# Informe del CISO

## El camino hacia la resiliencia digital comienza en su junta directiva

splunk>
a CISCO company

Los CISOs convivimos con el riesgo todos los días. Combatimos el malware, detenemos a los atacantes internos maliciosos y hacemos cumplir las normativas.

Si embargo, si no estamos en sintonía con la junta directiva, nos encontramos frente a otro tipo de riesgo. Si no podemos articular el impacto potencial de los problemas de seguridad, es muy probable que estos sigan representando una amenaza.

Este es un desafío esencial para los CISOs y sus juntas directivas: contar la historia de seguridad con la perspectiva adecuada para abordar a las personas que pueden respaldar nuestra visión. En el Informe del CISO de este año, analizamos esta relación bajo el microscopio para descubrir qué pensaba cada parte sobre la otra. La encuesta confirmó una tendencia que observamos en los últimos años: los CISOs están interactuando más con las juntas directivas.

Sin embargo, todavía hay muchas áreas con desajustes. Por ejemplo, qué habilidades principales deben desarrollar los CISOs, cómo emplean su tiempo y qué estrategias son eficaces para persuadir a las juntas directivas con el fin de obtener un presupuesto adicional.

Para superar estas brechas, los CISOs tendrán que hablar el mismo idioma que sus juntas directivas. En mi experiencia, eso significa pasar mucho más tiempo con ellos y otros líderes de la empresa para comprender mejor el negocio y convertir la seguridad en un habilitador del negocio. Los CISOs que puedan vincular la seguridad con los ingresos y sepan qué es lo que preocupa a la junta directiva demostrarán que tienen interés en el asunto y podrán ofrecer soluciones, no solo presentarán problemas que necesiten que la junta resuelva.

Esperamos que el Informe del CISO sea un recurso que le permita contar su historia, superar las brechas de comunicación y obtener el apoyo de la junta para el programa de seguridad.

Michael Fanning

CISO de Splunk

# Contenido


4 **Introducción:** ¿El comienzo de una gran amistad?

5 **Capítulo 1:** Los CISOs se instalan en la alta dirección

7 **Capítulo 2:** Los CISOs y las juntas directivas deben tener en cuenta las brechas

13 **Capítulo 3:** Los CISOs cada vez se interesan más en el cumplimiento normativo por motivos personales

15 **Capítulo 4:** Aportar mejores pruebas al debate presupuestario

19 **Capítulo 5:** La IA empodera a defensores y adversarios

22 **Capítulo 6:** Es mágico cuando los CISOs y las juntas directivas se alinean

24 **Capítulo 7:** Despeje el camino hacia la asociación con su junta directiva

27 Apéndice del sector

29 Apéndice de regiones

30 Metodología

31 Acerca de Splunk

# ¿El comienzo de una gran amistad?

Aceite y agua. Marte y Venus. Cualquiera que sea la metáfora, los CISOs y sus juntas directivas son seres inherentemente diferentes y pertenecen a mundos completamente distintos.

Las preocupaciones de los líderes empresariales sobre los resultados a menudo entran en conflicto con la insistencia de los CISOs en realizar inversiones vitales en ciberseguridad. Incluso un pequeño malentendido sobre las prioridades puede causar divisiones importantes en el futuro. Si esto ocurre, los CISOs y las juntas directivas pueden terminar en lugares muy diferentes de los que pretendían.

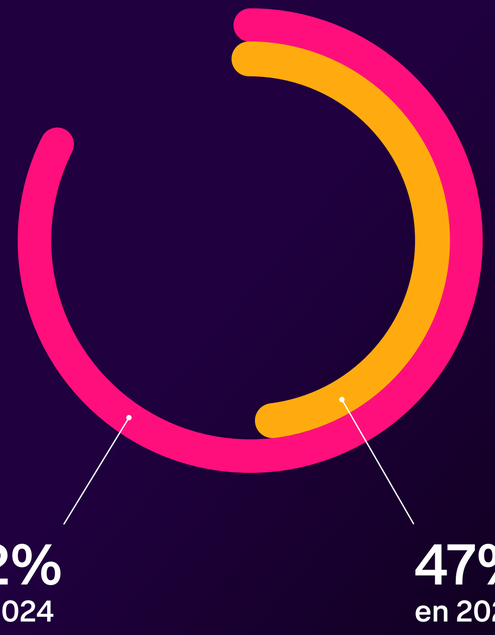
La relación entre los CISOs y la juntas directivas se está profundizando a medida que tienen más oportunidades de involucrarse en cuestiones de ciberseguridad y riesgo empresarial. La mayoría de los CISOs (el 82%) ahora presentan informes directamente al director ejecutivo. Esto representa un aumento considerable respecto del porcentaje correspondiente a 2023 (el 47%). Son como vecinos que evolucionan de ser conocidos a amigos cercanos y, con el tiempo, conversan y descubren intereses comunes.

A pesar de las brechas, comparten el deber de proteger la empresa. Las juntas directivas protegen la rentabilidad y el precio de las acciones; los CISOs protegen los datos y los sistemas. A partir de esto, podemos construir un vínculo productivo. Sin embargo, se necesitará comunicación, comprensión y una generosa dosis de paciencia lograrlo.

Para prosperar, cada parte tendrá que salir de su zona de confort y aprender el idioma de la otra parte. Para los CISOs, eso significa comprender el negocio más allá de la superficie y encontrar nuevas formas de transmitir el retorno de la inversión de las iniciativas de seguridad a sus juntas directivas. Para los miembros de la junta directiva, significa comprometerse con una cultura que priorice la seguridad y considerar a los CISOs como una parte interesada principal de las decisiones que tienen un impacto en el riesgo y la gobernanza de la empresa.

Cuando los CISOs y las juntas directivas comprenden su misión conjunta, se convierten en aliados imparables que pueden impulsar a la organización en su camino hacia la resiliencia digital.

**Cada vez más CISOs presentan informes al director ejecutivo**



# Los CISOs se instalan en la alta dirección

A medida que más CISO presentan informes directamente al director ejecutivo, consolidan su lugar en la alta gerencia y en la sala de juntas, e influyen en las decisiones comerciales estratégicas. Sin embargo, este elevado estatus ha generado problemas crecientes. Como ocurre en muchas relaciones, una de las partes piensa que tiene una relación ligeramente mejor de lo que la otra parte cree.

Si analizamos en términos generales cómo se comportan los CISOs, el 84% de los directivos encuestados afirman que los CISOs cumplen sus expectativas. A primera vista, esto parece ser positivo. Considerando los complejos desafíos que enfrentan los jefes de seguridad, ¿es suficiente cumplir con los estrictos estándares de excelencia de las juntas directivas? Se supone que los CISOs que van más allá de las expectativas generarán más confianza, pero solo el 8% de los miembros de juntas directivas encuestados indicaron que los CISOs superan las expectativas.

Cuando analizamos los detalles de la relación, los datos de la encuesta muestran que los CISOs constantemente piensan que están mejor posicionados con la junta en cuanto a responsabilidades centrales. En comparación con los encuestados de juntas directivas, los CISOs sienten que están en terreno más firme en todos los aspectos, incluidas la contratación y la capacitación de la organización de seguridad, la presupuestación adecuada y la alineación con los objetivos estratégicos de ciberseguridad.

## Los CISOs sobrevaloran sus relaciones con las juntas directivas en áreas clave

Encuestados que dijeron que la relación era *muy buena* o *excelente*

**Las juntas directivas son líderes empresariales que son muy buenos en la gestión del negocio y los resultados financieros. Sin embargo, materialmente, no comprenden que dependen de la tecnología y las ramificaciones de seguridad de cómo gestionan esa tecnología.**

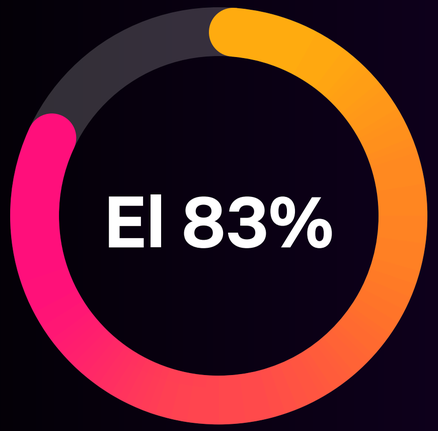
Christopher Kennedy, CISO, Group 1001

Sin embargo, la puerta se abre en ambos sentidos. Los CISOs no confían del todo en la capacidad de las juntas en materia de ciberseguridad. Si bien el 60% reconoce que los miembros de la junta directiva con experiencia en ciberseguridad tienen una mayor influencia en las decisiones de seguridad, no todas las juntas directivas tienen una autoridad como esa en la sala. Solo el 29% de los CISOs indicaron que su junta incluye al menos un miembro con experiencia en ciberseguridad.

En estas relaciones fundamentales de la junta directiva es donde comienza gran parte de la división futura. Una pequeña desconexión aquí puede crecer y desarrollarse en áreas críticas como la respuesta a incidentes y el crecimiento empresarial.

Sin embargo, algunas de estas percepciones pueden cambiar, dado que el 83% de los CISOs ahora participan en reuniones de la junta directiva *con cierta frecuencia* o *la mayor parte del tiempo*. Es posible que esta evolución determine el modo en que las juntas directivas abordan la política de ciberseguridad y la cultura organizacional.

Afortunadamente, las brechas actuales no son insuperables. La presencia regular de los CISOs en la sala de juntas y su asesoramiento sobre riesgos empresariales fortalecerán la confianza y la alineación de la junta.




**de los CISOs ahora participan en reuniones de directorio *con cierta frecuencia* o *la mayor parte del tiempo***

**Cuando comencé como CISO, lo más importante era conseguir un lugar en la mesa con la junta directiva. Eso cambió. Ahora bien, no hay discusión ni debate sobre si el rol de los CISOs debería ser el de entregar informes directamente a la junta directiva.**

Bruce Foreman, CISO, UMass Memorial Health

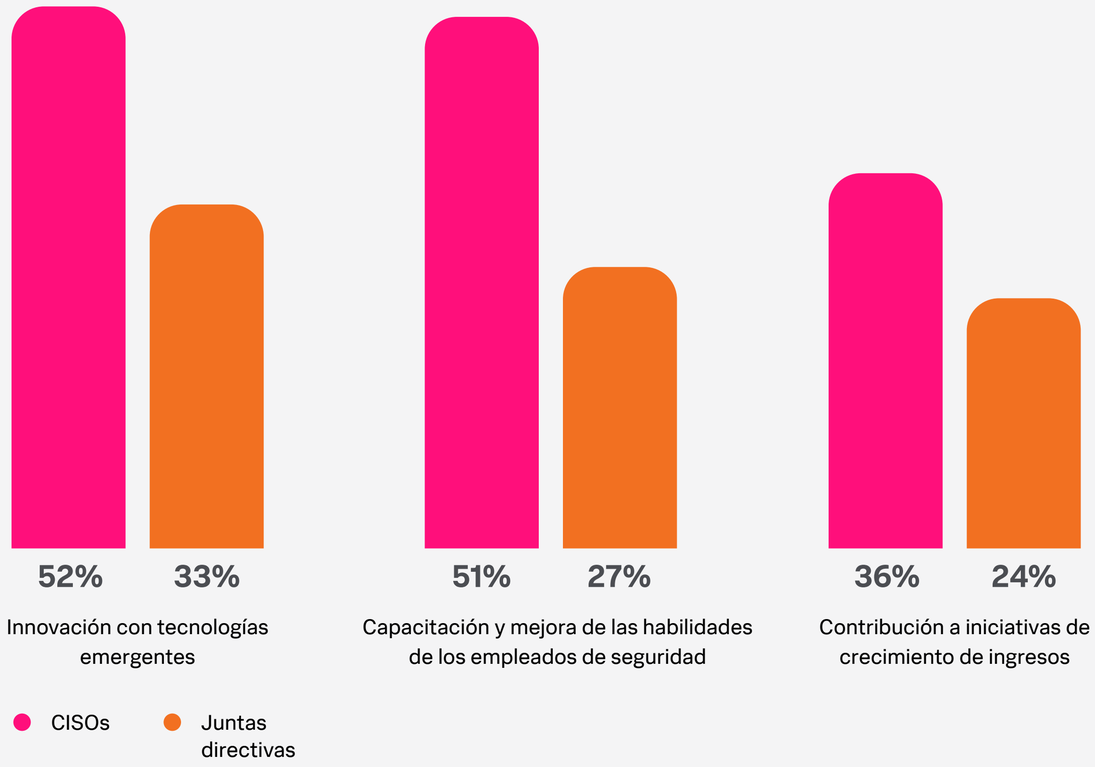
# Los CISOs y las juntas directivas deben tener en cuenta las brechas

Nuestra encuesta indica que la brecha entre las juntas directivas y los CISOs puede estar reduciéndose en ciertas prioridades de seguridad. Por ejemplo, están fuertemente alineados en la protección de la información confidencial de la empresa: el 70% de las juntas directivas y el 68% de los CISOs indican que es *muy importante* o *de máxima importancia*.

Sin embargo, algunas brechas importantes persisten. Las prioridades de los CISOs coinciden con su experiencia técnica, lo que determina cómo ejecutan esas prioridades y, en definitiva, logran sus objetivos a largo y corto plazo.

**Las mayores brechas en prioridades entre los CISOs y las juntas directivas**

Respuestas clasificadas como *muy importantes* o *de máxima importancia*



# Las juntas directivas quieren saber: ¿a qué se dedica el tiempo?

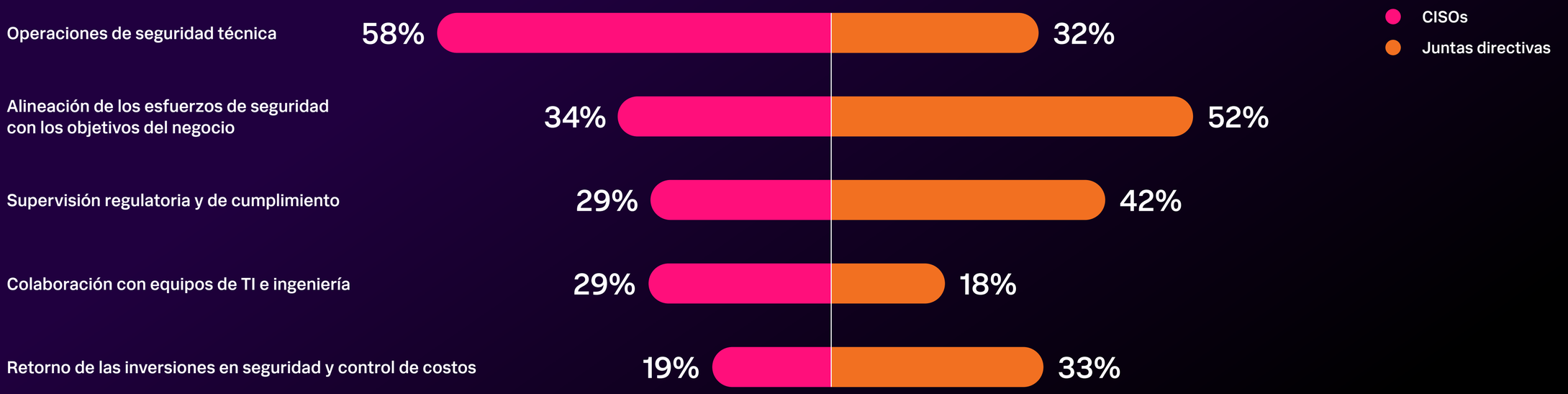
Dado que algunas de las prioridades más importantes están en desacuerdo, los CISOs y las juntas directivas también difieren en cómo los CISOs y los equipos de seguridad deberían usar su tiempo y energía para hacer que sus objetivos sean viables.

Entonces, ¿qué hacen exactamente los CISOs todo el día? Si bien el 63% de los CISOs y las juntas directivas están alineados y afirman que los CISOs dedican la mayor parte de su tiempo a la postura de seguridad y la mitigación de riesgos, sus percepciones difieren fuera de eso. El 52% de los miembros de juntas directivas encuestados cree que los CISOs pasan la mayor parte del tiempo asegurando el funcionamiento del negocio, alineando los esfuerzos de seguridad con los objetivos comerciales, en comparación con solo el 34% de los CISOs. En realidad, los aspectos técnicos de la ciberseguridad requieren mucho más tiempo de los CISOs de lo que la junta directiva cree. Según el 58% de los CISOs, la mayor parte de su tiempo y del tiempo de sus equipos se destina a elegir, instalar y utilizar la tecnología.

> **Si una empresa no está acostumbrada al alto costo de la ciberseguridad, entonces un CISO debe explicar todas las funciones del equipo de seguridad a la junta y delinear cómo las responsabilidades de seguridad están entrelazadas en la estructura de todo el negocio.**
>
> Christopher Kennedy, CISO, Group 1001

# Percepción y realidad

Cómo los CISOs y sus equipos pasan la mayor parte del tiempo



# Las habilidades empresariales ayudan a los CISOs a diversificarse

Las juntas directivas tienen grandes esperanzas depositadas en los CISOs. La mayor esperanza es que se conviertan en mejores líderes empresariales. Sin embargo, los CISOs podrían ver esa ambición de manera diferente o tomar caminos alternativos para alcanzarla.

Más que los CISOs, los miembros de juntas directivas enfatizaron la perspicacia empresarial y las habilidades blandas, como la empatía y la comunicación, como las principales habilidades en las que trabajar. Para los CISOs, la colaboración con los equipos de TI e ingeniería y el conocimiento sobre cumplimiento fueron áreas de desarrollo más importantes.

"Agregar nuevas habilidades para aprender y profundizar hace que el trabajo de los CISOs sea más complejo y posiblemente más desafiante", indicó Marcus LaFerrera, director del equipo de investigación de seguridad de SURGe.

Este podría ser el motivo por el que el 53% de los CISOs dicen que sus responsabilidades y expectativas se han vuelto más difíciles desde que asumieron el trabajo.

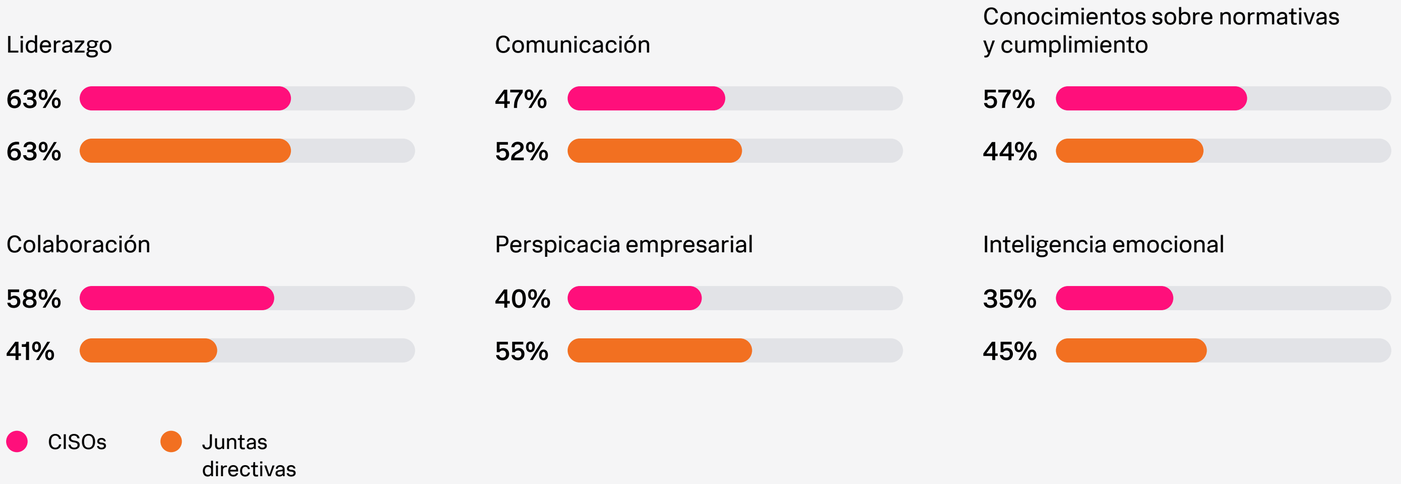
A pesar de la posición de los CISOs en los rangos ejecutivos y el deseo de las juntas directivas de que desarrollen conocimientos de negocios, es posible que las juntas aún no vean más allá de sus credenciales técnicas. Sin embargo, los CISOs pueden cambiar esta percepción. "A menos que los CISOs tengan la sabiduría y los medios para defender un lugar más apropiado en el orden jerárquico, creo que los CISOs todavía son considerados un rol de genio tecnológico que puede resolver los problemas con la tecnología, en lugar de entender materialmente cómo nuestra tecnología impulsa nuestro negocio", indicó Christopher Kennedy, CISO, Group 1001.

Dependerá de los CISOs aumentar su conocimiento de las prioridades del negocio y de la junta directiva, y cómo se relacionan con los objetivos de ingresos y crecimiento. Pueden superar las brechas mediante una comunicación ascendente proactiva y eficaz, y mediante el cultivo de una comprensión más profunda de la estrategia de la organización. Una vez que ven el panorama general, pueden determinar cómo debe encajar en él una estrategia de seguridad.

"Los CISOs deben colaborar y asociarse con otras funciones de la empresa. La seguridad no debe ser un departamento aislado. Necesitamos trabajar juntos con el departamento legal, con el departamento de riesgos, con los jefes de negocios. Por eso, los CISOs tienen que ser buenos comunicadores", afirmó Chenxi Wang, socia general de Rain Capital y miembro del directorio de MDU Resources.

**El 53%** de los CISOs indicaron que sus responsabilidades y expectativas se han vuelto más difíciles

## Las habilidades más importantes que deben desarrollar los CISOs



# Para los CISOs y las juntas directivas, el éxito se mide de forma diferente

En general, las juntas directivas y los CISOs coinciden en que los IRC centrales de ciberseguridad, como la cantidad de incidentes de seguridad materiales y la puntualidad en la gestión de vulnerabilidades, son importantes. Sin embargo, la mayoría de las juntas directivas y los CISOs (el 79%) afirman que los IRC de sus equipos de seguridad han cambiado sustancialmente en los últimos años.

"El negocio está cambiando. Tenemos aspiraciones de entrar en nuevos modelos de negocio y nuevas áreas de negocio, y vamos a tratar con datos de consumidores y datos personales. Mi postura ha cambiado porque ahora veo la seguridad como un riesgo mayor que hace dos años", afirmó Prasanna Ramakrishnan, CISO global de Clarios.

Las juntas directivas también tienen estándares específicos para evaluar el desempeño de los CISOs, como el retorno de la inversión en seguridad. Este es probablemente uno de los motivos por el que las juntas directivas esperan que los CISOs sean estratégicos en lugar de tácticos y que comuniquen de manera más integral cómo sus iniciativas tienen un impacto en el negocio.

"No consideraremos avanzar con una inversión en seguridad a menos que tenga un retorno de la inversión mínimo del 15%. De lo contrario, será difícil justificarla", indicó un miembro del consejo de administración de un grupo bancario multinacional con sede en el Reino Unido.

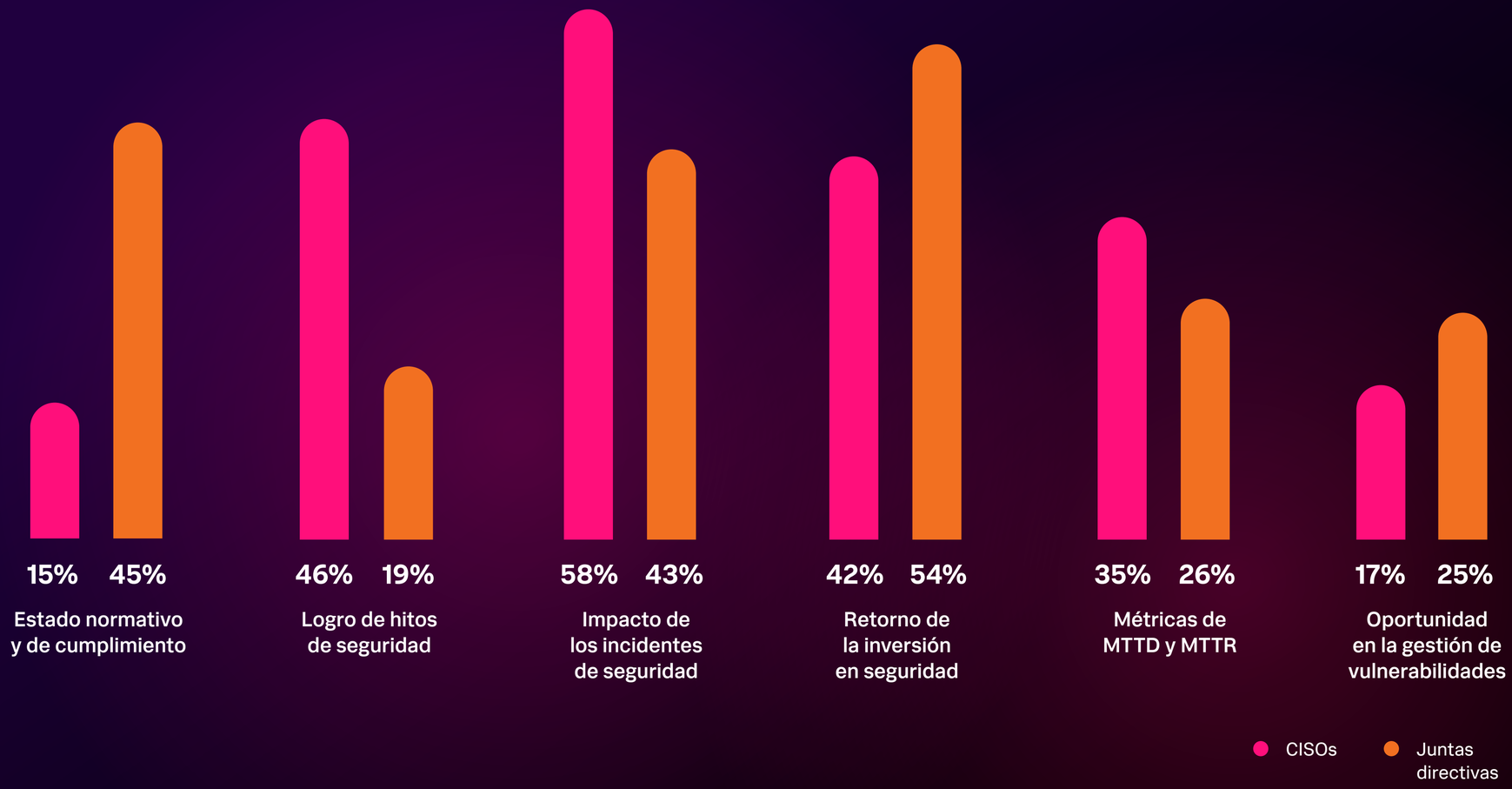
¿La conclusión? En primer lugar, las juntas directivas no quieren que los CISOs se ocupen exclusivamente de apagar incendios. Buscan un liderazgo maduro, estratégico, proactivo y facilitador del negocio, no solo control de daños cuando inevitablemente ocurre un incidente. Los CISOs que puedan educar a la junta sobre cómo sus IRC de seguridad pueden beneficiar al negocio tendrán más éxito.

Al presentar estimaciones para iniciativas futuras, los CISOs pueden persuadir a las juntas directivas enfatizando que los gastos relacionados con la pérdida de ingresos y el daño a la reputación probablemente serán menores que el costo del tiempo de inactividad debido a un incidente de seguridad.

**Los CISOs también necesitan cambiar sus tácticas para ser más escuchados. Deben usar su valioso tiempo en la junta directiva para justificar el retorno de la inversión de sus inversiones en seguridad y elevar la seguridad de modo que se considere un facilitador de negocios, no solo un centro de costos.**

Kirsty Paine, directora técnica de campo y asesora estratégica de Splunk

# Los CISOs y las juntas directivas miden el éxito de manera diferente



# Los CISOs se interesan cada vez más en el cumplimiento normativo por motivos personales

Los entornos normativos se han vuelto más complejos, expansivos y punitivos, lo que requiere informes de incidentes más rápidos y coloca más responsabilidad directamente sobre los hombros de los CISOs. Como resultado, están adoptando un enfoque más riguroso y personal respecto del cumplimiento.

## ¿Lo harán o no lo harán? La fricción de denunciar el incumplimiento

No es sorprendente que los CISOs se tomen en serio la postura de cumplimiento de su organización: muchos aspectos dependen de sus decisiones. Después de todo, los CISOs, no las juntas directivas, serán los principales responsables de los incidentes de seguridad. Los CISOs enfrentan un mayor escrutinio normativo, responsabilidad legal, fuertes sanciones financieras y la posibilidad de perder sus empleos si se descubre que han cometido infracciones.

**de los CISOs se convertirían en denunciantes si su organización ignorara los requisitos de cumplimiento**

Quizás aún más impactante, el 21% de los CISOs revelaron que fueron presionados para no informar un problema de cumplimiento. Afortunadamente, la mayoría de los CISOs encuestados están dispuestos a dar un paso adelante y hacer lo correcto: el 59% indicó que se convertiría en denunciante si su organización ignorara los requisitos de cumplimiento.

"Presionar a los CISOs para que no informen los problemas, en lugar de ser abiertos y transparentes sobre las fallas y las lecciones que deben aprender, significa que no se pueden tomar decisiones basadas en riesgos; las personas adecuadas no tienen la información real. Eso puede ser realmente peligroso", indicó Kirsty Paine, directora técnica de campo y asesora estratégica de Splunk, una empresa de Cisco.

Por supuesto, cuando un incidente se considera "material" (y la definición es poco clara), las empresas deben informarlo a las autoridades en cuestión de horas o días, según el lugar del mundo en el que operen. Mandatos recientes, como la normativa de ciberseguridad de la SEC de EE. UU., NIS2 de Europa y DORA, imponen plazos de notificación mucho más cortos (24 horas en el caso de NIS2) para divulgar incidentes de ciberseguridad. De manera similar, la Ley de Seguridad de Infraestructura Crítica (SOCI) de Australia exige que los incidentes se informen obligatoriamente en el transcurso de las 12 horas posteriores a su descubrimiento.

Al informar incidentes y otros protocolos de cumplimiento, los CISOs deben trabajar en la gestión de crisis mucho antes de que ocurra cualquier crisis. Un plan proactivo ayudará a alinear las expectativas con la junta y tener una respuesta establecida para el negocio más amplio.

**"Creo que todos aquellos que se desempeñan como jefes de seguridad o en la sala de juntas de empresas públicas deberían preocuparse por la responsabilidad personal si no están haciendo lo correcto.**

Chenxi Wang, socia general de Rain Capital y miembro de la junta directiva de MDU Resources

El 21%

**de los CISOs han sido presionados para no informar un problema de cumplimiento**

# Los CISOs se inclinan por el cumplimiento normativo... hasta cierto punto

En el riguroso entorno normativo actual, el cumplimiento se está convirtiendo en una parte importante del trabajo de los CISOs. Esto podría explicar por qué el 57% clasificó la "profundidad del conocimiento relacionado con las normativas y el cumplimiento" como una de las principales habilidades que se deben desarrollar.

Además, si bien mantener el cumplimiento es vital para el negocio, los CISOs no necesariamente creen que sea la mejor manera de medir su éxito en la supervisión de la seguridad. Solo el 15% de los CISOs clasificaron el estado de cumplimiento como una métrica de desempeño superior, una desconexión significativa en comparación con el 45% de las juntas directivas. Históricamente, los CISOs no lo han percibido como una actividad de seguridad estratégica.

Esta desconexión puede significar que las juntas directivas y los CISOs no se comunican entre sí sobre el cumplimiento. "Si bien las juntas directivas saben que el cumplimiento es importante, es posible que muchas no adviertan o no comprendan plenamente el trabajo que requiere lograrlo. Con la falta de información diaria, no sorprende que los miembros de la junta directiva piensen que debería ser fácil o que se confundan cuando los CISOs y sus equipos dedican una cantidad excesiva de tiempo a alcanzar y mantener una postura de cumplimiento sólida", indicó Kirsty Paine, directora de tecnología de campo y asesora estratégica de Splunk, una empresa de Cisco.

> **"HIPAA y cualquier otro cumplimiento (son casillas de verificación). "Hizo esto, cumple con la norma". Pero eso no significa que esté seguro. Es una línea de base, pero creo que es una línea de base muy básica.**
>
> Bruce Foreman, CISO, UMass Memorial Health

CAPÍTULO 4

# Aportar mejores pruebas al debate presupuestario

Los presupuestos cibernéticos reflejan un apoyo inconsistente y desalineado, lo que reduce las expectativas de los CISOs, frustra a las juntas directivas y amplía la brecha entre ambos.

Solo el 29% de los CISOs afirman que reciben el presupuesto adecuado para las iniciativas de ciberseguridad y el logro de sus objetivos de seguridad; en comparación con el 41% de los miembros de juntas que piensan que los presupuestos de ciberseguridad son adecuados. Es justificable que los CISOs estén preocupados por cómo esta falta de apoyo afectará la postura de seguridad de su organización. El 64% revela que el actual entorno normativo y de amenazas hace que les inquiete no estar haciendo lo suficiente.

**Cuando vamos a la junta y decimos que tenemos una amenaza cibernética potencial, es difícil justificar la inversión. El problema habitual al que nos enfrentamos es la certeza de una inversión frente a la probabilidad de una amenaza que puede no ocurrir.**

Miembro de la junta directiva de un grupo bancario multinacional con sede en el Reino Unido

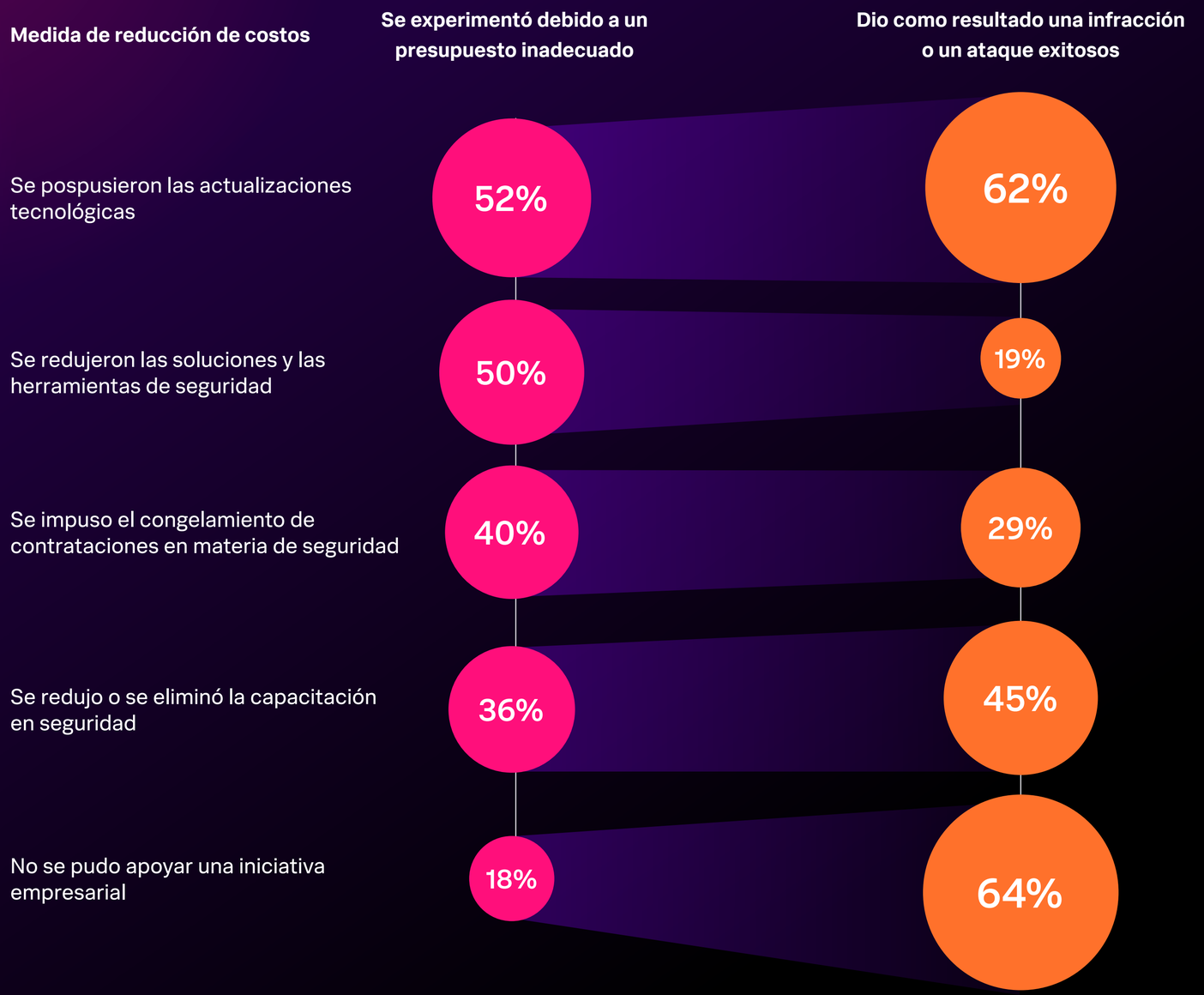
# Pequeños recortes, graves consecuencias

Muchos CISOs implementaron medidas de ahorro de costos debido a presupuestos inadecuados. Algunos de los recortes más importantes incluyeron posponer una actualización de seguridad; reducir el número de soluciones para disminuir los costos de licencia; y congelar promociones, aumentos y contrataciones. Sin embargo, estos recortes de seguridad no pasan simplemente inadvertidos: a menudo, tienen consecuencias graves, como ataques de seguridad exitosos o filtraciones de datos.

Mientras tanto, los ciberataques no muestran signos de desaceleración. Un importante 94% de los CISOs informaron haber sido víctimas de un ciberataque disruptivo. La mayoría, el 55%, afirmó haberlos experimentado al menos *un par de veces*, y otro 27% indicó haber sido víctima *muchas veces*.

Una financiación adecuada será crucial para garantizar defensas cibernéticas adecuadas. Los CISOs sostienen que el área más importante de inversión futura será la gestión del riesgo cibernético (64%). Estas y otras nuevas inversiones en infraestructura, herramientas, soluciones y servicios serán clave para ayudar a los CISOs y sus equipos a proteger los datos y sistemas de sus organizaciones.

# Los presupuestos de seguridad inadecuados traen consecuencias



# Los CISOs defienden la seguridad frente a la junta directiva

Entonces, ¿qué es lo que realmente convence a las juntas directivas para que desembolsen dinero? Muchas juntas directivas afirman que priorizan el crecimiento del negocio (44%) sobre el fortalecimiento del programa de ciberseguridad (24%), lo que significa que están inclinadas a respaldar iniciativas de ciberseguridad que brinden el mayor valor a los accionistas y a la organización. Presentar la seguridad como un facilitador de negocios es, claramente, el argumento más potente, según el 64% de los miembros de juntas directivas. Sin embargo, solo el 43% de los CISOs afirman que realizan esta práctica.

Para conseguir lo que quieren, los CISOs tendrán que aprender a comunicar lo que necesitan de una forma que resulte convincente para la junta directiva. En resumen, necesitan aprender a hablar el idioma de la junta con fluidez.

Para lograr que las juntas directivas escuchen las solicitudes de presupuesto y respondan a estas, los CISOs pueden presentarles cálculos concretos sobre los costos directos y secundarios del tiempo de inactividad, incluidos los ingresos perdidos, las multas por acuerdos de nivel de servicio y los factores que afectarán a los accionistas. El tiempo de inactividad cuesta a las empresas Global 2000 400 000 millones de dólares al año, con un promedio de 200 millones de dólares por empresa, o alrededor del 9% de las ganancias.

El 46% de las juntas directivas indicaron que este tipo de costos son convincentes en los debates presupuestarios. Si bien el 39% de los CISOs ya lo hacen, aún existen amplias oportunidades para que refinen sus poderes de persuasión, como presentar métricas y recomendaciones sobre riesgos cibernéticos que guíen las decisiones de gestión y educar a la junta sobre el impacto de los ciberataques.

Como dice el viejo refrán: el dinero habla. Además, si se asigna correctamente, puede prevenir costosas infracciones y violaciones de cumplimiento, salvar la reputación de su organización y ahorrarle millones de dólares en el futuro. La estrategia de comunicación ganadora es explicar cómo la seguridad impulsa el retorno de la inversión, ayuda a que el negocio crezca y protege los precios de las acciones. Esto llamará la atención de la junta directiva en todo momento.

## Enfoques que las juntas directivas encuentran más convincentes cuando se les pide que aumenten los presupuestos de ciberseguridad

CAPÍTULO 5

# La IA empodera a defensores y adversarios

Tanto para los CISOs como para las juntas directivas, la IA está plagada de incertidumbre y potencial. Están de acuerdo en que merece la pena invertir tanto en el presente como en el futuro. Aun así, una parte importante de los CISOs sienten que no están avanzando lo suficientemente rápido en IA para seguir siendo competitivos o seguir el ritmo de la innovación.

La IA puede ser un multiplicador de la fuerza de seguridad para el análisis de malware, la detección de amenazas, los estándares de configuración y otras funciones, pero solo si los CISOs ayudan a sus juntas directivas a ver las posibilidades y las motivan a invertir más en infraestructura, capacitación y gobernanza.

# La IA ofrece una ventaja a los adversarios cibernéticos

La IA todavía representa una amenaza en la frontera cibernética: el 53% de los CISOs creen que dará a los atacantes una ventaja leve o significativa. Sin embargo, ese grupo se está reduciendo notablemente a partir del 70% medido en 2023.

Las amenazas de IA percibidas como más preocupantes son los ataques de phishing más realistas y los *deepfakes* (57%), seguidos de nuevas cepas de malware (44%), ataques de ingeniería social adaptativa (40%) y explotación de soluciones generativas existentes (40%). El temor, especialmente en relación con la amenaza de los *deepfakes*, no es infundado. La ingeniería social ya es el vector de ataque más común experimentado en el último año, con una medición del 67%. Es concebible que este tipo de ataques crezca a medida que la IA continúe emulando el comportamiento y el habla humanos de manera más convincente.

## Las amenazas de la IA generativa más preocupantes para los CISOs

**57%** Correos electrónicos de phishing muy realistas

**44%** Nuevo malware que puede evadir la ciberseguridad

**40%** Tácticas de ingeniería social adaptativas

**40%** Explotación de herramientas de inteligencia artificial utilizadas por la empresa

**38%** Ataques más automatizados y eficaces

**33%** Ataques de fuerza bruta más rápidos

**30%** *Deepfakes* de voz e imagen realistas

# Las infinitas posibilidades de la IA

A pesar de sus preocupaciones sobre la IA en manos de actores de amenazas, la mayoría de los CISOs reconocen su promesa y la califican como *correctamente estimada* (70%) o incluso como *subestimada* (21%).

Los CISOs y sus equipos a menudo quedan tan atrapados en un juego defensivo contra los atacantes cibernéticos que soñar acerca de futuras inversiones a veces puede parecer un lujo. Por suerte, el auge de la IA como herramienta de defensa cibernética les permitirá ser más vanguardistas.

El 22% de los CISOs afirman que la IA dará a los defensores cibernéticos una ligera ventaja sobre los atacantes. La mayoría de los CISOs (el 53%) también creen que están adoptando la IA al ritmo adecuado, aunque más de un tercio (el 38%) cree que no se está moviendo lo suficientemente rápido. Las juntas directivas también sostienen que sus organizaciones están utilizando actualmente IA para la ciberseguridad (24%), tienen planes inmediatos de utilizarla el próximo año (41%) o tienen interés en hacerlo (33%).

Muchos CISOs están sentando las bases para nuevas defensas cibernéticas impulsadas por IA. Casi dos tercios (el 65%) de los CISOs están capacitando activamente a los equipos de seguridad en ingeniería rápida. Además, más de la mitad (el 56%) está estableciendo protocolos para determinar qué tareas son apropiadas para la IA y cuáles son más adecuadas para los humanos.

De cara al futuro, en términos de casos de uso, la IA será un área importante de inversión futura para los CISOs y sus juntas directivas. De esta forma, los CISOs tienen muchas oportunidades de destacar el retorno de la inversión de esta herramienta como facilitador de negocios. Demostrar que la IA aumentará la competitividad y el tiempo de comercialización será un gran paso para lograr la aceptación de la junta directiva. Podría incluso aumentar la asignación de presupuesto.

## Principales casos de uso de seguridad para la IA generativa según los CISOs

**47%**
Análisis de malware, detección de amenazas y enriquecimiento de alertas

**39%**
Creación de estándares de configuración de software de seguridad

**32%**
Creación de reglas de detección de amenazas

**30%**
Análisis de fuentes de datos para reducir la carga de alertas

**30%**
Búsqueda proactiva de amenazas

**28%**
Creación de informes de seguridad para la comunicación interna

**25%**
Desarrollo de políticas de ciberseguridad

# Es mágico cuando los CISOs y las juntas directivas se alinean

Dado que la ciberseguridad se ha convertido en un componente estándar de las conversaciones y decisiones empresariales, contar con uno o dos miembros de la junta directiva con experiencia en seguridad resulta cada vez más ventajoso. En virtud de la proximidad, tener un CISO en la junta directiva o una persona con experiencia en ciberseguridad tiende a fortalecer la relación entre los CISOs y la junta directiva. Debido a su profundo conocimiento en seguridad, los miembros de la junta con experiencia como CISOs pueden sentirse más seguros acerca de la postura de seguridad de la organización: es mucho menos probable que expresen preocupación por no estar haciendo lo suficiente para proteger a la organización (37% versus 62% del promedio de la encuesta).

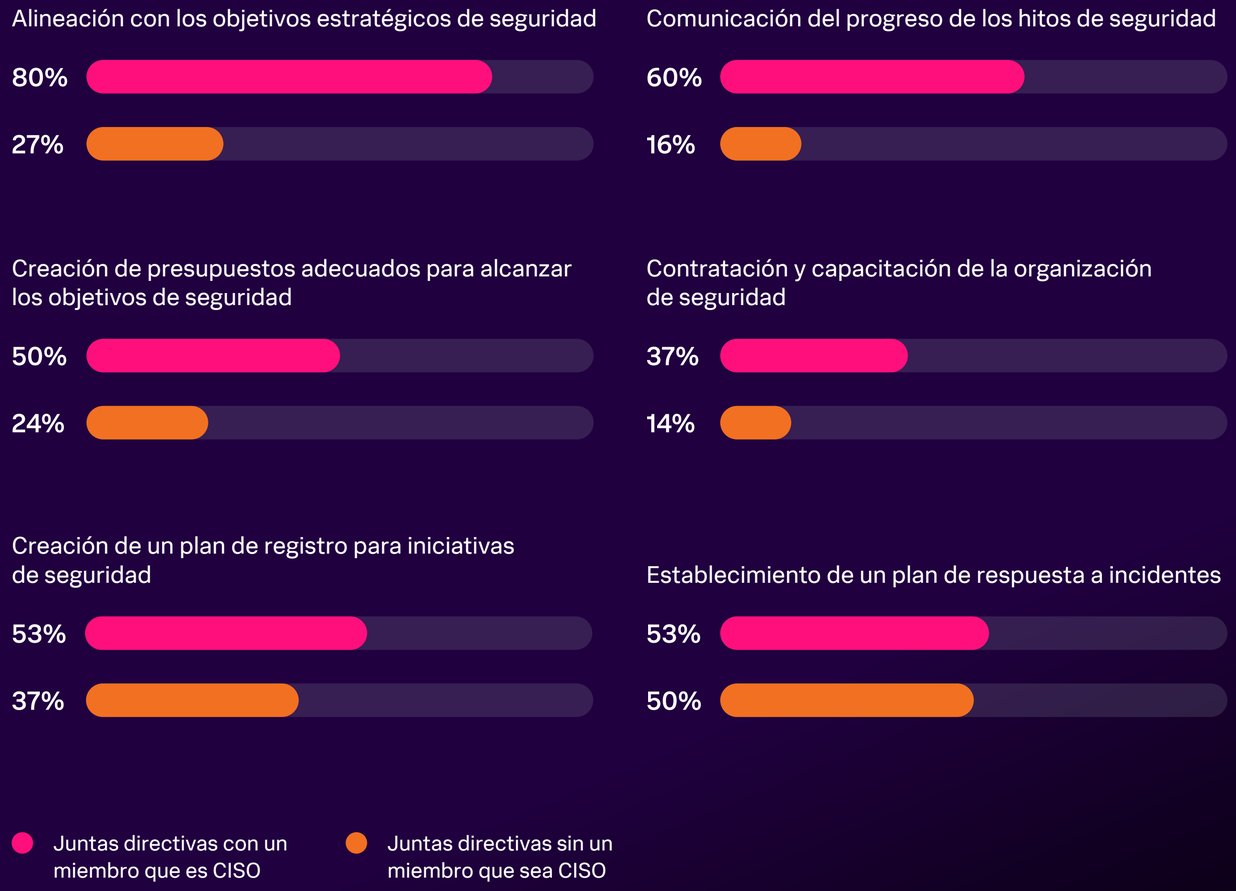
Tener los pies en ambos mundos les permite pintar un panorama preciso de la postura de seguridad de la organización, presentar mejores argumentos para futuras inversiones e ilustrar cómo la ciberseguridad impulsa el negocio hacia adelante.

Sin embargo, colocar un CISO en la junta directiva no será necesariamente una panacea para las deficiencias de seguridad. Es probable que una empresa que toma la seguridad en serio también tenga un CISO o alguien con experiencia en seguridad en la junta directiva, lo que refleja una dedicación a mejorar la cultura de seguridad y una voluntad de adoptar iniciativas relacionadas.

Sin embargo, independientemente de si forman parte de una junta directiva o no, los CISOs que tienen una buena reputación ante sus directivos obtienen un rendimiento considerablemente mayor de sus relaciones.

**Tener miembros de la junta directiva con experiencia en el rol de CISO es una ventaja en las relaciones**

Áreas en las que las relaciones se clasificaron como *muy buenas* o *excelentes*



# La comunicación potencia la colaboración y el presupuesto

La mejora de las relaciones de la junta directiva cuando los CISOs interactúan regularmente con ella es solo un aspecto, aunque esas relaciones, claramente, benefician a ambas partes. Los CISOs que mantienen relaciones saludables con las juntas directivas se benefician de una mejor colaboración en toda la organización e informan alianzas particularmente sólidas con las operaciones de TI (el 82% en comparación al 69% de otros CISOs) e ingeniería (el 74% en comparación con el 63% de otros CISOs). Esto puede deberse a que pueden comunicar con eficacia las necesidades y estrategias comerciales de la junta directiva a departamentos más técnicos de una manera que los conecta con el resto de la organización.

Los CISOs con buenas relaciones con las juntas directivas también reciben mayor confianza para probar y explorar nuevas inversiones en tecnología. Es más probable que se les dé la capacidad de buscar casos de uso para la IA generativa, como la creación de reglas de detección de amenazas (el 43% en comparación con el 31% de otros CISOs), el análisis de fuentes de datos (el 45% en comparación con el 28% de otros CISOs), la respuesta a incidentes e investigaciones forenses (el 42% en comparación con el 29% de otros CISOs) y la búsqueda proactiva de amenazas (el 46% en comparación con el 28% de otros CISOs).

Los CISOs son enlaces fundamentales, ya que traducen el lenguaje de los departamentos impulsados por la tecnología y defienden la seguridad de una manera que las juntas directivas puedan entender, y viceversa. En el futuro, tendrán aún más oportunidades de desarrollar y fortalecer esas relaciones. Las juntas directivas han demostrado que están dispuestas a aprender simplemente porque tiene sentido para su estrategia comercial, sus prácticas y sus inversiones. Esto significa que los CISOs pueden contribuir aún más a dar forma al negocio mediante la ciberseguridad.

CAPÍTULO 7

# Despeje el camino para la asociación con su junta directiva

El recorrido para los CISOs y las juntas directivas continúa. Han logrado grandes avances para armonizar objetivos, prioridades y estrategias de negocio. Sin embargo, existe la oportunidad de reducir las brechas.

A continuación, se presentan algunos pasos fundamentales que los CISOs pueden seguir para ayudar a impulsar la alineación y garantizar relaciones más sólidas, saludables y productivas con las juntas directivas.

1

## Enseñe a su junta directiva qué está haciendo y por qué

Siempre hay espacio para que las juntas directivas perfeccionen sus conocimientos sobre seguridad. Esto es especialmente cierto cuando se analiza la estrategia en torno a la respuesta a incidentes, que no solo les dará una ventana a los procedimientos estándar en cualquier momento dado, sino que también iluminará el valor de esos procedimientos al enfrentarse a auditores o durante una crisis.

Así que cree ejercicios de mesa para mostrarlo claramente. Use elementos visuales y narrativos para entregar su mensaje. Luego, desarrolle una estrategia y una cadencia, y siga su plan con sesiones iterativas.

2

## Aumente la confianza (y el presupuesto)

No estará de más practicar la conversación con la junta directiva. Si bien las juntas directivas se benefician de su experiencia en ciberseguridad, depende de usted hacerles comprender sus necesidades y prioridades. Enfatice el retorno de la inversión sobre el tiempo medio de detección (MTTD) y aprenda a comunicar el valor de sus inversiones y la importancia de la asignación de recursos de manera eficaz. (Quizás sea más difícil de hacer, pero ¿cuándo fue fácil la seguridad?).

También querrá profundizar en temas como proteger los ingresos y el valor para los accionistas, minimizar las interrupciones comerciales, mejorar la confianza en la marca y brindar experiencias de cliente seguras y fluidas. Las juntas directivas se preocupan por el crecimiento del negocio, así que hable de sus IRC.

3

## Asuma la responsabilidad del cumplimiento y conozca su responsabilidad personal

Los CISOs se enfrentan a un entorno normativo más riguroso y punitivo, por lo que es aconsejable estar preparado. Esto significa conocer su responsabilidad personal, contratar potencialmente un abogado en caso de un incidente, y adoptar un enfoque estratégico y bien documentado. Explique los riesgos que enfrenta la junta directiva y por qué los eventos materiales deben ser informados en primer lugar.

También debe saber qué esperan las juntas directivas en una crisis, codificar estas expectativas por escrito y asegurarse de que todas las partes estén de acuerdo antes de que ocurra un incidente, no durante el incidente. Relea su contrato de trabajo y, si hay brechas, ocúpese de aclararlas.

4

## Amplíe su alcance para incluir la estrategia empresarial

Sabemos que salir de la zona de confort no es fácil. Sin embargo, al asumir el rol de estratega empresarial, descubrirá cómo equilibrar las necesidades del negocio y, al mismo tiempo, proteger su organización. Si quiere aumentar la seguridad, debe mostrar cómo la seguridad hace crecer el negocio.

No se trata solo de desarrollar perspicacia empresarial, aunque la necesitará mucho. Desarrolle sus habilidades blandas. Esto incluye perfeccionar medios de comunicación más eficaces y comprender cómo su junta directiva prefiere recibir información. Refinar la inteligencia emocional también será de gran ayuda.

5

## Desarrolle liderazgo en toda la empresa, no solo en el área de la seguridad

Los CISOs y las juntas directivas coinciden en la importancia de las habilidades de liderazgo. Esto significa gestionar de forma ascendente, comprendiendo qué es importante para la junta directiva y por qué. También implica una comunicación efectiva con el departamento de recursos humanos, el departamento legal y los altos ejecutivos, quienes son cruciales para avanzar en sus prioridades y asegurar mayores inversiones en tecnología.

Para crear relaciones sólidas, identifique a las partes interesadas, pase tiempo con ellas y muestre un interés genuino en su trabajo y sus desafíos. Colabore en iniciativas importantes para que, cuando surja una crisis, sus colegas ya lo vean como un jugador de equipo y estén ansiosos por apoyar sus esfuerzos.

# Conviértase en un líder de seguridad con Splunk

**Perspectivas de Splunk: por líderes, para líderes**

¿Está buscando más liderazgo intelectual y perspectivas de los CISOs? Descubra cómo los líderes de seguridad abordan los desafíos más críticos de la actualidad, como el cumplimiento normativo, la inteligencia artificial y el panorama de amenazas en evolución.

Obtenga las opiniones de los ejecutivos

**El estado de la seguridad en 2024: La carrera para aprovechar la IA**

Descubra cómo los líderes y profesionales de seguridad abordan oportunidades y obstáculos como los mandatos de cumplimiento, la escasez de talentos y el auge de la IA generativa.

Lea el informe

# Apéndice del sector

## Fabricación

En comparación con sus contrapartes del sector, los CISOs de fabricación se sienten menos respaldados por sus altos ejecutivos y, en general, expresan menos optimismo sobre sus presupuestos de colaboración y ciberseguridad. Esta falta de apoyo podría ser un factor que explique por qué el sector manufacturero sufre más ciberataques que otros sectores.

Es menos probable que los CISOs digan que su alta gerencia apoya la estrategia del equipo cibernético y defiende sus políticas (41% en comparación con el 57% de los CISOs en todos los sectores). También es menos probable (52%) que sientan que los IRC de sus equipos cibernéticos son importantes para sus juntas directivas, en comparación con el 64% de todos los sectores.

En cuanto a la financiación de la ciberseguridad, solo el 20% de los encuestados del sector manufacturero indicó que sus organizaciones ofrecen presupuestos adecuados para la ciberseguridad. Además, solo el 50% cree que puede convencer a sus juntas directivas de que aumenten los presupuestos de sus equipos cuando sea necesario. El gasto en manufactura está por debajo del promedio mundial, con un gasto anual esperado de 65 millones de dólares frente a 75 millones de dólares.

Con un apoyo limitado y una aceptación menos estratégica de la ciberseguridad, las organizaciones manufactureras pueden ser cada vez más propensas a vulnerabilidades, como credenciales robadas (informadas por el 58% de los CISOs) y procesos de respuesta a incidentes indefinidos (44%), que han llevado a ataques exitosos. El 95% del sector informa haber sido víctima de ciberataques varias veces en los últimos 12 meses (en comparación con el 82% de las organizaciones de todos los sectores). A pesar de estos ataques, solo el 9% de las juntas directivas del sector citan el fortalecimiento de su programa cibernético como la inversión futura más significativa.

Es posible que los miembros de las juntas directivas de los fabricantes estén más preocupados por el panorama geopolítico. El 36% de ellos (en comparación con el 25% en todos los sectores) perciben la inestabilidad geopolítica como el mayor riesgo para la organización, posiblemente porque la fabricación está distribuida globalmente y se ve afectada por interrupciones en la cadena de suministro.

Para estar en sintonía con sus juntas directivas, los CISOs de fabricación tienen oportunidades de aumentar el enfoque en el cumplimiento normativo. El 64% de las juntas directivas citan el cumplimiento como una métrica principal para el éxito de los CISOs, pero solo el 26% de los CISOs informan que su equipo dedica mucho tiempo y esfuerzo a cuestiones legales y normativas.

## Servicios financieros

Los CISOs del sector de servicios financieros tienden a tener relaciones más exitosas con sus juntas directivas que los de otros sectores. Entienden que el retorno de la inversión en seguridad indica su éxito (el 60% está de acuerdo), una métrica esencial que utilizan las juntas directivas para evaluar el desempeño de los CISOs (64%).

Sin embargo, el sector no está exento de dificultades. Los servicios financieros tienen más probabilidades que cualquier otro sector de ser víctimas de ataques de ransomware: el 65% experimentó al menos uno en el último año, en comparación con el 48% de las organizaciones de todos los sectores. Mientras que los atacantes de ransomware buscan premios lucrativos, las juntas directivas de este sector priorizan el fortalecimiento de sus programas cibernéticos. El 55% se centrará en la ciberseguridad como su prioridad de inversión número uno, en comparación con el 24% de las juntas directivas de todos los sectores. Algunas de las brechas más amplias incluyen la seguridad de terceros y de la cadena de suministro (68%) y la infraestructura en la nube (56%).

Los CISOs a menudo tienen un lugar en la mesa, ya que el 42% participa en las reuniones de la junta directiva la mayor parte del tiempo (en comparación con el 20% de los CISOs de todos los sectores). Además, cuando colaboran en el presupuesto de ciberseguridad, es más probable que sus juntas directivas califiquen positivamente este aspecto de su relación de trabajo. El 73% piensa que la asociación entre la junta directiva y los CISOs es eficaz, en comparación con solo el 32% de las juntas directivas de todos los sectores. La salud de esta asociación puede influir en un mayor nivel de inversión del sector en ciberseguridad. Las organizaciones de servicios financieros gastan en promedio 105 millones de dólares anuales en ciberseguridad, muy por encima del promedio de 75 millones de dólares de todos los sectores.

Otro ámbito en el que los servicios financieros son líderes es la IA generativa. Los encuestados de FSI eran más propensos a creer que los defensores cibernéticos obtendrían una ventaja sobre los adversarios al usar la nueva tecnología (el 44% en comparación con el 25% de los encuestados de todos los sectores). Este optimismo se traduce en una mayor adopción de la IA generativa, ya que el 46% de las juntas directivas del sector de servicios financieros afirman que sus equipos de ciberseguridad están utilizando IA generativa, en comparación con solo el 24% en todos los sectores.

## Medios de comunicación

La relación entre el CISOs y la junta directiva en el sector de los medios de comunicación es compleja. Si bien los CISOs tienen cierto contacto directo, no suelen participar en las reuniones de la junta directiva. Aunque los equipos de ciberseguridad parecen recibir financiación adecuada, muchas organizaciones del sector no han realizado inversiones en medidas de ciberseguridad adecuadas que puedan evitar ataques exitosos.

Si bien la mayoría de los CISOs del sector de medios de comunicación están cumpliendo con las expectativas de sus juntas directivas, un preocupante 9% tiene un "rendimiento considerablemente inferior" (en comparación con el 1% de los CISOs de todos los sectores). Esto puede deberse a que los CISOs de los medios de comunicación tienen menos probabilidades de alinear las prioridades de su equipo con las prioridades de seguridad de la junta directiva (el 51% lo hace frente al 62% de los CISOs de todos los sectores).

Los CISOs también tienen dificultades para comunicar a sus juntas directivas el progreso logrado en sus objetivos de seguridad. El 35% de los CISOs indicaron que esta área de su relación laboral es muy buena o excelente, mientras que solo el 27% de sus juntas directivas indicaron lo mismo. Esta falta de alineación podría corregirse si los CISOs tuvieran más tiempo presente durante las reuniones de la junta directiva para brindar mayor transparencia a las iniciativas cibernéticas y garantizar que se alineen con las prioridades de la junta. Mientras el 78% de los CISOs tienen "al menos algún contacto directo" con sus juntas directivas, solo el 7% de los CISOs del sector de medios de comunicación participan la mayor parte del tiempo o siempre en las reuniones de la junta directiva.

A pesar de los desafíos de los CISOs y las juntas directivas, las juntas directivas de los medios de comunicación están dispuestas a aumentar la inversión en ciberseguridad: el 100% indicó que probablemente aumentará la financiación para ciberseguridad en los próximos tres años (frente al 89% de todos los sectores).

De cara al futuro, será fundamental contar con un apoyo financiero constante por parte de la junta directiva. En los últimos 12 meses, el 49% de las organizaciones de medios de comunicación experimentaron ciberataques disruptivos muchas veces, frente al 27% de todos los sectores. Los tipos de ataques más comunes incluyen ingeniería social (69%), DDoS (44%) y apropiación de cuentas (40%). Para abordar estas amenazas, los CISOs y las juntas directivas se beneficiarían de priorizar una mejor capacitación en seguridad destinada a mejorar la higiene de las contraseñas y ayudar a los empleados a reconocer estafas de phishing y otros ataques de ingeniería social.

## Sector público

En muchas áreas, los CISOs del sector público y sus juntas directivas no están sincronizados en lo que respecta a la ciberseguridad. Si bien el 80% de las juntas directivas creen que sus CISOs dedican mucho tiempo a la habilitación empresarial, solo el 26% realmente lo hace. Además, aunque el 51% de los CISOs creen que son capaces de crear con éxito un plan de registro con sus juntas directivas, solo el 20% de sus juntas están de acuerdo.

Para mejorar el consenso y la alineación, los CISOs del sector público deben comprender qué tanto valoran sus juntas directivas la eficacia operativa. El 80% de las juntas del sector público lo califican como *muy importante* o *de máxima importancia*, en comparación con el 29% de todas las juntas que indican lo mismo. Priorizar la eficacia operativa tiene sentido, considerando que el sector a menudo lucha con presupuestos y personal limitados. El gasto promedio en ciberseguridad del sector público fue de 55 millones de dólares en 2024, en comparación con los 75 millones de dólares de todos los sectores.

Al evaluar el desempeño de los CISOs, las juntas directivas enfatizan el retorno de la inversión de seguridad como una métrica clave (el 80% de las juntas directivas del sector público en comparación con el 54% de las juntas directivas de todos los sectores). De cara al futuro, los CISOs deberán comunicar mejor el valor de sus inversiones en seguridad, un cambio que los preparará para el éxito ante sus juntas directivas al presentar IRC, defender futuras inversiones y crear hojas de ruta de seguridad. Alinearse sobre cómo defender el presupuesto también ayudará a los CISOs y sus equipos a abordar la avalancha de ataques de ingeniería social, el tipo de ataque más común que afecta al 72% de las organizaciones del sector público.

Las futuras estrategias de defensa cibernética también podrían incluir IA. Los CISOs y las juntas directivas del sector público están de acuerdo en cuanto a invertir en esa tecnología y acelerar su adopción. Si bien actualmente nadie utiliza IA generativa para casos de uso de ciberseguridad, el 100% de las juntas directivas del sector público afirman que tienen planeado o están pensando hacerlo en los próximos doce meses.

# Apéndice de regiones

## EE. UU.

Los CISOs de EE. UU. generalmente tienen sólidas relaciones de trabajo con sus juntas directivas. Con una mayor alineación en prioridades y presupuestos en comparación con otras regiones, el 71% de los CISOs de los EE. UU. informan estar directamente alineados con las prioridades de su junta, en comparación con el 62% en todo el mundo. Las juntas directivas estadounidenses también son más comprensivas con los desafíos del trabajo de sus CISOs que sus contrapartes globales: el 67% observa que las responsabilidades y expectativas de los CISOs se han vuelto más complejas.

Cuando la junta directiva comprende el papel de los CISOs, y cuando estos, a su vez, comprenden las prioridades de la junta, su relación de trabajo mejora, y también lo hace el presupuesto. Las organizaciones estadounidenses indicaron que sus presupuestos de ciberseguridad son adecuados (el 44% en comparación con el 31% en todo el mundo). Sus CISOs también indicaron que pueden convencer a las juntas directivas para que aumenten el presupuesto si es necesario (el 68% en comparación con el 59% de los CISOs en todo el mundo). De hecho, las organizaciones estadounidenses tienen bolsillos más llenos: se espera que el gasto anual en ciberseguridad sea en promedio de 110 millones de dólares, en comparación con los 75 millones de dólares en todo el mundo.

Dado que los CISOs de los EE. UU. parecen entender qué valoran las juntas directivas, pueden ofrecer mejores resultados y cumplir con sus expectativas. El 15% de las juntas directivas de los EE. UU. afirman que sus CISOs tienen un rendimiento superior al esperado, en comparación con el 8% en todo el mundo. Por supuesto, hay oportunidades para progresar. Los CISOs de los EE. UU. pueden tener más éxito si enfatizan el retorno de la inversión de seguridad durante las conversaciones con los miembros de la junta directiva. Si bien el 55% de sus juntas directivas citan esto como una métrica para evaluar el éxito de los CISOs, solo el 35% de los CISOs lo clasifican como un indicador de desempeño superior.

Para seguir siendo competitivas en el escenario global, las organizaciones estadounidenses necesitarán aumentar la adopción de la IA generativa. Solo el 15% de los miembros de juntas directivas de la región utilizan tecnología para ciberseguridad, en comparación con el 24% en todo el mundo. Este hallazgo contrasta con el hecho de que más de la mitad (el 54%) de los encuestados en la región cree que la IA generativa dará una ventaja a los adversarios cibernéticos. De cara al futuro, los CISOs de los EE. UU. podrían tener que priorizar la adopción de la IA para mantener el ritmo de los competidores y superar a los ciberatacantes.

## Europa

En comparación con los CISOs de todo el mundo, los CISOs europeos pueden defender mejor sus respectivas organizaciones de ciberseguridad e invertir en tecnologías avanzadas, como la IA generativa. Es más probable que las juntas directivas europeas tengan un subcomité centrado en ciberseguridad (55%) que sus contrapartes globales. Los CISOs en Europa también tienen más probabilidades de participar en reuniones de directorio al menos con cierta frecuencia (87%) que sus contrapartes en otras regiones.

A pesar de estas tendencias positivas, los CISOs en Europa tienen margen de mejora a la hora de promover iniciativas de ciberseguridad y aumentos de financiación. El 49% tiene menos probabilidades de informar que su relación de trabajo con la junta directiva va bien, una cifra inferior al promedio mundial. La mayoría piensa que la mejor manera de defender las inversiones es debatir métricas y recomendaciones sobre riesgos cibernéticos (55%) y requisitos de cumplimiento (49%). Sin embargo, es más probable que sus juntas directivas aprueben aumentos presupuestarios cuando los CISOs demuestran que la seguridad es un facilitador del negocio (58%) y describen los costos del tiempo de inactividad (56%).

Algunos de estos aumentos presupuestarios podrían destinarse a la adopción de la IA generativa para la ciberseguridad, un área en la que Europa está a la vanguardia. El 39% de las organizaciones en Europa implementó la IA para iniciativas de ciberseguridad, en comparación con el 24% en todo el mundo. Los CISOs europeos también están a la vanguardia en el establecimiento de protocolos para determinar las tareas que pueden ser gestionadas mejor por la IA y aquellas que pueden ser abordadas mejor por los miembros del equipo de seguridad.

Cuando se trata de ataques de ransomware, las organizaciones europeas también están mejor protegidas. Solo el 3% de quienes sufrieron un ataque de ransomware pagaron el rescate directamente (menos que el promedio mundial) y el 23% indicó que el seguro cibernético lo cubre en caso de un ataque (más que los encuestados de todas las demás regiones).

## Asia Pacífico

Los CISOs de Asia Pacífico tienden a tener relaciones más débiles con sus juntas directivas que sus contrapartes globales. Además, tienen menos éxito cuando defienden la ciberseguridad y abogan por aumentos presupuestarios. Son pocos los que indicaron que es muy probable que sus juntas directivas apoyen el aumento de la inversión de la organización en ciberseguridad durante los próximos tres años (el 18% de los CISOs de Asia Pacífico frente al 27% en todo el mundo).

Mientras tanto, es menos probable que las juntas directivas de Asia Pacífico consideren el fortalecimiento de su programa cibernético como una alta prioridad de inversión para los próximos 12 meses (el 9% frente al 24% de las juntas directivas de todo el mundo). En cambio, los altos ejecutivos de Asia Pacífico están más centrados en el crecimiento empresarial: el 38% lo citó como la prioridad número uno.

Una ventaja que tienen los CISOs de Asia Pacífico es que participan con mayor frecuencia en las reuniones de la junta directiva, ya que el 22% indicó que está presente en la mayoría o en la totalidad de las reuniones de la junta directiva. Si reorientan sus conversaciones para educar a las juntas directivas sobre las amenazas cibernéticas, es más probable que estas respalden aumentos presupuestarios o una nueva iniciativa de ciberseguridad.

Otro desafío que enfrentan las organizaciones de Asia Pacífico es el cumplimiento. El 28% de los CISOs de esta región afirman que fueron presionados para no informar un incidente o problema de cumplimiento, el porcentaje más alto de todas las regiones. Esto puede deberse en parte a que Asia Pacífico está rezagada en el establecimiento de una gobernanza clara para la notificación de incidentes de ciberseguridad: el 40% de las organizaciones de la región han definido protocolos claros de notificación de incidentes, lo que la sitúa por detrás de las otras dos regiones.

Cuando se les preguntó en qué medida su organización utiliza actualmente IA generativa para la ciberseguridad, el 18% de las juntas directivas en Asia Pacífico informaron que la utilizan en cierta medida, muy por detrás del promedio mundial. Sin embargo, eso podría cambiar muy pronto. El 44% de las juntas directivas planean aplicar IA generativa para fines de ciberdefensa en los próximos 12 meses, y otro 35% expresó interés en la idea.

# Metodología

Los investigadores de Oxford Economics encuestaron a 600 personas (500 CISOs, directores de seguridad o líderes de seguridad equivalentes, y 100 miembros de juntas directivas) en junio y julio de 2024. Las categorías de encuestados incluyeron CISOs que se identificaron como miembros de la junta directiva. Los participantes se encontraban en Australia, Francia, Alemania, Italia, la India, Japón, Nueva Zelanda, Singapur, el Reino Unido y Estados Unidos. También representaron a 16 sectores: agricultura, servicios empresariales, construcción/ingeniería, educación, energía y servicios públicos, servicios financieros, gobierno, atención médica, ciencias biológicas, servicios de información, tecnología, fabricación, venta minorista, bienes de consumo, telecomunicaciones y medios de comunicación. Oxford Economics también realizó ocho entrevistas en profundidad con CISOs y miembros de juntas directivas para obtener información cualitativa.

# Acerca de Splunk

Splunk, una empresa de Cisco, ayuda a que las organizaciones sean más resilientes digitalmente. Las organizaciones líderes utilizan nuestra plataforma unificada de seguridad y observabilidad para mantener sus sistemas digitales seguros y confiables. Las organizaciones confían en Splunk para evitar que los incidentes de infraestructura, aplicaciones y seguridad se conviertan en problemas importantes; para recuperarse más rápido de los impactos en los sistemas digitales; y para adaptarse con rapidez a nuevas oportunidades.

Continúe en contacto con Splunk.

splunk> a CISCO company

Splunk, Splunk> y Turn Data Into Doing son marcas comerciales y marcas comerciales registradas de Splunk LLC. en Estados Unidos y otros países. El resto de los nombres de marcas, nombres de productos o marcas comerciales pertenecen a sus respectivos propietarios. © 2025 Splunk LLC. Todos los derechos reservados.

25_CMP_report_CISO-report-2025_ES_v13