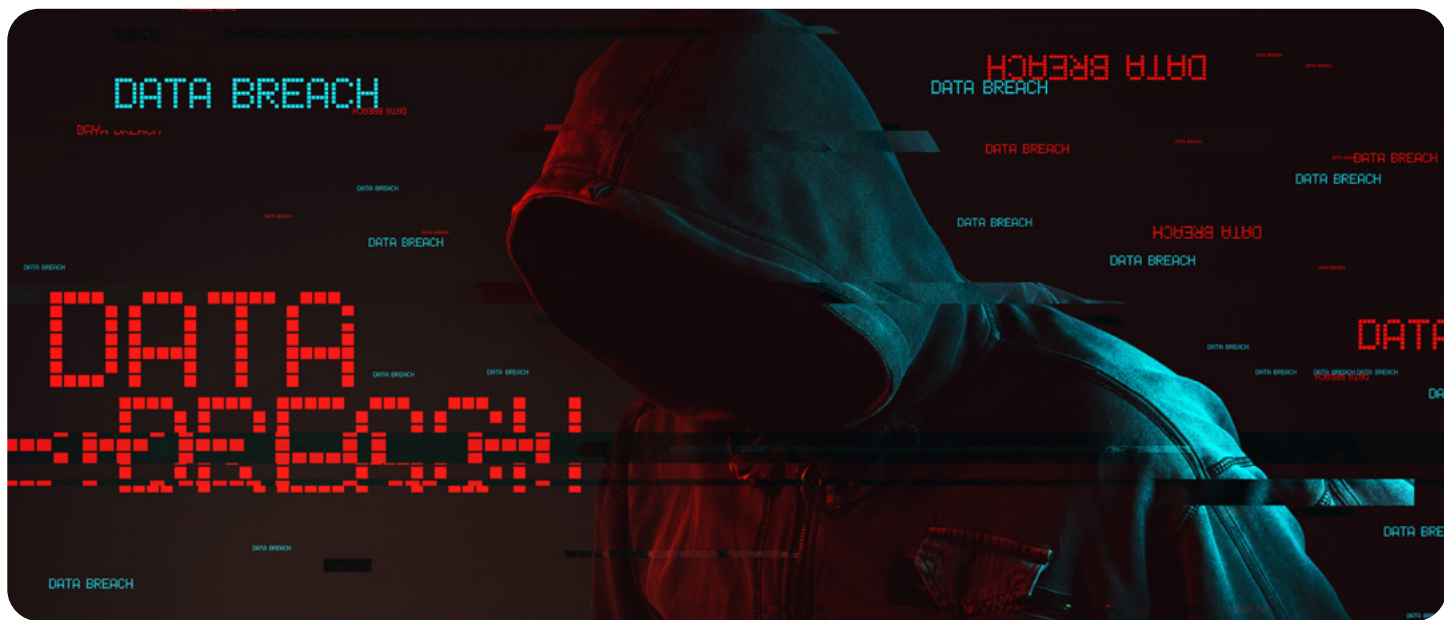


Proporciona a la alta dirección, juntas directivas y comités de auditoría, información concisa sobre temas relacionados con la gobernanza.

Edición 137 | Octubre 2026



De La Brecha de Seguridad a la Sala de Juntas: Fortalecimiento de la Supervisión de la Ciberseguridad

En febrero de 2024, un ataque de ransomware contra Change Healthcare, una filial de UnitedHealth Group, detuvo el procesamiento de reclamaciones y pagos en gran parte del sistema sanitario estadounidense. El daño: **\$2.200 millones de dólares en costos directos de respuesta**, otros 867 millones de dólares por interrupción de las operaciones y aproximadamente 190 millones de personas afectadas.

El punto de entrada fue un portal sin autenticación multifactor — un control de seguridad básico, [como reconoció](#) el CEO Andrew Witty ante el Comité de Finanzas del Senado. El presidente Ron Wyden culpó a la cúpula, argumentando en su [declaración inicial](#) que la empresa necesitaba un auténtico

experto en ciberseguridad en su consejo.

Eso ya no es solo un tema de conversación. En una serie de [Decisiones de 2025](#), El Tribunal de Cancillería de Delaware sostuvo que la ciberseguridad es un riesgo “crítico para la misión” que los consejos no pueden simplemente delegar a la dirección. Ahora se espera que los directores reciban informes periódicos, y la falta de actas en esas discusiones puede sugerir, en sí misma, un fallo de supervisión.

Este no es un riesgo que vaya a desaparecer pronto. En el [Informe Risk in Focus 2026/2027 del IIA](#), el 80% de los líderes de auditoría interna seleccionaron la ciberseguridad como una de los cinco principales riesgos a los que se enfrenta su organización, un 7% más que 2025 y un

22% superior al del segundo riesgo más seleccionado, la disrupción digital (incluida la IA).

Está claro que la ciberseguridad es un área crítica que requiere la máxima atención por parte de la cúpula de la organización. Los miembros del consejo tienen la obligación de tratar la supervisión de riesgos cibernéticos como parte de sus funciones y desarrollar la experiencia adecuada para llevarla a cabo.

Este Tone at the Top analiza posibles lagunas en los esfuerzos de ciberseguridad de las organizaciones, la creciente variedad de divulgaciones sobre gobernanza cibernética y cómo los auditores internos pueden ayudar a los consejos de administración a asumir sus responsabilidades de gobernanza en este ámbito.

Un Trabajo en Progreso

La ciberseguridad ha evolucionado de ser una preocupación estrictamente técnica a uno de los riesgos empresariales centrales a los que se enfrentan las empresas modernas. Como señala CrowdStrike en su informe, “[Supervisión de Riesgos de Ciberseguridad: Guía de Gobernanza para Directores de Juntas](#)”, los consejos actuales han visto cómo la ciberseguridad ha pasado “de un ejercicio de cumplimiento a un mandato central de gobernanza.”

La forma en que las organizaciones están tratando las divulgaciones de ciberseguridad es un claro ejemplo de este cambio. La Comisión de Bolsa y Valores de EE. UU. estableció [normas sobre divulgaciones de ciberseguridad](#) en 2023, pero muchas organizaciones van más allá, proporcionando voluntariamente detalles sobre la supervisión de la ciberseguridad y la experiencia del consejo de administración.

De hecho, a medida que inversores y partes interesadas siguen exigiendo más información sobre la supervisión de ciberseguridad, [un análisis de grandes empresas](#) realizado por EY encontró aumentos significativos en las divulgaciones en muchas áreas en los últimos años. Los principales hallazgos de la investigación de EY incluyen:

- El 78% de las empresas afirma que los comités de auditoría son responsables de la supervisión de la ciberseguridad.
- El 86% dice que revela la ciberseguridad como un área de especialización que tiene un director o que el consejo busca

contar con un director con esos conocimientos — frente al 53% de 2019.

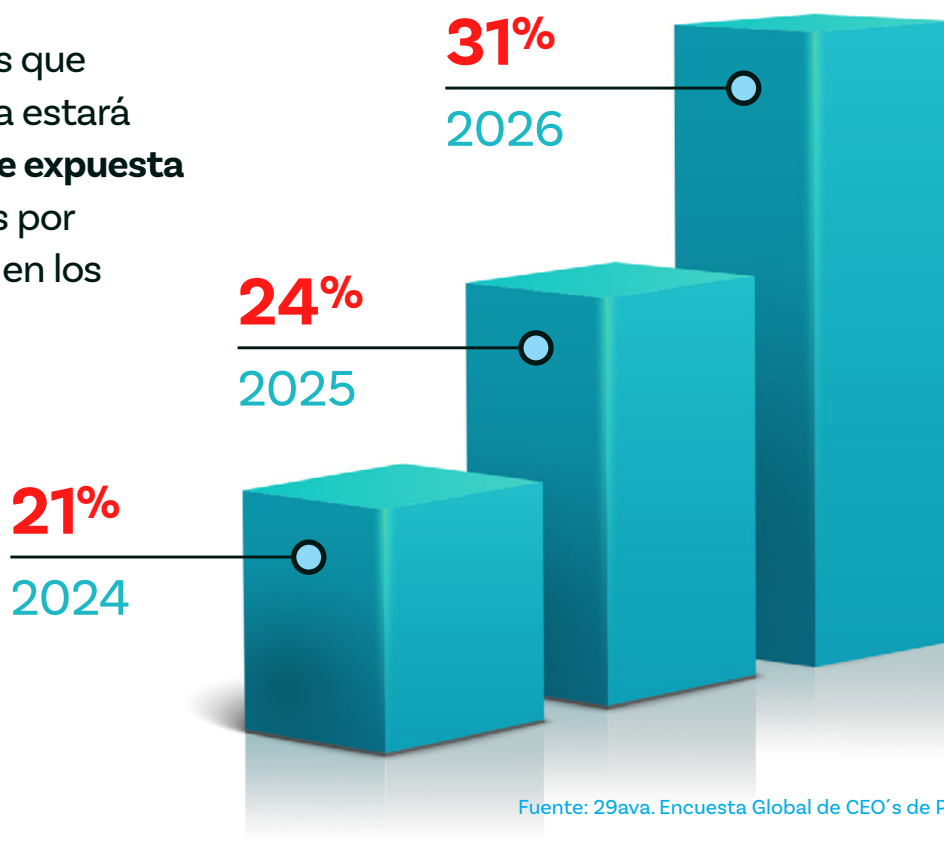
- El 73% está alineando sus esfuerzos de ciberseguridad con un marco externo, como el NIST CSF 2.0 o la ISO 27001.
- El 58% realiza actividades de preparación para la ciberseguridad, incluyendo simulaciones, ejercicios de mesa o pruebas de preparación para respuesta — un aumento respecto al 3% en 2019.

Sin embargo, aunque las organizaciones claramente se toman en serio los riesgos cibernéticos, existen carencias significativas en su capacidad para seguir el ritmo del riesgo. Esto se puede observar, por ejemplo, en el uso y comprensión de la IA, que, como mucho, sigue siendo un trabajo en progreso.

Según la Encuesta [Benchmark de Medio Año de Workiva 2026](#), el 84 % de los directivos afirma estar al menos algo confiados en la precisión de la producción de IA, incluso sin revisión humana. Al mismo tiempo, el 26% señala que las auditorías internas han detectado errores de IA que han llegado a audiencias externas o a miembros del consejo. Estos resultados indican una posible desconexión entre las suposiciones de los ejecutivos sobre la IA y la realidad de cómo funciona dentro de sus propias organizaciones.

“A medida que la IA transforma la empresa a una velocidad sin precedentes, está surgiendo un nuevo riesgo”, dice Workiva. “[T] La transformación podría estar superando los instintos de los líderes encargados de supervisarla.”

Los directores generales que afirman que su empresa estará **muy o extremadamente expuesta** a pérdidas significativas por amenazas cibernéticas en los próximos 12 meses.



Fuente: 29ava. Encuesta Global de CEO's de PwC.

Sobre El IIA

El Instituto de Auditores Internos (IIA) es una asociación profesional internacional sin fines de lucro que presta servicios a más de 265,000 miembros a nivel global 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 Gratuitas

Visite theiia.org/Tone para registrarse a una suscripción gratuita.

.....

Feedback del Lector

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

.....



Lugar de los Auditores Internos en la Discusión Cibernética

La función de auditoría interna es un socio valioso en los esfuerzos organizativos para mitigar los riesgos de ciberseguridad. El Requisito Temático de Ciberseguridad del IIA y la [Guía de Usuario relacionada](#), pueden ser un recurso esencial que ilustra claramente cuál debe ser el papel de la auditoría interna en el plan de gestión de riesgos de ciberseguridad – y lo que debe hacer para mantener la conformidad con las Normas Globales de Auditoría Interna™.

El Requisito está diseñado para proporcionar “un enfoque coherente y completo para evaluar el diseño e implementación de los procesos de gobernanza, gestión de riesgos y control de la ciberseguridad.” Para ello, la auditoría interna tiene la obligación de evaluar tres áreas clave:

- Gobernanza: Objetivos y estrategias básicas de ciberseguridad claramente definidas que apoyan metas, políticas y procedimientos organizativos.
- Gestión de riesgos: Procesos para identificar, analizar, gestionar y supervisar amenazas cibernéticas, incluyendo un proceso para escalar los riesgos cibernéticos de forma rápida.
- Controles: Procesos de control establecidos y evaluados periódicamente por la dirección para mitigar el riesgo cibernético.

En cuanto a la gobernanza en ciberseguridad, el Requisito Temático asigna los requisitos de gobernanza a marcos adecuados. La comprensión de dichos marcos debe ser un componente crítico de la base de conocimientos del comité de auditoría y la junta respecto al plan de gestión de riesgos cibernéticos de la organización. Además, el Requisito exige que la auditoría interna revise cómo se aplican los procesos de gobernanza a los objetivos de ciberseguridad, incluyendo la existencia de:

- Planes y objetivos formalizados.
- Políticas, procedimientos y otra documentación relevante utilizada para gestionar los procesos de ciberseguridad.
- Roles y responsabilidades que apoyan el logro de los objetivos de ciberseguridad, y si la función de ciberseguridad reporta a un nivel suficientemente alto dentro de la organización como para alcanzar el apoyo y la visibilidad adecuados.
- Evidencia de implicación con las partes interesadas relevantes, dentro y fuera de la organización.

En conjunto, estos requisitos deberían ofrecer a los consejos y comités de auditoría una visión clara de lo que pueden esperar de una auditoría interna en ciberseguridad. Además, dado que estos requisitos son obligatorios para cumplir con las Normas Globales de Auditoría Interna, los miembros del consejo pueden estar seguros de que una función de auditoría interna conforme a dichas Normas está maximizando el valor que puede aportar.

Creciente Atención a las Preocupaciones Cibernéticas

La industria de las telecomunicaciones es uno de los muchos sectores que se enfrentan al riesgo de ciberseguridad, y los recientes avances en defensa en este ámbito ofrecen un caso útil para ayudar a los consejos a comprender lo valiosa que puede ser la auditoría interna en este ámbito.

Los peligros en la industria de las telecomunicaciones incluyen “ciberataques a velocidad de máquina”, así como las respuestas, generalmente, lentas de las operaciones de seguridad ante amenazas emergentes, según el informe: “Cómo las telecomunicaciones pueden aumentar la ciberseguridad en la era de los ataques de IA” de EY.”

La legislación recientemente aprobada en Canadá mejora la capacidad del gobierno para proteger el sistema de telecomunicaciones del país frente a estos peligros. Exige que los operadores de sistemas cibernéticos críticos en sectores regulados por el gobierno federal tomen las medidas necesarias para proteger su infraestructura cibernética.

En sus comentarios sobre lo que se convertiría en la Ley de Protección de Sistemas Cibernéticos Críticos de Canadá, el IIA señala la necesidad de desarrollar procesos efectivos para identificar y mitigar posibles riesgos cibernéticos para las organizaciones, así como garantizar la presencia de controles internos apropiados y procedimientos de aseguramiento independientes. La ley exige “una auditoría interna en un operador designado regulado conforme a esta legislación.”

Las regulaciones cibernéticas en otras jurisdicciones incluyen:

- EE.UU.: Ley de Reporte de Incidentes Cibernéticos para Infraestructuras Críticas de 2022.
- Unión Europea: Directiva NIS2.
- Reino Unido: Reglamento de Sistemas de Redes e Información 2018.

Los Consejos Necesitan la Perspectiva de Auditoría Interna.

La ciberseguridad es un tema vasto y, en ocasiones, abrumador para cualquier organización. Con todas las variables técnicas y en evolución en juego, los consejos deberán confiar en estructuras sólidas de gobernanza y reporte para garantizar que se les proporcione la información más clara, precisa y relevante posible. Para ello, no hay función mejor posicionada para contribuir eficazmente a la discusión que la auditoría interna.

