen, pero están basados en soluciones desarrolladas por individuos claves. |
| **3** | Una empresa - la política global de respuesta a los riesgos define cuándo y cómo responder a los riesgos. Un proceso para tratar un tema clave de las TI de riesgo es por lo general una vez que se instituyó la identificó. | Las descripciones de trabajo incluyen las expectativas de respuesta a los riesgos. A los empleados se les capacita periódicamente en TI relacionados con las amenazas, los escenarios de riesgo, y los controles pertinentes a sus funciones y responsabilidades.<br>Las necesidades de competencias definidos y documentados para todas las áreas de riesgo empresarial, con plena consideración de las TI articulación de riesgo, mitigación y gestión de crisis. Capacitación incluye técnicas de respuesta a los riesgos más allá de las políticas de mínimos y las herramientas comunes de gestión de proyectos y gestión de crisis. Los gestores de riesgos de empresa y los propietarios de procesos de negocio orientados recibir la formación en respuesta a los riesgos.<br>Las exigencias de habilidad son definidas y documentadas para todas las áreas de respuesta de riesgo. Un plan de entrenamiento formal para la respuesta de riesgo ha sido desarrollado. Los datos están disponibles en cuanto al movimiento de habilidades de respuesta de riesgo críticas y capacidades. | El plan ha sido definido para el uso y la normalización de las herramientas para automatizar las actividades de reducción del riesgo, como el aprovisionamiento de usuarios. |

| Figura 41- RR Modelo detallado de Madurez la Parte 2 (cont.) | | | |
|---|---|---|---|
| 4 | Existen mecanismos ágiles para la comunicación de incidentes de riesgo al alza para la alta dirección, sin demoras.<br>Todos los aspectos del proceso de respuesta a los riesgos se documentan y cuantitativamente gestionado. Normas para el desarrollo y mantenimiento de los procesos y procedimientos que se adopten y se sigan. | Los requisitos de habilidad son rutinariamente actualizados de todas las zonas de riesgo de respuesta, incluyendo la articulación de riesgos, mitigación de riesgos, reaccionando a los acontecimientos y aprovechar las oportunidades. De competencia se garantiza a todas las áreas críticas, y la certificación se anima.<br><br>Las Técnicas de capacitación mayor se aplican en función del plan de formación, y se fomenta el intercambio de conocimientos. Todos los expertos respuesta interna de riesgo de dominio están involucrados, y la eficacia del plan de formación se evalúa.<br>La empresa se ocupa del desarrollo a más largo plazo las necesidades de personal con alto potencial en respuesta a los riesgos (por ejemplo, gestión de proyectos, gestión de crisis) y habilidades relacionadas | Se utilizan las herramientas en las principales zonas para permitir la gestión del riesgo de cartera y de la empresa para supervisar los controles críticos, las capacidades y recursos. |
| 5 | La gama completa de estrategias de respuesta de riesgo es aplicado de manera integral y, cuando sea plenamente justificado, costo-eficacia de los controles de mitigar la exposición al riesgo en forma continua.<br>La documentación de proceso es desarrollada a procesos laborales automatizados. Los procesos, la política y procedimientos son estandarizados e integrados para permitir de punta a punta la respuesta de riesgo y la mejora. | La organización exige formalmente la mejora continua de las capacidades de respuesta de riesgos (por ejemplo, la articulación de riesgo, la mitigación, la gestión de crisis) sobre la base de definir claramente los objetivos personales y de organización.<br><br>Hay frecuentes recordatorios y los debates de TI relacionados con las amenazas, los escenarios de riesgo, los controles y el progreso hacia el cumplimiento de los objetivos clave de respuesta a los riesgos. | La supervisión en tiempo real de los factores de riesgo emergentes y eventos con las herramientas estándar se produce. La tecnología es aprovechado en toda su extensión a los procesos de documento, determinar las carencias, y evaluar la eficacia de los controles de riesgos, las capacidades y recursos.<br>La empresa cuenta con tecnologías avanzadas de respuesta de riesgos de forma inteligente asumir riesgos adicionales y aprovechar las oportunidades competitivas. |

## APÉNDICE 1. VISIÓN GENERAL DE REFERENCIA DE MATERIALES

La siguiente lista es un resumen de los materiales que se han utilizado y que se hace referencia en el desarrollo de este marco.


AIRMIC, ALARM, IRM, 'A Risk Management Standard', 2002 , *www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf*

Alfred P. Sloan Foundation, *Framework for Voluntary Preparedness: Briefing Regarding Private Sector Approaches to Title IX of H.R. 1 and Public Law 110-53*, 'Implementing Recommendations of the 9/11 Commission Act of 2007', USA, 2007

Barnier, B.; 'Driving Value From Nonrevenue-generating Activities: Myths and Misunderstandings of Governance and Risk Management', *ISACA Journal*, ISACA, USA, 2009

Barnier, B.; 'Reducing Operational Risks by Creating Resilience in IT and Infrastructure', IBM, USA, 2008

Caralli, R.; J. Stevens; D. White; L. Young; S. Merrell; S. Bacon; 'CERT Resiliency Engineering Framework v0.95R', Carnegie Mellon, USA, 2008

Caralli, R.; J. Stevens; C. Wallen; D. White; W. Wilson; L. Young; 'Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes', Carnegie Mellon, 2007

Wallen, C.; B. Barnier; D. Nolan; D. O'Neill; 'Managing Resiliency, Taking a Strategic Approach', *FSTC Innovator*, USA, 2009

Club de la Securite de l'Information Français (CLUSIF), 'MEHARI 2007: Concepts and Mechanisms', France, 2007

Committee of Sponsoring Organizations (COSO) of the Treadway Commission, *Enterprise Risk Management—Integrated Framework*, USA, 2004, *www.coso.org*

Ernst & Young, *Managing Information Technology Risk: A Global Survey for the Financial Services Industry*, USA, 2008

Rasmussen, M.; 'Taking Control of IT Risk, Defining a Comprehensive IT Risk Management Strategy', Forrester Research Inc., 2006

Gerrard, M.; 'Increase the Value of IT Demand Governance: Add Investment Risk Management', Gartner, USA, 2005

HM Treasury, *Thinking About Risk (Managing your risk appetite: A practitioner's guide; Setting and communicating your risk appetite; Managing your risk appetite: Good practices examples*), UK, 2006

Holthause, D.; 'A Risk-Return Model With Risk and Return Measured as Deviations From a Target Return', USA, 1981

Hubbard, D.; *How to Measure Anything: Finding the Value of "Intangibles" in Business*, John Wiley and Sons Inc., USA, 2007

IBM, 'IT and Infrastructure Risk Management', USA, 2009

Information Security Forum, *Business Impact Assessment*, UK, 2008

Information Security Forum, *ISF Standard of Good Practice, SPRINT Risk Analysis Method*, UK, 2007

Institute for Internal Auditors, *Guide to the Assessment of IT Risk (GAIT)*, USA, 2007

ISO/IEC, ISO/DIS 31000, *Risk Management—Principles and Guidelines on Implementation*, Switzerland, 2009

ISO/IEC, ISO/FDIS 27005, *Information Technology—Security Techniques—Information Security Risk Management*, Switzerland, 2008

ISO/IEC, ISO/IEC27006, *Information Technology—Security Techniques—Requirements for Bodies Providing Audit and Certification of Information Security Management Systems*, Switzerland, 2007

ISACA, COBIT 4.1, USA, 2007, *www.isaca.org*

ISACA, *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*, USA, 2006

ISACA, *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*, USA, 2007

ISACA, *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, USA, 2008, *www.isaca.org*

ISACA; *IT Control Objectives for Basel II, The Importance of Governance and Risk Management for Compliance*, USA, 2007,*www.isaca.org*

Jones, J.; 'An Introduction to Factor Analysis of Information Risk (FAIR)', Risk Management Insight, USA, 2005, *http://fairwiki.riskmanagementinsight.com/*

Jones, J.; 'FAIR Taxonomy', Risk Management Insight, USA, 2008

Jones, J.; 'Risk Decisions: Whose Call Is It?', Risk Management Insight, USA, 2007

Jones, J.; 'The Case for Risk-based Security', Risk Management Insight, USA, 2007

Messmer, E.; 'Open Group's Security Forum Devising Risk-management Taxonomy', *NetworkWorld*, USA, 2008

Moody, M.; 'Risk and Insurance Management Society (RIMS): Data From Risk Managers Will Help Share ERM Initiatives', The Rough Notes Company Inc., USA, 2007

Open Compliance and Ethics Group (OCEG), *Red Book 2.0: Foundation Guidelines*, USA, 2009

Peccia, A.; 'An Operational Risk Rating Model Approach to Better Measurement and Management of Operational Risk', Citigroup, USA, 2004

Premier Ministre: Secrétariat Général de la Défense Nationale, Direction Centrale de la Sécurité des Systèmes d'Information, 'EBIOS: Expression of Needs and Identification of Security Objectives', France, 2003

PricewaterhouseCoopers LLP, 'A Practical Guide to Risk Assessment', USA, 2008

PricewaterhouseCoopers LLP, 'Extending Enterprise Risk Management (ERM) to Address Emerging Risks', USA, 2009

PricewaterhouseCoopers LLP, 'How to Prepare for Standard and Poor's Enterprise Risk Management Evaluations', webcast, USA, 2008

PricewaterhouseCoopers with IIA, 'IT Risk—Closing the Gap: Giving the Board What It Needs to Understand, Manage and Challenge IT Risk', USA, 2007

Protiviti, 'Credit Rating Analysis of Enterprise Risk Management at Non-Financial Companies: Are You Ready?', USA, 2008

Protiviti Flash Report, 'Societe Generale Aftermath a Call to Action', USA, 2008

Ren, F.; S. Dewan; *Information Technology and Firm Boundaries: Impact on Risk-Return Profile*, The Paul Merage School of Business, University of California, Irvine, USA, 2006

Reznik, S.; 'Back to Business with IT Governance', *The Journal of Corporate Accounting and Finance*, vol. 18, no. 6, Sep/Oct 2007, Wiley Periodicals Inc., USA, 2007

Reznik, S.; 'Make "MyCOBIT" Your COBIT', *COBIT Focus*, ISACA, USA, January 2008

Risk and Insurance Management Society (RIMS), *RIMS Risk Maturity Model (RMM) for Enterprise Risk Management*, USA, *www.rims.org/erm/pages/riskmaturitymodel.aspx*

Risk and Insurance Management Society (RIMS), *RIMS Risk Maturity Model (RMM) for Enterprise Risk Management: Executive Summary*, USA, *www.rims.org/erm/pages/riskmaturitymodel.aspx*

Risk and Insurance Management Society (RIMS), *RIMS: Risk Manager Core Competency*, USA, 2007

Ross, R.; S. Katzke; 'Managing Risk from Information Systems: An Organizational Perspective', US Department of Commerce, USA, 2008

Standards Australia, AS/NZS 4360:2004, *Australian/New Zealand Standard for Risk Management*, Australia, 2004, *www.saiglobal.com*

Symantec, *IT Risk Management Process 2: Myths and Realities*, Canada, 2008

The Open Group, 'Requirements for Risk Assessment Methodologies', Technical Guide, USA, 2009

Tanriverdi, H.; T. Ruefli; 'The Role of Information Technology in Risk/Return Relations of Firms', McCombs School of Business, The University of Texas at Austin, USA, 2005

Westerman, G.; R. Hunter; 'IT Risk—Turning Business Threats into Competitive Advantage', Harvard Business School Press, USA, 2007

# APÉNDICE 2. COMPARACIÓN DE ALTO NIVEL DE RIESGOS CON OTROS MARCOS DE GESTIÓN DE RIESGOS Y NORMAS

El marco de riesgo de TI se basa en los seis principios definidos en *The Risk IT Framework*. **La figura 42** compara el riesgo a un número de normas y marcos en el ámbito (relación - TI) la gestión del riesgo demuestra hasta qué punto se han incluido y aplicado estos principios. Entonces el lector puede decidir, basándose en su necesidad específica, que marco o combinación de marcos utiliza, teniendo en cuenta la situación heredada en su empresa, la disponibilidad de la norma o marco y otros factores.

Los marcos siguientes se incluyen en la comparación:

- Comité de Organizaciones Patrocinadoras (COSO) de la Comisión Treadway, *Enterprise Risk Management—Integrated Framework,2004*
- ISO/IEC, ISO/FDIS 31000, *Risk Management—Principles and Guidelines,* 2009
- Standards Australia, AS/NZS 4360:2004, *Australian/New Zealand Standard for Risk Management,* 2004
- AIRMIC, ALARM, IRM, 'A RISK Management Standard', 2002
- ISO/IEC, ISO/IEC 20000-1/2:2005, *Information Technology—Service Management—Part 1: Specification* and *Part 2: Code of Practice,* 2005
- Project Management Institute, *Project Management Body of Knowledge* (PMBOK® Guide), 4th Edition, 2008. This is described as 'the sum of knowledge within the profession of project management'. It is an American National Standard, ANSI/PMI 99-001-2004.
- ISO/IEC 27005:2008, *Information Technology—Security Techniques—Information Security Risk Management,* 2008,
- ISO/IEC 27001:2005, Information Technology—Security Techniques—Information Security Management Systems—Requirements and
- ISO/IEC IEC 27002:2005, Information Technology—Security Techniques—Code of Practice for Information Security Management, 2005

La **figura 42** muestra una comparación de principios-/futuros-basados de los diferentes marcos.

- La primera serie de columnas se describen los principios / las características y el hecho de que éstos puedan abarcar, como base de la comparación.
- La segunda serie de columnas proporcionan los mapas para la gestión de riesgos relacionados con el marco de trabajo.
- La última serie de columnas describen los principios y la cobertura característica por el dominio - Enfocados en el marco aquellos, como la gestión de servicios, gestión de proyectos y la seguridad. Estos marcos, por definición de su alcance, no se destinan a cubrir la anchura de todos los riesgos de TI, pero puede ser visto como un complemento de los riesgos de TI para ofrecer más detalles sobre cómo administrar los riesgos en determinados ámbitos.

**Figure 42— Comparativa de Marcos de Gestión de Riesgos**

| Principle/Feature | RIESGOTI | | COSOERM-Intrgrated framework,2004 | ISO/FDIS 3100: 2009 | AS/NZS 4360:2004 | ARMS,2002 | | ISO 20000:2005, Parts 1 and 2 | PMBOK | ISO /IEC27005: 2008 | ISO /IEC27001: |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Principales Riesgos de TI | | | | | | | | | | | |
| Conectar siempre con los objetivos de negocio | ■ | | ■ | ■ | ■ | ■ | | | ■ | ■ | |
| Alinear la gestión de negocios de TI relacionados con el riesgo global con el MTC | ■ | | | | | | | | | | |
| Balance de los costos y beneficios de la gestión del riesgo | ■ | | ■ | ■ | ■ | ■ | | | | | |
| Promover la comunicación justa y abierta de los riesgos de TI | ■ | | ■ | ■ | ■ | ■ | | | | | |
| Establecer el tono correcto de la parte superior, mientras que la definición y aplicación de la responsabilidad personal para operar dentro de los niveles de tolerancia | ■ | | ■ | ■ | ■ | ■ | | | | | |
| Si es un proceso continuo y parte de la actividad diaria | ■ | | ■ | ■ | ■ | ■ | | ■ | ■ | ■ | |
| Características adicionales | | | | | | | | | | | |
| Disponibilidad (para el público en general) | ■ | | | | | ■ | | | | | |
| Visión Integral (relacionadas) sobre riesgo de TI | ■ | | | | | | | | | | |
| Específicamente en las prácticas de gestión de riesgos para determinadas áreas de TI (gestión de proyectos, gestión de servicios, seguridad, etc.) | | | | | | | | ■ | ■ | ■ | |
| Proporcionar un modelo de proceso detallado con las directrices de gestión y modelos de madurez | ■ | | | | | | | | | | |

Leyenda:
Azul-Principio / función quede totalmente cubierta.
Gris- Principio / función está parcialmente cubierto.
Blanco- Principio / función no está cubierto.

Las principales características del marco de riesgo que la distinguen de las demás normas y marcos son las siguientes:
• Riesgo de TI enfocado en TI.
• Riesgo de que se ajusta a cualquier genérico / a través-del dominio de las normas de riesgo de la empresa.
• Riesgo de TI continuamente alineados con COBIT y Val IT (y de ahí a otras normas, tales como PMBOK y PRINCE2, como se explica en los documentos detallados mapas COBIT) [9].
• Riesgo de TI proporciona un respaldo de riesgo a través de otro marco mas, la práctica y el modelo de proceso (por ejemplo, 2700x, 25999, DRI Internacional [DRII] PAC, Business Continuity Institute [BCI] Mejores prácticas de Seguridad de la Información del Foro [FIA], biblioteca de la infraestructura de tecnología de la información [ITIL).

[9] ISACA, *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*, USA, 2006, and ISACA, *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*, USA, 2007

# APÉNDICE 3. RESUMEN DE LOS RIESGOS DE TI

| Termino | Explicación |
|---|---|
| Activo | Algo de valor ya sea tangible o intangible dignos de protección, incluidas las personas, la información, la infraestructura, las finanzas y la reputación |
| Objetivo de negocio | La traducción de la misión de la empresa de una declaración de intenciones en objetivos y resultados del rendimiento |
| Impacto de negocio | El efecto neto, positivo o negativo, sobre la consecución de los objetivos de negocio |
| Objetivo de caso de negocio | Un mayor desarrollo de los objetivos de negocio en objetivos tácticos y los resultados deseados y los resultados |
| Riesgo de negocio | Una situación probable con frecuencia incierta y la magnitud de la pérdida (o ganancia) |
| Gestión de riesgos de la empresa | La disciplina con la cual una empresa en cualquier industria valora, controla, explota, financia y supervisa los riesgos de todas las fuentes con el fin aumentar la empresa a corto y valor a largo plazo a las partes interesadas |
| Eventos | Algo que ocurre en un lugar específico y / o tiempo |
| Tipo de evento | Efectos de la gestión de riesgos de TI [10],<br>Eventos de amenazas<br>Perdida de eventos<br>Eventos de vulnerabilidad |
| Frecuencia | Una medida de la tasa por la que ocurren los eventos durante un determinado período de tiempo |
| Riesgo inherente | El nivel de riesgo o la exposición sin tener en cuenta las acciones que la administración ha adoptado o pueda adoptar (por ejemplo, la aplicación controles) |
| Riesgos de TI | El riesgo de negocios asociados con el uso, propiedad, operación, la participación, la influencia y la adopción de TI dentro de una empresa |
| Asuntos de riesgos de TI | 1.Una instancia de un los riesgos de TI<br>2. una combinación de control, el valor y las condiciones de amenaza que imponer un nivel notable de los riesgos de TI |
| Perfil de riesgos de TI | Una descripción del riesgo global (identificadas) de TI a los que está expuesta la empresa |
| Registro de riesgos de TI | Un repositorio de los atributos clave de los posibles problemas de TI y conocidos de riesgo. Los atributos pueden incluir el nombre, descripción, el titular, que se espera / frecuencia real, potencial / magnitud real, potencial o impacto de negocio real, disposición. |
| Escenario de riesgos de TI | La descripción de un evento relacionado con la IT que pueden conducir a un impacto en las empresas |
| Incidentes relacionados -TI | Un evento relacionado con la TI que las causas de funcionamiento, desarrollo y / o impacto en las empresas estratégicas |
| Pérdida de eventos | Cualquier caso de amenaza de un evento o amenaza en la perdida de los resultados [11] |
| Magnitud | Una medida de la posible gravedad de la pérdida o la ganancia potencial se dio cuenta de un evento relacionado con la IT / escenario |
| Riesgo residual | El riesgo que queda después de la gestión de riesgo ha puesto en marcha la respuesta |
| Agregación de riesgos | El proceso de integración de las evaluaciones de riesgo a nivel corporativo para obtener una visión completa sobre el riesgo global de la empresa |
| Análisis de riesgos | Un proceso por el cual la frecuencia y la magnitud de los riesgos de TI escenarios se estima |
| Apetito de riesgo | La cantidad de riesgo, en un nivel más amplio, que la entidad está dispuesta a aceptar en el cumplimiento de su misión |
| Cultura de riesgo | Serie de valores compartidos y las creencias que rige las actitudes hacia la asunción de riesgos, la atención y la integridad, y determina cómo abiertamente los riesgos y las pérdidas se presentan y discuten |
| Factor de riesgo | Condición que puede influir en la frecuencia y / o magnitud y, en última instancia, el impacto en el negocio de TI relacionados con eventos / escenarios |
| Indicador de riesgo | Una métrica que pueda demostrar que la empresa está sujeta a, o tiene una alta probabilidad de ser sometidos a un riesgo que superan el apetito riesgo se define |
| Gestión de riesgo | Ha sido utilizado en esta publicación como un término genérico global que abarca tanto el gobierno y la gestión |
| Mapa de riesgo | Un(gráfico) herramienta para visualizar y clasificar los riesgos por los rangos definidos para la frecuencia y la magnitud |
| Visión de cartera de riesgos | 1.Un método para identificar las interdependencias e interconexiones entre los riesgos, así como el efecto de las respuestas de riesgo sobre los múltiples riesgos<br>2. un método para estimar el impacto global de los múltiples riesgos (por ejemplo, la cascada de amenazas y los tipos de coincidencia / escenarios, concentración de riesgos y de correlación entre los silos) y El efecto potencial de la respuesta a los riesgos a través de los múltiples riesgos |
| Declaración de Riesgo | Una descripción de las condiciones actuales que pueden conducir a la pérdida, y una descripción de la pérdida. Fuente: Software Engineering Institut e (SEI). Para un riesgo de ser comprensible, debe expresarse con claridad. Dicha declaración debe incluir una descripción de las condiciones actuales que puedan conducir a la pérdida y una descripción de la pérdida. |
| Tolerancia de riesgo | El nivel aceptable de variación de que la administración está dispuesta a permitir un riesgo particular, ya que persigue objetivos |
| Amenazas | Cualquier cosa (por ejemplo, objeto, sustancia, humanos) que es capaz de actuar contra un bien de una manera que puede resultar en harm[11] |
| Caso de amenazas | Cualquier caso de que un elemento de amenazas y actos en contra de un actor activo de una manera que tiene el potencial de resultar en un daño directo |
| Vulnerabilidad | Una debilidad en el diseño, implementación, operacionales o de control interno |
| Caso de la vulnerabilidad | Cualquier caso cuando un material Aumento de los resultados de la vulnerabilidad. Tenga en cuenta que este aumento en la vulnerabilidad de los resultados pueden cambiar en las condiciones de control o de cambios en la capacidad de la amenaza/fuerza[11]. |

[10] Being able to consistently and effectively differentiate the different types of events that contribute to risk is a critical element in developing good risk-related metrics and well-informed decisions. Unless these categorical differences are recognised and applied, any resulting metrics lose meaning and, as a result, decisions based on those metrics are far more likely to be flawed.
[11] Jones, J.; 'FAIR Taxonomy', Risk Management Insight, USA, 2008

**Página en blanco intencionadamente**

**LISTA DE FIGURAS**

# Otras publicaciones de ISACA

Muchas de las publicaciones de ISACA contienen cuestionarios detallados de evaluación y programas de trabajo, www.isaca.org / downloads. Para obtener más información, visite www.isaca.org / bookstore o e-mail research@isaca.org.

**Marcos y Modelos**

- COBIT® 4.1, 2007, *www.isaca.org/cobit*—The COBIT framework, in versions 4.0 and higher, includes the:
  - Framework—Explains COBIT organisation of IT governance management and control objectives and good practices by IT domains and processes, and links them to business requirements
  - Process descriptions—Include 34 IT processes covering the IT responsibility areas from beginning to end
  - Control objectives—Provide generic best practice management objectives for IT processes
  - Management guidelines—Offer tools to help assign responsibility and measure performance
  - Maturity models—Provide profiles of IT processes describing possible current and future states
- *Enterprise Value: Governance of IT Investments: The Val IT™ Framework 2.0,* 2008, *www.isaca.org/valit*—Explains how to extract optimal value from IT-enabled investments; is based on the COBIT framework and organised into:
  - Three processes—Value Governance, Portfolio Management and Investment Management
  - IT key management practices—Essential management practices that positively influence the achievement of the desired result or purpose of a particular activity. They support the Val IT processes and play roughly the same role as do COBIT's control objectives.
- *An Introduction to the Business Model for Information Security* (BMIS), 2009, www.isaca.org/bmis—Provides a view of information security programme activities within the context of the larger enterprise, to integrate the disparate security programme components into a holistic system of information protection. The *Business Model for Information Security* is scheduled to be issued early in 2010.
- *ITAF™: A Professional Practices Framework for IT Assurance,* 2008, *www.isaca.org/itaf*—Compliance and good practice setting guidance consisting of:
  - Guidance on the design, conduct and reporting of IT audit and assurance assignments
  - Definiinition of terms and concepts specific to IT assurance
  - Establishing standards that address IT audit and assurance professional roles and responsibilities, knowledge, skills and diligence, conduct and reporting requirements
- *The Risk IT Framework,* 2009, *www.isaca.org/riskit*—Fills the gap between generic risk management frameworks and detailed (primarily security-related) IT risk management frameworks:
  - Three domains—Risk Governance, Risk Evaluation and Risk Response
  - Provides an end-to-end, comprehensive view of all risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top, to operational issues
  - Enables enterprises to understand and manage all significant IT risk types, building upon the existing risk-related components within the current ISACA COBIT and Val IT frameworks

- **Publicaciones relacionadas con COBIT**
- *Aligning COBIT® 4.1, ITIL V3® and ISO/IEC 27002 for Business Benefit,* 2008
- *Building the Business Case for COBIT® and Val IT™: Executive Briefing,* 2009
- *COBIT® and Application Controls,* 2009—Provides guidance primarily for business executives, business management and IT management, as well as for IT developers and implementers, internal and external auditors and other professionals on application controls (expanding on the six application controls discussed in COBIT) and the relationships and dependencies that application controls have with other controls (such as IT general controls).
- *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition,* 2007Provides guidance on the practices to be considered when improving processes and implementing solutions for control objectives. It also provides risk and value statements to help understand and justify the need to implement each control objective. Control practices are strongly recommended for use with *Implementing and Continually Improving IT Governance.* The control practices provide the more detailed guidance at the control objective level on why and what to implement as required by assurance professionals, management, service providers, end users and IT professionals.
- COBIT® Mappings:
  - *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0,* 2007
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT®, 2nd Edition,* 2006
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0,* 2006
  - *COBIT® Mapping: Mapping of ITIL With COBIT® 4.0,* 2007
  - *COBIT® Mapping: Mapping of ITIL V3 With COBIT® 4.1,* 2008
  - *COBIT® Mapping: Mapping of NIST SP 800-53 With COBIT® 4.1,* 2007
  - *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0,* 2006
  - *COBIT® Mapping: Mapping of PRINCE2 With COBIT®. 0,* 2007
  - *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.0,* 2006
  - *COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0,* 2007
  - *COBIT® Mapping: Overview of International IT Guidance, 2nd Edition,* 2006

**Publicaciones relacionadas con COBIT (cont.)**

- COBIT Online®—Although not a publication, this product is also available through the ISACA bookstore. It allows users to customise a version of OBIT for their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys, frequently asked questions, benchmarking and a discussion facility for sharing experiences and questions.
- COBIT® QuickstartTM, 2nd Edition, 2007—Provides a baseline of control for the smaller enterprise and a possible first step for the larger enterprise
- COBIT® Security BaselineTM, 2nd Edition, 2007—Focusses on essential steps for implementing information security within the enterprise. It also provides easy-to-understand guidance for addressing security aspects of IT governance.
- COBIT® User Guide for Service Managers, 2009—Focusses on service managers, providing them a better understanding of the need for IT governance and how to apply good practices in their specific roles and responsibilities. It facilitates easier use and adoption of COBIT and ITIL concepts and approaches, and encourages integration of COBIT with ITIL. It provides easy-to-understand guidance for addressing service manager aspects of IT governance.Implementing and Continually Improving IT Governance, 2009
- IT Assurance Guide: Using COBIT®, 2007—Provides guidance on how to use COBIT to support a variety of assurance tasks, supported by suggested testing steps aligned with the control practices. The guide can support audit teams that need to provide independent assurance that IT governance practices have been implemented effectively.
- IT Control Objectives for Basel II, 2007—Provides easy-to-understand guidance for addressing Basel II aspects of IT governance
- IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition, 2006—Provides guidance on how to assure compliance for the IT environment based on the COBIT control objectives. It also provides easy-to-understand guidance for addressing Sarbanes-Oxley aspects of IT governance.
- ITGI Enables ISO/IEC 38500:2008 Adoption, 2009

**Publiccaciones relacionadas con RISK IT**

The Risk IT Practitioner Guide, 2009—Contains practical and more detailed guidance on how to accomplish some of the activities described in the process model

**Publicaciones relacionadas con VAL IT**

Enterprise Value: Getting Started With Value Management, 2008—Provides an easy-to-follow guide on getting a value management initiative started for business and IT executives and organisational leaders

Enterprise Value: Governance of IT Investments: The Business Case, 2005—Focusses on one key element of the investment management process

Val ITTM Mapping: Mapping of Val ITTM to MSPTM, PRINCE2TM and ITIL V3®, 2009—Focusses on Managing Successful Programmes (MSP), Projects in Controlled Environments (PRINCE2) and IT Infrastructure Library (ITIL) V3, but there are other relevant frameworks, such as Gateway Reviews, the newly released Portfolio, Programme and Project Office Guidance (P3O) and The Standard for Portfolio Management. These and others may be referenced in future publications.

**Guías adicionales de ejecución y mantenimiento**

- An Executive View of IT Governance, 2008
- Board Briefing on IT Governance, 2nd Edition, 2003—Helps executives better understand IT governance concepts, what the issues are and how best to make it happen
- Building the Business Case for COBIT® and Val ITTM: Executive Briefing—Explores and demonstrates the business value of COBIT and Val IT
- Defining Information Security Management Position Requirements: Guidance for Executives and Managers, 2008
- Identifying and Aligning Business Goals and IT Goals: Full Research Report, 2008
- Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, 2006—Presents information security in business terms and contains tools and techniques to help uncover security-related problems.
- Information Security Governance: Guidance for Information Security Managers, 2008
- Information Security Governance—Top Actions for Security Managers, 2005
- IT Governance and Process Maturity, 2008
- IT GOVernanCe DOmaIn PraCtICeS and COmPetencies:
  - Governance of Outsourcing, 2005
  - Information Risks: Whose Business Are They?, 2005
  - IT Alignment: Who Is in Charge?, 2005
  - Measuring and Demonstrating the Value of IT, 2005
  - Optimising Value Creation From IT Investments, 2005
- IT GOVernanCe ROUndtableS:
  - Defining IT Governance, 2008
  - IT Staffing Challenges, 2008
  - Unlocking Value, 2009
  - Value Delivery, 2008
- Managing Information Integrity: Security, Control and Audit Issues, 2004
- Understanding How Business Goals Drive IT Goals, 2008
- Unlocking Value: An Executive Primer on the Critical Role of IT Governance, 2008—Provides executives with an insight into why IT governance is important and how it can add value to the enterprise

**Orientación Profesional Adicional**

- Auditoria/ programas de garantía:
  - *Change Management Audit/Assurance Program,* 2009
  - *Generic Application Audit/Assurance Program,* 2009
  - *Identity Management Audit/Assurance Program,* 2009
  - *IT Continuity Planning Audit/Assurance Program,* 2009
  - *Network Perimeter Security Audit/Assurance Program,* 2009
  - *Outsourced IT Environments Audit/Assurance Program,* 2009
  - *Security Incident Management Audit/Assurance Program,* 2009
  - *Systems Development and Project Management Audit/Assurance Program,* 2009
  - *UNIX/LINUX Operating System Security Audit/Assurance Program,* 2009
  - *z/OS Security Audit/Assurance Program,* 2009
- Cybercrime: Incident Response and Digital Forensics, 2005
- Enterprise Identity Management: Managing Secure and Controllable Access in the Extended Enterprise Environment, 2004
- Information Security Career Progression Survey Results, 2008
- Information Security Harmonisation—Classification of Global Guidance, 2005
- OS/390—z/OS: Security, Control and Audit Features, 2003
- Peer-to-peer Networking Security and Control, 2003
- Risks of Customer Relationship Management: A Security, Control and Audit Approach, 2003
- Security Awareness: Best Practices to Serve Your Enterprise, 2005
- Security Critical Issues, 2005
- Security Provisioning: Managing Access in Extended Enterprises, 2002
- Stepping Through the IS Audit, 2nd Edition, 2004
- Stepping Through the InfoSec Program, 2007
- TeChnICal and RISK Management ReferenCe SerIeS:
  - *Security, Audit and Control Features Oracle® Database, 3rd Edition, 2009*
  - *Security, Audit and Control Features Oracle® E-Business Suite, 2nd Edition, 2006*
  - *Security, Audit and Control Features PeopleSoft®, 2nd Edition, 2006*
  - *Security, Audit and Control Features SAP® ERP, 3rd Edition, 2009*
- Top Business/Technonogy Survey Results, 2008