Galvanize

# Un mejor enfoque para la gestión del riesgo de TI

Definición del riesgo de TI, los factores que lo potencian, los responsables y cómo puede ayudar la auditoría a generar un mejor enfoque para la gestión del riesgo de TI.

# Tabla de contenidos


| | |
|---|---|
| Las dificultades para gestionar el riesgo de TI | 3 |
| Definición de riesgo de TI | 4 |
| Qué factores potencian el riesgo de TI | 6 |
| Quién debe ser responsable de cada parte del riesgo de TI | 8 |
| Cómo puede ayudar la auditoría a enfrentar el riesgo de TI | 10 |
| Monitoreo continuo | 11 |
| Resumen: un mejor enfoque para la gestión del riesgo de TI | 12 |

# Las dificultades para gestionar el riesgo de TI

*La seguridad informática es fundamental para lograr los objetivos de negocios; eso significa que comprender y gestionar el riesgo de TI también es fundamental para lograr los objetivos de negocios.*

Para demasiadas empresas, decirlo es mucho más fácil que hacerlo.

**Esto se debe a que el riesgo de TI evoluciona entre dos frentes:**

1. El constante crecimiento de la cantidad de normas que rigen asuntos como la privacidad o la integridad de los sistemas.
2. El diseño siempre cambiante de los propios sistemas de TI.

La conjunción de estos factores puede confundir a los equipos de seguridad de TI en cuanto a su rol en la gestión del riesgo de TI.

Y sin embargo, *sin* la participación del equipo de seguridad, el control de esos riesgos quedaría librado a la buena suerte. Las normas relacionadas con la seguridad de los datos seguirán proliferando, la cantidad de proveedores que acceden a los datos corporativos seguirá creciendo y la capacidad de la empresa para evitar que el riesgo de TI ocasione fallas quedará cada vez más rezagada con respecto a las amenazas reales.

Lo que se necesita es una comprensión clara de cómo se manifiesta el riesgo de TI en su organización específica y cómo dividir las responsabilidades de evaluación, mitigación y monitoreo del riesgo entre las diversas funciones de negocios que estarán inevitablemente involucradas.

Eso es lo que aborda este libro electrónico. Definiremos qué es el riesgo de TI, cuáles son los factores que potencian el riesgo de TI hoy en día, por qué asignar "responsables" del riesgo de TI es particularmente difícil y cómo pueden cooperar las funciones de TI y auditoría para generar un mejor enfoque de la gestión del riesgo de TI.

# Definición de riesgo de TI

*Gartner Group define el riesgo de TI[1] como "el potencial para un resultado de negocios negativo no planificado que involucre la falla o el mal uso de TI".*

Dicho más claramente:

El riesgo de TI es la posibilidad de que sucedan cosas malas cuando los sistemas de TI de una empresa no funcionan como deberían.

No hay nada inusual en el riesgo de TI en sí mismo. Todas las empresas lo tienen en alguna medida y siempre lo tendrán. El objetivo de la gestión del riesgo de TI es operar dentro de niveles aceptables de riesgos de TI.

El peligro surge cuando una empresa tiene un riesgo de TI excesivo: cuando esos potenciales resultados negativos se convierten en probables resultados negativos porque los sistemas de TI no funcionan como deberían.

Pues bien, los sistemas de TI no funcionan "como deberían" cuando no logran los objetivos de negocios de la empresa y para las empresas de un tamaño apreciable, uno de esos objetivos es operar de acuerdo con los requisitos normativos.

Un camino por el cual una empresa termina con un riesgo de TI excesivo es permitir que los sistemas de TI dejen de cumplir las obligaciones normativas. Y lo que es peor: al observar el panorama empresarial actual, resulta penosamente claro que también se está transformando en la principal causa por la que una empresa termina con un riesgo de TI excesivo.

[1] **Gartner Group** *glossary of IT terms* **(glosario de términos de TI)**

## CONCLUSIONES CLAVES:

- El riesgo de TI es la posibilidad de que se produzca un evento adverso cuando los sistemas de TI de una empresa no funcionan de la forma esperada.
- Cierto nivel de riesgo de TI es inevitable; el peligro es el riesgo excesivo: demasiadas maneras en las que los sistemas de TI pueden dejar de funcionar de la forma esperada y provocar un evento adverso.
- Una forma en la que puede suceder es que los sistemas de TI dejen de cumplir las obligaciones normativas.

# Qué factores potencian el riesgo de TI

## *El riesgo de TI está aumentando aceleradamente por varios motivos.*

En primer lugar está el desplazamiento hacia los servicios tecnológicos prestados en la nube. Esto ha dado lugar a una explosión de proveedores externos con acceso a datos corporativos confidenciales: algunas veces con el consentimiento del Departamento de Seguridad y otras veces sin él. Un estudio de 2018, por ejemplo, estimó que una empresa promedio comparte información confidencial con 583 terceros.[2] Por eso, el equipo de seguridad de TI debe hacerse cargo de una compleja infraestructura de TI, repleta de riesgos de los proveedores.

En segundo lugar está la proliferación de leyes y normas que rigen la forma en la que las empresas protegen los datos confidenciales. Algunas de esas normas son:

+ **Reglamento General de Protección de Datos de la Unión Europea,** vigente desde 2018
+ **Ley de Privacidad del Consumidor de California,** vigente desde enero de 2020
+ **Ley General de Protección de Datos de Brasil,** anunciada para agosto de 2020
+ **DFARS,** un conjunto de normas de ciberseguridad para contratistas de defensa de EE. UU.
+ **NYCRR 500,** requisitos de ciberseguridad del Departamento de Servicios Financieros de Nueva York

Estas normas de última generación tienen un alcance muy amplio, generalmente global, por lo que es probable que cualquier empresa grande esté sujeta a varias de ellas al mismo tiempo. Además, estas normas consideran a las empresas responsables del procesamiento de datos que realizan terceros en nombre de la empresa, lo cual aumenta la importancia de una gestión eficaz del riesgo de proveedores a fin de evitar que una falla de seguridad de uno de esos proveedores genere un daño a la empresa en términos de reputación o de costos por incumplimiento normativo.

El factor potenciador del riesgo de TI más reciente es la COVID-19, que obligó a las empresas de todo el mundo a disponer que sus empleados trabajen desde sus casas. Es probable que esos empleados utilicen sus computadoras portátiles u otros dispositivos propios y procesen los datos en redes wifi domésticas aplicando procedimientos precarios que alguien improvisó durante un fin de semana. ¿En qué medida cumple este tipo de configuración de TI con los protocolos de seguridad esperados? Nadie sabe.

Además, la COVID-19 ha causado una recesión mundial. Por eso, es posible que los equipos de TI se expongan a recortes de presupuesto y de personal, mientras hacen frente a tareas adicionales para evaluar nuevo software, nuevos dispositivos y nuevas configuraciones de red, u otros acontecimientos inesperados.

[2] **Estudio del Ponemon Institute,** *noviembre de 2018, 'Data Risk in the Third-Party Ecosystem' (Riesgo de los datos en el ecosistema de terceros)*

## CONCLUSIONES CLAVES:

- Los equipos de seguridad deben evaluar y gestionar las amenazas de seguridad derivadas de una creciente cantidad de proveedores de tecnología basada en la nube.
- Por su parte, las empresas están cada vez más inmersas en una telaraña global de nuevas normas de seguridad y privacidad de datos.
- Mientras tanto, la COVID-19 echó por tierra las prácticas habituales de evaluación del riesgo de TI y sus controles, e impuso feroces restricciones presupuestarias a muchas empresas.
- La consecuencia es un aumento acelerado del riesgo de TI porque los equipos de seguridad deben administrar más sistemas, respetar más obligaciones de cumplimiento normativo y tienen menos certezas de cómo hacerlo.

# Quién debe ser responsable de cada parte del riesgo de TI

*El reto para la gestión del riesgo de TI radica en que atraviesa muchísimas partes de la empresa.*

Muchas personas estarán preocupadas por algunas partes, pero la mayoría de las empresas tienen dificultades para abordarlo en su totalidad de manera sistemática.

Por ejemplo, un mantra de la gestión de riesgos dice que "las unidades de negocios son responsables de sus propios riesgos"; pero en la práctica, la mayoría de las unidades de negocios de la Primera o Segunda Línea de Defensa no saben cómo identificar y gestionar los riesgos de seguridad. Simplemente, usan cualquier aplicación ingeniosa que encuentran en Internet o se conectan a cualquier red wifi disponible para trabajar en forma remota.

**Analice algunas de las demás funciones de negocios que tienen al menos algún interés en el riesgo de TI:**

+ **La función de cumplimiento:** desea garantizar el cumplimiento de las normas relevantes de privacidad y seguridad, pero no suele tener un conocimiento profundo de la seguridad;
+ **La función de TI:** desea implementar nuevas tecnologías para mejorar el rendimiento y ahorrar costos, pero no sabe mucho de los matices de la seguridad ni del cumplimiento normativo;
+ **La función de seguridad:** sabe de seguridad, pero no está necesariamente familiarizada con los requisitos normativos ni de qué forma se implementan las nuevas tecnologías en otras partes de la empresa;
+ **El equipo de ventas:** posiblemente esté clamando por una manera eficiente de completar las auditorías de seguridad exigidas por los potenciales clientes.

En otras palabras, la gestión del riesgo de TI está compartimentada: lo cual es un riesgo en sí mismo, si consideramos las consecuencias de una falla de la gestión del riesgo. (Costo promedio de una filtración de datos en 2019, según IBM: USD 3,92 millones. Cuando la filtración se produce a través de un tercero, normalmente se suman otros USD 370 000 al costo, o sea USD 4,29 millones.)[3]

La respuesta diplomática es "¡todos son responsables del riesgo!", desde la junta directiva que supervisa todo, hasta los equipos de seguridad que realizan la capacitación y los equipos de cumplimiento que documentan el cumplimiento de las normas. La realidad, obviamente, es más complicada.

[3] **IBM,** *2019 Cost of a Data Breach Report (Informe de costos de las filtraciones de datos en 2019)*

Las organizaciones solo pueden gestionar el riesgo de TI cuando se han definido con claridad los roles y las responsabilidades de cada uno en esta compleja tarea. Las partes que la componen son:

- Desarrollar políticas y herramientas fuertes para evaluar el riesgo de los proveedores
- Identificar los riesgos emergentes, tales como nuevas normas que afectan el negocio
- Identificar las debilidades internas, tales como la carencia de una autenticación de dos factores
- Mitigar los riesgos de TI, tal vez mediante capacitación, nuevas políticas o nuevos controles internos
- Comprobar la actitud general frente a la seguridad
- Documentar la gestión del riesgo de proveedores y la seguridad, ya sea para examen normativo o para calmar a los potenciales clientes

Es mucho trabajo y el Departamento de Seguridad de TI será solo uno de los integrantes de un equipo mayor que intenta hacerlo todo. La clave para gestionar eficazmente todo este riesgo de TI es tener un enfoque coordinado, disciplinado y sostenible para hacerlo.

## CONCLUSIONES CLAVES:

- El riesgo de TI atraviesa muchas funciones de negocios; por eso, muchas tienen algún interés en el riesgo de TI, pero ninguna es su principal responsable.
- Este enfoque compartimentado representa un riesgo significativo en sí mismo, teniendo en cuenta el daño financiero y operativo que genera una falla de la gestión del riesgo de TI.
- Un enfoque de equipo bien desarrollado, con roles y responsabilidades claros y coordinados, es esencial para el éxito.

# Cómo puede ayudar la auditoría a enfrentar el riesgo de TI

*Primero, la función de auditoría puede definir el riesgo de TI dentro de la organización mediante una rigurosa evaluación del riesgo.*

Esa evaluación debe centrarse tanto en los objetivos de negocios (riesgo de que las fallas de TI puedan interrumpir las operaciones o ahuyentar a los clientes) como en los objetivos de cumplimiento (riesgo de que las fallas de TI expongan a la empresa a una ejecución forzosa del cumplimiento normativo).

Más específicamente, la función de auditoría puede desarrollar la evaluación del riesgo a lo largo de estas líneas:

+ Comenzar con los riesgos de cumplimiento, para comprender cuáles son las normas aplicables a la organización en cuanto a seguridad de datos, privacidad de los consumidores e integridad del sistema
+ Realizar un inventario de los datos confidenciales de la empresa, incluida la ubicación del almacenamiento físico de los datos
+ Trabajar con el Departamento de TI para comprender cómo se gestionan los sistemas de TI de la empresa; en especial, los proveedores de software basado en la nube y otros terceros en contacto con los datos confidenciales de la empresa
+ Trabajar con el equipo de seguridad para comprender qué tan bien se realizan los controles de acceso, el cifrado y las evaluaciones del riesgo de proveedores
+ Desarrollar un plan de acciones correctivas para los controles internos débiles

El resultado de ese plan de evaluación y mitigación del riesgo debe ser un mapa de ruta que ayude a la seguridad de TI y otras funciones de negocios a crear capacidades eficaces para gestionar el riesgo de TI. Es decir, la auditoría no liderará directamente este proceso, debe hacerlo un jefe de riesgo o de seguridad de la información. Pero la auditoría puede identificar cómo debe funcionar ese proceso para obtener la máxima eficiencia y eficacia, y esto es una gran ayuda para la siempre sobrecargada función de seguridad de TI.

## CONCLUSIONES CLAVES:

- La auditoría interna puede ser clave para ayudar a otras funciones a desarrollar un enfoque eficaz para la gestión del riesgo de TI.
- Primero, la auditoría debe asociarse con otras funciones para la evaluación del riesgo.
- Luego, la auditoría puede desarrollar un plan de acciones correctivas para los controles internos débiles y un plan a nivel de toda la entidad para mantener controlado el riesgo de TI a largo plazo.

# Monitoreo continuo

*La última parte de la gestión del riesgo de TI es el monitoreo, para que la empresa pueda saber cuándo cambian las circunstancias y que tal vez los controles internos ya no se correspondan con los verdaderos riesgos de TI.*

En particular, la empresa deberá monitorear:

- **El cambio normativo,** para saber cuándo los actuales controles internos de la empresa dejarán de ser capaces de satisfacer las expectativas frente a los requisitos externos (por ejemplo, la nueva legislación de privacidad de un país)
- **El riesgo de proveedores,** para saber cuándo nuevos proveedores comienzan a procesar datos de la empresa y garantizar que la seguridad de esos proveedores se haya evaluado y documentado
- **Uso interno de TI,** en caso de que los empleados comiencen a utilizar las herramientas existentes de una manera nueva que represente un riesgo (su departamento de marketing comienza a usar una herramienta interna para realizar seminarios web o eventos virtuales con clientes)

Es fundamental contar con una importante capacidad de monitoreo de estas tres áreas porque el riesgo de TI nunca acaba. Al contrario, cambia constantemente; por eso, la revaluación, las nuevas pruebas y la mitigación constante forman parte de la gestión del riesgo de TI.

Por este motivo, es vital crear un enfoque eficaz y general para la gestión del riesgo de TI. No es una responsabilidad exclusiva de la seguridad de TI, ni de ninguna otra función de negocios. El riesgo de TI es un problema de toda la empresa, y se necesita un enfoque que involucre a toda la empresa para mantenerlo controlado.

# Resumen: un mejor enfoque para la gestión del riesgo de TI

## El daño por filtraciones de terceros

**Cuantos más terceros accedan a sus datos y a su red corporativa, mayor será el potencial de su empresa para que un tercero filtre datos en alguna parte de la cadena de suministros.**

**3,92**

**millones de USD:**

costo promedio de una filtración de datos

**4,29**

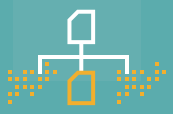
**millones de USD:**

costo promedio de una filtración que involucre a un tercero

**150**

**USD:**

costo promedio por registro perdido



**25 575**

**registros:**

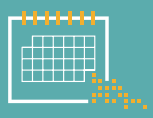
cantidad promedio de registros perdidos durante una filtración de datos

## Cómo puede ayudar la auditoría a enfrentar el riesgo de TI

**¿Busca detalles precisos sobre cómo puede ayudar la función de auditoría a enfrentar el riesgo de TI? Considere estos nueve pasos:**

+ Identificar y evaluar los riesgos de TI
+ Identificar los controles
+ Relacionar los controles con una biblioteca maestra
+ Planificar, definir el alcance y realizar pruebas de estrés de los microrriesgos
+ Señalar las excepciones, revisar y corregir
+ Mejora continua
+ Evaluar la eficacia de los controles
+ Capturar, seguir y reportar las deficiencias
+ Monitorear y automatizar las pruebas de los controles

*Fuente: 'Nine Steps to IT Audit Readiness' (Nueve pasos hacia la preparación de la auditoría de TI) de John Verver*



**279**

**días:**

cantidad promedio de días para contener la filtración

**59**

**por ciento:**

cantidad de empresas que dicen haber sufrido una filtración de datos por terceros

**16**

**por ciento:**

cantidad de empresas que confían en su programa de gestión de riesgos de terceros

*Fuentes: Opus/Ponemon Institute* ***Report on Data in Third-Party Ecosystem*** *(Informe sobre datos en el ecosistema de terceros), 2018; IBM 2019 Cost of a Data Breach Report (Informe de costos de las filtraciones de datos en 2019)*

## Requisitos críticos para las evaluaciones del riesgo de TI

Las evaluaciones del riesgo de TI son difíciles de realizar aún en los mejores momentos y, gracias a la COVID-19 y la recesión económica, los momentos actuales no son los mejores. Los presupuestos son ajustados y los procedimientos estándar de auditoría están patas arriba; por eso, la tecnología será crucial para hacer las evaluaciones del riesgo de TI. Estas son algunas de las capacidades que su organización va a necesitar.

+ **Herramientas de colaboración y comunicación:** para conectarse con varias personas de toda la empresa, en diferentes ubicaciones, husos horarios o países. Esas herramientas deben proporcionar un registro claro de la conversación que cualquiera pueda seguir, porque en las fases de evaluación del riesgo y mitigación participan diferentes personas.
+ **Marcos de gestión de riesgos:** para ayudar al equipo de auditoría a realizar un análisis de faltantes más rápido y preciso entre los requisitos de cumplimiento y las operaciones actuales.
+ **Estudios analíticos:** para ayudar al análisis de las causas principales**,** análisis predictivo de riesgos emergentes y otros similares.
+ **Un repositorio único de datos:** en el que los auditores puedan almacenar evaluaciones de riesgos, resultados de pruebas, documentación y otra información relevante.
+ **Herramientas de gestión de asuntos:** para asignar pasos de mitigación a personas específicas, con recordatorios automáticos para que los responsables de las tareas completen su trabajo a tiempo y con capacidad de elevación para notificar a los altos ejecutivos cuando algo no se esté cumpliendo.
+ **Versatilidad de generación de reportes:** porque muchos grupos**,** desde los jefes de unidades de negocios hasta los altos ejecutivos y la junta directiva, necesitan diferentes tipos de reportes sobre la gestión del riesgo de TI.

Galvanize

## ACERCA DEL AUTOR

**Matt Kelly**

Director ejecutivo de Radical Compliance

Matt Kelly es un analista y consultor independiente del sector del cumplimiento que estudia y escribe sobre temas de cumplimiento corporativo, gobernanza y gestión de riesgos.

Tiene un blog, RadicalCompliance.com, en el que comparte sus ideas sobre asuntos de negocios y da charlas con frecuencia sobre temas de cumplimiento, gobernanza y riesgo.

En 2018, ganó un premio Reader's Choice de JD Supra como uno de los diez mejores autores sobre cumplimiento corporativo. Antes de iniciar Radical Compliance, Matt fue editor de Compliance Week, entre 2006 y 2015.

## ACERCA DE GALVANIZE

Galvanize ofrece soluciones de software como prestación de servicios (SaaS) de gobernanza empresarial que ayuda tanto a gobiernos como a las empresas más grandes del mundo a cuantificar los riesgos, erradicar los fraudes y optimizar el desempeño.

wegalvanize.com

Nuestra familia integrada de productos, incluyendo nuestra solución basada en la nube para gobernanza, gestión de riesgo y cumplimiento (GRC) y los productos insignia para análisis de datos, se utilizan en todos los niveles de la empresa para ayudar a maximizar las oportunidades de crecimiento mediante la identificación y mitigación de los riesgos, la protección de los beneficios y la aceleración del desempeño.

*©2020 El software de Galvanize, Galvanize, el logotipo de Galvanize, HighBond y el logotipo de HighBond son marcas comerciales o marcas registradas de ACL Services Ltd. dba Galvanize. Todas las demás marcas son propiedad de sus respectivos dueños.*