IBM Institute for Business Value

El papel primoridial de los CIO y directores de TI

Conclusiones del Estudio Global de Riesgos de TI de IBM de 2010

Instituto IBM para el Valor Empresarial

IBM Global Business Services, a través del Instituto IBM para el Valor Empresarial, desarrolla una visión estratégica basada en hechos para los altos ejecutivos entorno a temas críticos tanto del sector público como privado. Este informe ejecutivo está basado en un estudio en profundidad del equipo de investigación de dicho Instituto. Forma parte del compromiso actual de IBM Global Business Services de ofrecer análisis y puntos de vista que ayuden a las empresas a lograr más valor empresarial.

Puede contactar con los autores o enviar un e-mail a *iibv@us.ibm.com* para más información. Hay disponibles más estudios adicionales del Instituto IBM para el Valor Empresarial en *ibm.com/iibv*

Por Linda B. Ban, Richard Cocchiara, Kristin Lovejoy, Rick Telford y Mark Ernest

El aumento de las regulaciones y normativas, el crecimiento de los negocios online 24x7 y la constante amenaza de una incertidumbre económica subraya la importancia de la gestión de riesgos en todas sus formas, ya sean relacionadas con el negocio, los datos o los acontecimientos. El Estudio Global de Riesgos de TI de IBM de 2010 destaca los retos asociados a los riesgos de TI y los pasos que los directores de TI y los CIO están dando para comprender, afrontar y resolver este asunto de la mejor manera posible. De los directores de TI encuestados, la mayoría espera que sus responsabilidades relacionadas con los riesgos aumenten. Sin duda, la gestión de riesgos de TI es un tema de amplio alcance y puede influir directamente en una posición competitiva de la empresa, así como en su reputación con los clientes, socios, reguladores y otras partes interesadas.

Desde una perspectiva empresarial, la infraestructura de TI juega un papel fundamental no sólo para soportar y salvaguardar los activos críticos de la empresa y garantizar un control de gobierno y un cumplimiento adecuados, sino también para dirigir el crecimiento empresarial. En consecuencia, la gestión de riesgos de TI no se contempla como una función estrictamente técnica, sino como una tarea de gestión fundamental que puede proporcionar beneficios empresariales directos a todos los niveles de la empresa.

Para comprender mejor cómo están trabajando las empresas para gestionar y mitigar los riesgos en sus negocios, especialmente como se aplica a nivel de TI, IBM puso en marcha el estudio Global de Riesgos de TI de IBM de 2010, que forma parte de la actual investigación de IBM en el área de riesgos de TI, y es el primero de una serie de estudios de investigación que examinan este tema. El estudio, que se llevó a cabo en mayo y junio de 2010 en colaboración con Economist Intelligence Unit (EIU), pretende entender mejor las áreas en las que se centran los directores de TI en la actualidad, y dónde contemplan los retos y oportunidades a corto plazo. La futura investigación explorará en profundidad estas cuestiones, y examinará las opciones y decisiones a las que se enfrentan los equipos de gestión de riesgos.

"Durante el periodo en que la TI se ha convertido en la base de más operaciones empresariales, la gestión del riesgo de TI no ha evolucionado del mismo modo"

Encuestado, Industria de Turismo y Viajes, Europa Occidental

"Aunque algunos afirman que la tecnología ha madurado y se ha instaurado en las empresas, vemos que la 'revolución' tecnológica solo está en sus inicios. Nuestra lectura de la evidencia sugiere que el valor estratégico de la tecnología en la empresa sigue creciendo".

Brynjolfsson, Erik y Adam Saunders. "Wired for Innovation: How Information Technology is Reshaping the Economy." Instituto de Tecnología de Massachusetts 2010.

Los resultados de este estudio están basados en un amplio sondeo online a 556 directores de TI y otros involucrados en sus cargos de TI en la empresa (incluyendo 131 CIO). Las regiones representadas incluyen a Norteamérica, Europa Occidental, Asia-Pacífico, Oriente Medio y África, Europa del Este y Latinoamérica, y el estudio abarca diferentes industrias, desde TI, servicios financieros, sanidad y farmacéuticas, hasta biotecnología, fabricación y gobierno. Las empresas sondeadas han informado de un baremo de ingresos que va desde 500 millones hasta más de 10.000 millones de dólares estadounidenses.

Los objetivos principales del estudio fueron:

- Sondeo multidisciplinar de empresas para medir de forma precisa el estado actual de la gestión de riesgos de TI.
- Identificar los factores que pueden hacer avanzar (o impedir) las estrategias de gestión de riesgos de una empresa.
- Descubrir hasta qué punto las empresas están implementando nuevas estrategias, programas y políticas de riesgos.
- Comprender cómo los avances en materia de TI, tales como la computación en nube, se alinean con las estrategias generales de riesgos de las empresas.
- Examinar el papel fundamental de los directores de TI, incluyendo a los CIO.

En general, las conclusiones del sondeo fueron uniformes en las diferentes regiones, tamaños de empresas, industrias y funciones. (Todas las regiones representadas en el estudio conocían la importancia de la gestión de riesgos de TI, y están trabajando en hacer mejoras al respecto). En general, los participantes del estudio expresaron su confianza sobre su gestión de riesgos y sus esfuerzos en materia de cumplimiento (ver figura 1).

Sin embargo, aunque más del 50% de los encuestados respondieron que sus presupuestos se habían mantenido o mejorado, el 36% todavía lucha por la obtención de fondos suficientes para dirigir los desafíos relacionados con el riesgo. Y a pesar del reconocimiento de que la gestión de riesgos de TI puede ofrecer auténticos beneficios empresariales, asegurar el apoyo de la alta

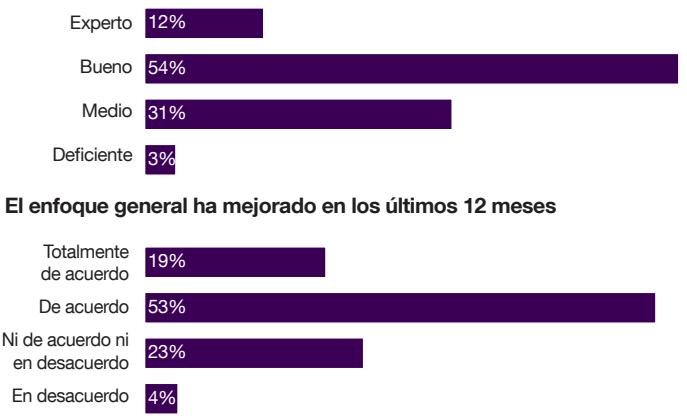

Figura 1: **Las empresas aportan su enfoque para mitigar las elevadas puntuaciones en materia de riesgos de TI**

dirección sigue siendo una preocupación real. Las respuestas de los encuestados parecen indicar una divergencia entre la forma en que la alta dirección contempla el coste de la mejora de la gestión del riesgo de TI y el valor que se puede derivar de ello.

Invertir tiempo en mejora continua

Reconociendo los beneficios potenciales empresariales de una gestión de riesgos de TI efectiva, muchos de los encuestados prevén ampliar sus iniciativas relacionadas con los riesgos en los próximos tres a cinco años. No obstante, también hay algunas discrepancias notables. Sólo la mitad de las empresas encuestadas tienen un departamento formal de riesgos (46%) o una estrategia de continuidad de negocio bien diseñada (54%). Asimismo, la línea del negocio y otros asuntos operativos en materia de riesgos (por ejemplo: estrategias financieras/empresariales) no son áreas prioritarias.

"Tradicionalmente, las empresas de TI efectúan extensas pruebas antes de introducir nuevos servicios empresariales de TI, con el objetivo principal de evitar las interrupciones. Pero los actuales ejecutivos de TI necesitan comprender el verdadero coste para la empresa de tales pruebas. No son solo los costes de TI, son los costes de las oportunidades perdidas debido a la interrupción del servicio en la actividad de la empresa. Cada día dedicado a las pruebas es un día perdido para generar ingresos y beneficios. ¿Cuál es el riesgo si el servicio se desequilibra frente al beneficio de obtener la puesta en marcha y el funcionamiento del servicio?"

Mark Ernest, IBM Distinguished Engineer

Al solicitarles que cualificaran el enfoque general de la empresa para mitigar los riesgos de TI, el 66% de los encuestados lo clasificó de bueno a especializado. Mientras esto representa a la mayoría de las empresas, más del 30% define a su empresa como deficiente en este área. Sin embargo, el 72% de los encuestados afirman que el enfoque del riesgo de su empresa ha mejorado en los últimos 12 meses.

No sorprende que el 47% de los encuestados indicara que la planificación de riesgos de TI es principalmente una función discreta que se lleva a cabo a nivel de silos empresariales. Por lo tanto, conseguir que las áreas de la empresa trabajen juntas es un reto importante. Otro apunte: muchos de los encuestados informaron de que a pesar de estar muy implicados en varias actividades de gestión de riesgos y cumplimiento, desearían participar aún más. (Mientras que cerca de la mitad de los encuestados afirmó que su empresa tiene un departamento de gestión de riesgos, muchos creen que la empresa falla en materia de educación y comunicación a los empleados con respecto a las políticas y asuntos relacionados con la gestión de riesgos de la empresa).

Una nota positiva: en un duro entorno económico, temas como la gestión del riesgo de TI y el cumplimiento han permanecido largamente inmunes a los recortes de presupuestos o a la reducción de costes. Al preguntar sobre los presupuestos de 2010 de sus empresas para la gestión de riesgos, el 14% (80 encuestados) esperaba un aumento significativo de los fondos, y el 39% contemplaba un ligero incremento. El 36% indicó que la financiación para la gestión de riesgos seguiría siendo la misma.

Los encuestados coincidieron en que la inversión en gestión de riesgos de TI puede proporcionar importantes beneficios empresariales, especialmente en las áreas de continuidad de negocio (74%) y salvaguarda de la reputación e imagen de la compañía (32%, ver figura 2). Según los encuestados, la gestión de los riesgos de TI debe contemplarse como algo más que una táctica defensiva; puede incrementar la agilidad de la empresa (19%) y crear oportunidades de crecimiento (12%) al tiempo que se reducen los costes (18%). Sin embargo, la mayoría de los directores de TI (57%) dedican su tiempo a centrarse en los riesgos relacionados con la infraestructura.

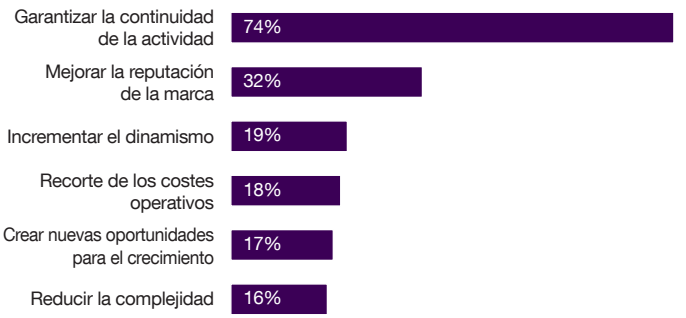

Figura 2: **Beneficios de mejorar la gestión de riesgos de TI**

La máxima prioridad: la seguridad informática

A pesar de que la gestión de riesgos de TI se aplica a los procesos, actividades y sistemas, la seguridad informática (vulnerabilidad a los hackers y acceso/uso no autorizado de los sistemas de la empresa) es la preocupación número uno entre el 78% de los profesionales de TI encuestados. Lo siguiente era el mal funcionamiento del hardware y del sistema, citado por el 63% de los encuestados. El fallo de suministro de potencia y la seguridad física (40%) no se quedaban a la zaga, seguidos por el robo, la calidad del producto, el cumplimiento, los desastres naturales, las solicitudes e-discovery, los fallos en la cadena de suministro y el terrorismo, en ese orden.

Los directores de TI tienen opiniones claras sobre la importancia de la gestión de riesgos, así como de las áreas de enfoque específicas. Sin embargo, hay importantes lagunas en lo que respecta a la confianza que tienen en la capacidad de su organización para abordar y responder al riesgo. Por ejemplo, solo el 22% de los encuestados creen que sus empresas están bien preparadas en términos de seguridad informática. El 23% de los encuestados piensan lo mismo acerca de la preparación de su empresa en material de hardware y fallos del sistema. La protección frente a los fallos de potencia obtiene más respaldo, con un 32% de los encuestados que opinan que sus empresas están bien preparadas en ese área. No obstante, hay una clara divergencia entre el reconocimiento de los encuestados sobre la importancia de dirigir los riesgos generales de TI y la confianza que tienen en la disponibilidad de su empresa para gestionarlos y mitigarlos de forma adecuada.

"La continuidad de la actividad abarca mucho más que la planificación para los desastres naturales o previsibles. Se trata realmente de construir una cultura de consciencia de los riesgos – garantizando que se implementan las herramientas, procesos y metodologías necesarios, y que cada persona de la empresa sea consciente de su propia responsabilidad con respecto a la seguridad e integridad de los datos. Por último, al implementar las herramientas y procesos, es fundamental buscar el equilibrio entre la rapidez de comercialización y el riesgo aceptable".

Jessica Carroll, Directora Gerente Information Technologies,
United States Golf Association

Ejemplo de caso

En la primera mitad de 2010, el equipo de I+D X-Force de IBM documentó 4.396 casos de nuevas vulnerabilidades – un 36% más con respecto al mismo periodo del año pasado. Según el informe, las vulnerabilidades de las aplicaciones de red continúan siendo la mayor amenaza – contabilizándose en más de la mitad de todas las divulgaciones públicas. No obstante, el informe afirma que las empresas están haciendo más esfuerzos que nunca para identificar y descubrir las vulnerabilidades en la seguridad. Esto a su vez está teniendo efectos positivos en la industria al incentivar una colaboración más abierta para identificar y eliminar las vulnerabilidades antes de que los delincuentes cibernéticos puedan explotarlas.[1]

El reto de las comunicaciones

No hay duda de que la gestión de riesgos de TI puede ofrecer auténticas ventajas a nivel empresarial. Sin embargo, a pesar de los diferentes métodos que las empresas pueden emplear para distribuir la información relativa al riesgo, la comunicación emerge como una auténtica barrera. Asegurar el respaldo de la alta dirección sigue siendo un reto, según el 25% de los encuestados. La comunicación a los empleados de las políticas de riesgos y de los procedimientos fue un problema para el 30% de los encuestados.

Muchas empresas adoptan un enfoque pasivo en lugar de uno proactivo a la hora de gestionar y mitigar los riesgos de TI. En muchos casos, la información se envía a la intranet de la empresa, donde los empleados deben dedicar su tiempo a buscarla. Algunas empresas incorporan políticas de gestión del riesgo en los materiales de formación para los nuevos empleados, sin tener en cuenta la necesidad de ponerlos a disposición de todos. (Sólo el 22% de los directores de TI indicaron que las políticas de gestión del riesgo formaban parte de la formación formal de cada empleado). Y lo más sorprendente: menos del 15% han incorporado un plan de gestión del riesgo integrado en la infraestructura física y técnica de su empresa.

"Luchamos para que la dirección y el personal acepten que su comportamiento debe modificarse para mejorar las prácticas en materia de seguridad".

Encuestado, Industria de Fabricación, Europa Occidental

"Cada vez es más difícil garantizar la provisión de fondos destinados a los riesgos de TI, incluso aunque los costes de NO hacer frente a los riesgos hayan sido claramente resaltados a los ejecutivos. A menudo, hay una falta de voluntad general para invertir".

Encuestado, Industria Aeroespacial y Defensa, Norteamérica

Dada la variedad de canales de educación y comunicación para construir la concienciación del riesgo, las empresas harían bien en adoptar un enfoque más detallado y organizado para establecerse en la cima de los temas relativos al riesgo, la comunicación de estos temas a los empleados, y la incorporación de la gestión de riesgos de TI en cada área de su empresa. En respuesta a la pregunta "¿Cómo se organiza su empresa para estar actualizado en la gestión de los riesgos?", la mayoría de los encuestados indicó que las amenazas de la seguridad se gestionaban tanto a nivel de recursos externos como internos (38%), un equipo trans-funcional de ejecutivos (26%), o un departamento específico para la gestión del riesgo (19%).

"Normalmente, los usuarios, la dirección y los socios contemplan el riesgo desde perspectivas diferentes. Tengo que hacérselo ver de una forma sensible".

Encuestado, Industria de Fabricación, Europa Occidental

Evaluación de las tecnologías emergentes

Los encuestados fueron preguntados sobre cómo se posicionaba su empresa para adquirir y desplegar cinco tecnologías emergentes (ver figura 3):

- Herramientas de redes sociales (foros de intranet e Internet, mensajería instantánea, blogs y wikis)
- Plataformas móviles (Windows® Mobile, BlackBerry OS y Google Android OS, por nombrar sólo tres)
- Computación en nube (cloud)
- Virtualización
- Arquitectura orientada al servicio (SOA)

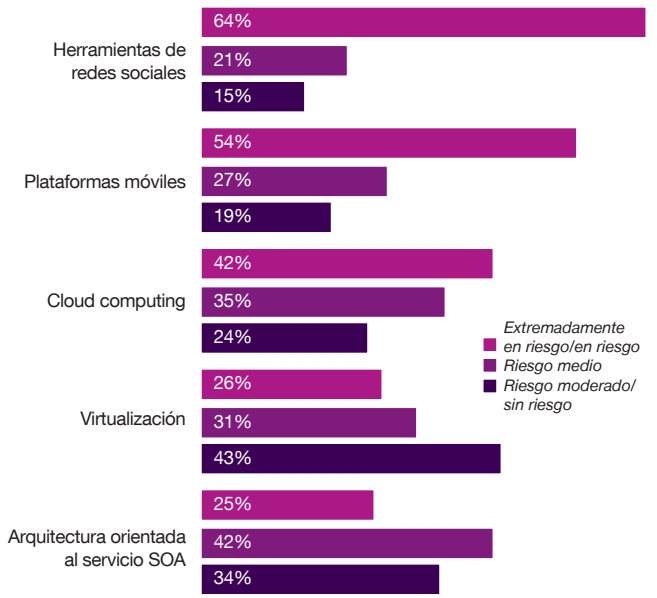

Figura 3: **Las redes sociales, las plataformas móviles y el cloud computing presentan el mayor nivel de preocupación.**

De estas cinco tecnologías, las redes sociales, las plataformas móviles y la computación en nube presentaron los mayores motivos de preocupación. Las herramientas de las redes sociales eran las mayores preocupaciones en términos de riesgo para el 64% de los encuestados, con las plataformas móviles y la computación en nube a la zaga (54% y 43%, respectivamente). La mayoría de los riesgos tenían que ver con la accesibilidad, el uso y el control de los datos, especialmente en las redes sociales y el peligro del acceso no autorizado a información personal y confidencial. (Muchas empresas no tienen establecidos métodos y procesos para integrar las herramientas de redes sociales en su flujo e infraestructura de trabajo).

Al solicitar que citaran dos riesgos elevados que asociaban con la cloud computing, la mayoría de los encuestados apuntó a la protección y privacidad de los datos (ver figura 4). La continuidad de negocio se situaba claramente en el pensamiento de más de la mitad de los encuestados, donde el 44% opinaba que las nubes privadas son más arriesgadas que los servicios de TI tradicionales, y el 77% expresó su preocupación en torno a la privacidad.

"El cloud solo es una oportunidad para resolver un problema si puedes aprovechar las mejores ventajas del cloud. De modo que es algo a tener en cuenta".

Encuestado, Sector Tecnología de la Información, Norteamérica

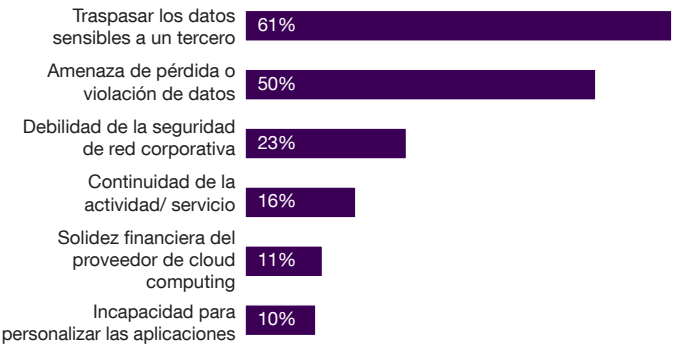

Figura 4: **Riesgos asociados con el cloud computing.**

La gestión de los datos a través de un tercero también la consideraron arriesgada un 61% de los encuestados, mientras que sólo el 23% mostró preocupación por las violaciones de red.

Sólo el 26% de los encuestados afirmó que la virtualización planteaba un riesgo importante para su empresa. Igualmente, la arquitectura orientada al servicio (SOA) era una preocupación sólo para el 25%.

Descansando en la nube

Los directores de TI se ven presionados para reducir los gastos relacionados con la infraestructura, aumentar la eficiencia y mejorar los niveles de servicio a través de la empresa. Muchos buscan en la cloud computing la ayuda para conseguir esos objetivos. La cloud computing representa un gran avance en los modelos informáticos, mucho más que sus predecesores, cliente/servidor y el mainframe computing. El procesamiento se gestiona a través de una red de recursos de TI distribuida y accesible a nivel global, que se dispensa a demanda, como un servicio. El cloud computing ofrece una alternativa dinámica y altamente automatizada para la adquisición y suministro de servicios de TI, lo que permite a los usuarios aprovechar las nubes híbridas, públicas y privadas para los recursos y servicios informáticos sin tener que tratar directamente con tecnologías subyacentes. En la actualidad, las empresas están aprovechando las capacidades de escalabilidad y colaboración masivas que ofrece el cloud computing para resolver los problemas como nunca antes había sido posible. Y están desplegando nuevos servicios rápidamente, sin inversión de capital adicional. Sin embargo, las empresas deben ser prudentes e informarse a la hora de elegir un proveedor, sobre todo teniendo en cuenta las preocupaciones relativas al riesgo.

Implicaciones para los directores de TI

De los directores de TI encuestados, la mayoría esperan que sus responsabilidades, que van desde la ejecución de las políticas y procedimientos y la aportación a las estrategias de mitigación de riesgos, hasta contribuir a establecer y/o supervisar las estrategias de riesgos de TI para la empresa, se incrementen en los próximos tres años (ver figura 5). Más del 65% de los encuestados coincide en que la mitigación del riesgo se está convirtiendo en una parte integral de su trabajo, mientras que el 83% cree que los directores de TI deben involucrarse más en la mitigación del riesgo.

Cuando se considera el crecimiento de la interdependencia de la empresa y la tecnología informática, estas respuestas no sorprenden. De hecho, los directores de TI y CIO encuestados opinan que sus trabajos integrarán el soporte a la estrategia empresarial general, así como a la marca corporativa (por ejemplo, en marketing y servicio al cliente). A medida que las empresas estabilizan o 'endurecen' sus estrategias de gestión de riesgos, procesos y procedimientos, la responsabilidad de la infraestructura puede pasar a un proveedor o a un socio, permitiendo a los directores de TI centrarse más en la seguridad, resiliencia y continuidad del negocio.

También es interesante observar que al cruzar los datos de los 131 CIO que respondieron al sondeo, las respuestas no variaron significativamente de las de los directores de TI encuestados.

Si bien la importancia de la gestión de riesgos de TI y del cumplimiento es fácilmente reconocida por las empresas a través de las industrias, muchas están trabajando para mejorar estos aspectos de su negocio, y algunas están totalmente preparadas para todas las situaciones relacionadas con el riesgo y cumplimiento que pudieran presentarse.

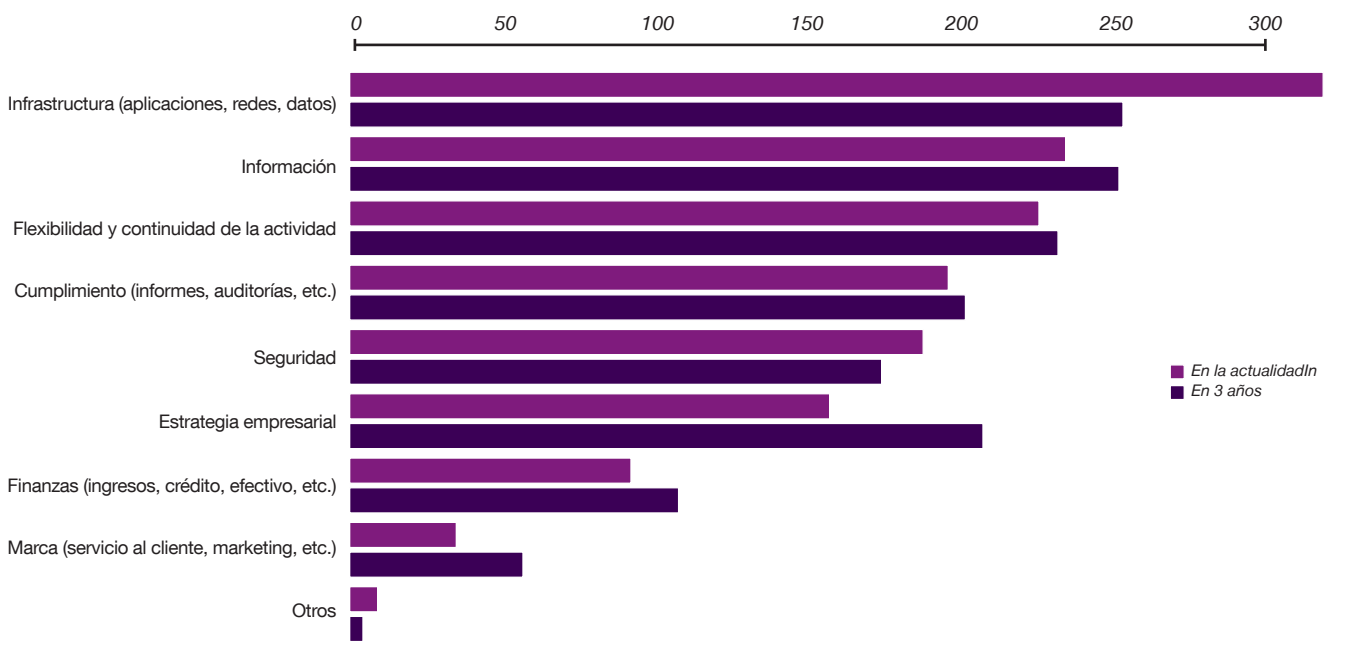

Figura 5: **Los directores de TI esperan que sus áreas de responsabilidad cambien en los próximos tres años.**

Las conclusiones del Estudio Global de Riesgos de TI de IBM 2010 revelaron áreas de enfoque que pueden ayudar a los directores de TI a evaluar su grado de madurez frente al riesgo, identificar lagunas, establecer las prioridades y desarrollar estrategias en diversas áreas:

- Dentro de una empresa, la concienciación del riesgo es responsabilidad de cada uno. Salvo que las políticas y procedimientos relativos al riesgo estén arraigados en la cultura corporativa, muchas iniciativas para la gestión y mitigación del riesgo de TI pueden quedarse cortas, o ser deficientes. Los resultados del estudio confirman que las empresas necesitan trabajar duro y educar, comunicar y respaldar las iniciativas de gestión del riesgo y cumplimiento en toda la empresa.
- Los datos son un problema común en todos los aspectos de la gestión del riesgo de TI, desde la seguridad, la resiliencia y la continuidad de negocio, hasta la disponibilidad, la recuperación tras los desastres, los hackers, el cumplimiento, la gestión de datos y la infraestructura. Con esto en mente, las empresas deben adoptar un enfoque holístico y unificado del riesgo de TI, teniendo en cuenta todos los elementos para apuntar hacia los objetivos generales de conseguir más beneficios y mayor eficiencia.

- Al adoptar tecnologías emergentes, arquitecturas y estrategias, en el desarrollo de nuevas aplicaciones o en la integración de los sistemas existentes, la mitigación del riesgo debe ser un punto de debate primario. Teniendo en cuenta tanto el riesgo positivo (que una empresa asume porque hay una oportunidad ligada al riesgo) como el riesgo negativo (los incidentes potenciales que pueden causar perjuicio a la empresa) puede aportarse más valor empresarial y posiblemente aumentar los ingresos, pero sólo si se incluye una provisión de fondos adecuada para la gestión del riesgo de TI.

  No todas las tecnologías emergentes están creadas del mismo modo, pero algunas, como la virtualización y el cloud computing, pueden ofrecer muchas ventajas en términos de soporte y opciones de mitigación del riesgo. Aunque el cloud comupting requiere cierto nivel de atención a la seguridad de los datos, si se despliega adecuadamente puede reducir los costes y aliviar los riesgos asociados con la resiliencia del negocio. Sin embargo, es vital contar con los procesos adecuados para dirigir los riesgos relacionados con cualquier tecnología nueva.

"A menudo tendemos a considerar un plan de proyecto de forma tan simplista, que creemos que sabemos donde están los riesgos, para enfocar la asignación de recursos sobre esa base".

Encuestado, Industria de Tecnología y TI Oriente Medio y África

Qué hacer a partir de aquí

Realmente, la gestión de riesgos de TI es una tarea polifacética. Si nos adentramos en ella, los directores de TI deben tener en cuenta lo siguiente:

Examinar y evaluar la capacidad frente al riesgo de TI de la empresa

- Instituir un plan empresarial transversal para todas las categorías de riesgos (datos, seguridad, resiliencia y recuperación tras desastres, y nuevas tecnologías).
- Considerar el abanico de desafíos en materia de riesgos y confirmar que hay un plan en marcha para dirigirlos (priorizando y mitigando los riesgos de 'baja' como fallos del sistema y brechas en la seguridad, por ejemplo) y verificar cómo aprovechar el riesgo 'de alta' (menos tiempo para la comercialización y nuevos puntos de contacto con el cliente, por ejemplo).

Buscar gurús entre los directivos senior

- Convertirse en un asesor de confianza y en un recurso valioso para el CIO; articular los beneficios que ellos y otros líderes brindan para dirigir los riesgos de TI.
- "Vender" los beneficios de la mitigación de riesgos, tales como un crecimiento más sólido del negocio, más agilidad y una mejor percepción de la marca.

Determinar cómo aumentar la concienciación del riesgo a todos los niveles, y dentro de la propia cultura organizativa

- Incorporar la concienciación del riesgo en los procesos de TI y en la empresa todos los días. Asegurarse de que existen métodos para la educación de toda la empresa.
- Crear una estrategia para comunicar regularmente la dimensión de la gestión del riesgo, así como los asuntos y temas relativos al cumplimiento, enfatizando en que es algo más que una actividad 'puntual'.

Buscar maneras innovadoras de implementar los procedimientos para la mitigación del riesgo

- Construir procedimientos relacionados con el riesgo en la infraestructura de TI, en lugar de sumarlos a las aplicaciones de forma poco sistemática.
- Examinar los procesos empresariales para los potenciales problemas de riesgos, y establecer un plan de gobierno de riesgos de TI específico que pueda ser ejecutado en toda la empresa.

Implementar la suficiente protección para ayudar a prevenir el acceso no autorizado a los datos y sistemas de la empresa

- Revisar los planes de continuidad de negocio. La continuidad de negocio requiere algo más que una planificación para un desastre natural; abarca una amplia gama de escenarios de interrupción del negocio, desde el fallo del servidor a una pandemia.
- Asegurar que todos son conscientes de su responsabilidad de mantener los datos seguros y protegidos y cómo ejecutar esa responsabilidad.
- Identificar las herramientas, procesos y metodologías para mantener los datos seguros y protegidos. Tener presente que muchos ya existen (acceso y control de identidad; gestión maestra de datos, gestión del ciclo de vida de la información; procesos de propiedad de los datos).

Ya no es una cuestión de *si* se introducen las nuevas tecnologías en la empresa, sino *cuándo*. Como se mencionó anteriormente, no todas las tecnologías han sido creadas del mismo modo, pero algunas pueden ofrecer importantes beneficios en términos de gestión de riesgos de TI. Las tecnologías más recientes, como la virtualización y el cloud computing, ofrecen excelentes opciones para mitigar los riesgos y reducir los costes.

¿Está preparado?

- **¿Qué estrategias adopta su empresa para seguir las mejores prácticas de TI y de la industria para la mitigación de riesgos, empezando por la seguridad, e incluyendo la resiliencia y la continuidad del negocio?**
- **¿Cómo se adoptan las iniciativas relacionadas con el riesgo de su empresa para ayudar a mejorar la visibilidad y el control, y asegurar el cumplimiento de los contratos, estándares del sector, normativas y controles internos?**
- **¿Cómo ayuda su infraestructura de TI a los objetivos de rendimiento de la empresa en términos de resiliencia, seguridad, disponibilidad, control de gobierno y escalabilidad?**
- **¿Qué tipo de plan tiene su empresa para garantizar que el capital humano, los procesos y los sistemas puedan recuperarse y responder a un evento perturbador?**

El control de los riesgos de TI con cadencia y persistencia, desde la perspectiva tecnológica y empresarial, evalúa continuamente la vulnerabilidad de la empresa frente a los riesgos de TI, prioriza esos riesgos, y actúa en consecuencia. Por lo tanto, es importante incorporar protocolos de gestión del riesgo en las nuevas tecnologías en cuanto se implementen.

Por último, considerar las necesidades de la empresa al implementar herramientas y procesos. Buscar el equilibrio entre la rapidez de comercialización y el riesgo aceptable. Asumiendo un enfoque proactivo en la gestión de riesgos de TI, las empresas pueden posicionarse un paso por delante de las posibles vulnerabilidades y seguir siendo más seguras y resilientes frente a posibles incidentes planificados o imprevistos.

Para más información

Para saber más sobre este Estudio del Instituto IBM para el Valor Empresarial, contacte con *iibv@us.ibm.com*. Para consultar el catálogo completo de nuestra investigación, visite:

ibm.com/iibv

Para acceder a los recursos adicionales para la gestión de riesgos de TI, visite:

ibm.com/smarterplanet/security

Autores

Linda Ban es la Directora del Programa del Estudio CxO y Directora de AIS del Instituto IBM para el Valor Empresarial. Entre sus funciones, dirige el equipo global responsable del desarrollo, despliegue y soporte del liderazgo de pensamiento de IBM de todo el programa de CIO, así como la organización de los Servicios de Innovación de Aplicación de IBM (AIS). El historial de Linda incluye una amplia experiencia en tecnologías colaborativas y emergentes, estrategias operativas y empresariales, desarrollo de sistemas y dirección de operaciones. Además de su trabajo con los clientes, ha publicado muchos artículos sobre una amplia gama de temas, retos y soluciones empresariales. La dirección de contacto de Linda es *lban@us.ibm.com*.

Richard Cocchiara es IBM Distinguished Engineer y el Chief Technology Officer para Business Continuity and Resiliency Services en IBM Global Services. Acumula 28 años de experiencia en I/S, y ha realizado trabajos de consultoría para muchas empresas listadas en Fortune 500, especialmente en el área de finanzas y seguridad. En la actualidad Rich es responsable de la investigación y desarrollo de Business Continuity and Resiliency solutions and services within IBM Global Technology Services. La dirección de correo de Richard es *rmcocch@us.ibm.com*.

Kristin Lovejoy es la Vicepresidenta responsable de la Estrategia de Seguridad de IBM. Fue reconocida como una de las Mejores 25 CTO por InfoWorld en 2005 y una de las 25 Ejecutivas de Seguridad Más Influyentes por la Security Magazine en 2006. Ostenta una patente en EE.UU y la UE por el Modelo y Metodología de Gestión del Riesgo Orientado al Objeto. La dirección de Kristin es *klovejoy@us.ibm.com*.

Ric Telford es Vicepresidente de los Servicios de Nube de IBM y encargado de definir nuevas oportunidades y servicios como parte de la amplia cartera de ofertas de computación en nube de IBM. Durante su trayectoria en IBM, Telford ha asumido varios cargos en algunas iniciativas de software y servicio para la empresa, incluyendo gestión de documentos, redes, gestión de sistemas y servicios de infraestructura de TI. Previamente, Ric fue VP de Autonomic Computing, dirigiendo el desarrollo hacia más sistemas de auto-gestión. La dirección de Ric es *rtelford@us.ibm.com*.

Mark Ernest es un Ingeniero Reconocido de IBM y miembro de la Academia de Tecnología de IBM. Atiende a los clientes en el diseño e implementación de los sistemas de gestión de TI para maximizar el valor de su inversión de TI y mejorar la eficacia y efectividad en el uso de la tecnología de la información. La dirección de Mark es *lernest@us.ibm.com*.

El socio correcto para un mundo cambiante

En IBM, colaboramos con nuestros clientes, brindándoles visión empresarial, tecnología e investigación avanzadas para ofrecerles una ventaja distintiva en el actual entorno en continuo cambio. A través de nuestro enfoque integrado en el diseño y ejecución empresarial, ayudamos a convertir las estrategias en acción. Y con nuestra experiencia en 17 industrias y nuestra capacidad global que abarca 170 países, podemos ayudar a los clientes a anticiparse a los cambios y a beneficiarse de las nuevas oportunidades.

Referencias

1 The IBM X-Force 2010 Mid-Year Trend and Risk Report. IBM Corporation, 2010.

IBM United Kingdom Limited
PO Box 41North Harbour
Portsmouth
PO6 3AU
Reino Unido

IBM Ireland Limited
Oldbrook House
24-32 Pembroke Road
Dublín 4

IBM Ireland Limited está registrada en Irlanda bajo el número de empresa 16226.La página web de IBM puede encontrarse en ibm.com

Por favor, reciclar

GBE03365-ESES-00