TONE at the TOP®

Proporcionar a la alta dirección, juntas directivas y comités de auditoría, información concisa sobre temas relacionados con la gobernanza.

Edición 125 | Octubre 2024

El Papel de la Junta en la Resiliencia Cibernética

¿Tu empresa está preparada para el próximo ciberataque? La mayoría de las organizaciones esperan uno en su futuro, y el 73% de los líderes empresariales y de ciberseguridad predicen que un incidente cibernético interrumpirá su negocio en los próximos 12 a 24 meses, según el **Índice de Preparación en Ciberseguridad 2024 de Cisco.**

Hay muchas consecuencias potenciales de un ciberataque, incluida la vulneración de datos confidenciales, la interrupción de las operaciones y el daño a las relaciones con terceros y a la reputación de la empresa. En el informe **Risk in Focus 2025** del IIA, los líderes de auditoría interna otorgan a la ciberseguridad las calificaciones de riesgo más altas por un amplio margen. También la citan como el área a la que la auditoría interna dedica más tiempo y esfuerzo.

Según el informe, la ciberseguridad sigue siendo el principal riesgo al que los líderes esperan que sus organizaciones se enfrenten dentro de tres años, con la disrupción digital (incluida la inteligencia artificial (IA)), creciendo rápidamente desde donde se encontraba en encuestas anteriores para ocupar el segundo lugar. "La IA está aumentando los riesgos de ciberseguridad y de fraude en todo el mundo", dice el informe. La ciberseguridad fue calificada como la principal área en la que la IA tendría el impacto más negativo.

En un entorno en el que la cuestión no es si se producirá un ataque, sino cuándo, la resiliencia cibernética es fundamental para ayudar a las empresas a afrontar un incidente. Las empresas pueden hacer grandes esfuerzos para protegerse contra los ciberataques, pero también deben estar preparadas para responder y recuperarse de dichos ataques.

La resiliencia cibernética es "la capacidad de anticipar, resistir, recuperarse y adaptarse a condiciones adversas, estrés, ataques o compromisos en los sistemas que usan o dependen por recursos cibernéticos. La resiliencia cibernética tiene como objetivo permitir que los objetivos de la misión o el negocio que dependen de los recursos cibernéticos se alcancen, en un entorno cibernético hostil". — Instituto Nacional de Estándares y Tecnología.

Nuevas Expectativas para los Consejos de Administración

Los reguladores y los accionistas están examinando la responsabilidad de la junta en materia de ciberseguridad y desarrollando nuevas expectativas para la supervisión de las vulnerabilidades de sus organizaciones por parte de los directores. A partir de una norma finalizada, **Gestión de Riesgos de Ciberseguridad, Estrategia, Gobernanza y Divulgación de Incidentes**, la Comisión de Bolsa y Valores de EE. UU. establece las divulgaciones necesarias para empresas públicas, abordando específicamente la divulgación de incidentes importantes de ciberseguridad y divulgaciones periódicas sobre cómo las entidades registradas evalúan, identifican y gestionan estos riesgos, así como el papel de la dirección en la evaluación y gestión de los mismos. Las reglas finales también requieren divulgaciones sobre la supervisión de los riesgos de ciberseguridad por parte de las juntas directivas.

Como parte de su función de supervisión, las juntas directivas deben asegurarse de que los ejecutivos y sus equipos establezcan un alto estándar de ciberseguridad, según un artículo de McKinsey, **"Consejos de Administración: La defensa final de ciberseguridad para las industrias".** Luego, ellos deberían supervisar los esfuerzos de ciberseguridad, determinando si se han alcanzado los objetivos y si los equipos están asumiendo la responsabilidad de la ciberseguridad. "La junta es la última línea de defensa para garantizar que tales iniciativas se planifiquen y financien", señala el artículo.

Un ciberataque está diseñado para dificultar que las organizaciones continúen con sus negocios como de costumbre. La resiliencia cibernética consiste en estar informado y preparado, de modo que las opciones y prioridades estén claras cuando se produzca una crisis. Para asegurarse de que sus organizaciones estén bien preparadas, las juntas directivas deben determinar si hay planes documentados de gestión de crisis, respuesta a incidentes y recuperación ante desastres, que la gerencia prueba periódicamente en ejercicios prácticos, según el informe de PwC **Supervisando el Riesgo Cibernético: El Papel del Consejo de Administración.** Los ejercicios deben centrarse en el establecimiento de funciones y responsabilidades claras para facilitar la toma de decisiones de la dirección durante una crisis.

Muchas juntas directivas reciben un cuadro de mando cibernético o un panel de control de la dirección que destaca los riesgos actuales y el progreso en los objetivos de ciberseguridad. PwC señala varias áreas que podrían formar parte de un informe a la junta:

- *Un plan estratégico plurianual y un plan de negocios para el año en curso.*
- *Detalles sobre la asignación de recursos de ciberseguridad desglosados por financiación y personal.*
- *Una evaluación de madurez medida en función de un marco reconocido, como el Marco de* **Ciberseguridad del NIST.**
- *Un inventario actualizado periódicamente de los sistemas críticos para la misión.*
- *Un resumen de los principales riesgos cibernéticos para la organización.*
- *Una revisión de los incidentes de seguridad significativos que la organización ha experimentado.*
- *Información sobre los esfuerzos de capacitación y concienciación de los empleados.*
- *Detalles sobre el marco de preparación para incidentes de la organización, incluida información sobre la póliza de seguro cibernético.*
- *Detalles sobre la estrategia de riesgo cibernético de terceros.*
- *Información que compara los esfuerzos de la organización con los de sus pares.*
- *Detalles sobre los principales desarrollos legales y regulatorios relacionados.*
- *Lecciones que se pueden aprender de ciberataques recientes.*

Si bien proteger a la organización de los ataques es fundamental, las juntas deben recordar que la protección por sí sola puede abordar únicamente los problemas que la organización ya conoce. Desafortunadamente, armados con herramientas tecnológicas emergentes que utilizan IA, los ciberdelincuentes innovadores desarrollan continuamente nuevas formas de causar daño. Como resultado, "para mitigar adecuadamente el riesgo cibernético, los líderes de la empresa deben contar con planes sólidos para responder y recuperarse rápidamente, para que la empresa pueda continuar operando", informa el artículo de MIT News, **"Ahora las Juntas Corporativas también tienen Responsabilidad de la Ciberseguridad".**

Sobre IIA

El Instituto de Auditores Internos (IIA) es una asociación profesional internacional sin fines de lucro que presta servicios a más de 245,000 miembros globales y ha otorgado más de 200,000 certificaciones de Auditor Interno Certificado (CIA) en todo el mundo. Establecido en 1941, el IIA es reconocido globalmente como líder de la profesión de auditoría interna en estándares, certificaciones, educación, investigación y orientación técnica. Para más información, visite: **theiia.org.**

El IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 USA

Suscripciones Complementarias

Visite **theiia.org/Tone** para registrarse y acceder a la suscripción.

Feedback del Lector

Envíe sus preguntas/comentarios a: Tone@theiia.org.

Auditoría Interna: Un Socio Fiable en Ciberseguridad

Los consejos de administración deben ser conscientes del valor que las funciones de auditoría interna pueden aportar a los esfuerzos de ciberseguridad. La auditoría interna proporciona servicios de aseguramiento y asesoramiento únicos, objetivos e independientes sobre la estrategia, la gobernanza y los controles de ciberseguridad. "Muchas empresas aprovechan a los auditores internos para revisar los procesos y controles cibernéticos, incluida la resiliencia y la respuesta", señala el artículo de PwC.

Las funciones de auditoría interna pueden contribuir a los esfuerzos de resiliencia cibernética de varias maneras, incluso a través de una auditoría de recuperación y respuesta a incidentes cibernéticos. El informe Risk in Focus del año pasado expone algunos de los valores que los auditores internos pueden agregar, y la lista sigue siendo válida hoy en día:

- Evalúe el nivel de concienciación, conocimiento y habilidades en las áreas clave del negocio, incluida la junta directiva, para garantizar que las respuestas de defensa cibernética sean relevantes y estén actualizadas.
- Evalúe las líneas de reporte entre el director de seguridad de la información, el director de información y la junta directiva para garantizar una comunicación clara de los riesgos y las recomendaciones, y que puedan escalarse al nivel más alto cuando sea necesario.
- Evalúe la frecuencia, la puntualidad y la eficacia de las campañas de pruebas simuladas de phishing y otras actividades de concienciación, así como el nivel de compromiso del personal y su grado de integración con los procesos de capacitación y seguimiento.
- Utilice simulacros de escenarios para educar a la junta directiva sobre sus responsabilidades de gobernanza y para probar que los procesos de mitigación estén completos y sean efectivos.
- Evalúe la efectividad del entorno de control interno y qué tan bien se integran los controles en la primera y segunda línea de acuerdo con el Modelo de **Las Tres Líneas del IIA**, prestando especial atención a las prácticas que el personal considera disruptivas o intrusivas y que probablemente ignore, olvide o eluda.
- Evalúe cómo la estructura de gobernanza de la organización facilita la colaboración entre las tres líneas.
- Determine cuán bien la organización monitorea los desarrollos globales en las regulaciones de ciberseguridad y tecnología y la facilidad con la que los controles internos se pueden cambiar para cumplir con los requisitos futuros.

Un Riesgo en Expansión y Evolución

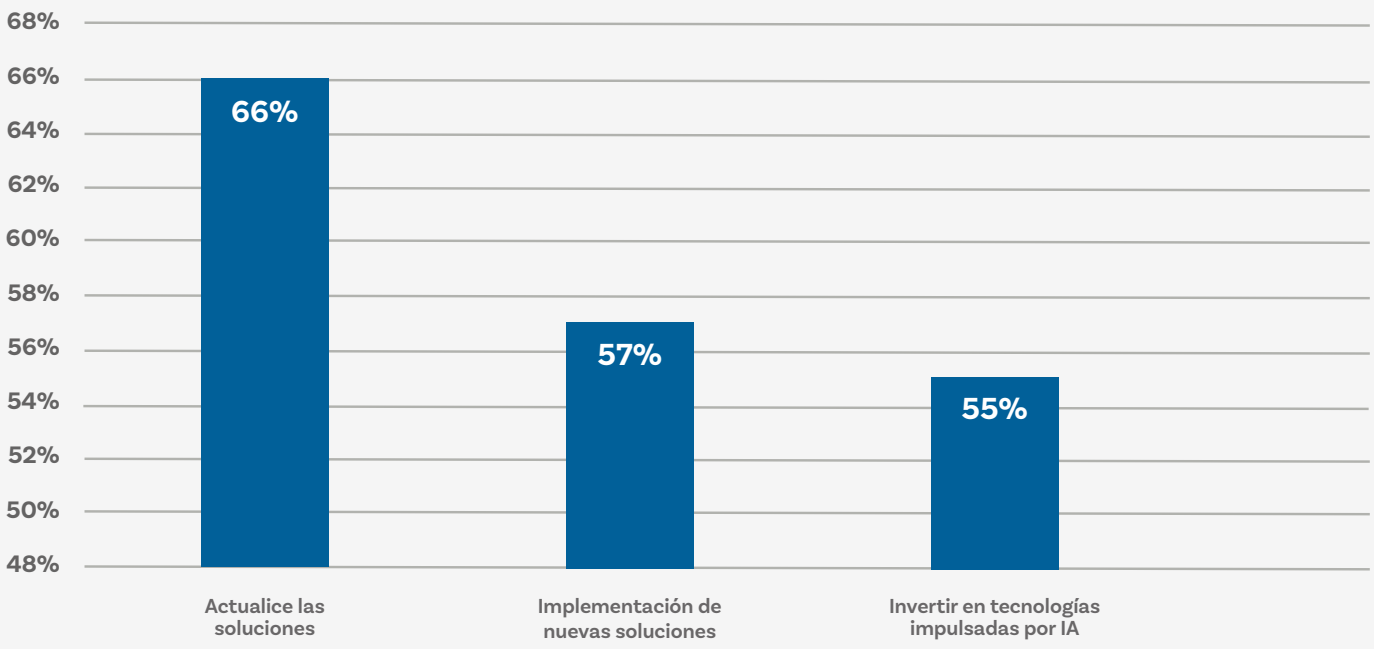
A medida que las nuevas tecnologías evolucionan rápidamente, muchas herramientas emergentes están haciendo que los ciberataques sean aún más fáciles de llevar a cabo. Aunque la IA y herramientas similares pueden mejorar los esfuerzos de ciberseguridad, también pueden simplificar el phishing y el spam, el chantaje y el terrorismo, y la desinformación y la interferencia electoral, según Jen Easterly, directora de la Agencia de Seguridad Cibernética y Seguridad de Infraestructura del gobierno federal. También **señala,** que la IA generativa está proporcionando a los atacantes cibernéticos nuevas oportunidades y permitiendo que los ciberdelincuentes menos sofisticados causen estragos.

Los miembros de la junta deben dirigirse a sus equipos de auditoría interna para obtener información y asesoramiento cruciales sobre la mejor manera de prevenir los ciberataques y evaluar la agilidad de sus respuestas una vez que se han producido. Los auditores internos pueden ofrecer evaluaciones independientes del entorno de control y cualquier riesgo identificado, lo que puede ayudar a que la organización se recupere de la mejor manera de un ataque.

PREGUNTAS PARA LOS MIEMBROS DE LA JUNTA

- ¿Cómo monitoreamos las nuevas amenazas cibernéticas, incluida la forma en que otras organizaciones han respondido a ellas?
- ¿Cómo mide y evalúa la organización su propia resiliencia cibernética?
- ¿Cómo utilizamos esta información para adaptar nuestra preparación para un ataque y nuestras posibles respuestas?
- ¿Cuáles son nuestros planes de recuperación ante desastres? ¿Qué tan bien han funcionado en el pasado? ¿Qué hemos aprendido de esas experiencias?
- ¿Qué funciones tienen responsabilidad directa en las estrategias de ciberresiliencia?
- ¿Todos los empleados comprenden la necesidad de la resiliencia cibernética y el papel que pueden desempeñar en ella?

¿Cómo están mejorando las empresas su seguridad cibernética?



Fuente: 2024 Cisco Cybersecurity Readiness Index.

El presente documento fue traducido al español por el IAI ECUADOR el 12/11/2024.