

Guía para los Directores de TI (CIOs) en la gestión de riesgos de TI: aprovechar el extraordinario potencial para el valor del negocio y el crecimiento financiero



Contenido	
2	<i>Introducción</i>
3	<i>Una extraordinaria oportunidad en la gestión de riesgos de TI</i>
4	<i>Cómo adoptar una visión holística de los riesgos</i>
5	<i>Nueva versión de gestión de riesgos de TI</i>
10	<i>La mayoría de los CIOs pueden mejorar el rendimiento en riesgos/rentabilidad</i>
15	<i>Conclusión</i>

Introducción

Los riesgos forman una parte inherente a la hora de hacer negocios dentro del actual mercado global en el que los cambios y la incertidumbre están a la orden del día, aumentando los riesgos de forma exponencial. Las adquisiciones corporativas, las alianzas de colaboración, la integración global y la aceleración de los avances tecnológicos crean riesgos, y las empresas más importantes de hoy en día han aprendido la forma de absorber y mitigar ese riesgo con relativa facilidad. Estas empresas no solo están superando los cambios, en algunos casos están beneficiándose de ellos, incluso provocándolos para revelar nuevas oportunidades. Esta flexibilidad es la clave de un crecimiento y una rentabilidad a largo plazo.

Con prácticamente cualquier aspecto en los negocios de hoy en día vinculado a la tecnología de la información (TI), cada vez más la flexibilidad depende de la capacidad de la empresa para gestionar de forma efectiva los riesgos que puedan encontrarse en sus procesos e infraestructura física de TI. No sorprende que para los CIOs de mayor rango, la gestión de riesgos no sea simplemente un tema dominante. Se ha convertido en una vocación, al igual que para sus colegas de las líneas de negocio. Sin embargo, el alcance de los esfuerzos en gestión de riesgos de muchos CIOs a menudo está limitado para obtener una rentabilidad real para el negocio. La realidad es que la mayoría de los ejecutivos de TI continúan prefiriendo evitar los riesgos en lugar de su gestión. Y cuando adoptan un enfoque demasiado estricto sobre los riesgos de la TI pasando por alto los riesgos para el negocio y los posibles beneficios, limitan sus oportunidades de impulsar la ventaja económica y operativa en sus empresas.

Una buena gestión de riesgos en el entorno empresarial actual altamente interconectado y orientado a la dependencia requiere que los líderes de TI sean capaces de ver y comprender la inversión empresarial y la parte positiva desde la perspectiva financiera que supone el correr riesgos. Una visión holística y más amplia de los riesgos les permitirá reconocer el impacto que pueden tener los procesos de TI y la infraestructura en las actividades comerciales. Asimismo, estarán mejor equipados para potenciar la capacidad de TI a la hora de reducir los riesgos para la empresa y aprovechar las oportunidades de beneficios.

Características principales

El alcance de los esfuerzos en gestión de riesgos de muchos líderes de TI a menudo se ve limitado para producir algún valor real para el negocio.

En un entorno de cambios constantes y de incertidumbre, se vuelve esencial poder asumir riesgos y mitigarlos para un crecimiento óptimo del negocio.

Una estructura de gobernanza que contemple los riesgos facilita esta amplia perspectiva comercial al proporcionar a los responsables de la toma de decisiones de toda la empresa una imagen global más completa de los riesgos y los posibles beneficios. Se obtiene una visión clara para tomar una decisión que aumente al máximo los potenciales beneficios mientras se adopta un nivel aceptable de riesgos. De esta forma, los directores de TI son capaces de implantar un análisis y una automatización efectivos para abordar los riesgos actuales a la vez que protegen los intereses emergentes de la empresa. En resumen, ayudan a conseguir un mejor equilibrio entre riesgo y beneficio.

Los CIOs que son capaces de comunicar la importancia comercial de la gestión de riesgos para TI y la infraestructura física relacionada, pueden transformar la forma en que los líderes de IT (y toda la empresa) se enfrenta a los riesgos. Y aún más importante, pueden convertir la gestión tradicional de los riesgos de IT en una convincente oportunidad de generar valor a la empresa.

Una extraordinaria oportunidad en la gestión de riesgos de TI

Las empresas que lanzan al mercado nuevos productos o que invierten en nuevas ideas generalmente se exponen a un riesgo considerable, pero si tienen éxito, como en el caso de muchas empresas farmacéuticas y mercados financieros, la rentabilidad puede ser enorme. Las empresas innovadoras asumen que el riesgo es una parte fundamental para el crecimiento de la empresa. Y en lugar de eliminarlo, estas empresas aprenden a prosperar en un entorno en el que los resultados no son seguros, llevando a cabo los pasos necesarios para mitigar las potenciales pérdidas.

Los CIOs como gestores de riesgos

Los esfuerzos de la gestión de riesgos de TI e infraestructura raramente se orientan con el propósito de obtener una ventaja para la empresa. Hay diversas razones, pero la mayoría de ellas está relacionada con la forma más fácil de reconocer y abordar los riesgos por parte de los líderes de TI. Un enfoque en la gestión de riesgos de TI aislado y centrado en los activos los excluye a la hora de buscar de principio a fin en las actividades y beneficios comerciales. En lugar de observar el cumplimiento de la normativa como un medio de evitar auténticas amenazas en la operación comercial, lo que ven es una lista de comprobación de las actividades de TI que deben completarse. De esta forma implantan mejoras de TI como son la virtualización y los servicios compartidos para resolver las cuestiones técnicas, pero sin tener en cuenta su impacto comercial.

¿Quién se encuentra en la línea de gestión del riesgo?

A pesar de la aversión cultural de asumir riesgos por parte del centro de datos, los directores de TI cada vez más deben asumir la responsabilidad de la gestión del riesgo en toda la empresa. En la encuesta global IBM de 2008 sobre los directores financieros (CFO),¹ el 25 % de éstos y otros representantes financieros importantes identificaban a los directores de TI (CIO) como los gestores del riesgo, por detrás de los directores financieros y directores generales. No obstante, el estudio indicaba que son menos los CFO y CEO que tendrán el rol de gestores del riesgo dentro de tres años. Los directores financieros estiman que serán más los directores de TI a quienes se les asigne esa responsabilidad.

Generalmente los CIOs se centran en la estabilidad, disponibilidad, protección y planes de recuperación como un resultado final en la gestión de riesgos de TI. Y aunque éstas son buenas medidas para el éxito de la gestión de riesgos, es posible que se pase por alto el papel que juegan en los procesos comerciales completos de la empresa. Los responsables de TI a menudo no perciben en qué medida estos objetivos protegen la operación comercial o de qué modo la seguridad real que proporcionan refuerza la expansión empresarial dentro de nuevos mercados, emprenden asociaciones internacionales y siguen avanzando. Simplemente no acostumbran a considerar la operación de TI como una posibilidad de reducir el riesgo comercial o la creación de nuevos beneficios. Después de todo, históricamente se ha considerado a los centros de proceso de datos como un centro de costes. Como la presión de reducir los costes de TI siguió aumentando, los directores de TI se inclinaron más en utilizar la gestión del riesgo de TI para mantener bajos los costes de TI en lugar de buscar nuevas formas de ayudar a las empresas a reducir los costes y riesgos de explotación.

Esta perspectiva puede dificultar a los directores la tarea de potenciar el centro de datos para obtener beneficios empresariales. Es posible que falten oportunidades de crecimiento válidas, a menudo debido a que se sobreestiman los riesgos asociados. El efecto de inercia que se genera puede constituir un problema real en un entorno global en constante evolución. En el estudio internacional de IBM sobre los directores generales (CEO) de 2008, éstos y otros representantes empresariales de alto rango expresaron su preocupación acerca de permanecer aún en dicho entorno.² Captar de forma exitosa oportunidades globales depende de la voluntad de la gente de impulsar el cambio, no de enfrentarse a él. Deben ser capaces de asumir riesgos.

Cómo adoptar una visión holística de los riesgos

Al estar prácticamente involucrado en todas las actividades comerciales de hoy, no hay duda de que el departamento de TI y los riesgos de infraestructura física relacionados son parte básica de los riesgos a los que se enfrentan muchas de las empresas. Cada vez más los ejecutivos de la dirección están reconociendo la necesidad de mejoras en la gestión del riesgo de TI. El informe del estado global de gobernanza de TI - 2008, del Instituto de Gobernanza de TI, comprobó que el 62% de los CEO y CIO encuestados implementó medidas de mejoras en 2007 en comparación con el 45% en 2005 y 18% en 2003.³

Características principales

Un criterio integral para la gestión del riesgo permite a los responsables de TI obtener un panorama completo de las amenazas y consecuencias potenciales para la empresa.

No obstante, un criterio basado en silos para la gestión del riesgo de TI puede dificultar cualquier mejora real. Tradicionalmente, los riesgos de TI se han catalogado en pequeñas categorías, como disponibilidad, seguridad de acceso y recuperación frente al desastre. El resultado es que no se capturan las interdependencias y el riesgo total para una actividad o proceso comercial determinado puede valorarse erróneamente. Este aspecto no sólo es importante desde una perspectiva de la preservación; también lo es desde una perspectiva de desarrollo. Consideremos una ampliación tecnológica destinada a incrementar la actividad global de un banco. Con una visión aislada del riesgo de TI no es posible que los responsables empresariales comprendan el riesgo real que plantean todas las amenazas potenciales para todos los activos del banco. Además, no hay ninguna visión que conecte los requisitos del banco en cuanto a competitividad y flexibilidad con sus dependencias respectivas en TI y la infraestructura. Lo que se necesita es una visión integral, ‘de todos los peligros’ de riesgo para la empresa.

Una visión integral del riesgo permite a los responsables de TI conectar los puntos con el negocio. Proporciona un punto de ventaja de 360 grados, permitiéndoles ver el amplio conjunto de amenazas potenciales para la empresa (naturales, perjudiciales, accidentales y operativas) y un conjunto igualmente amplio de consecuencias potenciales para los activos y recursos de la compañía (personal, información, hardware e instalaciones). Podrán comprender una serie de riesgos, totalmente conscientes de que aspectos de estabilidad operativos aparentemente pequeños, como capacidad insuficiente, pueden convertirse en pérdidas inconmensurables si no se resuelven. Al conocer los sistemas de los que depende cada actividad comercial, los responsables de TI están en mejores condiciones de priorizar los tiempos de recuperación e identificar cómo y cuándo deben implementarse las mejoras de TI. Conociendo los beneficios empresariales de las iniciativas deseadas de disminución de riesgos de TI, están en mejores condiciones de presentar argumentos a los ejecutivos senior.

Nueva versión de gestión de riesgos de TI

Es evidente que los directores de TI deberían adoptar un criterio más amplio orientado a la empresa para la gestión de los riesgos de TI. Después de todo, es un elemento fundamental en la alineación estratégica de TI con la empresa, permitiendo a los directores de TI operar en el mundo del riesgo/rentabilidad en el que vive la serie de ejecutivos de la dirección.

Un criterio orientado a la empresa considera los desafíos de la gestión del riesgo de TI y de la infraestructura física relacionada desde una perspectiva de los procesos empresariales, identificando los riesgos comerciales mediante el

Un criterio integral para la gestión del riesgo permite a los responsables de TI obtener un panorama completo de las amenazas y consecuencias potenciales para la empresa.

Características principales

El análisis de las dependencias permite a las compañías comprender las causas originales relacionadas con TI de los problemas comerciales potenciales antes de que se produzcan.

mapeo de los procesos comerciales con las fuentes de riesgo relacionadas con TI. Se utiliza el análisis de dependencias para identificar los modos en que el proceso comercial interactúa con elementos específicos de TI y de infraestructura. Al desglosar las actividades de TI en estratos, es posible entender más fácilmente las causas relacionadas con TI.

Un método implica la evaluación del proceso comercial y los riesgos en cuanto a resultados de las actividades de TI. Se identifican los resultados comerciales potenciales y los riesgos asociados en cada proceso TI. Utilizando la gestión del cambio como un proceso de muestra, donde los cambios pueden referirse a cambios tecnológicos (consolidaciones del centro de datos, nuevas configuraciones) así como cambios comerciales (adquisiciones, recorte de gastos), los posibles riesgos en cuanto a resultados podrían ser tiempo de inactividad, pérdida de datos, demoras del sistema y capacidad insuficiente. Estos resultados comerciales son todos indicativos de problemas en los procesos de TI, incluyendo planificación inadecuada, puesta en marcha acelerada y falta de preparación. Pueden estar originados por un diseño deficiente de los procesos, una ejecución deficiente (que podría apuntar a problemas de formación) o una respuesta incorrecta cuando surge un problema. El punto es que los resultados comerciales negativos tienen que ser analizados a partir de sus causas originales, incluyendo causas relacionadas con los procesos.

Beneficios de los métodos basados en procesos de la gestión de riesgos de TI

Los métodos basados en procesos permiten a las empresas ser más conscientes de sus deficiencias y de la necesidad de mejoras en la gestión de riesgos de TI. Según el informe del estado global de gobernanza de TI - 2008, los directores generales y los directores financieros que utilizaban COBIT tenían más propensión a clasificar la gestión del riesgo como 'muy importante' en comparación con el resto de los encuestados (57 % frente al 44 %). Con un mayor énfasis en la gestión del riesgo, estas empresas tienen mayor tendencia a realizar los tipos de mejoras que propicien la rentabilidad comercial.

La importancia de un marco de gobernanza estructurado

Una gestión óptima de los riesgos de TI no es posible sin un marco sólido de gobernanza. La gobernanza proporciona normas, controles y pautas operativas que permiten a los responsables de TI gestionar riesgos y sopesar su rentabilidad comercial. Pero para ofrecer beneficios duraderos, un marco de gobernanza debe tener capacidad de respuesta a las cambiantes condiciones comerciales. Afortunadamente, varios marcos de elevada calidad ya existen y los directores de TI pueden beneficiarse inmediatamente de sus estándares y mejores prácticas para la gestión de TI.

Es posible encontrar una guía excelente en los estándares abiertos, globalmente aceptados, desarrollados por el IT Governance Institute (ITGI). Los objetivos de control para la información y tecnología relacionada (COBIT) proporcionan las mejores prácticas para la gobernanza de tecnología y la infraestructura, incluyendo la gestión del riesgo. Mientras que COBIT se centra en la ejecución, Val IT de ITGI se centra en ayudar a las compañías a orientar sus inversiones empresariales preparadas para TI, incluyendo iniciativas relacionadas con los riesgos, con el fin de obtener la mayor rentabilidad.⁴ Otra pauta de utilidad para la gestión de los riesgos de TI procede de ISO

Características principales

Los directores de TI deben asumir un rol protagónico en la ejecución de procesos estructurados para mejorar la conciencia acerca de los riesgos de TI y la capacidad de prepararse, analizar y dar respuestas frente a los riesgos

(International Standards Organisation) y de la ITIL (Infrastructure Library) del Ministerio de Comercio del Reino Unido, entre otros. El modelo de referencias de procesos de IBM para TI (PRM-IT), el modelo comercial de componentes de TI (CBM-BoIT) y Resilient Enterprise Blueprint vinculan estas mejores prácticas y proporcionan una hoja de ruta para la implementación.

Además de aumentar la flexibilidad, los estándares y las mejores prácticas permiten a las compañías una mejor gestión de los riesgos financieros de los ingresos. Pueden ayudar a las compañías a evitar las penalizaciones contractuales, industriales y de la normativa, y pueden mejorar su capacidad de obtener contratos comerciales y mantener los existentes. Las empresas necesitan saber que podrán mantener las operaciones frente a una variedad de amenazas; sus clientes quieren garantizar que su información y otros activos estarán protegidos. Los marcos de gobernanza ayudan a cumplir con estos objetivos.

Mientras que los estándares y prácticas respaldados por cada marco pueden variar en terminología, sus recomendaciones de procesos para la gestión de TI generalmente son las mismas:

- **Definir el alcance del análisis de los riesgos.** *Identificar las actividades comerciales, iniciativas y elementos de infraestructura y tecnologías de soporte que se incluirán en el esfuerzo de gestión de los riesgos de TI*
- **Identificar y definir riesgos.** *Mapear cada actividad comercial con las amenazas potenciales y los recursos que podrían correr riesgos*
- **Valorar la probabilidad de ocurrencia de riesgos y el nivel de impacto** *Calcular la probabilidad y gravedad de una infracción real en lo que atañe al alcance de las actividades comerciales, obteniendo una visión global del riesgo*
- **Evaluar controles** *Valorar la calidad de controles existentes utilizados para evitar, detectar y mitigar riesgos, teniendo en cuenta el coste versus rentabilidad proporcionada*
- **Valorar el riesgo y determinar los tratamientos y respuestas.** *Revisar los riesgos relativos a la tolerancia de riesgos, luego priorizar las actividades de reducción de riesgo y seleccionar las inversiones basadas en el análisis de costes/beneficios*
- **Implementar acciones de reducción de riesgos** *Desarrollar, probar e implementar planes de tratamiento de riesgos*
- **Proporcionar supervisión e información continuas** *Recabar continuamente datos acerca de amenazas, impactos y eficacia de los procesos actuales para riesgos y ajustar los planes de acción y procesos contra riesgos*

Características principales

Procesos estructurados como éstos mejoran la conciencia proactiva de los riesgos de una compañía y la capacidad de prepararse, analizar y tener respuestas frente a los riesgos. No obstante, la complejidad organizativa puede dificultar la implementación de dichos procesos. Con la gestión del riesgo como parte cada vez más integral del trabajo de los directores de TI y un mayor número de riesgos que entran dentro de la esfera de control de TI, los directores de TI deberían asumir un rol protagónico en la ejecución de estos procesos mediante:

- *La asignación de fondos y recursos adecuados para iniciativas de análisis de riesgos*
- *Suministro de pautas y fomento del diálogo entre interlocutores y garantía de alineación continua con los objetivos comerciales y cumplimiento con normas de gobernanza*
- *Esforzarse por una mejora continua de los procesos*
- *Ayuda a incorporar una mayor conciencia de los riesgos dentro de la gobernanza comercial general de la compañía*
- *Establecimiento de las políticas de gestión de los riesgos para guiar la ejecución de las actividades.*

La importancia de los empleados, organización y automatización

Se entiende que los programas de gestión de los riesgos de TI que permiten que las amenazas comerciales potenciales sean más visibles, sencillas y menos costosas de tratar tengan mayor probabilidad de obtener la máxima aprobación por parte de los altos directivos. Los directores de TI cuentan con la gran oportunidad de producir estos resultados superando los obstáculos relacionados con el personal, la organización y la automatización:

Los programas óptimos de gestión de riesgos de TI dependen de una cultura de conciencia de los riesgos, de los ejecutivos que están efectuando importantes inversiones y de los procesos automatizados para facilitar el análisis y resolución.

- **Empleados:** *Para ser verdaderamente eficaz, la gestión del riesgo debe ser más que un programa: debe estar profundamente incorporado en el "inconciente corporativo" de los empleados. Las compañías tienen que desarrollar una cultura de conciencia acerca de los riesgos acorde con la amplia gama de amenazas potenciales a las que se enfrentan las empresas así como la estrategia de respuesta a los riesgos para mitigarlos. En lugar de centrarse en la recuperación después de los hechos, los programas de formación frente a los riesgos deben centrarse en la preparación de los empleados para detectar, identificar y responder frente a los riesgos. Todos los empleados deben sentirse capaces de preservar y crear valor para la empresa.*

Características principales

- **Organización:** *Si bien el soporte ejecutivo para la gestión de riesgos de TI es un hecho, su eficacia no lo es. Los procesos de gestión de riesgos, como los suministrados por COBIT, deben estar combinados con directivas de continuidad comercial y gobernanza en la conciencia total sobre los riesgos. La gestión del riesgo debe estar estratégicamente integrada en la estructura del negocio para operar como puente entre los silos de riesgos y las dependencias de interconexión empresarial y fallos que podrían comprometer la actividad empresarial.*
- **Automatización:** *La automatización puede facilitar la gestión de riesgos de TI de dos modos importantes. En primer lugar, puede mitigar la complejidad relacionada con el análisis vital de los riesgos y la generación de informes. Cuanto más grande es la empresa y mayores son los cambios comerciales y tecnológicos introducidos en ella, más complicados pueden resultar estos procesos. En segundo lugar, la automatización simplifica la evaluación y reducción de los riesgos reales para las operaciones reales. Las aplicaciones de gestión de las actividades comerciales y servicios, la supervisión de los controles y las aplicaciones de seguridad reducen la presión sobre los recursos, realizando diagnósticos de las causas y funciones de localización y respuesta. Pueden ayudar a identificar amenazas, proporcionar avisos anticipados y reducir el coste de respuesta a los riesgos y mejorar la coherencia de los procesos de gestión de riesgos.*

La madurez relacionada con los riesgos de los empleados de una empresa, la organización de los ejecutivos y la automatización deben estar en alineación para obtener la máxima rentabilidad empresarial de las iniciativas de gestión de riesgos.

Por lo general, las mejoras son necesarias en una o más de estas áreas; no obstante, las tres deben estar en continuo equilibrio para permitir una eficaz gestión de riesgos de TI (Figura 1). La conciencia sobre los riesgos en toda la compañía, por ejemplo, puede aumentar a través de una formación corporativa, pero no proporciona necesariamente a los empleados los procesos para emprender una acción productiva. De forma similar, los empleados que han recibido formación en procesos de respuesta a los riesgos no podrán resolver realmente los problemas sin suficiente automatización. Cuando los

Características principales

niveles de madurez de los tres elementos están fuera de alineación, es probable que las compañías obtengan poca rentabilidad de su inversión en la gestión de los riesgos. Para obtener mejores resultados, las compañías deben realizar continuas mejoras en las tres áreas.

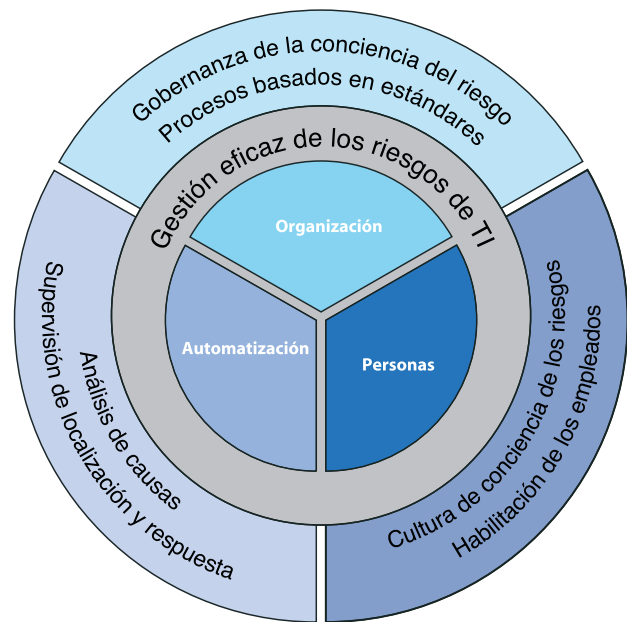


Figura 1. La gestión eficaz de los riesgos de TI depende de las inversiones equilibradas en empleados, organización y automatización.

La mayoría de los CIOs pueden mejorar el rendimiento en riesgos/rentabilidad

En la actualidad, los directores de TI tienen que reconocer que la gestión de TI consiste en obtener la mayor rentabilidad con el mínimo riesgo.

Gracias a la función cada vez más estratégica de los directores de TI en la alta dirección, las expectativas para la gestión de riesgos de TI son mayores que nunca. Los directores de TI comprenden el coste real de los riesgos de TI y eso significa conocer a fondo el impacto que sus decisiones tienen en los ingresos, fidelización de clientes y ventaja competitiva. En un mundo impulsado por la rentabilidad, la gestión de TI debe consistir en obtener la máxima rentabilidad con el menor riesgo (Figura 2).

Características principales

El presupuesto para riesgos permite a los directores de TI optimizar la rentabilidad comercial destinando su capital de riesgo de la manera más eficaz posible.

Adopción de un presupuesto para riesgos

El presupuesto para riesgos proporciona un marco para determinar los riesgos que merece la pena correr. Permite a los directores de TI potenciar los mismos principios que propician los responsables financieros, asignando suficientes recursos financieros para responder frente a los riesgos de TI ‘conocidos’, como disponibilidad, y destinar un mayor presupuesto para los riesgos comerciales realmente desconocidos. Por ejemplo, tomar decisiones para crear un nuevo portal para mantener la fidelización de los clientes o proporcionar mayor capacidad para cubrir los volúmenes de transacciones anticipadas de un producto recientemente lanzado. Los pasos emprendidos para reducir los riesgos de TI relacionados con estas iniciativas se comprenden mejor que el índice de aceptación real de los clientes de un nuevo producto o la eficacia de un nuevo canal de distribución. Los presupuestos para riesgos permiten a los directores de TI trabajar con responsables comerciales para tomar decisiones de asignación de recursos que aumentarán la rentabilidad. Al destinar prudentemente recursos para reducir los riesgos de TI, los directores de TI permiten que los responsables comerciales destinen su presupuesto en otro tipo de riesgo empresarial más complejo de gestionar y relacionado con una nueva iniciativa.

Estimular el debate sobre los riesgos

Los directores no quieren hablar sobre riesgos. Es más fácil y menos perjudicial creer que cada proyecto marchará de acuerdo con un plan y que nunca se producirán fallos. En esta atmósfera de evasión de riesgos, los empleados son justificadamente reacios a informar acerca de los problemas que podrían tener un impacto importante sobre un proyecto. Con frecuencia, esperan demasiado tiempo, resolviendo riesgos después de que una solución de TI está en producción, y convirtiéndose en héroes inconscientes en el proceso. Las compañías con este tipo de cultura se ven obligadas a reaccionar frente a los problemas cuando éstos se presentan, a menudo en modo de crisis.

Los directivos de TI deben acercarse a sus colegas para quienes el riesgo es prioritario y mostrar de qué modo TI puede resolverlo proactivamente y propiciar una mayor rentabilidad para el negocio.

La mayoría de los directores de TI cuentan con suficiente experiencia en los proyectos como para saber que los ‘proyectos sin riesgo’ simplemente no existen. Saben muy bien que anticipar lo que puede ser erróneo es mejor que esperar a reaccionar frente a ello. Acudiendo a los colegas para quienes el riesgo es una de sus máximas prioridades -directores financieros, responsables de riesgos y responsables de la continuidad comercial- e iniciando un diálogo, los directores de TI pueden adquirir una mayor conciencia del riesgo y fomentar una cultura que promueva su rápida notificación. Al trabajar con líneas comerciales e incluso socios externos (inversores, proveedores, departamentos de clasificación, reguladores), los directores de TI pueden

Características principales

La gobernanza de la conciencia del riesgo integra los equipos de riesgos de la empresa convirtiendo el riesgo y la flexibilidad en trabajo de todos.

Los directores de TI pueden ayudar a los responsables empresariales a considerar los méritos de un panorama de riesgos consolidado y operar como puente entre los silos de riesgos y los programas.

explicar de qué modo es posible trabajar conjuntamente para reducir el riesgo de TI y, lo que es más importante, identificar de qué modo TI puede resolver proactivamente los riesgos y propiciar una mayor rentabilidad para la empresa.

Crear un proceso para la gobernanza de la conciencia del riesgo

La gestión continua y proactiva de riesgos se lleva mejor a cabo mediante la gobernanza de la conciencia de riesgos. Si bien la gobernanza puede existir de muchas maneras, la gobernanza de la conciencia del riesgo proporciona la visión más integral del riesgos, integrando los equipos de riesgos de la empresa y convirtiendo el riesgo y la flexibilidad en trabajo de todos. Los empleados comprenden las dependencias interinstitucionales que conducen a riesgos y están mejor equipados para tomar las decisiones diarias que tendrán un impacto positivo en la posición de riesgo de la compañía. Los responsables de las líneas comerciales pueden ver más allá de sus propias preocupaciones empresariales y pueden priorizar las inversiones e impulsar el mejor curso de acción para la empresa. COBIT, Val IT y otros marcos de gobernanza guían y supervisan estas decisiones, permitiendo que los empleados analicen los riesgos en el contexto de su rentabilidad potencial.

La gobernanza de la conciencia del riesgo permite que los responsables comerciales consideren de forma más sencilla la gestión de riesgos de TI básicamente como un medio de aumentar la flexibilidad o de evitar las amenazas a la infraestructura tecnológica y física y luego como un medio de ayudar a la empresa a lograr sus objetivos de desarrollo. Ciertamente los directores de TI tienen un gran interés en comunicar esta visión de TI y de la gestión de riesgos de infraestructura física relacionada. Hay que empezar por eliminar los distintos silos de riesgo que existen dentro de TI y proporcionar una perspectiva unificada que identifique las interdependencias y la gama de amenazas potenciales e impactos en los activos comerciales, tecnológicos y de infraestructura.

A continuación, los directores de TI tienen que extender la lógica de unificación del riesgo al resto de la empresa, permitiendo que los responsables de las líneas de negocio comprendan con mayor facilidad la serie de riesgos a los que se enfrentan los procesos comerciales. Gran parte de ellos simplemente no son conscientes de los riesgos a los que se enfrentan desde las áreas comerciales o los riesgos que ellos generan para esas áreas. Considerar la totalidad de los aspectos es esencial porque revela exposiciones clave, pérdidas reales y tendencias. También simplifica la gestión de los riesgos porque elimina los tratamientos de los riesgos en silos separados.

Características principales

Los directores de TI tienen el conocimiento de las aplicaciones y la información para simplificar el análisis de los riesgos, la supervisión y la respuesta.

Las infraestructuras y aplicaciones complejas pueden introducir riesgos añadidos sin tener que proporcionar beneficios comerciales anticipados.

Para la cúpula directiva, que debe responder a los socios y miembros del consejo de administración, no puede exagerarse la importancia de una imagen de riesgo consolidada y los directores de TI pueden contribuir a proporcionar esta imagen. A medida que los directores financieros evalúen los méritos de los nuevos proyectos e inversiones, los directores de TI pueden prestar su ayuda indicando los riesgos en los cálculos de rentabilidad y riesgo de los directores financieros. Los directores de TI también pueden ilustrar de qué modo menos riesgos de TI se convierten en mayor estabilidad operativa y finalmente en mayor estabilidad financiera.

Las aplicaciones adecuadas pueden simplificar el análisis y supervisión de los riesgos, y los directores de TI cuentan con la experiencia para ponerlos en marcha. Las aplicaciones de análisis de dependencias pueden contribuir a identificar puntos potenciales únicos de fallo y posible contención de recursos compartidos. Pueden ayudar a los responsables empresariales a comprender las causas potenciales de los riesgos comerciales, reconocer los modelos de riesgo y luego beneficiarse del aviso anticipado que proporcionan. Si bien las dependencias de una actividad comercial, proceso o aplicación a menudo no son evidentes para los propietarios de la empresa, la perspectiva de los directores de TI les permite ver las dependencias en toda la empresa. Los directores de TI pueden utilizar técnicas predictivas para prever riesgos, no sólo para reaccionar frente a ellos. Por otra parte, su conocimiento de metodologías de mejora de los procesos como Six Sigma también puede contribuir en gran medida a reducir los riesgos y a establecer el terreno común con líneas comerciales que podrían estar utilizando ya estas aplicaciones.

Eliminar la complejidad

Las infraestructuras físicas y grandes de TI nunca son simples, pero muchas se han tornado demasiado complejas. Consideremos una infraestructura típica con múltiples plataformas separadas implementadas para satisfacer preferencias particulares en lugar de requisitos comerciales específicos. No sólo requieren más tiempo y recursos para mantener, introducen riesgo sin tener que añadir ningún beneficio comercial claro. Las aplicaciones complejas pueden tener el mismo efecto, incrementando la carga sobre la gestión sin tener que proporcionar rentabilidad anticipada.

Los directores de TI a menudo pagan el precio de la complejidad de TI y los riesgos que se generan. Demás está decir que nadie debería estar más interesado en simplificar la infraestructura. Desde la consolidación y virtualización a la arquitectura orientada a objetos (SOA), los directores de TI interesados en aumentar la rentabilidad deberían emprender los pasos para eliminar la complejidad.

Características principales

Creación de una plataforma de creación de rentabilidad a través de la gestión de riesgos de TI

- ✓ Generar una visión única y flexible de la gestión de riesgos estableciendo un puente entre los silos de gestión de riesgos en TI y la empresa
- ✓ Incrementar la conciencia de la empresa de la serie de amenazas potenciales y la serie de impactos potenciales en activos y recursos
- ✓ Potenciar el análisis de dependencias para exponer las interconexiones y causa de los riesgos
- ✓ Beneficiarse de la guía de gestión de riesgos de TI , estándares abiertos y mejores prácticas en marcos de gobernanza estructurados
- ✓ Mejorar la gestión de riesgos de TI a través de mejoras equilibradas en personal, organización y automatización
- ✓ Establecer un presupuesto de riesgos, asignando capital de riesgo basado en recompensa potencial
- ✓ Conectar con las responsables comerciales y socios externos de forma regular para eliminar barreras culturales y mantener en marcha el tratamiento de las cuestiones de gestión de riesgos
- ✓ Transmitir la importancia de la gobernanza de la conciencia del riesgo
- ✓ Eliminar las complejidades de TI e infraestructura que pueden aumentar el riesgo y limitar la rentabilidad

Figura 2. Pasos para mejorar el equilibrio riesgo/beneficio– una lista de control para los directores de TI.

La gestión proactiva del riesgo no sólo propicia el crecimiento sino también el desarrollo personal de los directores de TI, ampliando relaciones, influencia y credibilidad entre la alta dirección.

Una extraordinaria oportunidad de liderazgo en la gestión de riesgos de TI

Los directores de TI tienen la oportunidad de demostrar un liderazgo empresarial incrementando el impacto riesgo-rentabilidad de TI para los directores financieros y otros responsables de líneas comerciales. En las manos adecuadas, la gestión de riesgos de TI es un semillero virtual para la creación de valor, pero los directores de TI tienen que cambiar la forma de abordar el riesgo o renunciar a las oportunidades de desarrollo que se pudieran presentar. Además de la innovación y crecimiento de desarrollo, la gestión del riesgo proactiva puede también generar un desarrollo personal, ampliando las relaciones de los directores de TI, influencia y credibilidad estratégica con colegas de la alta dirección.

Conclusión

La mayoría de los responsables empresariales comprenden la conexión entre crecimiento y riesgo. Gracias a la función cada vez más estratégica de los directores de TI, se torna necesario trascender la frontera de TI y adoptar una visión más completa del riesgo basada en la actividad comercial que esté centrada en la creación de oportunidades, no sólo en la prevención de pérdidas. La eliminación del criterio de silos de TI para la gestión de riesgos es fundamental para la ampliación de la capacidad de TI para distribuir este tipo de valor comercial, y los directores de TI tienen la responsabilidad de emprender este esfuerzo. Gracias a su conocimiento de las aplicaciones y visibilidad de toda la empresa, pueden ayudar a los directores financieros y responsables empresariales a ver el potencial para la rentabilidad en la gestión de riesgos de TI. Lo que es más, al promocionar e implementar proactivamente un marco de gobernanza conciente del riesgo, los directores de TI pueden contribuir a la creación de capacidades comerciales en su empresa que mitiguen la crisis y propicien la rentabilidad y extraordinario valor comercial.

Para obtener información adicional

Para obtener más información acerca de la gestión de los riesgos de TI y la creación de valor, llame a su representante de IBM o visite:

ibm.com/services/es/cio



IBM España

Santa Hortensia 26-28
28002
Madrid

Para acceder a la página principal de IBM, visite **ibm.com**

IBM, el logotipo de IBM e ibm.com son marcas comerciales de International Business Machines Corporation en Estados Unidos y en otros países.

Las referencias efectuadas en esta publicación a productos, programas o servicios de IBM no implican que IBM tenga intención de comercializarlos en todos los países en los que opera. Las referencias a algún producto, programa o servicio IBM no pretenden dar a entender que sólo pueda utilizarse dicho producto, programa o servicio IBM. En su lugar, puede utilizarse cualquier programa, producto o servicio funcionalmente equivalente.

Los productos de hardware de IBM se fabrican a partir de componentes nuevos o de componentes nuevos y utilizados. En algunos casos, es posible que el producto de hardware no sea nuevo y se haya instalado anteriormente. Independientemente de ello, se aplican los términos de garantía de IBM.

Esta publicación sólo tiene carácter de orientación general.

La información está sujeta a cambios sin previo aviso. Póngase en contacto con su representante comercial o distribuidor de IBM local para conocer la información más reciente acerca de los productos y servicios de IBM.

Este documento contiene direcciones de Internet que no son de IBM. IBM no se hace responsable de la información que se encuentre en esos sitios Web.

IBM no ofrece asesoramiento jurídico, contable o de auditoría, y no asevera ni garantiza que sus productos o servicios cumplan con la legislación. Los clientes son responsables del cumplimiento de las disposiciones legales y normativas vigentes, incluidas las normativas y legislaciones nacionales.

Las fotografías pueden mostrar modelos en fase de diseño.

© Copyright IBM Corporation 2008
Todos los derechos reservados.

¹ IBM, *Balancing Risk and Performance with an Integrated Finance Organisation: The Global CFO Study 2008*, Octubre 2007.

www.ibm.com/gbs/2008cfostudy La encuesta global a directores financieros (CFO) 2008 (Global CFO Study 2008) fue realizada conjuntamente con la Wharton School de la Universidad de Pennsylvania y la Economist Intelligence Unit.

² IBM, *La Empresa del Futuro: The Global CEO Study 2008*, Junio 2008.

www.ibm.com/ibm/ideasfromibm/us/ceo/20080505/index.shtml.

³ IT Governance Institute, *Informe del estado global de gobernanza de TI - 2008*, 2008.

www.itgi.org/AMTemplate.cfm?Section=ITGI_Research_Publications&Template=/ContentManagement/ContentDisplay.cfm&ContentID=39735

TEI informe del estado global de gobernanza de TI - 2008 se basa en una encuesta global de los directores de TI y directores generales realizada por PricewaterhouseCoopers para el IT Governance Institute (www.itgi.org/).

⁴ COBIT y Val IT están disponibles como estándares abiertos a través del IT Governance Institute.

