Traducción al Español Auspiciada por:

FLAI
Fundación Latinoamericana
de Auditores Internos

# PERSPECTIVAS Y PERCEPCIONES GLOBALES

*Ciberseguridad*

PARTE I: Contratación y desarrollo de la próxima generación

PARTE II: Inteligencia artificial: amiga y enemiga de la ciberseguridad

PARTE III: Gestión de riesgos de ciberseguridad de terceros

AUDITBOARD

The Institute of Internal Auditors

# Contenido

# Parte 1: Contratación y desarrollo de la próxima generación

## Sobre los expertos

### Aneta Waberska, CISA

Aneta es Directora de Productos de Seguridad de la Información y Cumplimiento Normativo en AuditBoard. Cuenta con más de 15 años de experiencia en auditoría de IT y dominios de cumplimiento y se unió a AuditBoard para centrarse en los esfuerzos de desarrollo de productos al servicio de los usuarios de riesgo y cumplimiento de IT, aprovechando su experiencia en la industria. Aneta comenzó su carrera profesional en KPMG y PwC, donde ayudó a clientes a implantar y evaluar marcos como SOC 1 y SOC 2. Ha trabajado con empresas de distintos tamaños para implantar y gestionar programas de cumplimiento de diversa complejidad, incluida la gestión de políticas para toda la empresa, programas de gestión de riesgos de terceros, la implantación de controles para cumplir los requisitos del marco de seguridad y la colaboración con la dirección ejecutiva para garantizar que el cumplimiento respalda los objetivos estratégicos de la empresa.

### Uday Gulvadi, CIA, CPA, CAMS, CISA

Uday es director gerente del grupo de litigios, cumplimiento e investigaciones de Stout, y codirige su práctica de cumplimiento normativo y delitos financieros a escala nacional. Uday es un líder en delitos financieros, auditoría interna, auditoría de sistemas de información y asesoramiento de riesgos con más de 20 años de experiencia. Está especializado en asesorar a consejos de administración, comités de auditoría y altos directivos sobre sus mayores retos en materia de cumplimiento de delitos financieros, tecnologías de la información y ciber riesgos, gobernanza y asuntos de riesgo y cumplimiento, incluida la gestión del riesgo empresarial, gobernanza de programas de AML y sanciones, validaciones de modelos, auditorías internas basadas en riesgos, tecnologías de la información y auditoría y controles de ciberseguridad. Entre los clientes de Uday se encuentran desde algunos de los mayores bancos e instituciones financieras del mundo hasta pequeñas empresas de servicios financieros.

# INTRODUCCIÓN

**La ciberseguridad supone una amenaza importante para las organizaciones de cualquier tamaño.** Ejemplos recientes reflejan lo rápido que pueden ponerse las cosas difíciles. Un ciberataque interrumpió los envíos de Ace Hardware Corporation a sus distribuidores y obligó a desactivar temporalmente los pedidos en línea de los clientes. Un ataque de ransomware a una importante empresa chilena de telecomunicaciones interrumpió servicios como los centros de datos, el acceso a Internet y la voz sobre IP. Y, demostrando que las entidades más pequeñas también pueden verse afectadas, el acceso público en línea a los registros de la propiedad y a los índices de nacimientos, defunciones y matrimonios se vio interrumpido por un ciberataque en el condado de Cabarrus, Carolina del Norte.

La auditoría interna es idónea para desempeñar un papel clave a la hora de ayudar a gestionar los riesgos cibernéticos, pero debe contar con los recursos necesarios para cumplir esa función. Debe contar con los conocimientos y habilidades necesarios para identificar y asesorar sobre las ciber amenazas a las que se enfrenta la organización. Para llevar a cabo una evaluación de la ciberseguridad, "es fundamental contar con profesionales de la auditoría que posean las competencias técnicas y los conocimientos adecuados sobre el entorno de riesgo actual", según Deloitte.[1]

Este informe es el primero de una serie de tres partes sobre ciberseguridad. Debido a que los líderes de auditoría interna deben entender las amenazas antes de que puedan dotarse de personal para hacerles frente, comienza examinando los desafíos de la ciberseguridad para los auditores internos y sus organizaciones. También cubre las opciones y estrategias que los líderes de auditoría interna pueden seguir para asegurarse de que tienen el talento que necesitan para hacer frente a los riesgos cibernéticos en curso.

[1] "Cybersecurity and the Role of Internal Audit—An Urgent Call to Action," Deloitte Development LLC, 2017.

# Una Amenaza Evidente

## La ciberseguridad sigue siendo uno de los principales riesgos

### Crecen los Esfuerzos de Auditoría Interna en Materia de Ciberseguridad

**"Los auditores internos tienen que examinar toda la organización** y adoptar un enfoque basado en el riesgo", afirma Aneta Waberska, CISA, directora de productos de seguridad de la información y cumplimiento normativo de AuditBoard. "Los riesgos cibernéticos encabezan la lista de la mayoría de las organizaciones."

Los auditores internos parecen ser muy conscientes de la amenaza que suponen los ciber riesgos. La ciberseguridad fue identificada como el principal riesgo de cara a 2024, según una encuesta mundial realizada por The Internal Audit Foundation entre los líderes de auditoría interna. La ciberseguridad, junto con el capital humano y la continuidad del negocio, figuran como los tres principales riesgos en la encuesta Risk in Focus 20242 encuesta realizada a más de 4.200 jefes de auditoría (CAE), en la que el 73% de los encuestados señalaron la ciberseguridad como uno de los cinco principales riesgos.

En Norteamérica, el 78% de los responsables de auditoría interna calificaron la ciberseguridad como un riesgo alto o muy alto en sus organizaciones, según The Institute of Internal Auditors 2023 North American Pulse of Internal Audit.3 Los auditores encuestados dedicaban el 10% de sus planes de auditoría a la ciberseguridad, y los problemas de IT representaban otro 9%. Además, casi el 70% de las funciones revisaban las áreas de alto riesgo que incluyen la ciberseguridad y las IT anualmente o de forma continua, según los resultados de la encuesta Pulse.

Algunos peligros de ciberseguridad a tener en cuenta son:

- Brechas que permiten a los delincuentes robar información crítica o que exponen datos de clientes o socios comerciales.
- Ataques de ransomware que impiden a las organizaciones realizar funciones clave o acceder a la información necesaria sin pagar antes un rescate a los ciberdelincuentes.
- Software malicioso (Malware) que puede causar estragos en un sistema.

Los ciberataques tienen consecuencias que van más allá de lo obvio, como pérdidas financieras cuando las funciones empresariales se ven afectadas o si los clientes o socios comerciales pierden la confianza en una organización y dejan de hacer negocios con ella. Además, una vez descubierto un incidente cibernético, las organizaciones deben invertir tiempo y dinero en investigaciones forenses para comprender qué ocurrió y cuándo, emprender medidas correctoras para reparar cualquier daño y determinar si las consecuencias de tales ataques son importantes desde el punto de vista financiero y operativo a fin de cumplir los requisitos de información reglamentaria.

No es de extrañar, por tanto, que el gasto en ciberseguridad esté creciendo rápidamente. A principios de 2023, Canalys preveía que el gasto mundial en ciberseguridad aumentaría un 13.2% durante el año, con un potencial de 224,000 millones de dólares.[4]

"Las empresas se han dado cuenta de que estas amenazas tienen consecuencias empresariales y financieras muy reales", afirma Uday Gulvadi, CIA, CPA, CAMS, CISA, Director General del grupo de Litigios, cumplimiento e investigaciones en Stout. Los comités de

[2] "Risk in Focus 2024," The Internal Audit Foundation, 2023
[3] "2023 North American Pulse of Internal Audit," The Institute of Internal Auditors, 2023

[4] "Cybersecurity investment to grow by 13% in 2023", Canalys, Jan. 18, 2023, https://www.canalys.com/newsroom/cybersecurity-forecast-2023

auditoría tienen muy presentes estas amenazas, afirma, y "se pide a la auditoría interna que dé un paso adelante y ofrezca garantías en estas áreas".

# Los desafíos

## Enfoque en ciberseguridad, impacto de la madurez en la contratación

## Es Fundamental Comprender Claramente el Ciber Entorno

**Contratar a las personas adecuadas para ayudar a la auditoría interna a respaldar la gestión del ciber riesgo** y ofrecerles las oportunidades de desarrollo adecuadas, es importante comprender plenamente las circunstancias y los riesgos de ciberseguridad específicos de la organización. Deben tenerse en cuenta varios factores y retos.

### *Una Mentalidad Manual*

Muchos equipos de auditoría interna han estado acostumbrados tradicionalmente a pensar en los controles internos y en diversos procesos desde una perspectiva manual, dijo Waberska. Sin embargo, la actual transformación digital de las empresas exige que los equipos sean conscientes de cómo las soluciones digitales pueden potenciar y mejorar las auditorías internas y otros procesos en toda la organización, incluida la ciberseguridad. Al mismo tiempo, los auditores internos también deben comprender los riesgos que la propia transformación digital plantea a las organizaciones, ya que los ciberdelincuentes, cada vez más sofisticados, explotan las vulnerabilidades que pueden crear los entornos digitales.

Si, por ejemplo, una organización opera en la nube o utiliza o tiene previsto utilizar cualquier tecnología avanzada o emergente, necesitará personas que hayan trabajado con estas herramientas. No es necesario que los miembros del equipo sean expertos en la tecnología, dijo Waberska, pero la exposición al entorno de la nube o a otras soluciones proporcionará una mayor familiaridad con los riesgos relacionados. Además de contratar a personas con estas aptitudes, los equipos de auditoría deben asegurarse de incluir las nuevas tecnologías en la formación y el desarrollo del personal existente.

### *Controles Internos*

Los auditores internos están capacitados para garantizar que la organización dispone de los controles adecuados para protegerse de los riesgos a los que se enfrenta. En cuanto a los riesgos cibernéticos, los controles internos deben trabajar para garantizar que la tecnología de la información de una organización no se vea comprometida y que las funciones de negocio puedan seguir siendo operativas.

Para identificar y asesorar sobre los riesgos de ciberseguridad, los equipos de auditoría interna tendrán que estar familiarizados con los controles de seguridad informática de las tecnologías utilizadas por su organización. Al trabajar con la nube, por ejemplo, los controles diferirán de los utilizados con los centros de datos internos, dijo Waberska. También tendrán que entender qué controles son apropiados teniendo en cuenta la amenaza que la ciberdelincuencia puede suponer para la privacidad y las implicaciones para los planes de auditoría del programa de privacidad de su organización.

### *Normativa Sobre Divulgación y Protección de Datos*

Ahora se pide a las organizaciones que sean más abiertas a la hora de informar sobre sus esfuerzos en materia de ciberseguridad. Los auditores internos tendrán que entender qué normas afectan a sus empresas y ser capaces de evaluar las necesidades de cumplimiento. Como ejemplo significativo, en agosto, la Comisión de Bolsa y Valores de EE. UU. publicó una norma final sobre Gestión de Riesgos de Ciberseguridad, Estrategia, Gobernanza y Divulgación de Incidentes, que exige a las empresas que cotizan en bolsa a proporcionar una mayor transparencia cuando hayan sufrido un ciberataque y a revelar información específica sobre sus esfuerzos para mitigar los ciber riesgos. El IIA formuló observaciones sobre la norma cuando estaba en fase de propuesta. Tiene previsto seguir

trabajando con la SEC para desarrollar directrices de aplicación, especialmente sobre la determinación de la materialidad de un ciber incidente y una mejor definición del término "ciberseguridad".

Debido a la naturaleza cada vez más multinacional de hacer negocios y al creciente número de normativas de ciberseguridad en todo el mundo, los auditores internos deben familiarizarse con todas las leyes de seguridad y privacidad de datos que puedan afectar a sus organizaciones, como la Reglamento General de Protección de Datos de la Unión Europea. De hecho, según la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, 137 de 194 países habían promulgado leyes para garantizar la protección de los datos y la privacidad.

### *Sistemas de IT*

Cualquier organización que cuente incluso con tecnología básica está involucrada en algún tipo de sistema informático, y todos ellos son vulnerables al riesgo cibernético. Dado el volumen de sistemas y las debilidades y amenazas potenciales que entrañan, es importante que las empresas y la auditoría interna sepan qué sistemas son los más importantes. "Nunca podremos poner el mismo nivel de control en todos los sistemas", señala Waberska. Establecer prioridades implica plantearse preguntas como:

- ¿Qué sistemas son fundamentales para el funcionamiento de la organización? Es posible responder a esta pregunta considerando si - y durante cuánto tiempo- la organización podría seguir desarrollando su actividad o alcanzar sus objetivos clave sin ellos.
- ¿Cuáles procesan los datos más sensibles? Por ejemplo, información confidencial de la empresa o datos de identificación personal ("PII" por sus siglas en inglés).
- ¿Cuáles contienen datos únicos o difíciles de sustituir?[5]

### *Terceros*

Incluso las organizaciones pequeñas y medianas se relacionan con terceros que manejan sus datos. Puede ocurrir a través de una aplicación en la nube o, en el caso de organizaciones más grandes, tal vez un centro de procesamiento en el extranjero. Estos proveedores pueden manejar datos importantes de la organización y la PII de los clientes, y los datos pueden estar alojados en cualquier parte del mundo, señaló Gulvadi. Por esta razón, "es extremadamente importante comprender todo el panorama de los activos de IT", incluyendo dónde están y si existen los controles adecuados en torno a esos activos, dijo.

Las organizaciones deben evaluar los procesos de ciberseguridad de terceros antes de compartir datos con ellos y supervisar dichos procesos una vez que los terceros empiecen a utilizar los datos, reservándose en algunos casos el derecho a auditar a los terceros. "Si comparte datos de clientes con terceros, debe asegurarse de que los protegerán de la misma manera que lo haría su empresa", afirma Waberska. Las empresas deben revisar los informes de certificación de terceros, como el SOC 2, que evalúa sus controles internos para ver hasta qué punto aborda los riesgos, u otros tipos de certificaciones relacionadas con la protección de categorías relevantes de datos.

### *Garantizar el Acceso Seguro y la Disponibilidad*

Existe un equilibrio entre asegurarse de que la organización puede proteger los datos y los sistemas y, al mismo tiempo, garantizar que la información y los sistemas están disponibles para su uso según sea necesario para alcanzar los objetivos empresariales, señaló Gulvadi. Para mantener el equilibrio, las organizaciones tendrán que elegir controles que salvaguarden los datos sin hacer gravoso el acceso a la información necesaria para el servicio al cliente u otras funciones empresariales importantes. Esta determinación debería ser más fácil de tomar una vez que la organización haya considerado qué sistemas requieren el mayor nivel de seguridad. Es posible

[5] "*CISA Insights – Cyber, Secure High Value Assets (HVAs),"* U.S. Department of Homeland Security, https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-SecureHighValueAssets_S508C.pdf

que algunos deban protegerse con autenticación multifactor, protocolos de cifrado y software de prevención de pérdida de datos, mientras que otros no requerirán ese nivel de granularidad.

# Reforzar los Recursos de Auditoría Interna

La contratación de personal de ciberseguridad sigue siendo una prioridad alta

## Contratación y Desarrollo del Ciber Talento de Auditoría Interna

**Teniendo en cuenta estos riesgos, ¿cómo puede la auditoría interna crear y mantener** un equipo que pueda abordarlas? La respuesta concreta variará según la organización, pero hay algunas recomendaciones que se aplican a todas.

### *Busque una Combinación de Capacidades*

Para abordar el riesgo cibernético, los equipos de auditoría interna necesitan un profundo conocimiento del aspecto técnico de la ciberseguridad, así como la capacidad de comprender las consecuencias que los problemas de seguridad pueden tener para la empresa, dijo Gulvadi. En el pasado, los auditores de IT tendían a ser fuertes en los aspectos técnicos de la seguridad de la información, pero a menudo no se centraban en cómo los riesgos relacionados afectaban a la capacidad de la organización para cumplir sus objetivos empresariales. La capacidad de articular el impacto en el negocio puede ser especialmente valiosa si la auditoría interna necesita obtener la aprobación de la dirección para las inversiones necesarias en tecnología o controles mejorados o personal adicional.

Gulvadi está observando más esfuerzos por crear equipos que combinen los conocimientos técnicos con la comprensión de los objetivos empresariales, los procesos y las cadenas de valor. En algunos casos, los equipos de auditoría interna están encontrando profesionales que tienen ambas habilidades, pero en otros, los equipos incluyen profesionales cuyas habilidades se complementan entre sí. La organización puede considerar ofrecer formación para dar a cada tipo de profesional un conocimiento práctico básico de la otra disciplina.

### *Integrar Competencias en Tecnologías Emergentes*

Muchos equipos de auditoría interna están incorporando profesionales con experiencia en análisis de datos, inteligencia artificial y aprendizaje automático a medida que se alejan de las pruebas basadas en muestras. "Se puede utilizar la inteligencia artificial para analizar toda la población y mejorar la detección de anomalías", afirma Gulvadi. Esto no solo mejora la eficiencia y la fiabilidad, sino que también ayuda a los auditores internos a seguir el ritmo de los ciberdelincuentes, que cada vez son más sofisticados en el uso de las nuevas tecnologías.

### *Investigar el Outsourcing*

Algunos equipos de auditoría interna recurren a un equipo subcontratado para mejorar las competencias técnicas o empresariales. Los profesionales con conocimientos especializados en ciberseguridad o seguridad informática pueden incorporarse al equipo de auditoría interna por proyectos o a largo plazo, según sea necesario. Cuando los miembros del equipo de auditoría interna trabajan junto a estos expertos, pueden ayudar a los contratistas a mejorar sus conocimientos y a desenvolverse mejor en los procesos y procedimientos de la empresa. Al mismo tiempo, la exposición a expertos externos puede ayudar a ampliar la base de conocimientos de los miembros del equipo. Al evaluar una opción de externalización, Gulvadi recomienda examinar las certificaciones y la experiencia previa de los miembros del equipo para asegurarse de que coinciden con las habilidades actuales del equipo o las mejoran.

### *Considerar la Colaboración*

A veces, la experiencia que necesita el equipo de auditoría interna puede estar disponible internamente en áreas como IT, seguridad o cumplimiento. Una buena asociación, al tiempo que mantiene la independencia del auditor, introduce a los miembros del equipo de auditoría interna en una serie de nuevas perspectivas y conocimientos sobre el ecosistema tecnológico y los riesgos de la organización. También sienta las bases para auditorías fructíferas en el futuro porque otros equipos sabrán que la auditoría interna comparte su objetivo de proteger a la organización de riesgos innecesarios y garantizar que pueda alcanzar sus objetivos. La comunicación abierta también puede ayudar a otros equipos a superar cualquier ansiedad sobre los objetivos de auditoría interna. "Los equipos de IT y seguridad se centran en resolver problemas importantes y encontrar soluciones", afirma Waberska. "Comprenden los riesgos y la necesidad de mitigarlos. La capacidad de la auditoría interna para mantener con ellos una conversación muy centrada en los riesgos explica por qué son necesarios determinados controles para que la auditoría interna sea mucho más eficaz."

### *Construir Relaciones Internas*

Todos los miembros de un equipo de auditoría interna pueden beneficiarse de entablar y mantener relaciones con otros profesionales de los equipos de seguridad, cumplimiento e IT de su organización para conocer su trabajo actual, aunque no estén colaborando en un proyecto concreto. "Entender lo que ocurre en el entorno de la empresa es muy importante", afirma Waberska, y estas relaciones pueden garantizar que el equipo reciba actualizaciones puntuales. Las auditorías específicas revelarán tendencias y amenazas, "pero es mejor saber lo que está cambiando lo antes posible", afirma.

### *Aprovechar los Recursos Disponibles*

"Si los equipos de auditoría interna dedican tiempo a aprender, al menos a un alto nivel, las tecnologías modernas y los riesgos que conllevan, se mantendrán al día de los riesgos actuales y emergentes", afirma Waberska. Las opciones incluyen el Centro de Recursos de Ciberseguridad del IIA, que incluye una variedad de orientación sobre ciberseguridad, investigación, programas de certificación e información sobre conferencias relacionadas, como la Conferencia Virtual de Ciberseguridad anual del IIA. AuditBoard también ofrece una amplia variedad de recursos de ciberseguridad, accesibles a través de su página de recursos.

Risk in Focus 2024, de la Fundación de Auditoría Interna, explora los riesgos de ciberseguridad a escala mundial y ofrece perspectivas regionales únicas sobre cómo se perciben y gestionan la ciberseguridad y otros riesgos importantes en todo el mundo.

# Conclusión

**La encuesta Pulse 2023 del IIA reveló que el crecimiento del personal de auditoría interna** está aumentando, pero que aún no ha vuelto a los niveles anteriores a la COVID. Los responsables de la auditoría interna deben recordar que las generaciones que se incorporan al mercado laboral son expertas en el mundo digital. Es inteligente considerar las mejores formas de utilizar los conocimientos que aportan, señaló Gulvadi. El área de auditoría interna también se diferenciará en un entorno de personal competitivo ofreciendo a una nueva generación la oportunidad de utilizar tecnologías emergentes como IA/ML para ofrecer conocimientos que ayuden a resolver problemas empresariales críticos. Mientras la auditoría interna sigue reconstruyendo equipos o ampliando su experiencia para asumir nuevos retos, debería utilizar los consejos y las ideas de este informe en su planificación.

# Parte 2: Inteligencia Artificial - Amiga y Enemiga de la Ciberseguridad

## Sobre los expertos

### Aneta Waberska, CISA

Aneta es Directora de Productos de Seguridad de la Información y Cumplimiento Normativo en AuditBoard. Cuenta con más de 15 años de experiencia en auditoría de TI y cumplimiento normativo, y se incorporó a AuditBoard para centrarse en el desarrollo de productos para usuarios de riesgos de TI y cumplimiento normativo, aprovechando su experiencia en el sector. Aneta comenzó su carrera en KPMG y PwC, donde ayudó a los clientes a implantar y evaluar marcos como SOC 1 y SOC 2. Ha trabajado con empresas de diferentes tamaños para implantar y gestionar programas de cumplimiento de diversa complejidad, incluida la gestión de políticas para toda la empresa, programas de gestión de riesgos de terceros, Ha colaborado estrechamente con la dirección en la implantación de controles para cumplir los requisitos del marco de seguridad, y ha trabajado con la dirección ejecutiva para garantizar que el cumplimiento respalda los objetivos estratégicos de la empresa.

### Terry Grafenstine, CIA, CPA, CISSP, CISA, CRISC, CGAP, CGEIT

Terry es la vicepresidenta senior 2023-24 de la Junta Directiva Mundial del Instituto de Auditores Internos (IIA) y directora ejecutiva de auditoría de Pentagon Federal Credit Union (PenFed). Ha sido reconocida por el IIA como uno de los "Diez principales líderes del pensamiento de auditoría de la década" por sus contribuciones a la profesión relacionadas con la cibernética y la tecnología, y también ha sido incluida en el Salón de Profesionales Distinguidos de Auditoría del IIA. Ha ocupado cargos directivos en Citi y Deloitte y ha sido nombrada Inspectora General de la Cámara de Representantes de los Estados Unidos.

# INTRODUCCIÓN

**La ciberseguridad es el principal riesgo para los auditores internos**, y así seguirá siendo en un futuro próximo. De hecho, es el único riesgo que les consume más tiempo y esfuerzo, según Risk In Focus 2024. En este informe, elaborado por la Fundación de Auditoría Interna del Instituto de Auditores Internos (IIA), se pregunta a directores y jefes de auditoría de todo el mundo cuáles son los principales riesgos a los que se enfrentan sus organizaciones y cómo prevén que cambie el panorama de las amenazas en los próximos tres años.

Las conclusiones de Risk in Focus 2024 demuestran la complejidad de la ciberseguridad como riesgo y los retos añadidos derivados de los cambios casi constantes en la tecnología y en la forma de utilizarla. Esto también se refleja en las conclusiones del informe. Los responsables de auditoría interna prevén que la amenaza de interrupción digital pase del quinto puesto actual al segundo dentro de tres años.

Este informe, el segundo de una serie de tres partes sobre ciberseguridad, examina cómo la inteligencia artificial (IA) contribuye a los retos y oportunidades de la ciberseguridad, y lo que los auditores internos necesitan saber sobre esta área de riesgo emergente y en evolución como una consideración de ciberseguridad. La IA es muy prometedora como herramienta sofisticada para mejorar la eficiencia, la productividad y la gestión de riesgos en prácticamente cualquier organización. Sin embargo, también presenta nuevos retos de gestión de riesgos, incluyendo consideraciones éticas, los peligros del sesgo algorítmico y la confianza excesiva o ciega en el uso de la IA. Aunque puede ser una herramienta valiosa en la batalla contra los ciberataques, los malos actores también la están utilizando para perpetrar sus delitos.

# La IA en el Trabajo

Ciber espada de doble filo

## La Auditoría Interna Debe Explorar los Usos y Amenazas de la IA

**El término inteligencia artificial se refiere a la tecnología que puede imitar la inteligencia humana**, como aprender, razonar y trabajar para resolver un problema difícil. Abarca varios tipos de tecnologías, incluido el aprendizaje automático, o la capacidad de un sistema para aprender de los datos y aplicar ese aprendizaje.

Según Aneta Waberska, directora de productos de seguridad de la información y cumplimiento normativo de AuditBoard, la IA y el aprendizaje automático pueden mejorar significativamente los esfuerzos de ciberseguridad en la detección de amenazas y el análisis de datos. Los ciberdelincuentes intentan infiltrarse en la red de una organización buscando puntos débiles y rompiendo las defensas de la red. En el pasado, las organizaciones confiaban en los administradores de sistemas para bloquear estas amenazas externas. Sin embargo, debido al avance de la automatización y otras tecnologías, el creciente volumen de entradas de malos actores ha desbordado la capacidad de revisión humana eficaz, dijo. La IA puede resolver este problema. Puede revisar grandes volúmenes de entradas en la red y reconocer patrones y aprender de ellos con el tiempo, comprendiendo si un determinado evento o grupo de eventos puede suponer una amenaza para una organización. "Este es uno de los usos más impactantes de la IA en este entorno", afirmó.

Además, las herramientas de detección de malware más sofisticadas tienen mejores capacidades, incluida la de bloquear una de las principales causas de brechas e incidentes de seguridad: el phishing. Esto puede reducir o eliminar la posibilidad de errores humanos -como abrir un enlace en un correo electrónico de phishing y exponer las redes de la empresa al malware- porque las herramientas los filtran antes de que lleguen a la bandeja de entrada de alguien, dijo Waberska. (Consulte la barra lateral para obtener más información sobre algunas de las formas en que la IA puede mejorar las defensas contra la ciberseguridad.)

La IA también puede buscar rápidamente anomalías e identificar problemas que ya se estén produciendo en la red de la organización, algo que los humanos no pueden hacer con datos a tan gran escala. El acceso no autorizado a los sistemas de la empresa es un ejemplo. Un antiguo empleado podría dar inadvertidamente el acceso disponible a un ciberdelincuente compartiendo o anotando una contraseña, o podría volver a entrar él mismo en el sistema con intenciones maliciosas. En el pasado, un auditor interno que buscara accesos no autorizados entre antiguos trabajadores habría tenido que realizar una comparación manual de las personas con acceso y las que ya no deberían tenerlo, y luego escribir un correo electrónico al equipo de IT detallando cualquier problema, señaló Terry Grafenstine, director ejecutivo de auditoría de Pentagon Federal Credit Union. La IA, en cambio,

### Utilizando la IA como Herramienta de Ciberseguridad

Según la IEEE Computer Society, algunas de las formas en que la IA puede mejorar las defensas de ciberseguridad de una organización incluyen:

- Detección de actividades maliciosas, mediante el benchmarking de actividades aceptables y la identificación de anomalías y amenazas de forma continua y en tiempo real.
- Apoyo a la identificación de amenazas de malware mediante el examen de las características de los archivos o patrones de código para detectar los no seguros.
- Mejorar la capacidad de una empresa para hacer frente a ataques de día cero u otras amenazas desconocidas.
- Mejorando la inteligencia sobre amenazas reuniendo información de seguridad procedente de diversas fuentes, buscando amenazas de forma proactiva y ayudando en la gestión de amenazas aligerando la carga de trabajo de los analistas de seguridad de la empresa. [6]

[6] "AI for Cybersecurity and Cybercrime: How Artificial Intelligence Is Battling Itself," Gaurav Belani, IEEE Computer Society, September 6, 2023.

puede buscar en varias plataformas, comparar los datos del sistema de nóminas y del sistema de acceso, y enviar un correo electrónico a los equipos correspondientes sobre cualquier anomalía.

Los auditores internos deben ser conscientes de que los objetivos de los ciberdelincuentes a menudo no son simplemente robar datos, sino infiltrarse y perturbar los sistemas modificando los datos, dijo Grafenstine. En el nivel más amplio, los malos actores de los estados-nación pueden manipular infraestructuras críticas, como el transporte, la energía nuclear, la banca y muchas otras, pero las consecuencias también pueden ser importantes para organizaciones de cualquier tamaño.

# Consideraciones en la Gestión de Riesgos

Ética, Parcialidad y Exceso de Confianza

## La auditoría Interna Puede Ayudar a las Organizaciones a Evitar los Escollos de la IA

**Además de sus numerosas ventajas**, la IA conlleva su propia lista de consideraciones de riesgo. Algunas de las amenazas son internas, pero pueden ser tan dañinas como los ciberataques.

### *Ética*

Muchas de las preocupaciones en este ámbito están relacionadas con la IA generativa y los grandes modelos lingüísticos que pueden utilizar los auditores internos para crear informes, escribir código y esbozar recomendaciones y análisis, entre otras posibilidades. Sin embargo, estas herramientas también plantean cuestiones éticas y de seguridad para las organizaciones. "Existe el riesgo de que los empleados consideren estas herramientas como un juego de salón o un juguete", afirma Grafenstine.

Los controles cibernéticos tradicionales utilizados en tecnologías anteriores también se aplican a estos sistemas, pero "las repercusiones de no hacerlo bien se magnifican", dijo. Entre otras cosas, como se verá con más detalle, los sistemas pueden proporcionar información sesgada, inexacta o completamente fabricada, dependiendo de cómo se les entrene. Grafenstine también señala las consecuencias costosas y potencialmente embarazosas para el negocio y la reputación de una empresa si utiliza un chatbot orientado al cliente que ha sido entrenado con datos de Internet mal obtenidos y las respuestas incorrectas del chatbot tienen un impacto negativo significativo en los clientes. Por estas razones, debe haber una revisión humana de cualquier cosa producida por un sistema de IA generativa cuando la organización no es completamente consciente de los datos con los que se ha entrenado. "La empresa debe ser la propietaria de las respuestas", afirma Grafenstine.

Aunque el uso de programas de IA generativa como ChatGPT se ha disparado desde que debutaron a finales de 2022, publicar información disponible públicamente en la IA generativa puede exponer datos de la empresa o del cliente e información personal identificable, al igual que podría hacerlo un incidente de piratería informática, y es una consideración de riesgo importante. Cuando los empleados publican consultas que incluyen información de la empresa en programas públicos de IA generativa, el programa retendrá esa información y potencialmente la utilizará para responder a otras consultas fuera de la organización, exponiéndola a la vista del público. Esto no sólo puede hacer pública la información confidencial, sino que los malos actores también pueden utilizar los detalles que descubren en la IA generativa disponible públicamente para ingeniárselas para entrar en los sistemas de la empresa, con phishing u otras herramientas, advirtió Grafenstine.

### *Excesiva Confianza Ciega en los Resultados de la IA*

Cualquier profesional es responsable en última instancia de las herramientas que utiliza y de la información que genera. Esto es especialmente cierto en el caso de los auditores internos, que podrían infringir sus propias normas si confían demasiado en datos o contenidos no validados. "Nos ganamos la vida siendo fiables", afirma Grafenstine.

### *Parcialidad Algorítmica*

Las máquinas se entrenan para aprender basándose en algoritmos específicos y la información que producen puede verse influida, intencionadamente o no, por esos algoritmos. Por ejemplo, los algoritmos pueden filtrar los currículos de mujeres que se utilizan en

una decisión de contratación si los empleados existentes en un determinado puesto son predominantemente hombres o pueden favorecer las solicitudes de hipotecas de compradores blancos si la mayoría de los titulares de hipotecas actuales son blancos. [7] "No pretenden ser malintencionados, pero los prejuicios están presentes", afirma Grafenstine.

[7] "For minorities, biased AI algorithms can damage almost every part of life," The Conversation, www.theconversation.com, August 24, 2023.

# Proteger la IA - y Protegerse Contra Ella

## Los Controles Internos Son Fundamentales

### Protección de la Integridad de los Sistemas de IA, Acceso

**La seguridad sobre la propia IA y la capacidad de utilizarla son otras consideraciones importantes** para las organizaciones y los auditores internos. Debe haber controles sobre quién puede acceder a los recursos de IA, cómo se protege la autoridad para cambiar el código y quién está autorizado a llevar información de un área de pruebas a producción. Como auditor interno, "quiero asegurarme de que puedo saber si se ha modificado un algoritmo de IA o si alguien puede interrumpirlo en mitad de un proceso y alterarlo", afirma Grafenstine. Los auditores internos también deben ser conscientes del alcance potencial de la interferencia. "Si puedo acceder a la IA de su empresa, no es sólo una transacción lo que puedo alterar", dijo. En lugar de eso, el malhechor puede acceder a todo el lago de datos o almacén de datos de una organización, o a cualquier otra cosa a la que la IA tenga acceso".

> "El mero hecho de que haya implantado una solución que aprovecha la IA no significa que ahora sea a prueba de balas,"
>
> Aneta Waberska
> AuditBoard

Al mismo tiempo, es importante ser consciente de que la IA está facilitando a los ciberdelincuentes la creación rápida de malware, la automatización de ataques y la mejora de la eficacia de sus estafas o ataques de ingeniería social mediante el uso de herramientas como la manipulación del aspecto facial (deepfakes), que alteran digitalmente vídeos o imágenes, y generadores de voz de IA para crear imágenes o mensajes falsos. "El panorama de las ciber amenazas es cada vez más peligroso, y la IA juega un papel importante en él", según un artículo de la IEEE Computer Society.[8]

Según Waberska, los auditores internos deben considerar la IA como una herramienta ofensiva y defensiva. "El mero hecho de haber implementado una solución que aprovecha la IA no significa que ahora se esté a prueba de balas", afirmó. Mientras que los ataques del pasado solían ser lanzados por un hacker contra una sola organización, la IA puede llevar a cabo ataques a una escala mucho mayor, golpeando a múltiples organizaciones. La IA puede mejorar el malware aprendiendo de programas anteriores y utilizar ese conocimiento para generar malware más fuerte y mejor, haciéndolo por sí misma sin necesidad de desarrolladores. "Si la IA está tratando de entrar en su organización, puede ser mucho más poderosa que su solución existente", dijo Waberska. Los auditores internos pueden asegurarse de que sus organizaciones comprenden esos riesgos y están preparadas para afrontarlos. El equipo de auditoría interna no puede implantar soluciones, pero puede mantener una conversación informada con el equipo de seguridad para ver si están teniendo en cuenta estas amenazas e implementando soluciones. "Las organizaciones tardarán tiempo en adoptar nuevas soluciones, pero es importante conocer las amenazas y tener un plan para defenderse", afirma Waberska.

### No Olvide el Elemento Humano

Mientras las organizaciones se preparan para protegerse de las ciber amenazas externas, los auditores internos deben tener presente el peligro que suponen las amenazas inadvertidas planteadas por su propio personal. Los intentos de phishing, por ejemplo, tienen éxito debido al error humano de no reconocer que un ciberdelincuente está intentando entrar en el sistema o en una contraseña

[8] "AI for Cybersecurity and Cybercrime: How Artificial Intelligence Is Battling Itself," Gaurav Belani, IEEE Computer Society Tech Trends, September 6, 2023.

importante u otros datos confidenciales. "Los auditores internos deben examinar cómo educa la organización a los usuarios sobre estas amenazas", afirma Waberska. En particular, es posible que los empleados no comprendan que los correos electrónicos de phishing han evolucionado. Mientras que antes era fácil detectar señales de alerta como faltas de ortografía o fuentes extrañas, la IA se está utilizando para escribir correos electrónicos de phishing que son mucho más sofisticados y realistas. "Parecen muy reales, y es mucho más fácil para los delincuentes generarlos", afirma.

# Conclusión

**La amenaza de ciberataques es una característica permanente de los negocios** en el mundo digital, y la IA y su uso en evolución presenta un giro nuevo y provocador en la batalla de la gestión de riesgos contra esa amenaza. Los auditores internos tienen un importante papel que desempeñar en:

- Garantizar que la dirección y los equipos clave son conscientes de los beneficios y peligros relacionados con la IA.
- Determinar y proporcionar recomendaciones sobre cómo la IA puede mejorar diversos esfuerzos de ciberseguridad dentro de la organización.
- Promover la concienciación sobre la necesidad de considerar defensas actualizadas contra las herramientas de ciberataque impulsadas por IA.
- Garantizar la comprensión y el uso de las tecnologías de IA por parte de la empresa.

La IA y las tecnologías afines pueden servir como recursos valiosos, pero no son una respuesta definitiva. "Los avances tecnológicos pueden ser magníficos siempre que se sepa cómo utilizarlos de forma inteligente y segura", afirma Waberska. "Siempre hay que utilizar el juicio profesional a la hora de considerar lo que se obtiene."

Recuerde también que, aunque ser conservador es una ventaja para los auditores internos, no deben ser "la oficina del no", dijo Grafenstine. Los auditores internos deben ofrecer un buen asesoramiento en materia de control y riesgos, incluida la información sobre el riesgo de no estar al día con la tecnología. "No adoptar la tecnología es un riesgo enorme, pero hay que hacerlo de forma meditada", dijo.

# Parte 3: Gestión de Riesgos de Ciberseguridad de Terceros

## Sobre los expertos

### Richard Marcus, CISA, CRISC, CISM, TPECS

Richard Marcus es Vicepresidente de Seguridad de la Información en AuditBoard, donde se centra en la seguridad de los productos, la infraestructura y la IT corporativa, así como en liderar las iniciativas de cumplimiento interno de AuditBoard. En este puesto, se ha convertido en un usuario avanzado de los productos de AuditBoard, aprovechando el sólido conjunto de funciones de la plataforma para satisfacer los casos de uso de auditoría, evaluación de riesgos y cumplimiento normativo.

### John A. Wheeler

John A. Wheeler es el fundador y consejero delegado de Wheelhouse Advisors, una empresa de asesoramiento a altos ejecutivos que ayuda a las empresas globales a lograr una mayor visibilidad y comprensión de los riesgos. Aprovecha su experiencia en gestión de riesgos, ciberseguridad, negocio digital, riesgo operativo y gestión integrada de riesgos para ofrecer orientación estratégica y soluciones tecnológicas a sus clientes.

# INTRODUCCIÓN

**El mundo está cada vez más interconectado, y la industria no es una excepción.** Hoy en día, casi todos los sectores empresariales importantes dependen en cierta medida de terceros. En generaciones anteriores, esto podría haber sido principalmente desde una perspectiva física, en la que una parte dependía de otra para obtener bienes o servicios. Aunque esto sigue siendo cierto, ahora la conexión entre las partes se ha entrelazado con el ámbito digital.

Naturalmente, aunque esta tendencia tiene muchas ventajas -sobre todo en cuanto a eficiencia, productividad y mejor cumplimiento de los compromisos de sostenibilidad-, también hay riesgos que deben tenerse en cuenta. Según la Encuesta mundial sobre gestión de riesgos de terceros 2022 de Deloitte, el 73 % de los encuestados tiene actualmente una dependencia de moderada a alta de terceros proveedores de servicios en la nube, y se espera que esta cifra aumente hasta el 88 % en los próximos años.[9] Sin embargo, para que estas relaciones tengan éxito, debe existir una confianza implícita entre las organizaciones en que los datos transferidos estarán lo más seguros posible frente a ciberataques, violaciones de datos u otros incidentes cibernéticos relacionados. Para ganarse esa confianza, las organizaciones deben contar con un programa específico y amplio de gestión de riesgos de terceros (TPRM, por sus siglas en inglés) que ejerza la debida diligencia a la hora de incorporar proveedores externos y los supervise continuamente a lo largo del ciclo de vida de la relación.

Sin embargo, lo cierto es que, con demasiada frecuencia, las empresas dan por sentada su confianza sin haber actuado primero con la debida diligencia. "Cualquier tercero -vendedor, proveedor de componentes de productos, socio o cliente- puede presentar nuevos riesgos cibernéticos para su organización", afirma Richard Marcus, Vicepresidente de Seguridad de la Información de AuditBoard. "La necesidad de una sólida gestión de riesgos de terceros ha ido creciendo con el tiempo, y muchas organizaciones no están al día."

Como parte final de esta serie de tres partes sobre ciberseguridad, este Informe Global de Conocimiento (Global Knowledge Brief) destacará la importancia que han adquirido los riesgos cibernéticos asociados a terceros y abordará dónde pueden encajar los auditores internos en la gestión de riesgos cibernéticos de terceros.

9. 2022 Global Third-Party Risk Management Survey, Deloitte, 2022, https://www.deloitte.com\content\dam\Deloitte\us\Documents\TPRM_Survey_Report_Interactive.pdf.

# Un Gran Reto

## Los Riesgos Cibernéticos Dominan el Debate Sobre la Gestión de Riesgos de Terceros

### Un riesgo en alza

**Un informe reciente de CyberRisk Alliance**, patrocinado por AuditBoard, encuestó a 209 responsables y ejecutivos de seguridad e IT, administradores de seguridad y profesionales del cumplimiento de Estados Unidos. La encuesta reveló lo vasto que se ha vuelto el riesgo cibernético de terceros. Los resultados de la encuesta incluyen:

- En promedio, las empresas utilizan 88 socios tercerizados (incluidos proveedores de software, proveedores de servicios informáticos, socios de servicios informáticos, socios comerciales, intermediarios, subcontratistas, fabricantes subcontratados, distribuidores, agentes y revendedores). Las cifras varían significativamente en función del tamaño de la organización: las empresas de 1 a 99 empleados utilizan una media de 16 socios, mientras que las de 10,000 o más empleados utilizan una media de 173 (véase el gráfico 1).
- El 57% de los encuestados declararon haber sido víctimas de un incidente de seguridad informática (un ataque o una infracción) en los últimos 24 meses. Además, las organizaciones experimentaron en promedio dos incidentes de seguridad relacionados con terceros en los últimos dos años.
- Entre los afectados, el 52% afirmó que el origen del ataque fue un proveedor de software, mientras que el 39% dijo que un socio comercial, subcontratista o proveedor de servicios informáticos fue el responsable del incidente (véase el gráfico 2)[10].

**Gráfico 1**

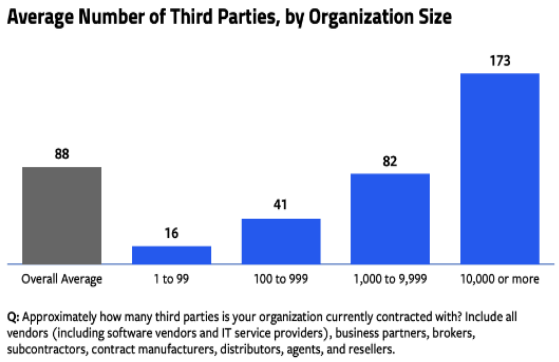
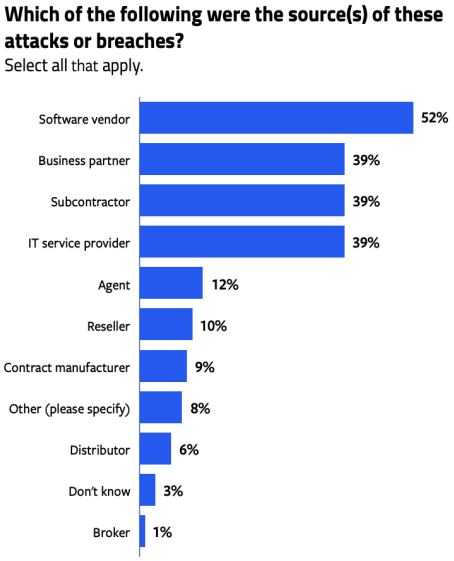



**Gráfico 2**




*Nota: Los gráficos y datos de las figuras 1 y 2 proceden de "Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations", de CyberRisk Alliance y Auditboard. p. 9 y p. 18, enero de 2023.*

10. "Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations," CyberRisk Alliance and AuditBoard, January 2023, https://www.auditboard.com/resources/ebook/third-party-risk-more-third-parties-limited-supply-chain-visibility-big-risks-for-organizations/.

## Mantenerse al Día con el Cambio

Según John Wheeler, fundador y Consejero Delegado de Wheelhouse Advisors, las razones principales de estos problemas son variadas, pero surgen de una combinación de modelos de negocio que cambian rápidamente y la incapacidad de actualizar los procesos de gestión de riesgos de terceros para adaptarse al cambio. Según mi experiencia", afirma Wheeler, "los riesgos mayores y más relevantes se generan por cambios importantes". El reto del crecimiento está impulsando grandes cambios al estimular a las empresas a crear nuevos productos y servicios digitales."

A este respecto, Wheeler es autor del "Informe sobre riesgos digitales 2023" de AuditBoard: Riesgo omnipresente, fragmentación persistente y aceleración de la inversión en tecnología". En una encuesta realizada a más de 130 líderes de riesgo de Estados Unidos, el 21% informó que no realiza una evaluación cualitativa o cuantitativa del riesgo al gestionar y supervisar el riesgo digital de terceros, y el 56% confía solo en los enfoques de evaluación cualitativa, que es limitada en comparación con las evaluaciones cuantitativas.[11]

44%

EL PORCENTAJE DE ORGANIZACIONES QUE RECURREN A TECNOLOGÍAS MANUALES PARA GESTIONAR LOS CIBER RIESGOS DE TERCEROS

AuditBoard 2023 Digital Risk Report
Pervasive Risk, Persistent Fragmentation, and Accelerating Technology Investment

Según Wheeler, resulta igualmente preocupante que, de las empresas que gestionan riesgos digitales como los ciber riesgos de terceros, un asombroso 44% sigue dependiendo de tecnologías manuales (hojas de cálculo, correo electrónico, unidades compartidas y Sharepoint) para hacerlo. "Es un enfoque que lleva mucho tiempo", afirmó. "La realidad es que el software anticuado (legacy) que es fragmentado, inflexible y orientado al cumplimiento de gobernanza, GRC [gobernanza, riesgo y cumplimiento] simplemente no puede proporcionar las capacidades conectadas de riesgo necesarias para seguir el ritmo del riesgo digital - y como resultado, la mayoría de las organizaciones todavía dependen de procesos manuales fragmentados."

Esto es especialmente preocupante en lo que respecta a los cambiantes patrones de ataque de los malos actores, que cada día son más sofisticados. "Si nos fijamos en las causas profundas de los ataques de las últimas décadas, la mayoría se han producido en la puerta principal, en los niveles de aplicación o infraestructura. Ahí es donde los equipos de seguridad han invertido su tiempo y sus recursos. Pero los atacantes son listos. Van a buscar el camino de menor resistencia, y la mayoría de las veces va a ser a través de las puertas traseras causadas por lagunas en las medidas de ciberseguridad de terceros", dijo Marcus.

## Presiones Regulatorias

También contribuye a la presión que sienten las organizaciones en torno a los riesgos cibernéticos de terceros el siempre cambiante panorama normativo, que recientemente ha acelerado su ritmo para equipararse a la velocidad del riesgo. Entre estos cambios se incluyen los nuevos mandatos que el gobierno federal de EE. UU. está imponiendo a sus socios de la cadena de suministro, lo que ha tenido efectos indirectos en múltiples sectores. "Se podría pensar que los mandatos federales para una mayor transparencia en materia de seguridad de los datos sólo afectarían a las empresas que hacen negocios con el gobierno federal, pero luego hay requisitos de terceras y cuartas partes que fluyen por la cadena de suministro y se extienden en cascada a través de la jerarquía o los proveedores de servicios", dijo Marcus. "Eso crea una cultura de responsabilidad que impregna muchas industrias."

Los organismos reguladores también han empezado a tomar medidas más formales para abordar los riesgos de ciberseguridad de terceros. Esto incluiría las nuevas normas promulgadas recientemente por la Comisión del Mercado de Valores de Estados Unidos (SEC), como las nuevas normas que exigen a las empresas registradas revelar los incidentes materiales de ciberseguridad. "Incluso si

11. "Digital Risk Report 2023: Pervasive Risk, Persistent Fragmentation, and Accelerating Technology Investment," John A. Wheeler, Auditboard, July, 2023, https://www.auditboard.com/resources/ebook/digital-risk-report-2023/.

su empresa no es directamente aplicable a las nuevas normas o reglamentos, estas normas impregnan la cultura de la ciberseguridad", dijo Marcus.  Es un cambio cultural que está creando una expectativa de transparencia y responsabilidad."

## Establecer una cultura de ciber acción

**Las organizaciones no ignoran estas deficiencias.** De hecho, la mayoría son conscientes de ellas de alguna manera, incluso si esa conciencia no siempre se traduce en la comprensión y la acción de toda la organización. Aunque pocas funciones de auditoría interna pueden presumir de tener conocimientos de ciberseguridad adecuados para abordar directamente los aspectos técnicos de la ciberseguridad de terceros, lo que sí pueden hacer es aprovechar su posición única para aunar los puntos de vista de las distintas partes interesadas que intervienen en la gestión de este riesgo (por ejemplo, los departamentos jurídicos, de compras, de IT y los propios terceros). Además, los auditores internos pueden utilizar su interacción directa con el comité de auditoría y el consejo para asegurarse de que este punto de vista se comunica con regularidad y precisión.

Este punto de vista es extremadamente crítico para los CEO y los líderes de la organización para impulsar la acción apropiada, dijo Wheeler, y es algo que las funciones de gestión de riesgos deben hacer un esfuerzo para entender lo suficiente como para articular. "Los CEO necesitan información en tiempo real tanto dentro como de fuera de la organización, a través de todo el ecosistema de activos tecnológicos que cambian dinámicamente", afirmó. "A través de este proceso, tendrán una mejor comprensión de sus productos y servicios digitales."

Sin embargo, la unidad dentro de la organización no es suficiente. Debe incluir a las partes interesadas de fuera de la organización. "Cada relación con terceros debe tener un propietario designado o una persona responsable del mantenimiento de la relación con el proveedor, de la información de contacto del proveedor y de la gestión de los términos del contrato", afirma Marcus. "Las relaciones con terceros difieren de un proveedor a otro: algunos pueden proporcionar a su organización un equipo designado de atención al cliente que preste servicios complementarios, mientras que otros adoptan un enfoque 'off-the-shelf' (enfoque estándar). Mantener las líneas de comunicación abiertas y claras entre su organización y sus terceros es un componente importante, pero a menudo pasado por alto, de la gestión eficaz del riesgo de terceros."

La creación de una cultura de este tipo no sólo puede estimular la acción preventiva, sino que también puede aumentar la velocidad de reacción cuando se produce un ciberataque o una brecha. En el informe de la CyberRrisk Alliance, el 20% de los encuestados afirmaron que podían tardar una semana o más en evaluar un ataque o una brecha, y atribuyeron la prolongación del plazo a las dificultades para conseguir que los proveedores o socios informaran o asumieran la responsabilidad.[12] La creación de una cultura cibernética positiva y transparente dentro de la organización y en toda su cadena de suministro puede reducir estos tiempos de una semana a horas, disminuyendo drásticamente las pérdidas en el proceso.

"Todo el proceso de gestión de riesgos de terceros", dijo Marcus, "debe construirse en torno a una cultura de responsabilidad en la que todo el mundo sea consciente de los riesgos de terceros."

## Un enfoque de supervisión continua basado en el nivel de riesgo

Más allá de marcar la pauta, la auditoría interna puede y debe actuar como un recurso valioso en la elaboración del programa de gestión de riesgos de terceros en lo que respecta a los riesgos cibernéticos, y evaluarlo continuamente.

12. "Third-Party Risk: More Third Parties + Limited Supply-Chain Visibility = Big Risks for Organizations," CyberRisk Alliance and AuditBoard, February, 2023, https://www.auditboard.com/resources/ebook/third-party-risk-more-third-parties-limited-supply-chain-visibility-big-risks-for-organizations/.

"Yo diría que la principal responsabilidad de la auditoría interna, como en la mayoría de los casos, es evaluar la eficacia del programa de gestión de riesgos de terceros (TPRM)", afirma Marcus. Esto puede incluir un inventario completo o una imagen de todos los terceros que se utilizan en la organización, la comprensión de los riesgos a los que esos terceros pueden exponer a la organización, y la comprensión de cómo la organización está evaluando la solidez de los controles en esas organizaciones de terceros."

Una vez más, aunque se debe recurrir a expertos en la materia para el análisis técnico, muchos de los principios de gestión de riesgos utilizados por la auditoría interna son aplicables a este tema.

Por ejemplo, la auditoría interna debe tener una comprensión firme del análisis de riesgos, a menudo visualizado mediante herramientas de representación de data (Heat maps en Ingles) u otras herramientas. Estas tácticas pueden servir de guía a las partes interesadas responsables de la incorporación y supervisión de terceros para comprender mejor a quién y a qué dar prioridad.

"El factor de éxito más importante para un programa TPRM es estructurar y formalizar las actividades de supervisión continua en función del nivel de riesgo", afirma Marcus. "Los terceros de mayor riesgo deben recibir más atención con más frecuencia, y los de menor riesgo deben recibir menos atención con menos frecuencia". Hay que tener en cuenta, continúa, que, aunque el tercero en cuestión puede no ser de alto riesgo en sí mismo, la naturaleza de la relación -como qué tipo de datos se transfieren (por ejemplo, datos confidenciales, datos de clientes, datos de propiedad) - podría elevar o bajar la categorización de riesgo.

Para ayudar en esta tarea, AuditBoard utiliza el siguiente ejemplo (Gráfico 3) como punto de partida sobre cómo estructurar las revisiones relacionadas con las tres categorías de niveles de riesgo siguientes:[13]

## Gráfico 3

| Risk Tier Characteristic | Tier 1 – High Risk | Tier 2 – Medium Risk | Tier 3 – Low Risk |
|---|---|---|---|
| Data Access | Confidential | Proprietary | Public or None |
| Review Frequency | 1 Year | 2 Years | 3 Years |
| Review Requirements | Onsite Audit<br>Controls Questionnaire<br>Certification Review | Certification Review | None |

*Nota: Los gráficos y datos de las figuras 1 y 2 proceden de "Effective Third-Pary Risk Management: Key Tactics and Success Factors" de AuditBoard. p. 8, 2022.*

La investigación de terceros no termina con su incorporación, sino que debe revisarse continuamente en función del nivel de riesgo percibido. Garantizar que las partes interesadas se mantengan al corriente de sus propios compromisos en materia de revisiones periódicas, así como de los procesos que utilizan para llevar a cabo dichas revisiones, debería entrar de lleno en el universo de riesgos de la auditoría interna. Las ideas para tales procesos podrían incluir:

- Comprobación de certificaciones e informes de conformidad, como SOC 2. Los marcos comunes para comprobar las certificaciones de cumplimiento incluyen SOC 2, ISO 27001, y NIST SP 800-161.

13. "Effective Third-Party Risk Management: Key Tactics and Success Factors," AuditBoard, January, 2022, https://www.auditboard.com/resources/ebook/effective-third-party-risk-management-key-tactics-and-success-factors/?utm_campaign=effective-third-party-risk-management-key-tactics-and-success-factors-0122022&utm_medium=download-image&utm_source=blog.

- Uso de cuestionarios estandarizados. Por ejemplo, el Cuestionario Normalizado de Recopilación de Información (SIG) o el CCM y el CAIQ de la Cloud Security Alliance.
- Cuestionarios sobre controles de seguridad.

## Adoptar Soluciones de Software

Para mantener unidas tantas variables, la auditoría interna, así como otras funciones de gestión de riesgos, también deberían dar prioridad al abandono de los procesos manuales en favor de soluciones de software. "La auditoría interna puede abogar por la inversión en tecnologías que hagan más eficientes los procesos de gestión de riesgos de terceros", afirma Marcus. "En muchas situaciones, las eficiencias de escala simplemente lo requieren. Recuerdo una de las primeras organizaciones en las que implementé prácticas de riesgo de terceros: realizamos evaluaciones de riesgo para cinco o seis proveedores y luego consideramos ampliar este proceso a todos los proveedores. Sin embargo, nos sorprendió descubrir que había 17,000 proveedores en esta empresa. No hay forma de hacerlo sin una plataforma tecnológica que facilite la ampliación a cientos, miles o decenas de miles de proveedores."

Además, estas soluciones también presentan una excelente oportunidad para que la auditoría interna colabore más estrechamente con otras funciones de riesgo de terceros. "Muchos de los obstáculos a la colaboración tienen que ver con el intercambio de datos y los problemas de flujo de trabajo", afirma Marcus. Disponer de una plataforma tecnológica en la que los dos equipos puedan evaluar juntos el panorama de los proveedores -utilizando el mismo cuadro de mandos, la misma base de datos de proveedores, etc.- les permite trabajar juntos de forma mucho más eficiente y avanzar hacia resultados comunes".

## Enfocarse tanto en la incorporación como en la salida

Las relaciones con terceros rara vez duran para siempre. Sin embargo, el hecho de que una relación termine formalmente no siempre significa que las líneas de datos entre las partes se cierren. Por obvio que parezca, estas líneas olvidadas son responsables de algunas de las mayores lagunas encontradas en los sistemas de ciberseguridad de terceros de las organizaciones, creando "puertas traseras digitales" que están maduras para ser explotadas intencionada o involuntariamente. Al evaluar las prácticas de revisión de terceros, esto es algo que la auditoría interna no debe pasar por alto.

"Es esencial ser detallista en la fase de baja", afirma Marcus. "En el entrelazado ecosistema digital actual, es fácil pasar por alto cuentas, servicios o usuarios de terceros que deben eliminarse o desactivarse. Es necesario revocar los privilegios de acceso, desactivar las cuentas de usuario y eliminar cualquier software o aplicación de terceros. Esto es algo que la auditoría interna debería tener absolutamente en cuenta."

# Conclusión

**El futuro de las organizaciones es cibernético.** Cada año que pasa, está claro que esta tendencia ha llegado para quedarse, y el hecho de que la ciberseguridad requiera conjuntos de habilidades más especializados no significa que el panorama empresarial vaya a esperar a que las partes interesadas se eduquen a sí mismas. La ciberseguridad es un viaje continuo de aprendizaje, y todas las partes implicadas en las relaciones con terceros deben considerarlo como tal.

Afortunadamente, hay indicios positivos de que las organizaciones están aceptando esta realidad. En el informe CyberRisk Alliance Business Intelligence, casi dos de cada tres encuestados afirmaron que la medida más común que utilizaban para prevenir o mitigar el riesgo de ataques de terceros era la formación de los empleados. Aunque los riesgos asociados a terceros nunca terminarán, las políticas y respuestas madurarán hasta el punto en que sean tan fáciles de gestionar como cualquier otro riesgo establecido. Ese momento no es hoy, pero estamos llegando a él, y una garantía eficaz de gestión de riesgos de auditoría interna ayudará a las organizaciones a llegar a llegar a salvo.

## Acerca del IIA

El Instituto de Auditores Internos (IIA) es una asociación profesional internacional sin ánimo de lucro que cuenta con más de 235.000 miembros en todo el mundo y ha concedido más de 190.000 certificaciones de Auditor Interno Certificado (CIA) en todo el mundo. Fundado en 1941, el IIA es reconocido en todo el mundo como el líder de la profesión de auditoría interna en normas, certificaciones, educación, investigación y orientación técnica. Para más información, visite theiia.org.

## Disclaimer

En la Parte III: El papel de la auditoría interna en la ética de la IA, los puntos de vista y opiniones expresados son ofrecidos por los expertos a título personal y no reflejan los puntos de vista y opiniones de Cboe Global Markets, Inc. y sus filiales.

El IIA publica este documento únicamente con fines informativos y educativos. Este material no pretende ofrecer respuestas definitivas a circunstancias individuales específicas y, como tal, sólo está destinado a ser utilizado como liderazgo de pensamiento informado por pares. No constituye una guía formal del IIA. El IIA recomienda buscar asesoramiento experto independiente en relación directa con cualquier situación específica. El IIA no acepta ninguna responsabilidad por cualquier persona que confíe exclusivamente en este material.

Los Resúmenes de Conocimientos Globales pretenden abordar temas que son oportunos y relevantes para una audiencia global de auditoría interna, y cada tema cubierto es revisado por miembros del Comité Asesor de Contenido Norteamericano voluntario del IIA. Los expertos en la materia se identifican y seleccionan principalmente a partir de la lista de colaboradores de Global Guidance del IIA.

Para solicitar su inclusión en la lista de colaboradores de Global Guidance, envíe un correo electrónico a Standards@theiia.org. Para sugerir temas para futuras Síntesis de Conocimiento Global, envíe un correo electrónico a Content@theiia.org.

## Copyright



Enero 2024

Traductora: Andrea Correa (servicios contratados), revisor: Roberto Loo, control de calidad

Traducción al Español Auspiciada por:
FLAI
Fundación Latinoamericana de Auditores Internos

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101