



LA GESTIÓN DE RIESGOS DE TI EN EL MARCO CORPORATIVO

La medida del riesgo, la evaluación y selección de opciones para mitigarlo, gestionando las amenazas que pueden afectar al éxito del negocio, es una disciplina por todos conocida como gestión del riesgo. Sin embargo, la propia definición de riesgo puede variar sustancialmente según la experiencia y formación de cada profesional o del contexto dentro de la organización.

Típicamente cuando un profesional de seguridad de la información piensa en riesgo lo hace en términos del impacto que podría suponer en el negocio una pérdida de confidencialidad, integridad o disponibilidad de la información. Sin embargo, y cada día más debido a la madurez de las organizaciones y a los requisitos de cumplimiento, la definición—e incluso la catalogación de riesgos—es mucho más amplia dentro de lo que la organización

negocio; del mismo modo, habría que identificar los procesos susceptibles de fraude interno, como por ejemplo la venta de información confidencial, relaciones con los proveedores, etc.

- **Pérdidas generadas por una interrupción del negocio.** Sería necesario identificar los procesos expuestos a una interrupción del servicio, es decir aquellos procesos para los cuales una interrupción puede suponer una pérdida financiera por el abandono del servicio al cliente o incluso por penalizaciones por incumplimiento de pagos o por violación de regulaciones. Este análisis se suele realizar usualmente en el marco de la disciplina de continuidad de negocio.

- **Pérdidas generadas por errores en la ejecución.** Sería necesario identificar las causas más usuales de error en relación con la complejidad y

seguridad TI.

En esta situación, la gestión de riesgos de TI toma otra perspectiva en la que es necesario crear programas de gestión del riesgo de TI que combinen la gestión de una amplia gama de riesgos específicos relacionados con la tecnología dentro de un programa de gobierno de los riesgos a un nivel superior. Este programa se enfrenta al reto de elaborar unos resultados y controles lo suficientemente flexibles como para poder encajar en este contexto más global de gestión del riesgo, donde las expectativas son más amplias desde el nivel corporativo, en el marco de unos servicios globalizados y con el cada día más extendido uso de proveedores de servicio externos.

La identificación de cualquier riesgo de TI requiere siempre conectar el riesgo a los servicios de TI y, a su vez, estos a los riesgos de negocio. Por ejemplo, el negocio puede enfrentarse a la contingencia de no poder ofrecer determinados servicios debido a la inestabilidad de un sistema TI. Anticiparse a este tipo de situaciones da sentido a la gestión de riesgos de TI más que centrarse en la generación de una serie de medidas puntuales que mitigan ciertos riesgos tecnológicos.

El reto actual del profesional de gestión de riesgos de TI se basa en definir un programa continuo, objetivo, repetible y medible, en el que la evaluación de costes, la valoración de activos y las métricas de rendimiento convivan de manera integrada con el resto de requerimientos corporativos.

considera como riesgos corporativos dentro del marco del gobierno de la empresa.

La exposición al riesgo operacional en una organización la podríamos dividir, por ejemplo, en tres grandes áreas: los riesgos inherentes a cualquier entidad, de los procesos que realiza la organización y los relacionados con la estrategia.

Los riesgos inherentes a la entidad abarcan los provenientes de:

- **Los recursos humanos,** tales como diferencias con los empleados o dependencias de personas clave para la organización, clima social en la compañía y política social, y exposición al riesgo de conflictos con los sindicatos o los representantes de los empleados.

- **La regulación.** Los requisitos regulatorios suponen un riesgo creciente: es necesario identificar y gestionar las obligaciones de cumplimiento normativo, especialmente en sectores como el financiero, seguros, u hospitalario. Esta gestión dependerá mucho del modelo de negocio o de los países en los que la organización se encuentre. Ejemplos de estas regulaciones son: Sarbanes-Oxley, PCI y DSS.

- **Los clientes.** Se torna necesaria la identificación de los puntos de conflicto con clientes, de las áreas de la compañía más expuestas al fallo en el servicio al cliente, e, incluso, de los tipos más significativos de riesgo reputacional.

- **El entorno.** En él se encuadran las situaciones de riesgo más relevantes relacionadas con agentes externos (tormentas, inundaciones, terremotos, pandemias etc.).

Dentro de los riesgos de los procesos de una organización, se podrían incluir:

- **Fraude interno y externo.** Sería necesario identificar los procesos expuestos al fraude externo basándonos en la experiencia histórica y en entrevistas con los responsables del proceso de

la automatización del proceso: errores humanos, fallos en la integridad TI... Los procesos en los que estos errores podrían impactar son los de pagos, desarrollo de productos financieros y aquellos con fechas de entrega obligatorias.

Por último, los riesgos relacionados con la estrategia incluyen:

- **La gestión del cambio.** La innovación y la política de gestión del cambio son parámetros que conducen a la exposición al riesgo. Sería por tanto necesario identificar en una organización como factores de riesgo los nuevos proyectos de TI relativos a cambios significativos o a la implementación de nuevos sistemas, el lanzamiento de productos y la adquisición de compañías.

- **La política de outsourcing/offshoring.** Las decisiones de externalización de las partes no esenciales del negocio para beneficiarse de economías de escala conducen a nuevos riesgos como la exposición a la ejecución de errores de los proveedores de servicio, a su salud financiera, al riesgo de exponer información confidencial a terceros o los derivados de un plan inadecuado de continuidad de negocio del proveedor.

Desde esta perspectiva del concepto de riesgo y su clasificación, cada área de la organización implicada en la identificación, monitorización y gestión de estos riesgos, y a su vez cada área afectada directamente por una regulación (finanzas, departamentos legales, auditoría, RRHH), puede desarrollar su propia estrategia y metodología para mitigar los riesgos o cumplimientos con las regulaciones. La gestión de riesgos de TI debe responder a esta realidad, ya que se enmarca dentro de la gestión de riesgos de la organización. Su objetivo es proteger la información de la organización y sus sistemas. Adicionalmente, la gestión de riesgos de TI debe considerarse como un programa y no como un proyecto periódico focalizado en controles de

Conclusión

En respuesta a las crecientes problemáticas, la gestión de riesgos de TI ha sufrido muchos cambios durante los últimos años. Sin embargo, más recientemente, la habilidad para definir y comunicar el marco de los riesgos de TI ha tomado mucha más relevancia. La disciplina de gestión de riesgos de TI se enmarca no solo dentro de los requerimientos regulatorios, sino también dentro de los de negocio. Un profesional de la gestión del riesgo TI debe ser especialista en tecnología y sistemas de gestión de seguridad de la información, y también tener un amplio conocimiento del negocio de la empresa en la que desarrolla su actividad.

El reto actual del profesional de gestión de riesgos de TI se basa en definir un programa continuo, objetivo, repetible y medible, en el que la evaluación de costes, la valoración de activos y las métricas de rendimiento convivan de manera integrada con el resto de requerimientos corporativos. La creación del programa debe realizarse desde una perspectiva de arriba hacia abajo, totalmente enmarcada en la gestión global de los riesgos y respondiendo a los diferentes requerimientos de las distintas unidades de negocio, consiguiendo gestionar y definir unos controles flexibles y adaptables a los distintos tipos de riesgos y de requerimientos regulatorios que no obliguen a la organización de TI a reinventar las tareas, y los controles y las evidencias de cumplimiento. ■



Carolina de Oro Gómez
IT Compliance & Risk
Management Manager
Región Mediterránea y Latinoamérica
AXA SEGUROS