II Estudio

Radiografía de la ciberseguridad en directorios de Chile

2024

INSTITUTO DE DIRECTORES DE CHILE

CIC -IOT IIOT

Equipo de trabajo:

Instituto de Directores de Chile

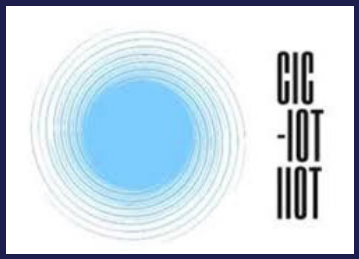
Fadua Gajardo, directora ejecutiva
Paulina Ramírez, consultora senior
Carolina Prieto, gerente de comunicaciones y marketing
Marcelo Díaz, subgerente de comunicaciones y marketing
Victoria Duch, periodista
Camila Herrera, diseñadora

Centro de Investigación de Ciberseguridad IOT-IIoT

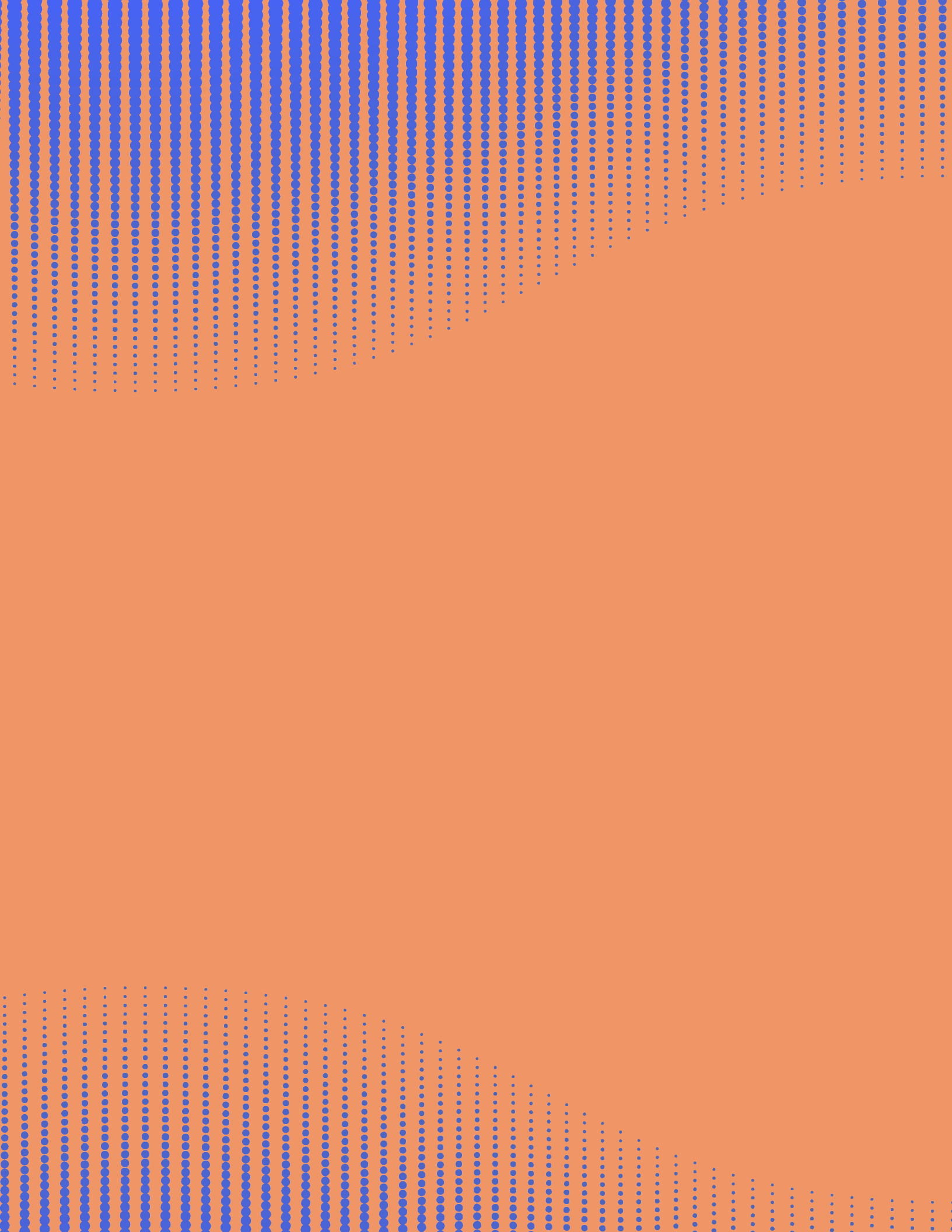
Freddy Macho, presidente del directorio
Adriana Rodríguez, gerente de operaciones
Luigi Castoro, consultor de ciberseguridad

Fecha de publicación: **Noviembre 2024**

INSTITUTO DE
DIRECTORES
DE CHILE



Índice



CARTA

Instituto de Directores de Chile

Actualmente, la ciberseguridad se ha convertido en una prioridad crítica para las organizaciones que buscan no solo garantizar su sostenibilidad, sino también protegerse de las crecientes amenazas en el entorno digital. Conscientes de la importancia de resguardar la información y asegurar la continuidad operativa, el Instituto de Directores de Chile (IdDC), en conjunto con el Centro de Investigación de Ciberseguridad IOT-IIoT, ha desarrollado el Estudio Radiografía de la ciberseguridad en directorios de Chile 2024, el cual tiene como objetivo analizar el grado de preparación, las mejores prácticas y los desafíos clave que enfrentan los directorios en Chile en materia de ciberseguridad.

Este estudio presenta un análisis detallado sobre el nivel de preparación de los directorios empresariales frente a las amenazas cibernéticas emergentes, ofreciendo una visión completa de cómo las organizaciones están abordando estos desafíos cada vez más complejos. A través de la recopilación y el análisis de datos, se busca no solo evaluar cuán preparados están los directorios para gestionar estos riesgos, sino también identificar tanto los éxitos destacados en materia de seguridad, como las áreas que requieren mayor atención y mejora.

En esa línea, el objetivo es proporcionar una hoja de ruta clara para que las organizaciones fortalezcan su estrategia de ciberseguridad a nivel directivo.
Es fundamental que los directorios evolucionen sus agendas para incluir de manera proactiva la ciberseguridad, no solo como una cuestión técnica, sino como una prioridad estratégica. Las crecientes regulaciones y la transformación digital exigen una comprensión más profunda de estos riesgos, así como la implementación de políticas y estrategias que resguarden la integridad de la información y la continuidad del negocio.

Este informe, fruto del compromiso del IdDC y el Centro de Investigación de Ciberseguridad IOT-IIoT, busca contribuir a la mejora de la gobernanza de la ciberseguridad en Chile, ofreciendo una radiografía clara sobre las áreas de oportunidad y recomendando acciones concretas que permitirán a los directorios liderar con mayor eficacia en un entorno cada vez más digitalizado.

Agradecemos profundamente a todos los participantes por su contribución. Confiamos en que los hallazgos de este estudio serán una herramienta clave para guiar las discusiones estratégicas y fortalecer la resiliencia organizacional frente a los desafíos del futuro.

Fadua Gajardo
Directora ejecutiva del IdDC

CARTA

Centro de Investigación de Ciberseguridad IOT-IIoT

En el entorno empresarial actual, cada vez más complejo e incierto, la composición de los directorios es un factor clave para el éxito. El rol del director ha evolucionado significativamente, y hoy se necesita un equipo de gobierno diverso y complementario en términos de experiencias, conocimientos y habilidades, no solo un grupo de expertos sectoriales.

La ciberseguridad se presenta como uno de los principales desafíos para los directorios, pues los riesgos cibernéticos impactan directamente en la sostenibilidad de las empresas, inmersas en un escenario de transformación y disrupción. Un liderazgo firme en ciberseguridad ofrece ventajas competitivas y permite el desarrollo de nuevas líneas de negocio, mejorando el rendimiento financiero y captando la atención de inversores.

Para los directorios comprometidos, la adopción de medidas concretas que mitiguen los riesgos cibernéticos es una prioridad ineludible. La implicación del directorio en la estrategia de ciberseguridad y su reflejo en el presupuesto son determinantes para que las iniciativas en este ámbito se conviertan en acciones efectivas y financiables, lo cual es crucial no solo por responsabilidad, sino también por competitividad y resiliencia.

Con el Instituto de Directores de Chile, hemos lanzado la segunda "Radiografía de la Ciberseguridad en los Directorios de Chile 2024", un estudio que examina los avances y desafíos en ciberseguridad para los directores de empresas en Chile. Esta iniciativa ofrece herramientas para aumentar la concientización y acelerar acciones que fortalezcan la seguridad y el gobierno corporativo en las organizaciones.

Desde el Centro de Investigación de Ciberseguridad IoT – IIoT, nos comprometemos a impulsar la ciberseguridad en las empresas de Chile. Con este propósito, proveemos módulos de ciberseguridad robustos para los directorios a través de los programas del Instituto de Directores de Chile (IdDC).

Una empresa preparada en ciberseguridad es sinónimo de un directorio capacitado, y esperamos que la "Radiografía de la ciberseguridad en directorios de Chile 2024" sea un aporte valioso para todas las organizaciones en su camino hacia una mayor protección y éxito sostenido.

Una empresa preparada en ciberseguridad es sinónimo de un directorio capacitado.

Esperamos que esta "Radiografía de la ciberseguridad en directorios de Chile 2024" sea un aporte para todas las empresas en Chile. Estamos convencidos de que cuando el directorio de una empresa asume un rol activo en la ciberseguridad puede ayudar a garantizar el éxito de la organización.

Freddy Macho
Presidente del Centro de Investigación de Ciberseguridad IoT – IIoT

INTRODUCCIÓN

Resumen ejecutivo

El presente estudio, "Radiografía de la ciberseguridad en directorios de Chile 2024", desarrollado por el Instituto de Directores de Chile en colaboración con el Centro de Investigación de Ciberseguridad IoT - IIoT, explora los desafíos que enfrentan los directorios en la gestión de la ciberseguridad, así como los avances en su percepción y reporte. En 2024, se ha observado un aumento en la frecuencia y claridad de los informes de riesgo, destacándose un crecimiento en los reportes trimestrales y mensuales, lo cual refleja un enfoque más proactivo. El estudio también revela que un menor número de organizaciones reporta incidentes solo en casos críticos y que ha mejorado el conocimiento sobre la práctica de informes, disminuyendo la cantidad de directores que desconocen si estos se realizan. Entre las principales recomendaciones para fortalecer la ciberseguridad corporativa se encuentran la implementación de una estructura de gobernanza sólida, la asignación de un presupuesto estratégico, la capacitación continua de colaboradores y la contratación de expertos en ciberseguridad. La carencia de estos perfiles especializados incrementa la vulnerabilidad de las empresas frente a amenazas que cada vez son más frecuentes.

Además, el estudio resalta un incremento en la presencia de integrantes calificados en ciberseguridad dentro de los directorios o como asesores externos, evidenciando un compromiso creciente en la protección de la información dentro de las organizaciones. Asimismo, un mayor número de empresas ha adoptado metodologías de evaluación de riesgos en línea con estándares internacionales. La nueva Ley Marco de Ciberseguridad en Chile se percibe como un impulsor clave para mejorar la preparación de las empresas, aunque un 65% de los directores aún desconoce su impacto.

El compromiso de los directorios con la ciberseguridad es cada vez mayor. El informe no solo evidencia una mejora en la proactividad y estructuración de la ciberseguridad a nivel de directorios, sino que también resalta la necesidad urgente de acelerar la adopción de buenas prácticas en gobernanza, evaluación de riesgos y capacitación del personal. Esto es especialmente relevante en un entorno donde las amenazas de ciberataques son cada vez más constantes y complejas.

INTRODUCCIÓN

Metodología

Objetivo

El objetivo principal de este estudio es analizar y evaluar en profundidad la situación actual de la ciberseguridad en los directorios de Chile, proporcionando una radiografía clara y detallada del estado de preparación frente a las amenazas digitales emergentes. Mediante la recopilación exhaustiva de información a través de un instrumento de evaluación diseñado específicamente para este propósito, el Instituto de Directores de Chile, en colaboración con el Centro de Investigación de Ciberseguridad IOT-IIoT, busca no solo entender el nivel de preparación existente, sino también identificar las mejores prácticas y debilidades en la gestión de la ciberseguridad por parte de los directorios de nuestro país.

Este análisis permitirá detectar con precisión las áreas críticas que necesitan mejoras, así como los riesgos que podrían comprometer la seguridad de la información y la operación empresarial. Además, se buscará identificar las oportunidades estratégicas que las organizaciones pueden aprovechar para fortalecer sus políticas y mecanismos de defensa cibernética.

Con una visión orientada al futuro, este estudio pretende proporcionar recomendaciones basadas en datos que permitan a las empresas chilenas mejorar su gobernanza en ciberseguridad, no solo para cumplir con las regulaciones actuales, sino para adelantarse a posibles cambios normativos y proteger de manera efectiva sus activos digitales en un entorno cada vez más complejo y globalizado.

Grupo muestral

La encuesta fue enviada a la red del Instituto de Directores de Chile a través de correo electrónico, a una muestra de 100 participantes.

Metodología de elaboración del informe

El cuestionario utilizado para la evaluación comprende un conjunto de 18 preguntas en total:

Tema 1:

Gestión de riesgos cibernéticos en el directorio

1. ¿Es usted director de empresa y/o reporta directamente al directorio?
2. ¿La primera línea de gerencia presenta al directorio dashboard y métricas sobre las amenazas cibernéticas emergentes?
3. ¿Su organización cuenta con una metodología de riesgo de seguridad?

3.1 ¿El directorio conoce la existencia de la metodología mencionada en la pregunta anterior?

3.2 En caso de contar con una metodología de riesgo de seguridad en la organización, por favor indique el nombre de la misma.

4. ¿Con qué regularidad se presentan informes de riesgo cibernético al directorio?
5. ¿Ha sido su organización víctima de pérdidas de datos o filtración de actas de directorios?

5.1 ¿Cuál fue el impacto de la pérdida de datos o filtración de actas en su organización?

6. ¿Qué importancia le asigna a tener toda la información en un solo lugar?

Tema 2:
Conciencia, preparación y estrategias
7. ¿El directorio conoce la existencia de la nueva Ley Marco de Ciberseguridad de Chile?
8. ¿El directorio conoce la existencia de las sanciones y multas consideradas en la nueva Ley Marco de Ciberseguridad de Chile?
9. ¿El directorio conoce la creación de la Agencia Nacional de Ciberseguridad (ANCI) como nuevo ente regulador en el ámbito de la ciberseguridad en Chile?
10. ¿El directorio conoce el impacto que tendrá la aplicación de la nueva Ley Marco de Ciberseguridad de Chile en su empresa?
11. ¿El directorio asigna un uso estratégico del presupuesto de seguridad, realizando el gasto de manera coherente en herramientas / soluciones / servicios de seguridad y capacitación?
12. ¿La organización dispone de una adecuada protección que permite resguardar y proteger la operación en el escenario de que sea objeto de un ataque?
12.1 ¿El directorio conoce la existencia de un plan de protección de ciberataque?
13. ¿El directorio considera los aspectos de seguridad en las principales decisiones comerciales, como fusiones y adquisiciones, asociaciones, lanzamientos de nuevos productos o servicios, entre otras acciones de la organización de manera oportuna?
Tema 3:
Supervisión y gobernanza en la ciberseguridad
14. ¿El directorio cuenta con una estrategia de comunicación segmentada para el público, reguladores, agencias de calificación, que estén alineadas a los escenarios de ciberseguridad de su organización?
15. ¿El directorio supervisa que la organización esté verificando adecuadamente la legislación, las regulaciones y las normativas técnicas actuales y potenciales relacionadas con la seguridad?
16. ¿El directorio facilita a la organización una estructura de gobernanza de seguridad que entregue un estatus de la seguridad de la información, la seguridad informática, la ciberseguridad y la protección de los datos respectivamente?
17. ¿El directorio cuenta con un punto de control de ciberseguridad?
17.1 Por favor indique en qué estructura del directorio asigna esta responsabilidad.
18. ¿El directorio cuenta con al menos un integrante calificado en materias de ciberseguridad?

Técnica utilizada

Los participantes decidieron contribuir de forma anónima y voluntaria, garantizando la confidencialidad de sus respuestas.

La ventana de tiempo para completar la encuesta abarcó desde el 5 de septiembre hasta el 30 de septiembre, permitiendo a los participantes tener un período adecuado para compartir sus opiniones y percepciones. El tiempo promedio necesario para finalizar la encuesta fue de 8 minutos, asegurando una experiencia eficiente para los encuestados.

El análisis de los datos se llevó a cabo entre el 30 de septiembre y el 7 de octubre, la cual fue realizada por el Instituto de Directores de Chile. Durante este período, se aplicaron métodos tanto cuantitativos como cualitativos para explorar en profundidad los resultados obtenidos en el estudio. Este enfoque dual permitió una comprensión integral de las tendencias numéricas y de las perspectivas cualitativas proporcionadas por los participantes.

Resultados

Resultados

¿Está el directorio realmente informado?

En un entorno empresarial cada vez más digitalizado, la ciberseguridad ha dejado de ser una preocupación técnica exclusiva del área de TI para convertirse en un asunto de suma relevancia en la agenda directiva. En este contexto, uno de los aspectos clave para una gestión efectiva de los riesgos cibernéticos es la capacidad de los directorios para recibir información clara y actualizada sobre las amenazas emergentes que puedan comprometer la seguridad de una organización.

A través de esta pregunta, el estudio busca identificar la frecuencia con la que los directorios reciben información clave sobre la ciberseguridad, evaluando si esta comunicación es regular, ocasional o inexistente, y cómo esto afecta la preparación de las organizaciones para responder a posibles amenazas. La capacidad de actuar proactivamente frente a los riesgos depende, en gran medida, de la visibilidad que los directores tengan sobre el panorama de amenazas, lo que hace imprescindible contar con reportes periódicos y bien estructurados.

01.

Gestión de riesgos cibernéticos en el directorio

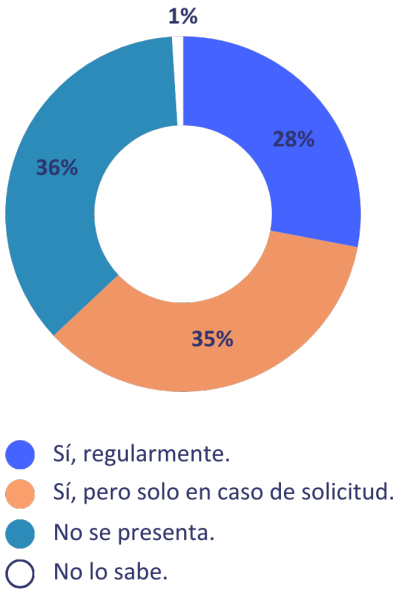
¿La primera línea de gerencia presenta al directorio dashboard y métricas sobre las amenazas cibernéticas emergentes?

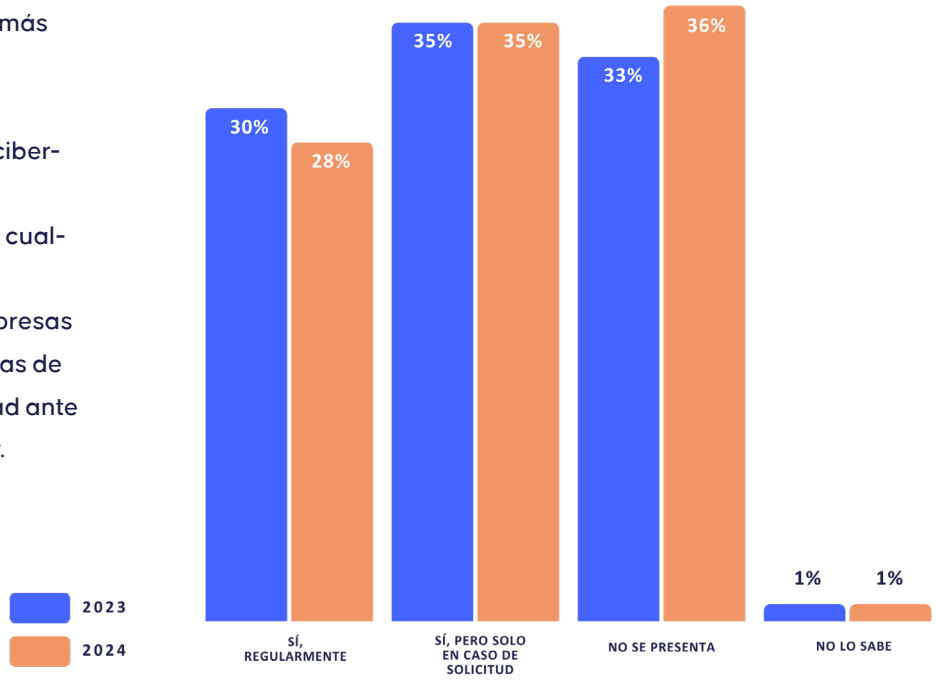
La comunicación de riesgos cibernéticos y presentación de métricas al directorio es un área que requiere fortalecimiento en la mayoría de las organizaciones. Con solo el 28% presentando métricas de forma regular, hay un claro margen de mejora.

El 36% que no presenta ninguna métrica debe abordar esta falta de comunicación para garantizar que el directorio esté informado de las amenazas emergentes y pueda participar activamente en la definición de la estrategia de ciberseguridad.

Aquellas organizaciones que presentan métricas solo a solicitud (35%), podrían considerar la implementación de reportes periódicos para mejorar la toma de decisiones y fomentar una gestión más proactiva de los riesgos.

La gestión eficaz de los riesgos de seguridad cibernética es un pilar clave en la protección de los activos digitales y la continuidad operativa de cualquier empresa. Contar con una metodología formal de gestión de riesgos permite a las empresas identificar, evaluar y mitigar riesgos o amenazas de manera proactiva, reduciendo la vulnerabilidad ante los incidentes de seguridad que pueden surgir.





Las respuestas reflejan una leve tendencia hacia la falta de presentación regular de información sobre amenazas cibernéticas emergentes al directorio. En 2024, el porcentaje de respuestas que indica que esta información "no se presenta" aumentó ligeramente al 36%, en comparación con el 33% en 2023. Esto sugiere una posible desconexión o falta de prioridad en la comunicación de riesgos cibernéticos a niveles directivos. Aunque el 35% de las respuestas en ambos años señala que la presentación ocurre solo "en caso de solicitud", solo alrededor del 30% reporta una presentación regular.

Esta falta de coherencia en la actualización de datos críticos puede representar un riesgo para la organización, al no mantener al directorio completamente informado sobre amenazas cibernéticas emergentes.

Un estudio realizado por Amcham y el IdDC en 2022, titulado "Las claves de una estrategia saludable en ciberseguridad", destacó la necesidad de desarrollar un modelo dinámico y ágil de gestión de riesgos de ciberseguridad. Este enfoque no solo facilita el crecimiento ordenado de las organizaciones, sino que también permite anticipar los riesgos en constante evolución. Implementar una metodología de gestión de riesgos es fundamental para mantener la seguridad en un entorno empresarial que cada vez está más digitalizado y expuesto. Invertir en ciberseguridad no solo protege a la organización, sino que también genera valor al proporcionar una protección sólida y adaptable a las vulnerabilidades. [1]

1 Instituto de Directores de Chile, A. (s/f). Las claves de una estrategia saludable en ciberseguridad. https://iddc.cl/wp-content/uploads/2024/02/Las-claves-de-una-estrategia-saludable-en-ciberseguridad.pdf

La siguiente pregunta busca evaluar cuántas organizaciones han adoptado un enfoque estructurado y estandarizado para la gestión de riesgos de seguridad cibernética. La existencia de una metodología bien definida no solo refleja un compromiso con la seguridad y protección de datos, sino que también es un indicativo de la capacidad de la organización para anticiparse a los posibles ciberataques y gestionarlos de forma efectiva.

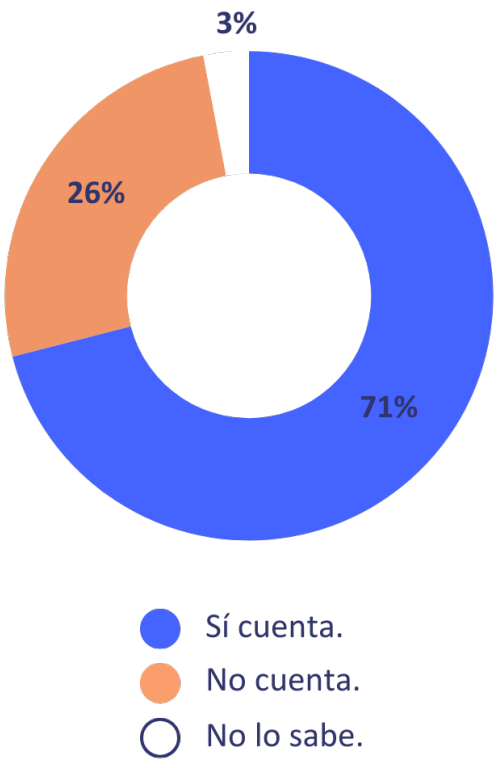
Además, el nivel de conocimiento que el directorio tiene sobre la metodología implementada es fundamental, ya que este es el órgano encargado de tomar decisiones estratégicas y asignar los recursos necesarios para garantizar una ciberseguridad robusta. Para aquellas organizaciones que aún no cuentan con una metodología formal, esta representa un punto crítico que debe ser abordado. La ausencia de una estrategia clara expone a la empresa a mayores riesgos, afectando su capacidad de respuesta ante incidentes y limitando su resiliencia en un entorno digital cada vez más desafiante para todos.

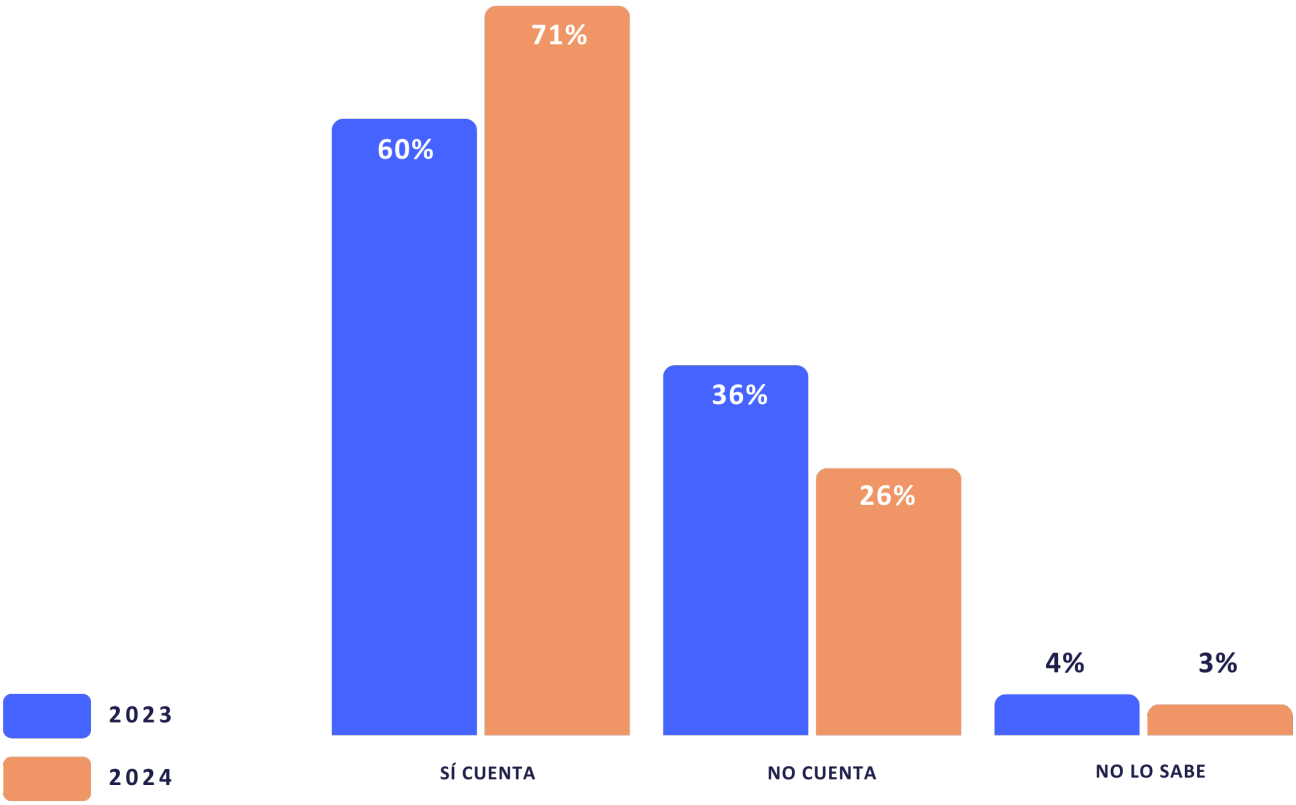
¿Su organización cuenta con una metodología de riesgo de seguridad?

Un 71% de las organizaciones cuenta con una metodología de riesgo de seguridad y, de estas, el 94% afirma que su directorio la conoce. Esto muestra un nivel significativo de adopción y conciencia por parte de su directorio, lo cual es fundamental para una gestión efectiva de riesgos.

El 26% que no cuenta con una metodología representa un área crítica que necesita ser abordada. La falta de una metodología formal puede dejar a estas organizaciones expuestas a amenazas y limitar su capacidad para gestionar incidentes de manera eficaz.

La mayoría de las organizaciones que cuentan con una metodología utilizan estándares internacionales, lo cual es positivo. Sin embargo, el 24% que muestra incertidumbre o falta de conocimiento sobre su metodología apunta a la necesidad de mejorar la comprensión y la formación en la gestión de riesgos dentro de la organización.





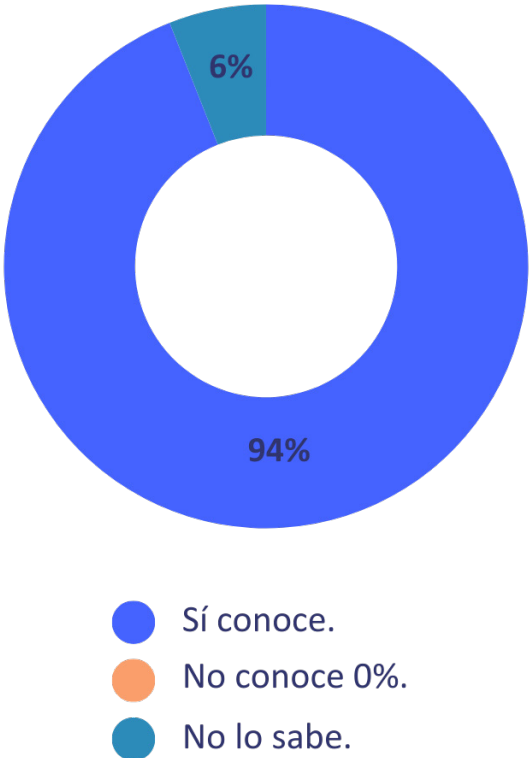
Se puede observar una mejora en 2024 respecto al 2023 en el porcentaje de organizaciones que ya cuentan con una metodología de riesgo de seguridad, aumentando del 65% al 71%. Además, el porcentaje de organizaciones que no tienen una metodología ha disminuido, lo que refleja un avance positivo en la adopción de prácticas de gestión de riesgos de ciberseguridad.

El número de organizaciones que no saben si cuentan con una metodología también ha disminuido, lo cual es un indicativo de una mayor concienciación interna sobre la gestión de riesgos.

Esto indica que existe una tendencia hacia la profesionalización y adopción de prácticas de ciberseguridad en las organizaciones, aunque aún queda un margen para mejorar.

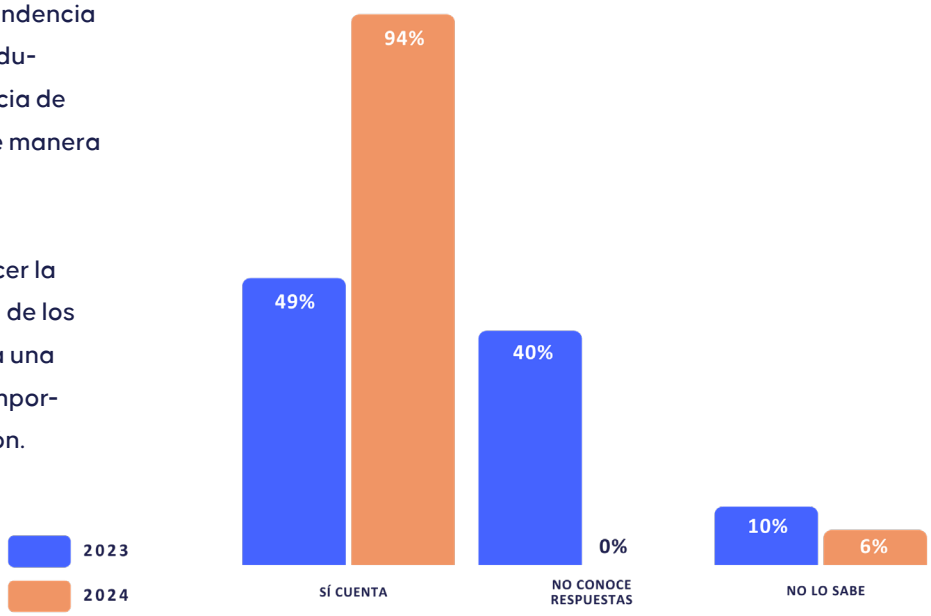
¿El directorio conoce la existencia de la metodología mencionada en la pregunta anterior?

Las mejores prácticas indican que las organizaciones que utilizan estándares internacionales o metodologías específicas no solo demuestran un compromiso sólido con la seguridad, sino que también están mejor preparadas para enfrentar las amenazas emergentes. Sin embargo, la incertidumbre o el desconocimiento sobre el enfoque adoptado puede indicar una falta de alineación interna o de formación adecuada en la gestión de riesgos. Es necesario que todas las áreas claves dentro de la organización estén informadas y alineadas en torno a una misma estrategia, garantizando así una respuesta coherente y coordinada ante cualquier incidente o amenaza.



En 2024, un mayor porcentaje de directorios (94%) está al tanto de la metodología de riesgo de seguridad, lo que muestra una mejora en comparación con 2023, donde el 90% lo conocía. Esta tendencia sugiere un avance en la sensibilización y educación de los directores sobre la importancia de gestionar los riesgos de ciberseguridad de manera formal.

Este año, ningún directorio indicó no conocer la metodología, mientras que en 2023, un 5% de los directorios no estaban al tanto. Esto refleja una mejora en la transmisión de información importante a los altos niveles de una organización.



Analizando riesgos y amenzas

La frecuencia con la que se presentan informes de riesgo cibernético al directorio es un indicador clave de la capacidad que tiene una organización para mantenerse informada y preparada frente a las amenazas cibernéticas.

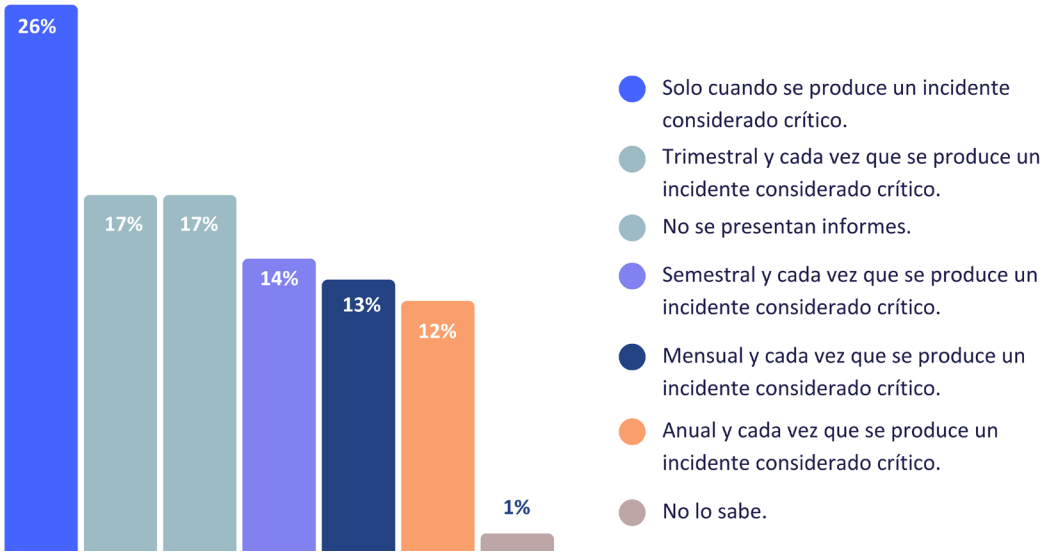
Presentar informes de manera constante y bien estructurada es fundamental para mejorar la toma de decisiones estratégicas dentro de las organizaciones.

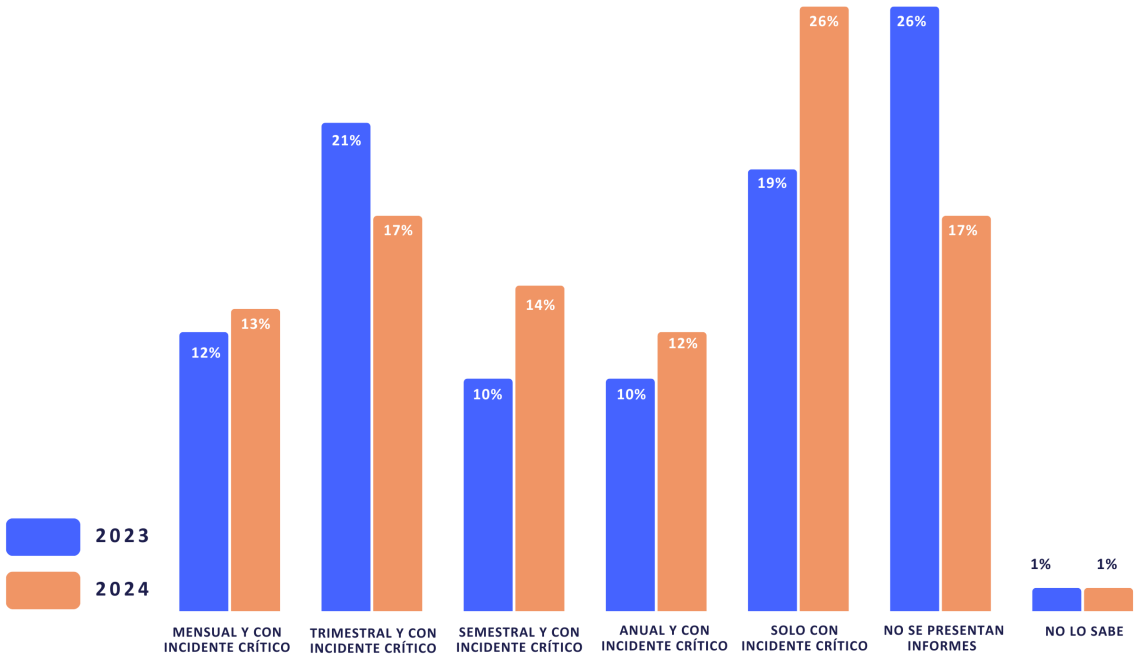
La regularidad en la presentación de estos informes no solo entrega visibilidad sobre el estado actual de la seguridad, sino que también permite a los directorios evaluar proactivamente las vulnerabilidades y ajustar las estrategias de forma oportuna.

La siguiente pregunta busca evaluar cómo las organizaciones gestionan la presentación de estos informes y si existe una regularidad en la comunicación de los riesgos. La variabilidad en las respuestas revela que muchas empresas adoptan enfoques diferentes, desde reportes mensuales hasta aquellos que solo se presentan ante incidentes críticos. Si bien cada empresa puede adaptar la periodicidad de los informes según sus necesidades, la falta de regularidad puede dejar a las empresas expuestas a riesgos no detectados que podrían comprometer a la seguridad de la información y la continuidad operativa.

¿Con qué regularidad se presentan informes de riesgo cibernético al directorio?

La variabilidad en la frecuencia de informes indica que las organizaciones adoptan enfoques diferentes para la gestión de riesgos cibernéticos. Sin embargo, el hecho de que un 17% no presente informes de riesgo cibernético y que otro 26% solo lo haga ante incidentes críticos revela áreas de mejora. Un enfoque más consistente y proactivo en la presentación de informes ayudaría a fortalecer la seguridad cibernética y a mejorar la toma de decisiones estratégicas. Las mejores prácticas recomendarían al menos informes trimestrales o semestrales combinados con la presentación de informes cuando ocurren incidentes críticos.





La frecuencia en la presentación de informes de riesgo cibernético al directorio entre 2023 y 2024 revela una leve tendencia hacia una mayor regularidad. Sin embargo, la proporción de organizaciones que presentan informes solo cuando ocurre un incidente crítico se mantuvo estable en 26%.

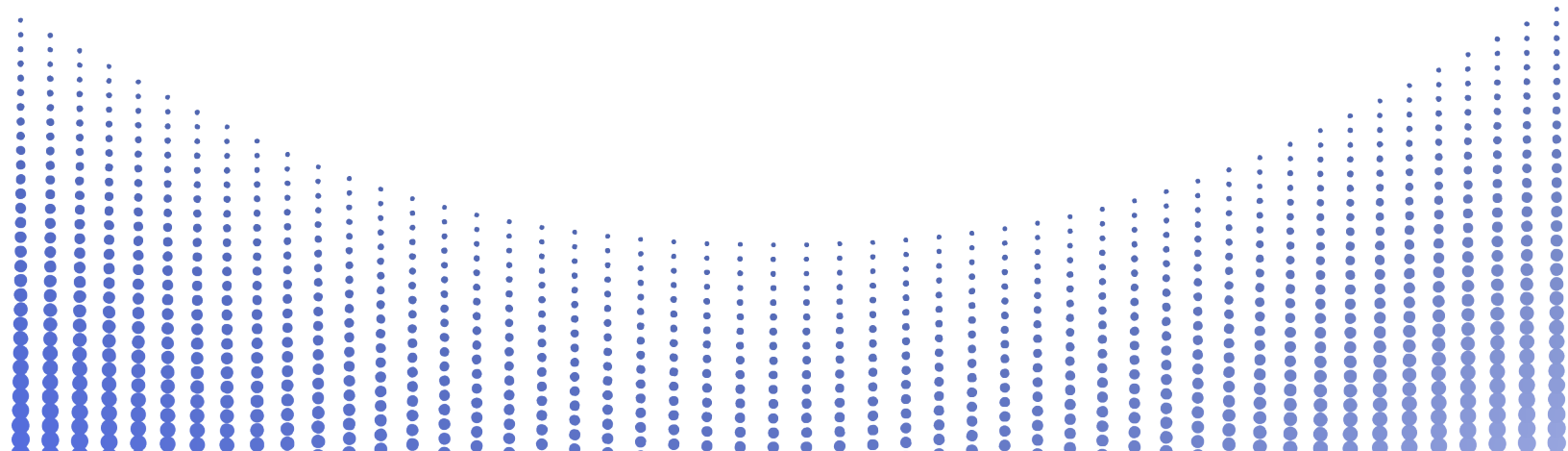
Además, se puede destacar la reducción en el porcentaje de empresas que no presentan informes, del 26% en 2023 al 17% en 2024, lo cual sugiere un compromiso creciente en informar al directorio sobre riesgos cibernéticos.

Este cambio indica una mayor concienciación sobre la importancia de mantener al directorio informado de manera proactiva respecto a las amenazas cibernéticas, contribuyendo a una mejor gestión de riesgos en las organizaciones.

Incidencias y vulnerabilidades en los directorios

Las filtraciones de datos son incidentes de seguridad en los que se accede, se comparte o se hace uso de información sensible y confidencial, sin el permiso adecuado.

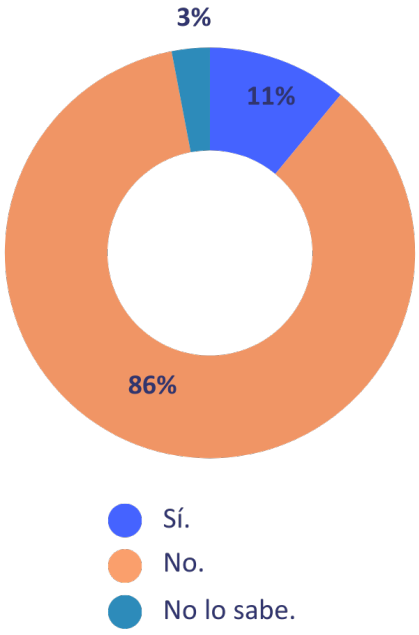
Proteger los datos de una organización es fundamental para su reputación y continuidad. La pérdida o filtración de datos, como las actas de un directorio, puede tener un impacto directo y significativo en las operaciones de una empresa, afectando tanto su imagen como su estabilidad financiera.



¿Ha sido su organización víctima de pérdidas de datos o filtración de actas de directorios?

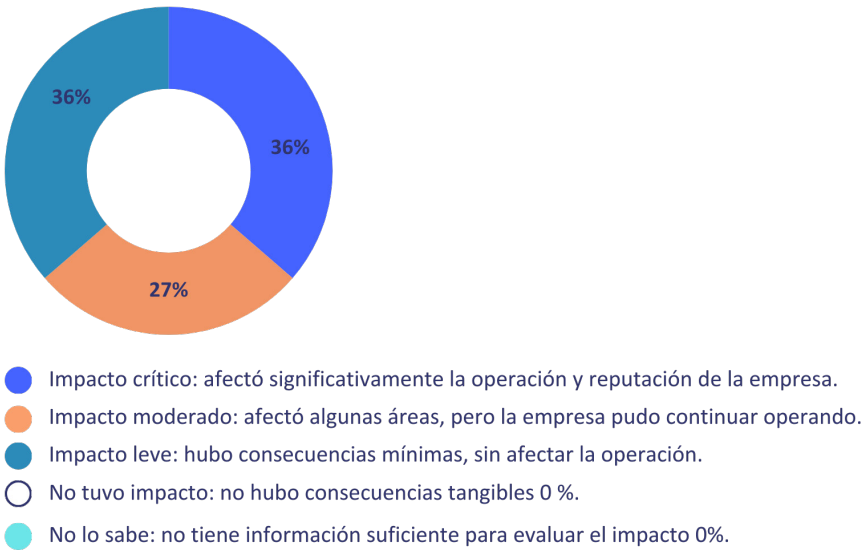
La mayoría de las organizaciones (86%) no han sido víctimas de pérdidas de datos o filtraciones de actas, lo que sugiere que la implementación de medidas de seguridad cibernética puede estar funcionando de manera efectiva en muchas empresas. Sin embargo, el hecho de que un 11% haya sufrido estos incidentes evidencia que aún existen vulnerabilidades que necesitan ser abordadas.

Para aquellas organizaciones que sí fueron víctimas, el impacto varía: el 36% experimentó consecuencias críticas, lo cual puede afectar la continuidad del negocio y su reputación. Esto subraya la importancia de contar con estrategias de prevención, detección y respuesta efectiva para minimizar los riesgos.



Si bien un 86% dice no haber sido víctima de pérdida o filtración de datos, lo que indica que tienen medidas efectivas en materia de ciberseguridad, el hecho de que un 11% haya enfrentado este tipo de incidentes nos dice que persisten vulnerabilidades en los sistemas y que deben ser atendidas. Para eso, las organizaciones y sus directorios deben contar con estrategias sólidas de prevención, detección y respuesta para mitigar riesgos.

¿Cuál fue el impacto de la pérdida de datos o filtración de actas en su organización?

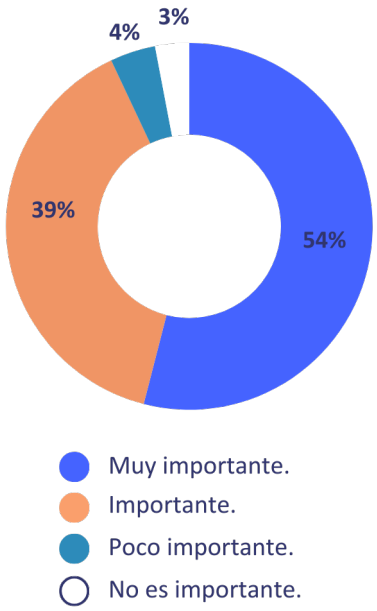


Centralizar la información es un aspecto que las organizaciones deben tomar en cuenta para llevar a cabo la gestión eficiente de sus datos. Mantener toda la información en un solo lugar no solo facilita el acceso rápido y la toma de decisiones más informadas, sino que también mejora la transparencia y simplifica la gestión de riesgos, particularmente en el ámbito de la ciberseguridad.

La siguiente pregunta busca medir la percepción de las organizaciones respecto a la importancia de la centralización de datos y cómo esto influye en su operación del día a día. Un entorno en el que la información centralizada también favorece la implementación de mejores prácticas en seguridad, permitiendo el control mucho más estricto y riguroso sobre los accesos y la protección de datos sensibles.
Las empresas que asignan valor a este aspecto son empresas que indican un enfoque muy claro hacia eficiencia operativa y la seguridad de la información.

¿Qué importancia le asigna a tener toda la información en un solo lugar?

La alta valoración (93% entre "muy importante" e "importante") asignada a la centralización de la información indica que las organizaciones valoran el acceso rápido y eficiente a los datos, lo que podría ser clave para la toma de decisiones, la transparencia y la gestión de riesgos, incluyendo los cibernéticos.
La centralización también puede estar relacionada con mejores prácticas en seguridad, ya que gestionar la información en un solo lugar permite una protección más robusta y un control más efectivo de acceso y permisos.



Nuevo marco regulatorio

En los últimos años, el país ha avanzado en la creación de un marco legislativo para la seguridad de la información y la ciberseguridad, estableciendo bases en la Constitución y diversas leyes, como la Ley de Transformación Digital del Estado y la Ley de Delitos Informáticos, entre otras.

Recientemente, se aprobó la actualización de la Política Nacional de Ciberseguridad 2023-2028, que busca enfrentar los desafíos de la ciberseguridad, como la falta de resiliencia en infraestructuras, la carencia de especialistas y el aumento de delitos cibernéticos.

Sus objetivos incluyen fortalecer la infraestructura, proteger los derechos de las personas, fomentar una cultura de ciberseguridad y mejorar la coordinación nacional e internacional.

En línea con esta política, se aprobó la Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información, que establece una institucionalidad y un marco regulatorio para las acciones de ciberseguridad en el país. Esta ley crea la Agencia Nacional de Ciberseguridad (ANCI), con facultades para fiscalizar y sancionar, y define los criterios para identificar a los servicios esenciales (SE) y Operadores de Importancia Vital (OIV).

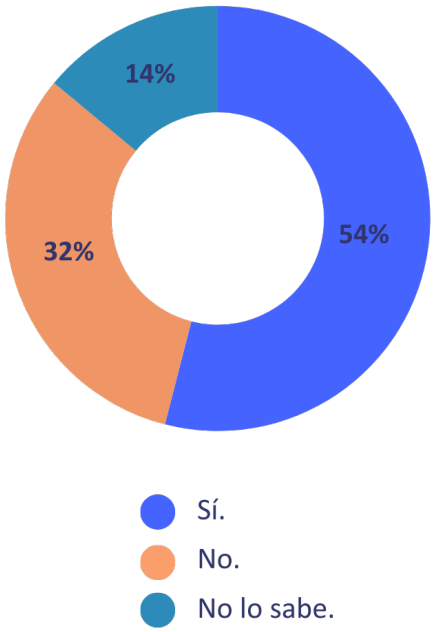
02.

Conciencia, preparación y estrategias

¿El directorio conoce la existencia de la nueva Ley Marco de Ciberseguridad de Chile?

Existe una brecha significativa en el conocimiento de la nueva Ley Marco de Ciberseguridad de Chile a nivel de los directorios de las organizaciones, ya que solo el 54% está informado al respecto. Esto destaca la necesidad de fortalecer la comunicación y la educación sobre regulaciones de ciberseguridad.

La falta de conciencia de la Ley, reflejada en el 32% que no la conoce y el 14% que no tiene claro si su directorio está informado, señala la oportunidad de impulsar programas de capacitación y sensibilización para asegurar que los directivos estén informados y preparados para cumplir con los requisitos legales.



Dado que esta Ley crea la Agencia Nacional de Ciberseguridad (ANCI) con facultades de fiscalización y sanción, resulta preocupante que un 32% de los directorios no esté al tanto de esta regulación y que otro 14% no esté seguro de si su organización la conoce.

El conocimiento de las sanciones y multas asociadas a la nueva Ley Marco de Ciberseguridad es fundamental para que los directores de las organizaciones comprendan las implicaciones legales de no cumplir con las normativas establecidas. La Ley no solo busca regular la ciberseguridad en el país, sino también garantizar que las instituciones, tanto públicas como privadas, adopten las medidas necesarias para proteger sus infraestructuras críticas.

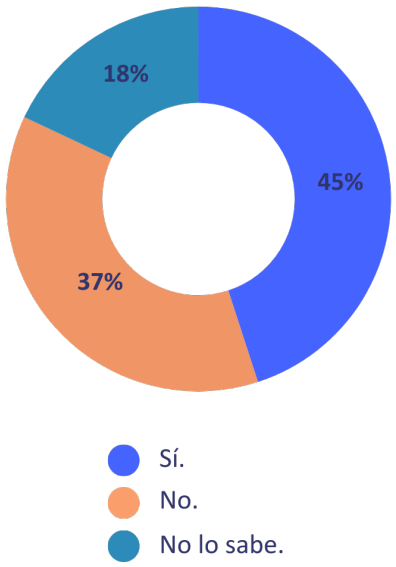
El desconocimiento de estas sanciones podría tener consecuencias graves, desde multas significativas hasta impactos en la reputación de las organizaciones.

¿El directorio conoce la existencia de las sanciones y multas consideradas en la nueva Ley Marco de Ciberseguridad de Chile?

Menos de la mitad de los directorios (45%) está informado sobre las sanciones y multas de la nueva Ley Marco de Ciberseguridad, lo cual es preocupante. La falta de conciencia sobre las consecuencias legales podría llevar a un enfoque inadecuado en la gestión de riesgos y al incumplimiento de las regulaciones.

El 37% que desconoce la existencia de las sanciones, junto con el 18% que no tiene claro si el directorio está informado, resalta la necesidad de implementar programas de capacitación y concienciación dirigidos a la alta dirección. Esto permitiría a los directores comprender mejor las responsabilidades legales y las posibles consecuencias de no cumplir con la Ley.

La Agencia Nacional de Ciberseguridad (ANCI) establece un marco regulador destinado a fiscalizar y garantizar el cumplimiento de las normativas de seguridad digital. Es preocupante que muchos directorios aún no estén al tanto de la creación de esta entidad, dado que desempeñará un rol crucial en la protección de las infraestructuras críticas del país. Es fundamental que las empresas refuercen la concienciación y la formación en ciberseguridad para que sus directores comprendan plenamente la relevancia de esta nueva institución y su impacto en el futuro de la seguridad corporativa.

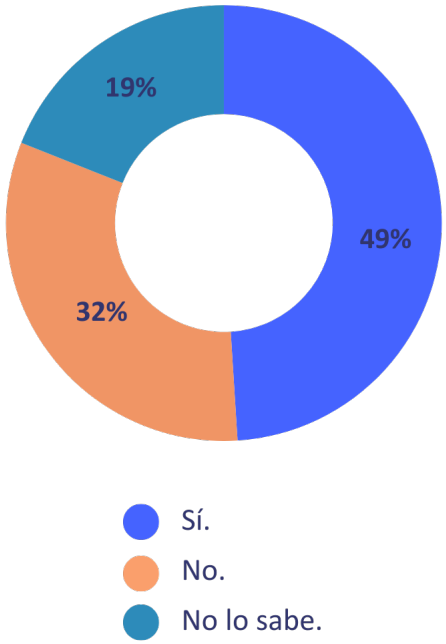


¿El directorio conoce la creación de la Agencia Nacional de Ciberseguridad (ANCI) como nuevo ente regulador en el ámbito de la ciberseguridad de Chile?

Menos de la mitad de los directorios (49%) está informado sobre la creación de la ANCI, lo que es preocupante, dado que se trata de un cambio relevante en el marco regulatorio de ciberseguridad en Chile. Esto sugiere una falta de sensibilización y formación sobre los temas regulatorios clave que afectan a las organizaciones.

El 32% que desconoce la existencia de la ANCI y el 19% que no tiene claro si su directorio está informado resaltan la importancia de fortalecer la comunicación interna y las actividades de formación para garantizar que la alta dirección esté actualizada sobre los cambios regulatorios.
La aplicación de esta ley tiene un impacto directo en la forma en que las organizaciones y sus directorios operan y gestionan su seguridad.
La falta de conocimiento expone a las empresas a consecuencias graves, que pueden ser de índole legal, financiero y operativo.

En este sentido, es fundamental que los directorios entiendan en profundidad cuáles son los impactos que tiene la ley en las gestiones y operaciones diarias de la empresa. La falta de conciencia por parte de los directorios resalta la urgencia de mejorar la educación y comunicación interna dentro de las organizaciones.

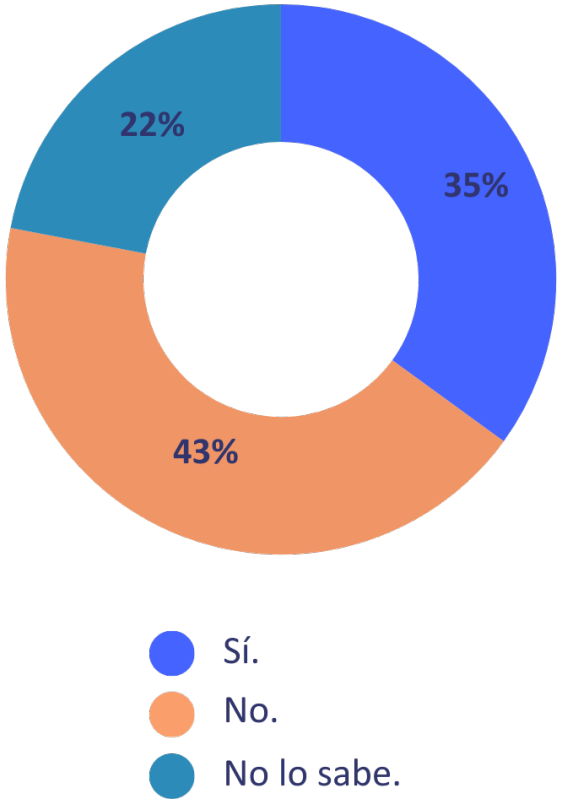


"Solo en el momento en el que exista una comprensión clara de la ley y sus impactos, será posible tomar decisiones estratégicas que garanticen el cumplimiento de la legislación y, junto con eso, se mitiguen todos los riesgos asociados", destaca Fadua Gajardo, directora ejecutiva del IdDC.

¿El directorio conoce el impacto que tendrá la aplicación de la nueva Ley Marco de Ciberseguridad de Chile en su empresa?

El hecho de que solo el 35% de los directorios conozca el impacto de la nueva Ley Marco de Ciberseguridad refleja un preocupante nivel de desconocimiento y falta de preparación. Esto sugiere que la mayoría de las organizaciones no ha evaluado adecuadamente cómo la ley afectará sus operaciones y procesos, lo cual podría acarrear riesgos legales, financieros y operativos.

La falta de conciencia en el 43% de los directorios y la incertidumbre en el 22% indican una necesidad clara de mejorar la educación y la comunicación interna sobre las implicaciones de la nueva ley. Es fundamental que la alta dirección entienda cómo esta normativa impactará sus actividades para tomar decisiones informadas y estratégicas.



La asignación del presupuesto de seguridad es un factor clave para la efectividad de las medidas de ciberseguridad en las organizaciones.

A pesar de la creciente amenaza de ciberataques, muchas empresas aún no destinan los recursos necesarios para proteger adecuadamente sus activos.
La falta de inversión puede tener consecuencias graves, ya que, sin los fondos suficientes, las organizaciones no pueden implementar tecnologías de seguridad avanzadas ni contratar personal especializado para gestionar y mitigar riesgos. Además, no contar con el presupuesto adecuado limita la capacidad de las empresas para llevar a cabo capacitaciones necesarias para preparar a sus empleados en la detección y prevención de amenazas cibernéticas.

¿El directorio asigna un uso estratégico del presupuesto de seguridad, realizando el gasto de manera coherente en herramientas / soluciones / servicios de seguridad y capacitación?

La mayoría de las organizaciones (51%) tiene un presupuesto de seguridad básico o limitado, lo que evidencia una falta de inversión significativa en ciberseguridad. Esto puede poner en riesgo la infraestructura y los datos de la empresa, ya que un presupuesto insuficiente limita la capacidad para implementar soluciones avanzadas, contratar expertos o capacitar al personal.

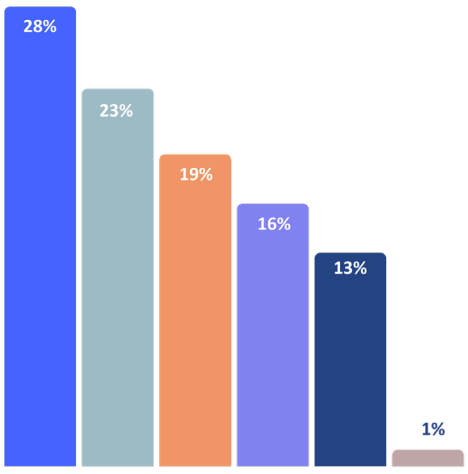
Solo el 13% utiliza un enfoque estratégico basado en un Business Impact Analysis (BIA) para priorizar su presupuesto de seguridad. Esto indica que la mayoría de las organizaciones no está alineando sus inversiones de seguridad con los riesgos y el impacto potencial en el negocio, lo que puede llevar a una asignación de recursos menos efectiva.

El 16% que no cuenta con un presupuesto dedicado para seguridad representa una grave vulnerabilidad. Estas organizaciones pueden enfrentar mayores riesgos debido a la falta de inversión planificada en medidas preventivas y de respuesta a incidentes.

La falta de un enfoque estratégico en el uso del presupuesto, evidenciada en el hecho de que más del 50% de las organizaciones maneja presupuestos limitados o básicos, expone a las empresas a riesgos significativos. Esta insuficiencia puede limitar su capacidad para adoptar soluciones avanzadas, contratar expertos en ciberseguridad o capacitar a su personal, lo cual resulta fundamental para una defensa.

En el 2024, aumentó el porcentaje de organizaciones que cuentan con un presupuesto básico de seguridad, del 14% al 28%, lo cual **podría indicar un mayor compromiso inicial hacia la seguridad.**

Además, el porcentaje de organizaciones sin presupuesto **disminuyó de 32% en 2023 a 16% en 2024**, lo que sugiere una mejora en el financiamiento destinado a seguridad, es decir, un aumento en el presupuesto asignado.



16% Indicó que no se cuenta con un presupuesto.

En 2023 fue **32%**

- Presupuesto de seguridad básico.
- Presupuesto de seguridad limitado.
- Presupuesto de seguridad robusto.
- No se cuenta.
- Presupuesto de seguridad priorizado por un Business Impact Analysis (BIA).
- No lo sabe.

La clave de contar con un plan de protección

Un reporte elaborado por Entel digital llamado **"Reporte Ciberseguridad 2024"**, reveló que hoy en día tanto las empresas como las organizaciones utilizan grandes cantidades de datos para llevar a cabo sus operaciones y así cumplir sus objetivos estratégicos.

"El problema es que gran parte de los ciberataques tienen como objetivo principal robar información clasificada, para obtener un beneficio económico a cambio. Por lo mismo, independientemente de dónde almacene sus datos cada empresa (nubes compartidas, centros locales, etc.) es fundamental que se cumplan ciertos estándares de seguridad que garanticen la integridad, confidencialidad y disponibilidad de la información".

Contar con una protección adecuada no solo implica tener sistemas de defensa tecnológicos avanzados, sino también disponer de planes de respuesta y recuperación bien definidos que minimicen el impacto operativo y financiero de un ciberataque.

La preparación para estos escenarios es un indicador claro de la madurez en ciberseguridad de una organización y su capacidad para adaptarse y resistir en un panorama de amenazas en constante evolución.

Una protección efectiva incluye la capacitación continua del personal para poder identificar y reaccionar de manera adecuada ante las amenazas, así como también la implementación de políticas y procedimientos que aseguren una rápida detección y contención de los incidentes.

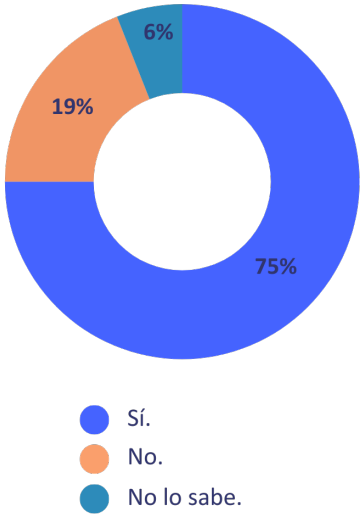
Si no existe una preparación integral que abarque tanto los avances tecnológicos como el factor humano, las empresas se arriesgan a sufrir interrupciones en sus operaciones, daños en su reputación y sanciones legales por incumplimiento de normativas.

¿La organización dispone de una adecuada protección que permite resguardar y proteger la operación en el escenario de que sea objeto de un ataque?

Un 75% de las organizaciones cuenta con una protección adecuada contra ciberataques y un porcentaje igual de directorios conoce la existencia de un plan de protección. Esto indica que muchas organizaciones están tomando medidas para prepararse contra ciberataques y que existe un nivel significativo de conocimiento y participación por parte de la alta dirección.

La existencia de un 19% de organizaciones sin una protección adecuada y un 25% de directorios que no conocen la existencia de un plan de protección contra ciberataques evidencia áreas críticas que necesitan atención. La falta de protección y de conocimiento del directorio podría llevar a mayores riesgos y pérdidas en caso de un incidente de seguridad.

El 6% de encuestados que no está seguro sobre la existencia de medidas de protección indica una necesidad de mejorar la comunicación y concienciación interna respecto a la seguridad y preparación de la organización frente a ciberataques.



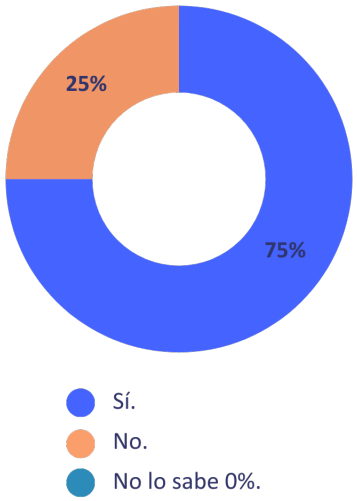
¿El directorio conoce la existencia de un plan de protección de ciberataque?

25%

Indicó que el directorio **no conoce** la existencia de un plan de protección de ciberataque.

En 2023 fue 35%

Incorporar la seguridad en decisiones comerciales, como fusiones y adquisiciones, asociaciones estratégicas, lanzamiento de nuevos productos y servicios, es fundamental para mitigar los posibles riesgos y vulnerabilidades. Sin embargo, el nivel de compromiso de los directorios en este ámbito varía considerablemente.



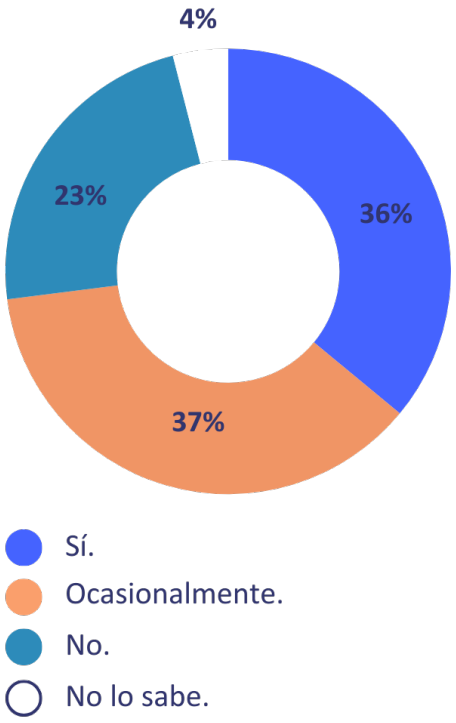
¿Están estos aspectos en la agenda del directorio?

Aún existen muchas organizaciones que tratan la ciberseguridad como un tema secundario y esta falta de enfoque proactivo expone a las empresas a riesgos que sí son evitables y que podrían mitigarse si se priorizara la seguridad desde un principio. En este contexto, el rol del directorio es esencial para garantizar que la ciberseguridad se convierta en un punto integral de la estrategia comercial y que proteja no solo los activos tecnológicos de la organización, sino también su sostenibilidad.

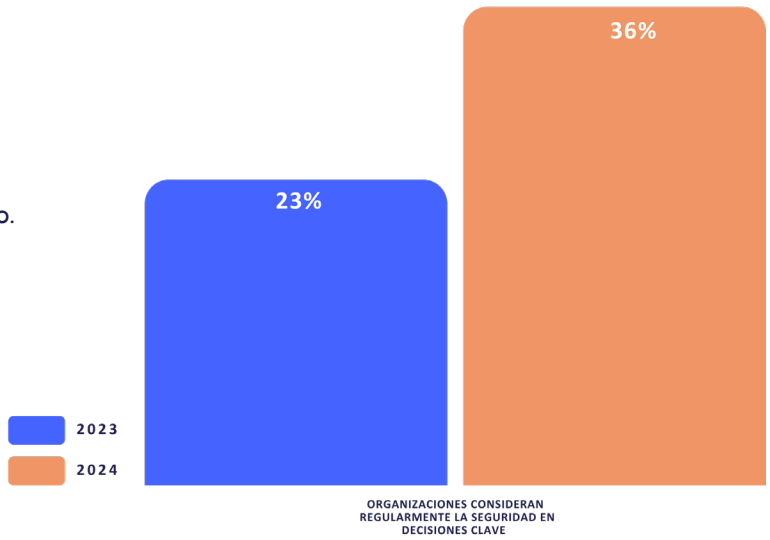
¿El directorio considera los aspectos de seguridad en las principales decisiones comerciales, como fusiones y adquisiciones, asociaciones, lanzamientos de nuevos productos o servicios, entre otras acciones de la organización de manera oportuna?

Con solo el 36% de los directorios que consideran la seguridad de manera oportuna en las decisiones comerciales, queda claro que la ciberseguridad no está siendo tratada como una prioridad estratégica en muchas organizaciones. Esto puede dejar a las empresas expuestas a riesgos que podrían ser mitigados si se incluyera la seguridad en el proceso de toma de decisiones desde el principio.

La cifra significativa de directorios que ocasionalmente (37%) o nunca (23%) consideran la seguridad en sus decisiones destaca la necesidad de reforzar la concienciación y la importancia de la ciberseguridad a nivel estratégico. Integrar la seguridad de manera constante en todas las decisiones comerciales clave es crucial para proteger los activos, la reputación y la continuidad del negocio.



El gráfico a la derecha muestra una positiva tendencia hacia una mayor integración de la seguridad. En el 2024, el porcentaje de respuestas afirmativas aumentó de un 23% a 36%, indicando que más organizaciones consideran regularmente la seguridad en decisiones clave como fusiones y lanzamientos de productos, lo que sugiere una mayor concienciación sobre la importancia de la seguridad en decisiones estratégicas del directorio.



Comunicación efectiva: un elemento clave de confianza y reputación empresarial

Bien sabemos que las amenazas cibernéticas son una realidad constante y frente a eso la comunicación estratégica se ha convertido en una herramienta indispensable para gestionar la confianza y reputación de las organizaciones.

Cuando hablamos de ciberseguridad, no solo nos referimos a la protección de datos y sistemas, sino también a la capacidad de informar de manera clara y proactiva a nuestros stakeholders -público, reguladores, clientes, sobre las medidas preventivas y correctivas que tiene la organización en caso de que surja algún incidente.

Una estrategia de comunicación segmentada y alineada a los riesgos de la ciberseguridad es fundamental para garantizar que cada uno de los grupos de interés reciba la información necesaria y oportunamente en el formato correcto. Si una organización no cuenta con una estrategia clara de comunicación, corre el riesgo de generar confusión, perder la confianza y, en el peor de los escenarios, dañar su imagen y reputación.

Es necesario que los directorios comprendan que la comunicación es un factor clave en la estrategia de su negocio y que comunicar de manera eficaz puede ser un punto diferenciador a la hora de gestionar una crisis.

03.

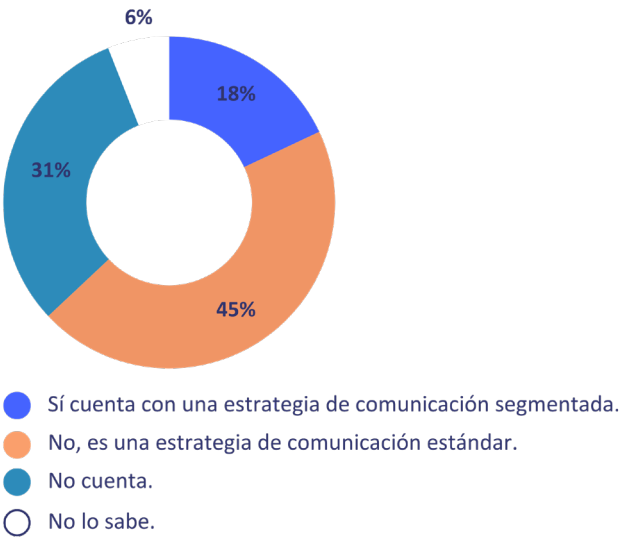
Supervisión y gobernanza de la ciberseguridad

¿El directorio cuenta con una estrategia de comunicación segmentada para el público, reguladores, agencias de calificación, que estén alineadas a los escenarios de ciberseguridad de su organización?

El bajo porcentaje (18%) de organizaciones con una estrategia de comunicación segmentada refleja una falta de preparación para abordar de manera efectiva las necesidades de comunicación durante escenarios de ciberseguridad. Las estrategias de comunicación estándar o la ausencia de ellas pueden ser inadecuadas, ya que no se adaptan a las expectativas y requisitos específicos de cada grupo de interés.

La existencia de un 45% con una estrategia estándar y un 31% sin estrategia señala una clara oportunidad de mejora. Las organizaciones deben desarrollar estrategias de comunicación que no solo sean proactivas, sino también adaptadas a las particularidades de reguladores, agencias de calificación, clientes y el público en general.

El 6% que no tiene conocimiento de si existe una estrategia destaca la importancia de mejorar la comunicación interna y la concienciación sobre las estrategias de ciberseguridad y su alineación con las comunicaciones externas.



Los resultados indican que la mayoría de las organizaciones **aún no** han implementado una estrategia de comunicación segmentada en ciberseguridad, lo que podría afectar su capacidad para responder eficazmente en caso de incidentes y comunicar adecuadamente a sus stakeholders.

Además, se recomienda establecer una estrategia de comunicación segmentada dentro de las organizaciones, desde los altos ejecutivos hasta los colaboradores, para asegurar una comprensión clara de los mensajes de ciberseguridad y fomentar así la prevención de incidentes.

En el entorno regulatorio actual, que es cada vez más complejo, la supervisión de las normativas y legislaciones relacionadas con la seguridad de la organización ha adquirido una relevancia importante. Las leyes y regulaciones que se encuentran en constante evolución buscan proteger tanto a las empresas como a sus stakeholders de riesgos cibernéticos, estableciendo estándares de seguridad que deben ser cumplidos.

Como bien dijimos anteriormente, no cumplir con estas normativas puede traer consecuencias graves, incluyendo sanciones financieras, daños en la reputación y pérdida de confianza.

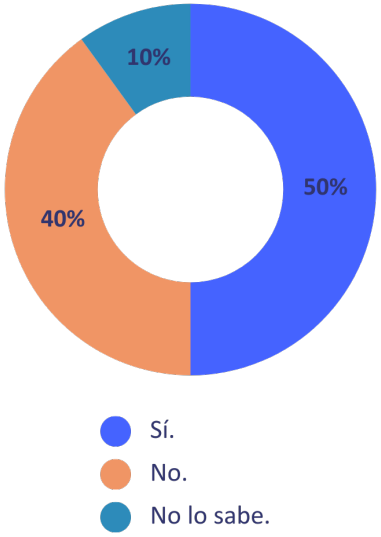
El rol del directorio es garantizar que sus empresas no solo conozcan y apliquen las normativas vigentes, sino que también se mantengan actualizadas de las que emergen.

¿El directorio supervisa que la organización esté verificando adecuadamente la legislación, las regulaciones y las normativas técnicas actuales y potenciales relacionadas con la seguridad?

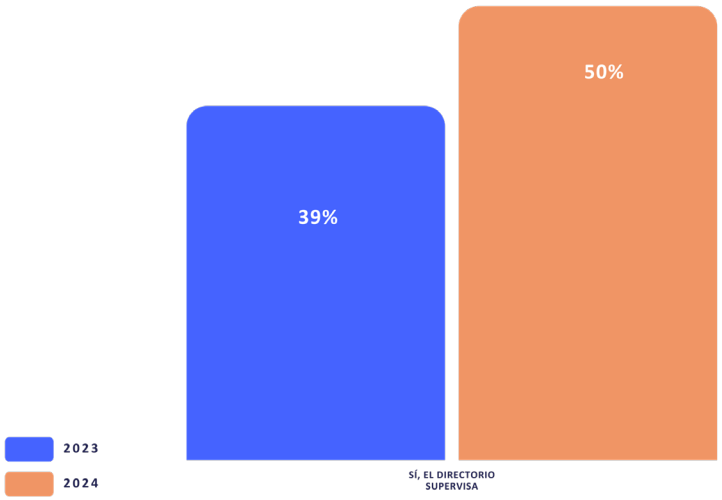
El hecho de que solo el 50% de los directorios esté supervisando adecuadamente la verificación de la legislación y las regulaciones de ciberseguridad implica que la otra mitad de las organizaciones puede estar en riesgo de incumplimiento normativo. Dado el creciente número de regulaciones de ciberseguridad y protección de datos, la falta de supervisión puede tener consecuencias graves, incluyendo sanciones legales, daños a la reputación y pérdida de confianza por parte de clientes y socios.

El 10% que no sabe si el directorio está supervisando estos aspectos refleja una desconexión en la comunicación interna. La falta de claridad sobre las responsabilidades y las prácticas de cumplimiento pueden llevar a la inacción y a una gestión ineficaz de la seguridad.

El 40% de los directorios no supervisan la verificación de la normativa relacionada con la seguridad, lo que está dejando a sus organizaciones expuestas a riesgos potenciales. La supervisión directiva es esencial para garantizar que la organización se mantenga alineada con las mejores prácticas y regulaciones en constante evolución.



Si se hace un análisis comparativo entre el año 2023 y 2024 sobre la supervisión del directorio en el cumplimiento de normativas de seguridad, se puede ver un avance positivo. En 2024, el 50% de los directorios reportan que supervisan adecuadamente la verificación de legislación y regulaciones de seguridad, en comparación con el 39% en 2023, indicando un aumento en la responsabilidad y compromiso en esta área que es fundamental.



Gobernanza de seguridad: el pilar fundamental que los directorios no pueden olvidar

La falta de una estructura de gobernanza adecuada no solo pone en riesgo a las empresas, sino que también trae consigo sanciones legales y repercusiones financieras. Por eso, es fundamental que los directorios adopten un enfoque integral y supervisen de manera activa la implementación de estrategias de seguridad bien estructuradas.

Cuando la gobernanza en seguridad no es completa, los riesgos tienden a ser abordados de manera fragmentada, lo que aumenta la posibilidad de sufrir ciberataques y otros incidentes que comprometen la operación de las empresas.

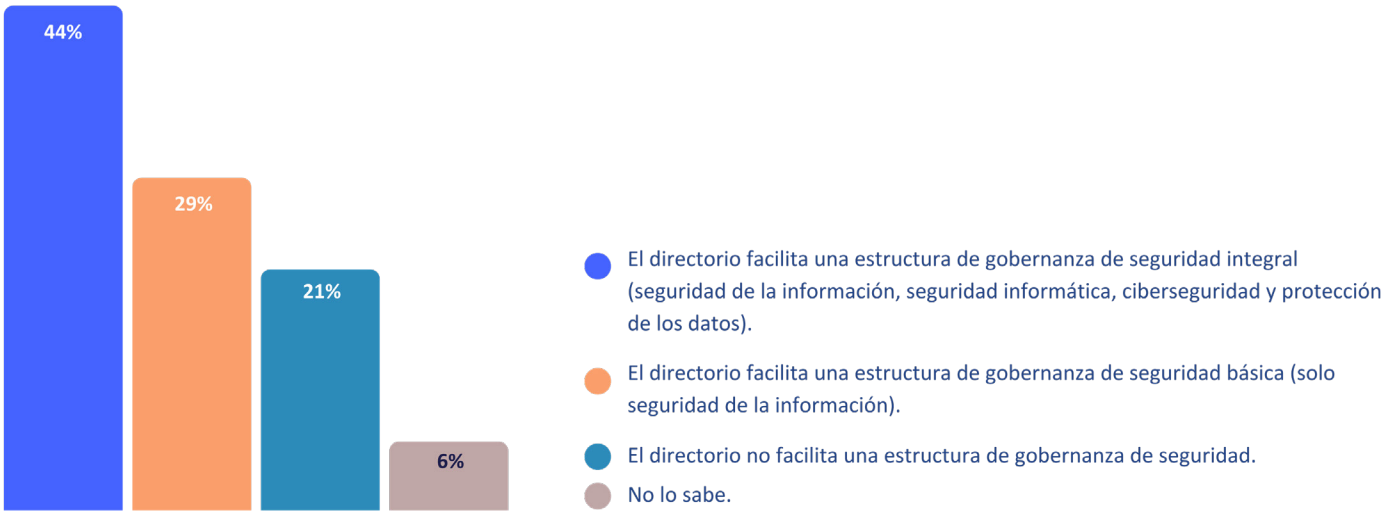
¿El directorio facilita a la organización una estructura de gobernanza de seguridad que entregue un estatus de la seguridad de la información, la seguridad informática, la ciberseguridad y la protección de los datos respectivamente?

El hecho de que solo el 44% cuente con una estructura de gobernanza integral muestra que la mayoría de las organizaciones no está gestionando la seguridad de manera completa. La falta de un enfoque integral puede provocar una gestión fragmentada de los riesgos, lo que aumenta la vulnerabilidad ante ciberataques y posibles brechas de datos.

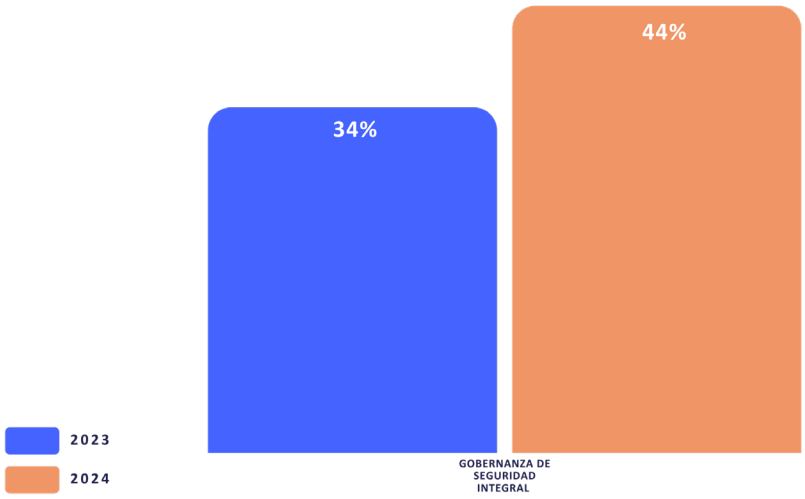
El 29% que tiene una estructura de gobernanza básica, enfocada únicamente en la seguridad de la información, lo que indica que estas organizaciones pueden estar ignorando otros aspectos críticos, como la ciberseguridad y la protección de datos. Esta visión limitada puede dar lugar a brechas de seguridad y a una falta de preparación ante amenazas cibernéticas modernas.

El 21% que carece de cualquier estructura de gobernanza de seguridad refleja una situación de riesgo significativo.

Sin una estructura clara y supervisada por el directorio, estas organizaciones están expuestas a riesgos de seguridad que pueden resultar en pérdidas financieras, daños reputacionales y sanciones legales.



En el año 2024, el 44% de los directorios dice facilitar una estructura de gobernanza integral de seguridad, esto refleja un aumento respecto al 34% del año 2023. Además, sugiere una tendencia positiva hacia una cobertura más completa de la seguridad organizacional, que entregue un estatus de la información, seguridad informática, ciberseguridad y protección de datos permanente.



Ciberseguridad en la estrategia del negocio: la importancia de un punto de control en los directorios

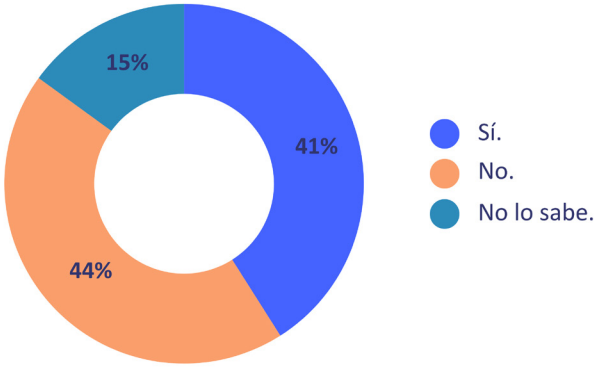
Actualmente, es imperativo que los directores asuman un rol protagónico en la gobernanza de la ciberseguridad, estableciendo puntos de control claros y efectivos que los ayuden a monitorear y gestionar los riesgos de manera adecuada y activa.

El punto de control de ciberseguridad permite supervisar la protección de datos y activos digitales y, junto con eso, garantizar que la organización esté preparada para responder ante cualquier ataque o incidente que pueda poner en peligro su operación y reputación.

¿El directorio cuenta con un punto de control de ciberseguridad?

Solo el 41% de las organizaciones ha establecido un punto de control de ciberseguridad en el directorio, lo que muestra que muchas empresas no están supervisando proactivamente los riesgos cibernéticos a nivel estratégico. Esto es preocupante dado el aumento de las amenazas cibernéticas y su potencial impacto en la operación y reputación de las empresas.

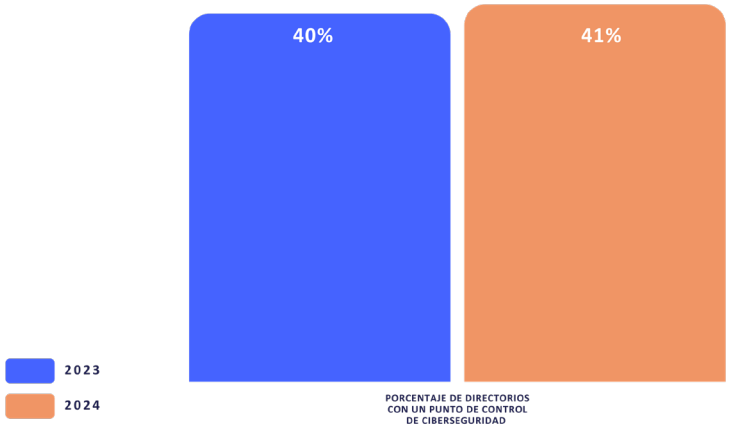
La asignación de responsabilidades a diferentes comités (Comité de Ciberseguridad, Comité de Riesgo, Comité de Auditoría, o Comités Híbridos) sugiere que no existe un enfoque unificado en la gobernanza de ciberseguridad. Cada enfoque tiene sus ventajas y desventajas, y la clave es garantizar que el comité asignado tenga los recursos, el conocimiento y la autoridad necesaria para supervisar eficazmente la ciberseguridad.
El 15% que no sabe si existe un punto de control en el directorio destaca la necesidad de mejorar la comunicación interna respecto a la estructura de gobernanza de ciberseguridad.



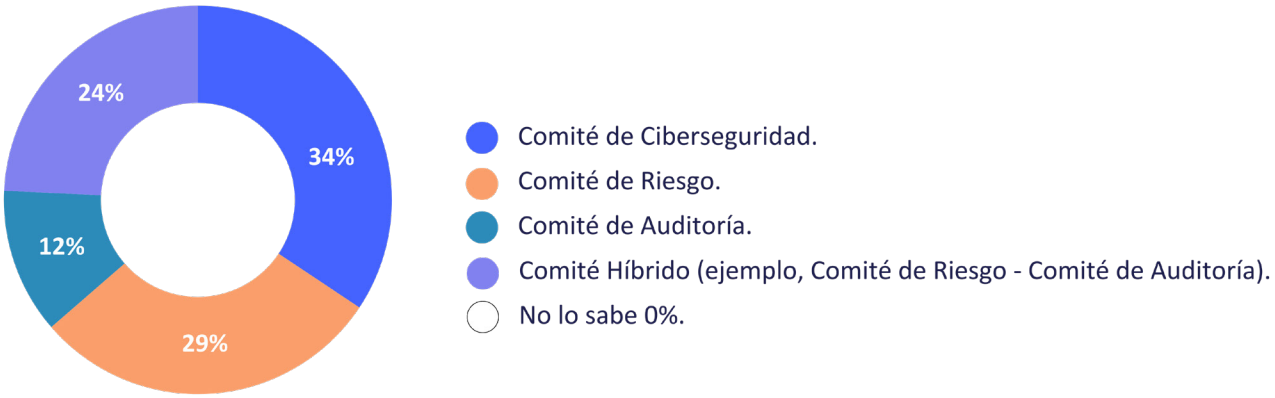
Solo un 1%

Este gráfico muestra una mejora muy mínima en el 2024 respecto al 2023, con solo un incremento del 1%. Esto refleja un avance muy leve y sugiere que aún hay mucho trabajo por hacer para fortalecer el punto de control de ciberseguridad dentro de los directorios.

Crear un punto de control específico dentro del directorio ayuda a centralizar la supervisión y a coordinar las acciones necesarias para prevenir ataques. Sin una buena estructura, las decisiones relacionadas con la seguridad pueden dispersarse en distintos comités, lo que puede generar una falta de coordinación y respuestas reactivas en vez de preventivas.



Por favor indique en qué estructura del directorio asigna esta responsabilidad.



En los directorios que han establecido un punto de control, se observa una tendencia a asignar responsabilidades a comités especializados. Un 34% lo designa a comités de ciberseguridad, el 29% lo designa a comités de riesgo y el 12% de auditoría. Por otro lado, el 24% prefiere comités híbridos, que combinan los comités de riesgo y auditoría.

La clave de todo esto está en que, sea cual sea el enfoque que adopten los directorios, el punto de control debe estar siempre respaldado de los recursos y conocimientos necesarios para gestionar y evaluar las amenazas cibernéticas que surgen en el entorno.

Expertos en ciberseguridad: un componente indispensable

En el último tiempo, la ciberseguridad es un tema que ha estado muy presente en la agenda del directorio debido a que las amenazas cibernéticas han evolucionado hasta convertirse en uno de los mayores riesgos para las empresas. Para mitigar los riesgos de manera efectiva, es necesario que los directorios cuenten con al menos un integrante calificado en estas materias. Este experto en ciberseguridad no solo aportará el conocimiento técnico que toda organización requiere, sino que también permitirá integrar la ciberseguridad como un componente estratégico dentro de la toma de decisiones.

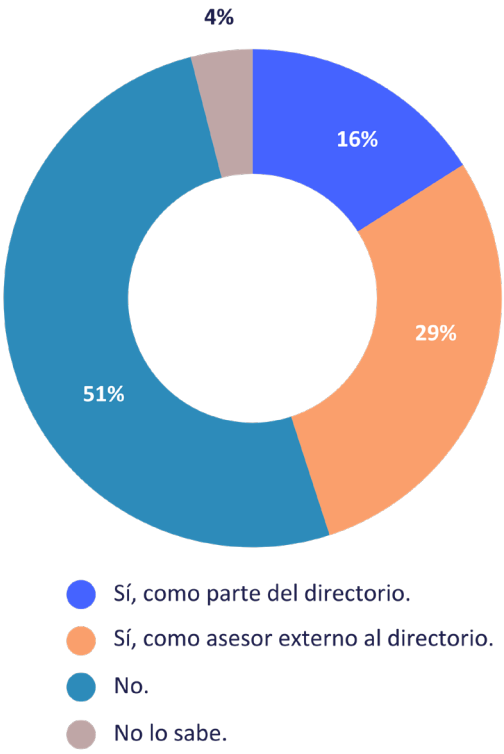
¿El directorio cuenta con al menos un integrante calificado en materias de ciberseguridad?

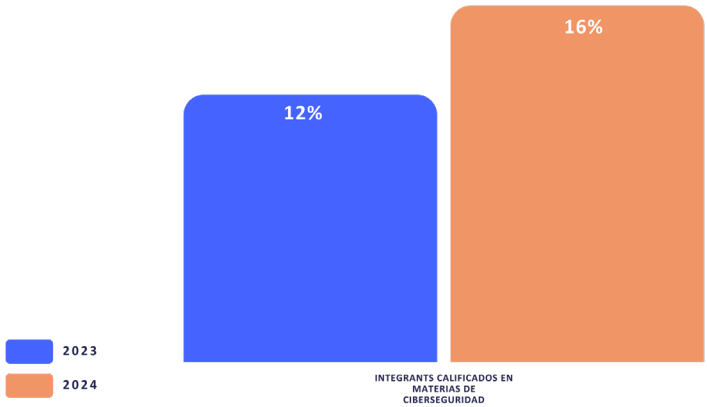
La baja proporción de integrantes calificados en ciberseguridad dentro del directorio (16%) y la dependencia parcial de asesores externos (29%) muestran que la mayoría de las organizaciones no están equipadas con el conocimiento especializado necesario en sus niveles estratégicos. Esto puede afectar la capacidad de los directorios para comprender y gestionar eficazmente los riesgos cibernéticos.

Con un 51% de organizaciones sin acceso directo a un experto en ciberseguridad, existe una necesidad clara de mejorar la inclusión de especialistas en ciberseguridad en la estructura de gobernanza, ya sea integrando miembros capacitados dentro del directorio o trabajando estrechamente con asesores externos.

El 4% que no tiene claro si existe un miembro calificado en ciberseguridad refleja la necesidad de mejorar la comunicación interna sobre la composición y competencias del directorio y sobre las prácticas de ciberseguridad.

Si bien los resultados de este año son algo más positivos que el anterior, es preocupante que solo el 16% de las empresas cuenten con un miembro especializado en ciberseguridad, ya que deja a muchas organizaciones en una posición vulnerable ante el entorno. La falta de conocimiento especializado en los niveles más altos de la toma de decisiones
limita a los directorios a poder identificar y gestionar riesgos cibernéticos. Incluir especialistas dentro del directorio, o garantizar una relación estrecha con colaboradores externos, es fundamental para fortalecer la protección contra ataques cibernéticos y continuidad operativa de los negocios.





Recomendaciones y conclusión

10 recomendaciones para el directorio

1. Capacitación de colaboradores:

La capacitación continua es esencial, ya que una parte significativa de las brechas de ciberseguridad son causadas por empleados que, ya sea de forma malintencionada o por negligencia, permiten el acceso no autorizado a sus redes. El directorio debe priorizar la capacitación en ciberseguridad de todo el personal y establecer directivas claras para el manejo y protección de la información confidencial, tanto interna como de los clientes.

2. Evaluación de riesgos:

El directorio debe evaluar los riesgos que comprometen la seguridad de la empresa, identificando y analizando amenazas para diseñar planes de acción que cubran las brechas de ciberseguridad. Si se utilizan servicios en la nube, es esencial solicitar evaluaciones de riesgos a los proveedores. Con la información obtenida, se debe ajustar la estrategia de seguridad y actualizarla regularmente para asegurar la protección de los datos.

3. Gobernanza de ciberseguridad:

Es esencial que los directorios impulsen estructuras de gobernanza que permitan cumplir con los requisitos regulatorios y gestionen los desafíos en seguridad de la información. Las regulaciones requerirán perfiles especializados capaces de responder a las diversas necesidades, y la separación de funciones será clave en este proceso.

4. Establecimiento de puntos de control:

El directorio debe establecer un punto de control que permita una supervisión clara y efectiva. Dependiendo del nivel de madurez de la empresa, se pueden crear comités dedicados o híbridos para abordar la ciberseguridad. Esta decisión estratégica es crucial para una supervisión constante y adecuada de los riesgos cibernéticos de los clientes.

5. Comunicación y presentación de métricas:

Se recomienda implementar reportes periódicos que informen al directorio sobre el estado de la ciberseguridad y permitan una evaluación proactiva de las amenazas. La falta de presentación regular de métricas disminuye la capacidad del directorio para monitorear riesgos y tomar decisiones informadas.

6. Frecuencia de informes:

El 17% de las organizaciones no presenta informes de riesgo cibernético y el 26% solo lo hace ante incidentes críticos. Se recomienda establecer un sistema de informes trimestral para fomentar una gestión de riesgos más proactiva y evitar la dependencia de la gestión reactiva ante incidentes.

7. Conocimiento de la legislación:

Es urgente que los directores se capaciten sobre las normativas vigentes, como la Ley Marco de Ciberseguridad y la creación de la Agencia Nacional de Ciberseguridad (ANCI), para asegurar que la empresa cumpla con los requisitos legales y evite sanciones.

8. Presupuesto de seguridad:

Muchas organizaciones destinan un presupuesto insuficiente para ciberseguridad, lo que reduce la efectividad de las medidas implementadas. Es recomendable aumentar los recursos destinados a ciberseguridad, asegurando que la inversión esté alineada con los riesgos reales de la empresa y que se utilice un análisis de impacto en el negocio (BIA) para priorizar la inversión.

9. Protección y preparación:

Aunque muchas organizaciones cuentan con protección adecuada, un porcentaje significativo carece de suficientes medidas de protección o desconoce la existencia de un plan de respuesta ante ciberataques. Es esencial reforzar los planes de respuesta y asegurar que los directores conozcan y supervisen la actualización continua de estos planes.

10. Involucramiento estratégico del directorio:

Solo el 36% de los directorios integra la ciberseguridad en sus decisiones estratégicas, lo que indica que se le otorga una baja prioridad. Es crucial que los directorios integren la ciberseguridad en decisiones clave como fusiones, adquisiciones y lanzamientos de nuevos productos para mitigar riesgos de manera efectiva y estar alineados con los objetivos comerciales de la empresa.

Conclusión general

El estudio "Radiografía de la ciberseguridad en directorios de Chile" revela que, aunque ha habido avances en la adopción de prácticas de ciberseguridad en las organizaciones chilenas, aún persisten importantes brechas en la preparación, inversión y gobernanza a nivel de directorio.

La falta de comunicación fluida, la carencia de enfoque estratégico en la asignación de recursos y la escasa integración de la ciberseguridad en la toma de decisiones comerciales son aspectos que exponen a muchas empresas a riesgos significativos. Además, la insuficiente formación en normativas, como la Ley Marco de Ciberseguridad, y la falta de expertos calificados dentro de los directorios, limitan la capacidad de respuesta frente a las amenazas cibernéticas que cada vez son más frecuentes.

Para enfrentar estos desafíos, es fundamental que los directorios asuman un papel mucho más activo y estratégico que priorice la ciberseguridad como un pilar clave para la sostenibilidad y resiliencia de las organizaciones. La hora de reaccionar es ahora: los directorios deben invertir en protección, capacitación de talento, y asegurar que la ciberseguridad sea parte del ADN de las empresas, porque este no solo protegerá a las organizaciones, sino que las fortalecerá en este competitivo mundo globalizado.

INSTITUTO DE DIRECTORES DE CHILE