TONE at the TOP®

Proveemos información concisa sobre temas relacionados con Gobierno a la Alta Dirección, Juntas Directivas y Comités de Auditoría.

Edición 113 | Octubre 2022

Mitigación de Amenazas Cibernéticas

La ciberseguridad se ha convertido en un elemento permanente en el panorama de riesgo moderno, y las juntas se enfrentan a una presión cada vez mayor para brindar una supervisión adecuada de una amenaza que es multifacética y está en constante evolución. Un total del 70 % de los directores de juntas calificaron la seguridad cibernética como "un riesgo empresarial estratégico" en una Encuesta de la Junta Directiva de la NACD[1]. Una amplia gama de temas se encuentra bajo el paraguas de la seguridad cibernética — todas son preocupaciones críticas, incluida la protección de la privacidad; ransomware, malware y ataques de denegación de servicio o phishing; políticas de ciberseguridad inadecuadas; y planes de recuperación y respuesta a incidentes, por nombrar algunos.

Las organizaciones también se enfrentan a nuevas regulaciones que les obligan a informar sobre las infracciones que han experimentado. La Ley de Informes de Incidentes Cibernéticos para Infraestructura Crítica[2], por ejemplo, requiere informes que permitan a la Agencia Federal de Seguridad de Infraestructura y Ciberseguridad brindar asistencia a las víctimas durante los ataques cibernéticos, identificar tendencias y compartir información con otras posibles víctimas. La Comisión de Bolsa y Valores también ha propuesto regulaciones[3] que estandarizarían las divulgaciones relacionadas con la gestión de riesgos de ciberseguridad, la estrategia, la gobernanza y los informes de incidentes de las empresas públicas.

La auditoría interna, que brinda a las organizaciones aseguramiento y asesoramiento independientes y objetivos, puede ser un recurso poderoso para que las juntas aborden los riesgos cibernéticos. Según un informe de PwC[4], "muchas empresas aprovechan la auditoría interna para revisar los procesos y controles cibernéticos, incluida la resiliencia y la respuesta."

Pasos para mejorar la seguridad

A medida que las juntas consideran las amenazas de seguridad cibernética que enfrentan, hay una serie de áreas en las que la auditoría interna puede marcar la diferencia.

Reconociendo el riesgo. Las amenazas cibernéticas se han movido a la cima de las clasificaciones de riesgo de las empresas. "La creciente sofisticación y variedad de los ataques cibernéticos continúan causando estragos en las marcas y reputaciones de las organizaciones, lo que a menudo genera impactos financieros desastrosos", según OnRisk 2022[5] del Instituto de Auditores Internos (IIA). El informe, que se basa en entrevistas con miembros de la junta, altos ejecutivos y directores ejecutivos de auditoría (DEA), identificó la ciberseguridad como el principal riesgo este año.

Desafortunadamente, es posible que algunos líderes de la empresa no reconozcan completamente la amenaza. En el informe OnRisk, de particular preocupación fue la brecha entre la relevancia del riesgo asignada a la seguridad cibernética por los DEA, los miembros de la junta y la gerencia ejecutiva. Mientras el 97 % de los DEA calificó la ciberseguridad como un riesgo muy relevante para su organización (calificándola con 6 o 7 en una escala de 7 puntos), solo el 87 % de los miembros de la junta lo hicieron y solo el 77 % de los directores ejecutivos.

La fuerte calificación de relevancia entre los DEA sugiere su alto nivel de conciencia sobre los problemas de ciberseguridad. Eso no es sorprendente, dado el conocimiento holístico de auditoría interna de una organización. A medida que las juntas buscan aprovechar y mejorar el aseguramiento de riesgos más allá de los riesgos financieros y de cumplimiento, pueden recurrir a la auditoría interna para ayudar a describir las preocupaciones de seguridad cibernética y cuantificar su impacto potencial. Esto puede incluir detectar fallas en la cobertura de riesgos, monitorear los riesgos emergentes y hacer el mejor uso de las herramientas tecnológicas en los esfuerzos de seguridad cibernética.

Aprovechando el Valor del Modelo de tres líneas. El Modelo de las Tres Líneas del IIA[6] permite a las organizaciones identificar las estructuras y los procesos que mejor ayudan al logro de los objetivos y que facilitan una gobernanza sólida y la gestión de riesgos, incluida la ciberseguridad. El Modelo de las Tres Líneas identifica los roles clave desempeñados por:

About The IIA

El Instituto de Auditores Internos Inc. (IAI) es una asociación profesional mundial con más de 210 000 miembros en más de 170 países y territorios. El IAI actúa como principal defensor de la profesión de auditoría interna, emisor de estándares internacionales y principal investigador y educador.

El IIA

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

Suscripciones a Disposición

Visite theiia.org/Tone para registrarse a suscripciones complementarias.

Comentarios de los Lectores

Envíe sus preguntas y/o comentarios a: tone@theiia.org.

- El órgano de gobierno, que es responsable ante las partes interesadas de la supervisión de la organización.
- La administración, que actúa para lograr los objetivos de la organización.
- La auditoría interna, que proporciona un aseguramiento independiente y objetivo sobre el logro de dichos objetivos.

La investigación ha demostrado que la cooperación entre las tres líneas tiene un impacto positivo en la eficacia de la gestión de riesgos de ciberseguridad. Según un artículo del ISACA Journal[7], la auditoría interna puede ofrecer un aseguramiento valioso e identificar amenazas y vulnerabilidades. Esto puede incluir la identificación de las tendencias de ciberseguridad y las expectativas de las partes interesadas, la realización de una evaluación inicial del riesgo cibernético y la definición de criterios de auditoría efectivos. Al informar y asesorar sobre sus hallazgos, "los auditores pueden ayudar significativamente a la [junta de directores] a ejercer su supervisión", afirma el artículo.

Asegurar que los inputs de auditoría interna sean óptimos. En muchas organizaciones, los comités de auditoría son responsables de abordar todo tipo de riesgos, incluidas las amenazas cibernéticas[8]. Sin embargo, algunos asignan las preocupaciones cibernéticas a otros comités, por varias razones. Según el tamaño y la industria de la organización y las amenazas que enfrenta, el comité encargado de supervisar los problemas cibernéticos puede ser un comité de seguridad cibernética separado, un comité de riesgos, un comité de tecnología, el comité de nominación y gobierno u otro comité. Las juntas pueden determinar que el comité de auditoría ya tiene un alcance completo o que puede no tener la experiencia necesaria para supervisar las preocupaciones cibernéticas, entre otras razones.

La auditoría interna generalmente informa al comité de auditoría, pero la organización puede perder recomendaciones y aseguramientos valiosos sobre el riesgo cibernético si la auditoría interna no ofrece también informes a cualquier comité separado que esté a cargo de la seguridad cibernética. Tener relación con cualquier comité que supervise los problemas cibernéticos garantiza que los conocimientos de auditoría interna se comprendan y se actúe de manera efectiva.

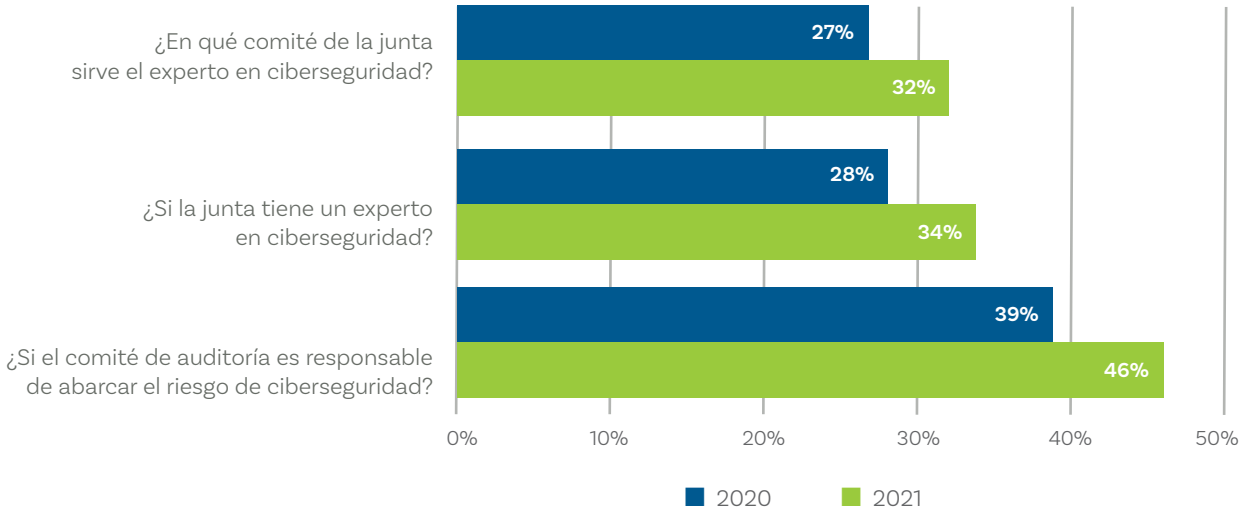
Identificación de amenazas ocultas. Las juntas pueden sorprenderse por la cantidad de descuidos aparentemente pequeños que pueden dañar los esfuerzos de seguridad cibernética y potencialmente conducir a un desastre. La auditoría interna puede ofrecer información para ayudar a las juntas a determinar qué tan bien el plan de auditoría de su organización puede identificar amenazas pasadas por alto y detectar riesgos emergentes. Según un informe de Deloitte[9], solo algunas de las amenazas cibernéticas que la gerencia suele subestimar incluyen:

- El número de ex empleados que aún pueden iniciar sesión en el sistema de la empresa y la cantidad de proveedores externos que tienen acceso a los sistemas corporativos. En ambos casos, las empresas pueden tener poca idea de cuántos usuarios externos no identificados y no autorizados pueden ingresar.

PREGUNTAS PARA LOS MIEMBROS DE JUNTA

- ¿Estamos haciendo el mejor uso de la información y el asesoramiento de la auditoría interna en nuestra planificación estratégica relacionada con la ciberseguridad?
- ¿Hemos dotado de personal y financiado adecuadamente los esfuerzos de seguridad cibernética?
- ¿La organización ha definido su tolerancia al riesgo en lo que respecta a la ciberseguridad en términos financieros?
- ¿Se asigna un comité específico para la supervisión de la ciberseguridad?
- ¿Los directores entienden los procedimientos de la empresa en caso de una brecha cibernética y conocen su propio rol si sucede?

Cúantas Empresas del S&P 500 revelan:



Fuente: 2021 Audit Committee Transparency Barometer, Center for Audit Quality, Noviembre 2021.

- El número de cuentas en la nube que utiliza la empresa. Una mayor participación en la nube puede dejar más oportunidades para los ataques cibernéticos. El informe de Deloitte recomienda que las organizaciones pregunten a los proveedores de la nube sobre la resiliencia de la infraestructura, el tiempo de inactividad del servicio, el rendimiento y otras métricas, así como sobre el cumplimiento normativo y las evaluaciones de controles independientes.
- Tl número total real de ataques cibernéticos que la organización ha experimentado Contrariamente a la intuición, si la empresa ha experimentado pocos ataques cibernéticos, eso puede ser una señal de advertencia de que los incidentes simplemente no se están detectando. El equipo de auditoría interna puede ayudar a garantizar que se controlen estos tipos de señales de advertencia.

Abordar las preocupaciones en las relaciones con los socios comerciales.
Gartner [10] predice que para el 2025, 60% de las organizaciones considerará el riesgo de ciberseguridad cuando participe en transacciones de terceros y compromisos comerciales. En la actualidad, solo el 23 % de los líderes de gestión de riesgos y seguridad supervisan la exposición a la ciberseguridad de terceros en tiempo real, y es posible que limiten su control a los vendedores y proveedores inmediatos en lugar de a toda la cadena de suministro.

Una vez más, los líderes de auditoría, los directores ejecutivos y los miembros de la junta no están sincronizados en sus opiniones, según OnRisk 2022. Si bien los DEA calificaron la capacidad organizacional en esta área en un 37 %, los ejecutivos creen que se situó en un 53 % y los directores en un 57 %. Es probable que la menor confianza del DEA en esta área se deba en parte a la calificación de mayor relevancia que asignan a este riesgo, que fue 17 puntos más alta que la calificación de los directores (77 % frente a 60 %).

En cualquier caso, las juntas deben asegurarse de obtener el valor total de los aportes y experiencias de la auditoría interna en esta área. Debido a que la auditoría interna trabaja con equipos en toda la organización, puede alertar a la junta directiva sobre los riesgos cibernéticos asociados o identificados con un proveedor en particular o en toda la cadena de suministro. Cuando los socios comerciales de la organización quieren estar seguros de la confiabilidad de sus medidas de seguridad cibernética, la auditoría interna puede proporcionar los tipos de datos y aseguramientos que buscan.

Optimizando los Recursos

A medida que las organizaciones luchan con preocupaciones de ciberseguridad abrumadoras, deberán optimizar todos sus recursos existentes. Las juntas pueden mejorar la seguridad de su empresa entendiendo y aprovechando el valor que los auditores internos pueden aportar a toda la organización al identificar oportunidades para mejorar la eficiencia y la eficacia.

Notas Finales

1 Principles for Board Governance of Cyber Risk, **National Association of Corporate Directors, Internet Security Alliance, and World Economic Forum, In Collaboration with PwC, March 2021.**

2 https://www.cisa.gov/circia

3 https://www.sec.gov/rules/proposed/2022/33-11038.pdf

4 Overseeing Cyber Risk: The Board's Role, **PwC, January 2022.**

5 OnRisk 2022: A Guide to Understanding, Aligning, and Optimizing Risk, **The Institute of Internal Auditors, 2021.**

6 The IIA's Three Lines Model: An Update of the Three Lines of Defense, **The Institute of Internal Auditors, July 2020.**

7 "How Effective Is Your Cybersecurity Audit?," Matej Drašček, et al., ISACA Journal, June 1, 2022.

8 "Cybersecurity: An Evolving Governance Challenge," **Harvard Law School Forum on Corporate Governance, Phyllis Sumner, et al., March 15, 2020.**

9 Internal Audit: Risks and Opportunities for 2022, **Deloitte, 2021.**

10 Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem, **Sam Olyaei, et al., Gartner, January 24, 2022.**

Encuesta Rápida

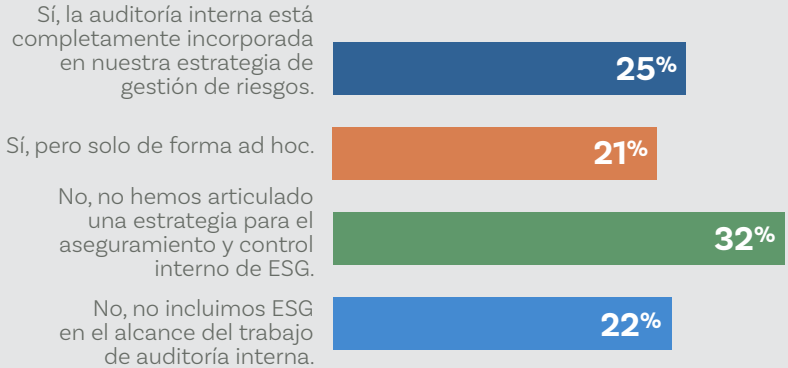
¿Qué comité de la junta se encarga de revisar la gestión de riesgos de seguridad cibernética para su organización?

- ◯ Comité de Auditoría
- ◯ Comité de Ciberseguridad
- ◯ Comité de Tecnología
- ◯ Comité de Nominación y Gobierno
- ◯ Otro

Visite theiia.org/Tone para responder la pregunta y ver las respuestas de otros participantes.

RESULTADOS DE LA ENCUESTA RÁPIDA

Su organización aprovecha la auditoría interna para el aseguramiento de ESG?



Fuente: Encuesta Tone at the Top Junio 2022.

El presente documento fue traducido al español por el IAI ECUADOR el 16/11/21.