KPMG

Auditoría interna y los riesgos de la ciberseguridad

KPMG.com.ar

Contenido

Dado el creciente número de ciberataques y violaciones en los datos, la ciberseguridad es una prioridad para el logro de los objetivos empresariales de todos los sectores y por lo tanto ocupa un lugar privilegiado en la agenda de los Directorios.

Los costos asociados con estos eventos han llegado a ser tan significativos que las organizaciones están centrando su atención en cómo proteger sus activos, en especial los datos sensibles: información personal, datos bancarios o de titulares de tarjetas, información financiera de la empresa, propiedad intelectual y cualquier otra información significativa que no es pública.

Los riesgos involucrados son graves y pusieron en alerta a las organizaciones, pero muchas de ellas no se sienten preparadas. Según la encuesta *Harvey Nash / KPMG CIO Survey 2019*[1], el presupuesto asignado por las empresas para temas relacionados con la tecnología ha aumentado. Un 14% de los encuestados indicó que el incremento está destinado a inversiones en ciberseguridad, por considerarlo un tema prioritario. Este informe además resalta que sólo el 26% de los líderes de TI sienten que están "muy bien preparados" para defenderse de un ciberataque.

Contando con el apoyo creciente de la Dirección, ¿cómo pueden las organizaciones cerrar la brecha en la preparación para enfrentar los desafíos de la ciberseguridad? y ¿cómo pueden ayudar las funciones de auditoría interna en este proceso?

Lo primero es entender qué es una "violación de datos", que generalmente se define como un evento en el que los datos sensibles o confidenciales son copiados, vistos, robados o utilizados por una persona o entidad no autorizada para hacerlo.

Las actividades que contribuyen a la violación de datos u otras formas de ciberdelincuencia incluyen el error humano, la intencionalidad política o criminal, las tecnologías emergentes o el cambio en los negocios, entre otros.

Los "malos" han evolucionado desde criminales aislados o los *script kiddies*[2] que apuntaban al robo de identidad, oportunidades de autopromoción o robo de servicios, a convertirse hoy en día en delincuentes organizados, estados nacionales, activistas o personas con información privilegiada que se centran en la propiedad intelectual, la información financiera o el acceso estratégico a los recursos clave.

---

1 La encuesta Harvey Nash / KPMG CIO Survey 2019 es la mayor encuesta de líderes de tecnología informática en el mundo, con más de 3.600 respuestas de los CIOs y otros ejecutivos de tecnología a lo largo de 108 países.

2 Es un término utilizado para describir a aquellos que utilizan programas y scripts desarrollados por otros para atacar sistemas de computadoras y redes. Es habitual asumir que son personas sin habilidad para programar sus propios exploits (un fragmento de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo), y que su objetivo es intentar impresionar sin tener alguna base firme de conocimiento informático.

¿Cómo puede la auditoría interna evaluar los riesgos de la ciberseguridad?

Las funciones de auditoría interna pueden realizar una variedad de técnicas y procesos de evaluación para ayudar a identificar, evaluar y mitigar los riesgos de la ciberseguridad. La siguiente tabla incluye una selección de las mismas:

Evaluaciones técnicas	
Operaciones y tecnología	Análisis de vulnerabilidades y pruebas de penetración
	Acceso a la red y monitoreo / evaluación de amenazas
	Revisiones de configuraciones de dispositivos (infraestructura, firewalls, routers, etc.)
	Wi-Fi: configuraciones y pruebas de vulnerabilidades / explotación Wi-Fi no autorizado
	Puntos de acceso remoto / VPN: evaluación técnica de los puntos de acceso remoto y de la configuración para ayudar a garantizar su protección
	Evaluación de aplicaciones / bases de datos, por ejemplo, análisis de vulnerabilidades, pruebas de penetración y configuración de bases de datos
	Seguridad por diseño
	Revisiones y análisis de arquitectura
	Configuración de seguridad del sistema operativo / base de datos
	Proceso de parcheo / procedimientos de remediación
	Revisión de código

Evaluaciones de procesos y controles	
	Gestión de identidades y accesos: - Centralización vs. descentralización - Inicio de sesión único / Single sign-on - Procedimientos de gestión de acceso - Gestión de acceso remoto y autenticación - Gestión de acceso privilegiado
	Seguridad física y personal: - Controles de acceso lógico y físico - Conciencia de seguridad / ingeniería social
	Seguridad de los dispositivos móviles
	Evaluaciones de seguridad de las operaciones
Factores humanos	Gestión del talento y formación en TI
Dirección y gobierno	Gobierno de ciberseguridad, funciones y responsabilidades
	Integración de la gestión de riesgos cibernéticos y empresariales
Legal y cumplimiento	Consideraciones reglamentarias e integración en el marco cibernético
Gestión de riesgos de la información	Gestión de riesgos de los proveedores y seguridad
	Análisis de amenazas cibernéticas y proceso de gestión de riesgos: - Identificación de amenazas, evaluación y proceso de actualización - Gestión del cambios, incluida su integración en el ciclo de vida de desarrollo de software
	Seguridad informática en la nube y evaluación continua
	Clasificación, protección y cifrado de datos, programas de formación y sensibilización en toda la organización

Fuente: "The role of internal audit in cyber security readiness" de KPMG publicado en 2019.

Continuidad del negocio y gestión de crisis	Respuesta a incidentes de seguridad y comunicación: - Plan de comunicación de crisis - Funciones y responsabilidades del equipo - Procedimientos de notificación (legales, regulatorios, etc.) - Proceso de cierre - Controles durante un incidente - Investigación - Formación y sensibilización
	Integración con la seguridad
	Recuperación ante los desastres / resiliencia
	Proceso de evaluación del impacto empresarial
	Estrategia de prueba

Factores de riesgo de ciberseguridad que la auditoría interna debería tener en cuenta

Muchas organizaciones creen que están adecuadamente protegidas cuando realizan pruebas de penetración periódicas o cuentan con las mejores herramientas técnicas disponibles.

La participación de la auditoría interna para combatir la ciberdelincuencia y minimizar el riesgo de violaciones de datos es cada vez mayor e incluye un gran número de procesos operativos, entre otras áreas como las que se mencionan a continuación.

Amenazas emergentes

El panorama de las amenazas de ciberseguridad cambia y evoluciona continuamente. La mayoría de los equipos de defensa dentro de una organización intentan abordar y mitigar el entorno de amenazas emergentes a través de una combinación de controles y técnicas. Por ejemplo, las organizaciones confían en suscripciones con proveedores de información que proporcionan actualizaciones en tiempo real sobre las amenazas nuevas y emergentes que prevalecen en un momento dado. Adicionalmente, las organizaciones pueden realizar su propio reconocimiento, investigando y accediendo a portales de discusión de medios sociales conocidos. Esta inteligencia es luego aplicada en los planes de remediación y en los controles preventivos.

Por ejemplo, una organización fue informada de un ataque inminente de negación de servicios a menos que se cumpliera con las condiciones del rescate. La organización respondió inmediatamente con controles adicionales para la mitigación de la negación de servicio, así como con una mayor supervisión de los sistemas potencialmente afectados.

La SEC[3] publicó recientemente un informe de investigación para que las organizaciones tomen conciencia de la existencia de amenazas de comunicaciones electrónicas fraudulentas y que deberían ser consideradas en los sistemas de controles internos. Las investigaciones de la SEC se centraron en las "comunicaciones electrónicas fraudulentas" o "afectación de correos electrónicos corporativos", en los cuales los perpetradores se hicieron pasar por ejecutivos o vendedores de la compañía y usaron correos electrónicos para engañar al personal de la compañía y enviar grandes sumas de dinero a cuentas bancarias controladas por los perpetradores. Los fraudes en algunos casos duraron meses y se detectaron después de la intervención de la policía o de terceros. Cada una de las compañías perdió, al menos, US$ 1 millón, dos perdieron más de US$ 30 millones y una perdió más de US$ 45 millones. En total, las nueve compañías incluidas en el informe transfirieron casi US$ 100 millones como resultado de los fraudes, la mayoría de los cuales no se pudieron recuperar.

La auditoría interna debería evaluar la estrategia general de la organización para hacer frente a las amenazas emergentes desde una perspectiva de gobierno, arquitectura, operaciones y tecnología. Las organizaciones líderes en la práctica cuentan con un enfoque bien definido para hacer frente al nuevo entorno de amenazas emergentes.

3 Securities and Exchange Commission es una institución independiente del gobierno de Estados Unidos encargada de vigilar el cumplimiento de las leyes federales del mercado de valores, la regulación de las bolsas de valores y el mercado de opciones de Estados Unidos.

Cambios tecnológicos

El ritmo actual del impacto de la innovación tecnológica en las organizaciones va en aumento. Las organizaciones, después de muchos años, están incrementando su gasto en nuevas tecnologías para lograr un ritmo de crecimiento cada vez mayor en sus negocios. La adopción de la nube, el aumento de la demanda de automatización inteligente, la robótica y el auge de la Internet de las Cosas[4] han añadido nuevos y más complejos riesgos de seguridad al entorno empresarial.

La auditoría interna se enfrentará al reto de evaluar los riesgos de ciberseguridad de estas tecnologías nuevas y emergentes. Será importante evaluar los riesgos actuales asociados al cambio tecnológico en términos de su impacto en los negocios existentes.

Adicionalmente, se deberían tener en cuenta las nuevas iniciativas que podrían introducir riesgos en la organización como resultado de las tecnologías emergentes.

Sería conveniente que la auditoría interna se preguntara si la organización ha adoptado los principios de "seguridad por diseño" y está llevando a cabo revisiones de diseño o de tecnología antes de la adopción e implementación final de la tecnología. La ejecución de su plan de auditoría debería responder estos interrogantes.

Cambios en el negocio

El cambio en los negocios se ve afectado por el cambio tecnológico y en el entorno regulatorio, los nuevos modelos de negocios, y el impacto de las fusiones, adquisiciones o desinversiones.

Tradicionalmente, las funciones de auditoría interna han sido proactivas a la hora de abordar los riesgos de negocio asociados con estos cambios. Sin embargo, hasta hace poco, el riesgo de ciberseguridad y su impacto asociado no siempre fueron considerados con la profundidad y la envergadura que ameritaban.

Los principales riesgos de ciberseguridad que deberían tenerse en cuenta incluyen el entorno de amenazas de negocio y los riesgos de ciberseguridad que originan las fusiones y adquisiciones para la entidad adquirente. Por ejemplo, si una organización se encuentra en proceso de adquisición de otra compañía, la evaluación del riesgo de ciberseguridad y el impacto de las violaciones conocidas de datos deberían formar parte de los procedimientos de debida diligencia.

4 La Internet de las Cosas es un concepto que se refiere a una interconexión digital de objetos cotidianos con internet.

Cambios regulatorios

En todas las industrias, el cambiante panorama regulatorio tiene un impacto en la organización. La reciente legislación del Reglamento General de Protección de Datos[5] y otras leyes y requisitos de seguridad de datos y privacidad, tales como los del *New York Department of Financial Services*, han impuesto requisitos adicionales de control a las organizaciones. Algunas organizaciones, al no haber estado preparadas para abordar estos nuevos requisitos, abrieron la posibilidad de sufrir sanciones o multas.

Adicionalmente, en el Informe de prioridades de examen de la SEC de 2019, la ciberseguridad se destacó como una prioridad en los cinco programas de examen de la *Office of Compliance Inspections and Examinations*. Estos exámenes se centran en las configuraciones, los dispositivos de almacenamiento en red, el gobierno de la seguridad de la información y las políticas y procedimientos relacionados con la seguridad de la información.
La SEC también hace hincapié en las organizaciones con múltiples oficinas que realizaron fusiones recientemente y en otras áreas tales como las evaluaciones de riesgo, los controles de acceso y la prevención de pérdida de datos. No sería extraño que otros organismos de supervisión internacionales o nacionales tomaran uno o varios de los aspectos antes mencionados para realizar sus revisiones o auditorías, y valdría la pena que las organizaciones estuvieran preparadas para atender los requerimientos del órgano de control que corresponda.

La auditoría interna puede desempeñar un papel clave en la evaluación del impacto de las nuevas regulaciones o de las existentes, así como en la evaluación del grado de preparación de su organización para afrontarlas.

Riesgo de terceros

La mayoría de las organizaciones tienen una cadena de suministro cada vez más compleja y han aumentado su dependencia de proveedores externos para que proporcionen bienes y servicios a su organización. Esta dependencia ha incrementado, en muchos casos, el riesgo de ciberseguridad al permitir que terceros accedan directamente a los sistemas de la organización, o a través del procesamiento de su información privada o confidencial o la de sus clientes. Todas las industrias deberían tener un sólido control sobre la naturaleza de la información que está siendo utilizada por el tercero, cómo se transmite la información, cómo es almacenada y procesada por el tercero. En muchos casos, una cuarta parte puede estar involucrada.

La auditoría interna puede realizar evaluaciones a nivel global del programa de la interrelación con terceros, así como evaluaciones detalladas de los proveedores de alto riesgo.

5 *Reglamento General de Protección de Datos* es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos.

La participación de auditoría interna en la preparación de la ciberseguridad

Cada organización es única, así como las amenazas que enfrenta. En consecuencia, cada estrategia de respuesta ante esas amenazas será diferente. Sin embargo, para las funciones de auditoría interna existen algunas áreas prioritarias en ciberseguridad que deberían ser consideradas al momento de determinar el alcance del plan de auditoría en esta área. El gráfico siguiente proporciona un ejemplo:

Objetivos y estrategias de negocio

- Entender el entorno del negocio, objetivos, expectativas de las partes interesadas, y del regulator.
- Alinear los objetivos de ciberauditoría a las metas empresariales y a los objetivos de TI.
- Comprender las deficiencias anteriores en ciberseguridad.
- Revisar la cobertura del plan de auditoría anterior.

Alineación del marco

- Definir prácticas líderes en ciberseguridad y los marcos de trabajo aplicables a la industria.
- Adaptar los marcos de trabajo al entorno de la organización.
- Alinear el plan de ciberauditoría con el marco respectivo (p.e. ISO, Marco de Ciberseguridad NIST).

Riesgos y amenazas emergentes

- Entender las tecnologías adoptadas por la organización.
- Comprender las amenazas y vulnerabilidades introducidas por la tecnología.
- Abordar los riesgos emergentes en la adopción digital, cibernética, de automatización y de la nube, etc.

Talento humano calificado

- Desarrollar un plan de auditoría para identificar los requisitos de talento y el conjunto de habilidades para apoyar las ciberauditorías.
- Definir el modelo de aprovisionamiento para lograr la calidad, el rendimiento y el valor de las ciberauditorías.
- Calibrar el plan de auditoría en respuesta a la evolución del panorama de riesgos, las prioridades del negocio y la adopción de tecnología.

Fuente: "The role of internal audit in cyber security readiness" de KPMG publicado en 2019.

Se necesita una comprensión integral de la organización, sus objetivos, sus riesgos y sus procesos para poder abordar completamente los desafíos de ciberseguridad que puede enfrentar en la actualidad. La auditoría interna necesita estudiar a fondo su organización, y poseer un sólido conocimiento técnico para alinear la ejecución de sus procesos con los objetivos organizacionales.

Elegir el enfoque correcto para evaluar su programa de ciberseguridad puede ser un desafío, especialmente porque poder contar con el talento calificado en ciberseguridad sigue siendo un desafío para muchas funciones de auditoría interna.

Contactos

Servicios de IT Advisory | Riesgos de ciberseguridad

Walter Risi
Socio Líder de Consulting y servicios de IT Advisory
+54 11 4316 5841
wrisi@kpmg.com.ar

Nicolás Manavella
Socio
+54 11 4316 5841
nmanavella@kpmg.com.ar

Graciela Rodríguez
Directora
+54 11 4316 5745
gmrodriguez@kpmg.com.ar

Instituto de Comités de Auditoría (ICA)

Para más información, por favor visítenos online en www.home.kpmg/ar/ICA o envíenos un email a ica@kpmg.com.ar:

Ariel Eisenstein
Socio Líder de Auditoría
+54 11 4316 5812
aeisenstein@kpmg.com.ar

Viviana Picco
Socia
+54 11 4316 5729
vpicco@kpmg.com.ar

Romina Bracco
Socia
+54 11 4316 5910
rbracco@kpmg.com.ar

En el Instituto de Comités de Auditoría patrocinado por KPMG brindamos una variedad de recursos diseñados para asistir a Directores y miembros de Comités de Auditoría a mantenerse actualizados y a compartir experiencias que son esenciales para cumplir apropiadamente con su rol. Ofrecemos un programa integral que contempla el patrocinio de eventos y sesiones de capacitación, y la publicación de artículos de especialistas que abordan temas de actualidad.

kpmg.com.ar