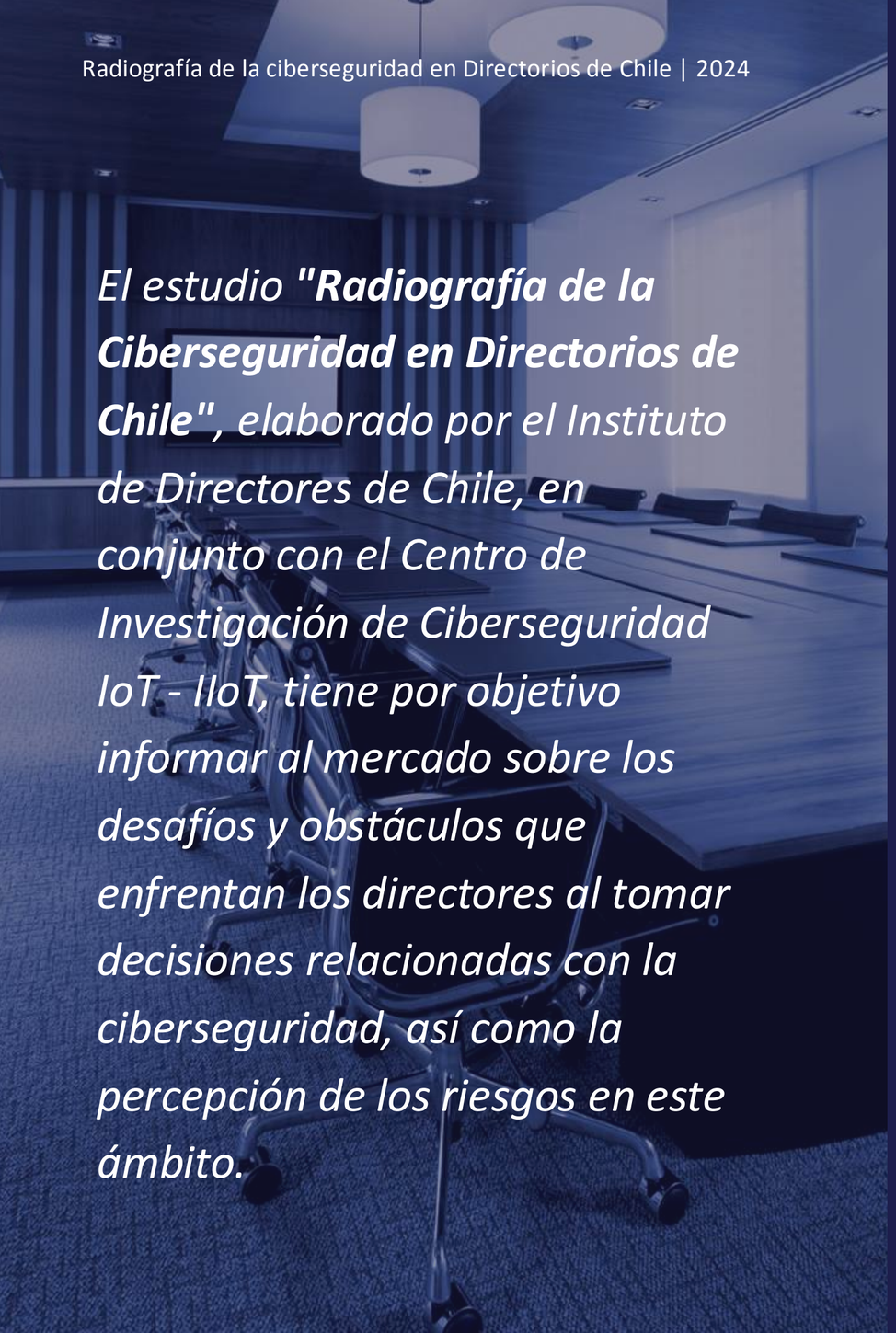
INSTITUTO DE DIRECTORES DE CHILE

CIC -IOT IIOT

Estudio

Radiografía de la ciberseguridad en Directorios de Chile



*El estudio **"Radiografía de la Ciberseguridad en Directorios de Chile"**, elaborado por el Instituto de Directores de Chile, en conjunto con el Centro de Investigación de Ciberseguridad IoT - IIoT, tiene por objetivo informar al mercado sobre los desafíos y obstáculos que enfrentan los directores al tomar decisiones relacionadas con la ciberseguridad, así como la percepción de los riesgos en este ámbito.*

Grupo muestral

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

18 preguntas de selección

Técnica utilizada

1

Los participantes decidieron contribuir de forma voluntaria a la **encuesta** enviada por **email y publicada en LinkedIn.**

2

La ventana de tiempo para completar la encuesta abarcó desde el **05 de septiembre hasta el 30 de septiembre**, permitiendo a los participantes tener un período adecuado para compartir sus respuestas.

3

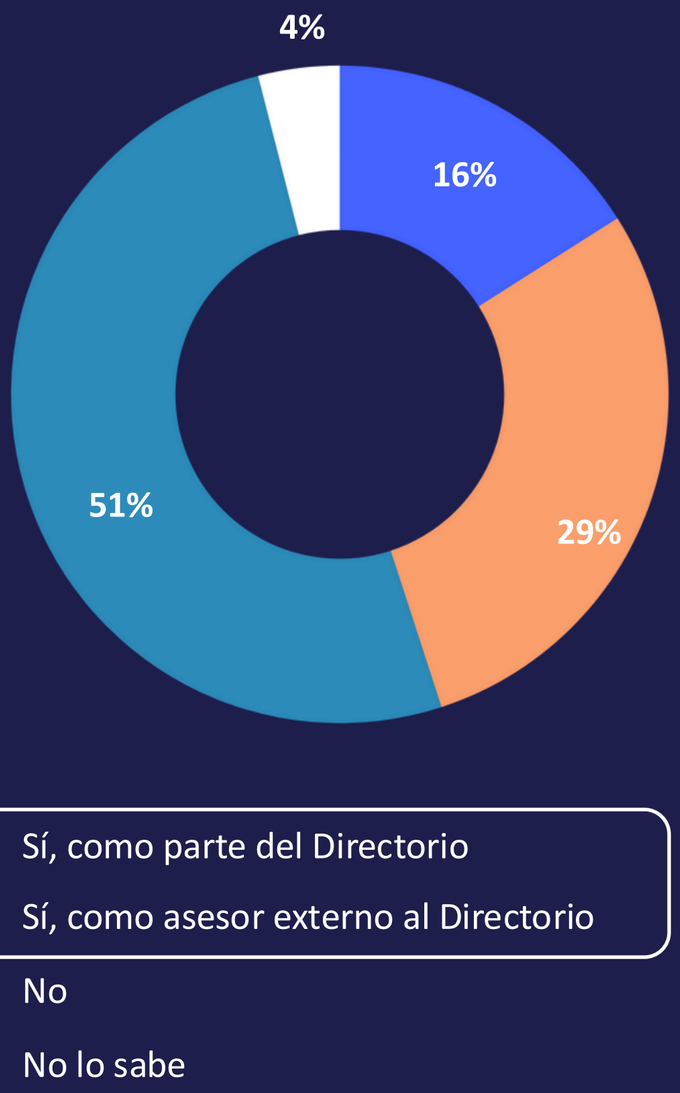
El tiempo promedio necesario para finalizar la encuesta fue de **8 minutos**, asegurando una experiencia eficiente para los encuestados.

4

El análisis de los datos se llevó a cabo entre el **30 de septiembre y el 07 de octubre**, la cual fue realizada por el Instituto de Directores de Chile. Durante este período, se aplicaron métodos tanto cuantitativos para explorar en profundidad los resultados obtenidos en el instrumento de evaluación.

Resultados

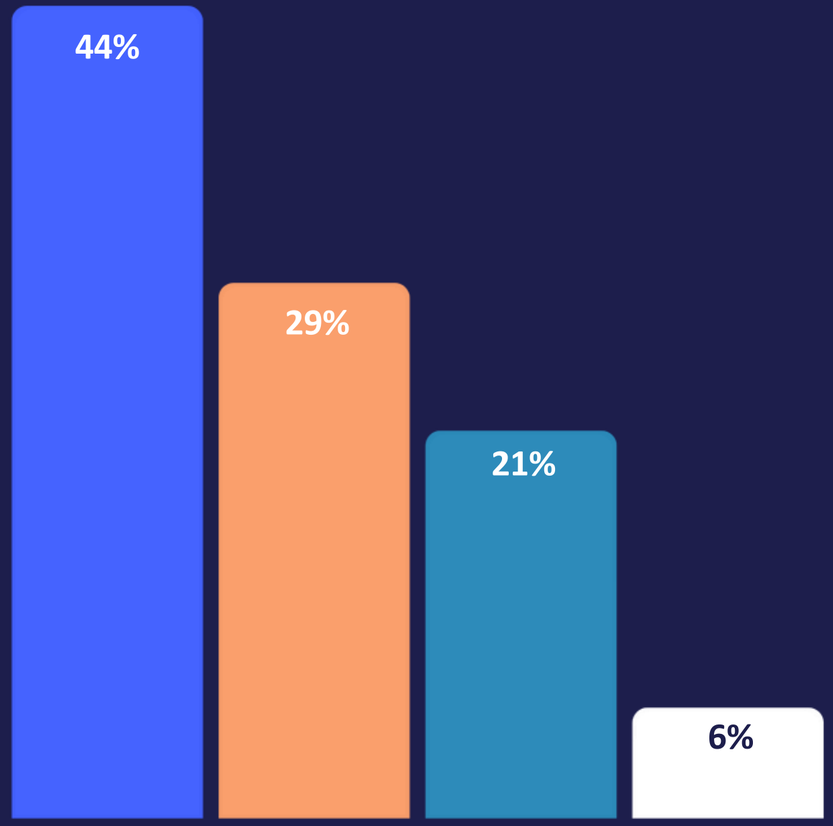
¿El Directorio cuenta con al menos un integrante calificado en materias de Ciberseguridad?



45% indicó que sí en 2024

22% indicó que sí en 2023

¿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?

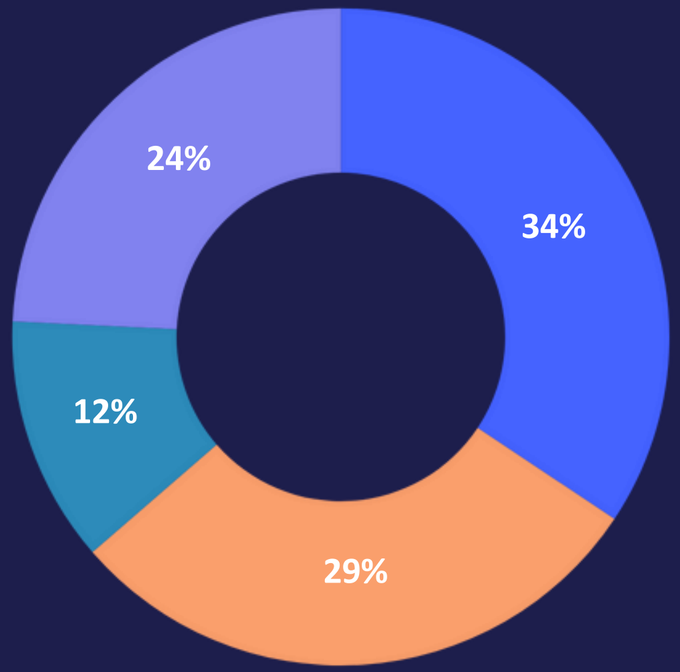


44% **indicó que el Directorio facilita una estructura de gobernanza de seguridad integral.**

En 2023 fue 34%

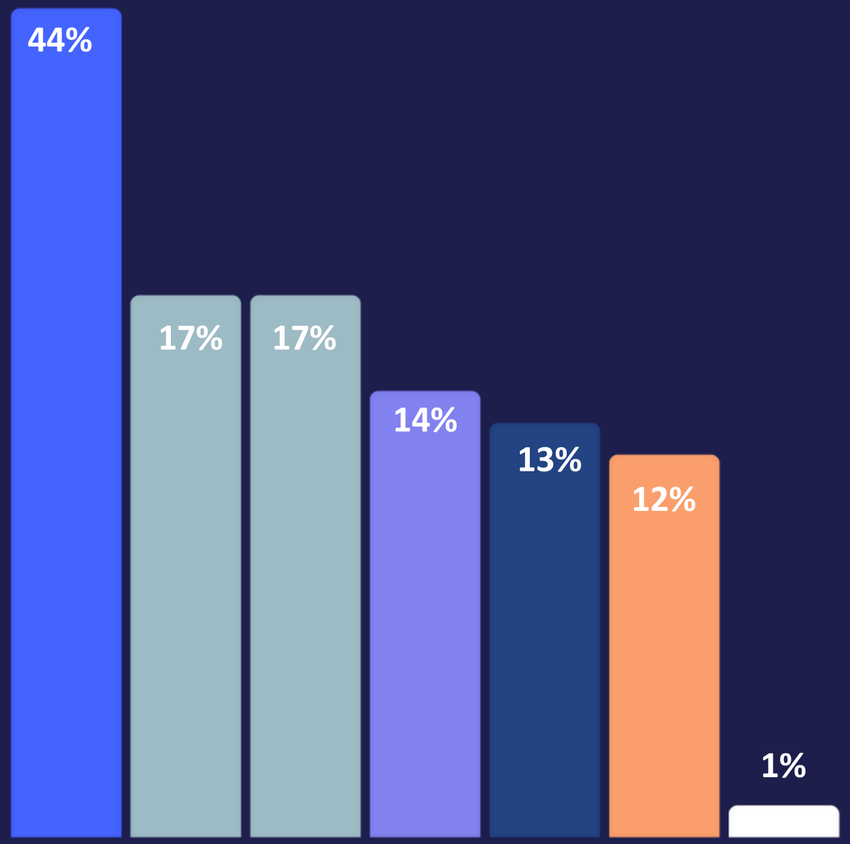
- El Directorio facilita una estructura de gobernanza de seguridad integral (seguridad de la información, seguridad informática, ciberseguridad y protección de los datos)
- El Directorio facilita una estructura de gobernanza de seguridad básica (solo seguridad de la información)
- El Directorio no facilita una estructura de gobernanza de seguridad
- No lo sabe

¿En qué estructura del Directorio asigna esta responsabilidad?



- Comité de Ciberseguridad
- Comité de Riesgo
- Comité de Auditoría
- Comité Híbrido (ejemplo, Comité de Riesgo - Comité de Auditoría)

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

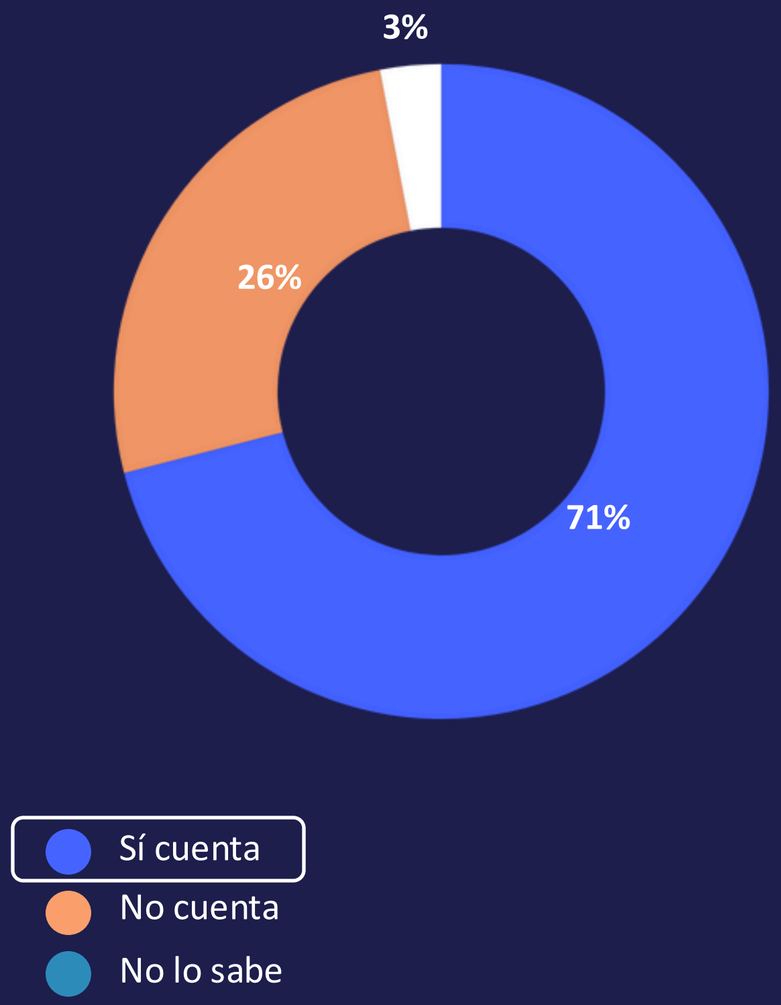


17% indicó que no se presentaron informes de riesgo cibernético al directorio en 2024.

En 2023 fue **26%**

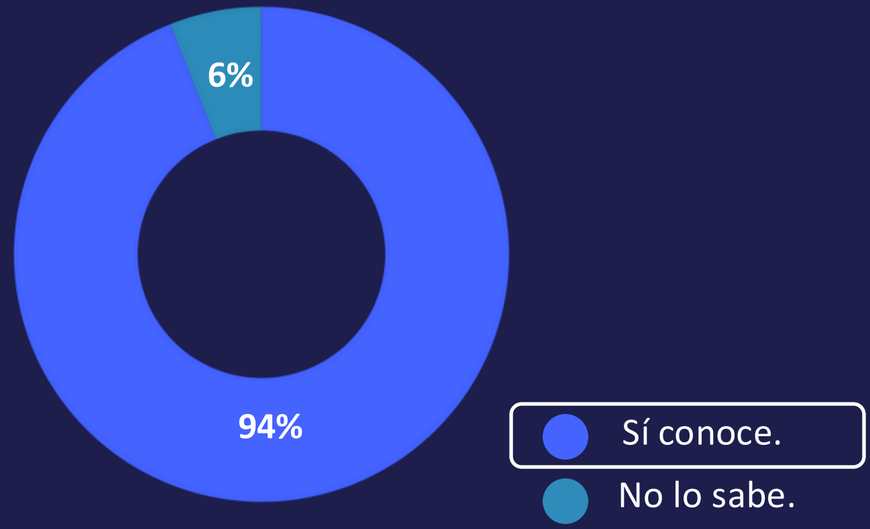
- Solo cuando se produce un incidente considerado crítico.
- Trimestral y cada vez que se produce un incidente considerado crítico.
- No se presentan informes.
- Semestral y cada vez que se produce un incidente considerado crítico.
- Mensual y cada vez que se produce un incidente considerado crítico.
- Anual y cada vez que se produce un incidente considerado crítico.
- No lo sabe.

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



Al responder sí

¿El Directorio conoce la existencia de la metodología?



Al consultar el nombre de la metodología de riesgo de seguridad en la organización:

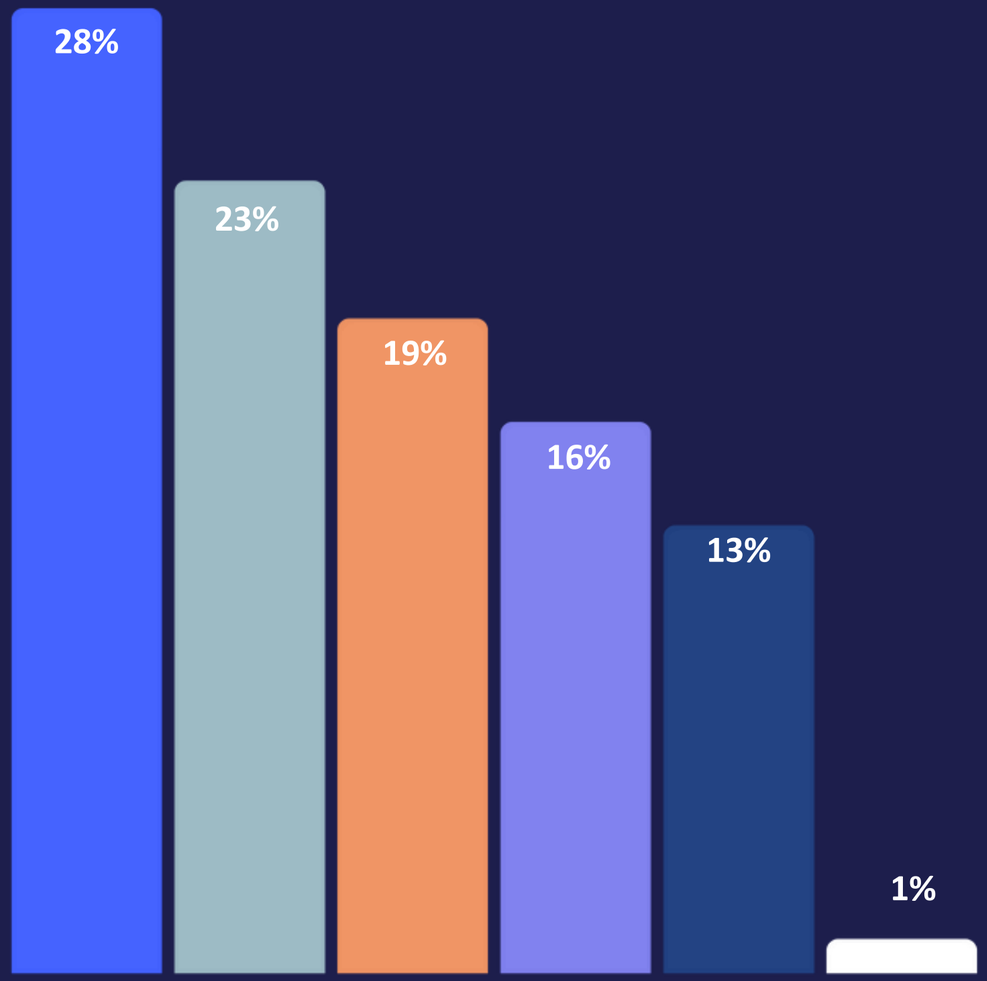
52% **indicó que su metodología está relacionada con estándares internacionales y metodologías específicas.**

26% **indicó una descripción en términos generales de la metodología.**

4% **indicó que su metodología se encuentra basada en la normativa legal vigente.**

17% **indicó desconocer la metodología.**

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

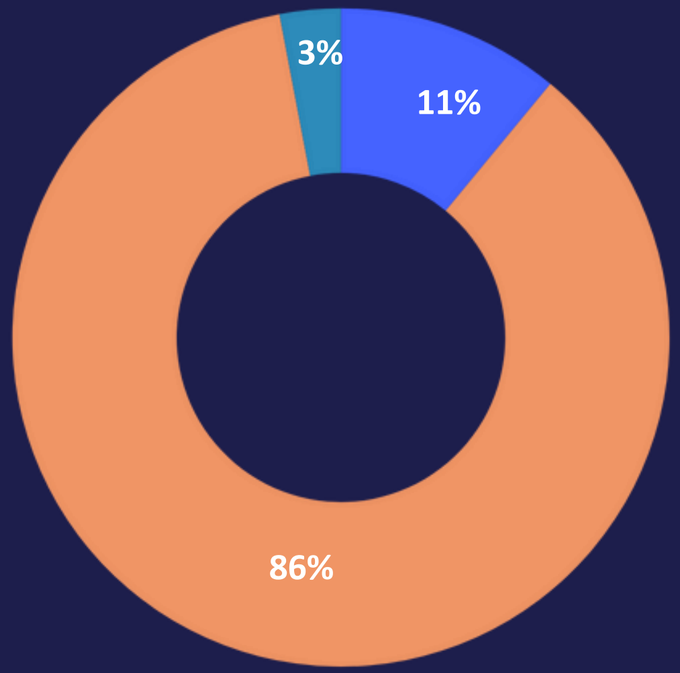


16% indicó que no se cuenta con un presupuesto.

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

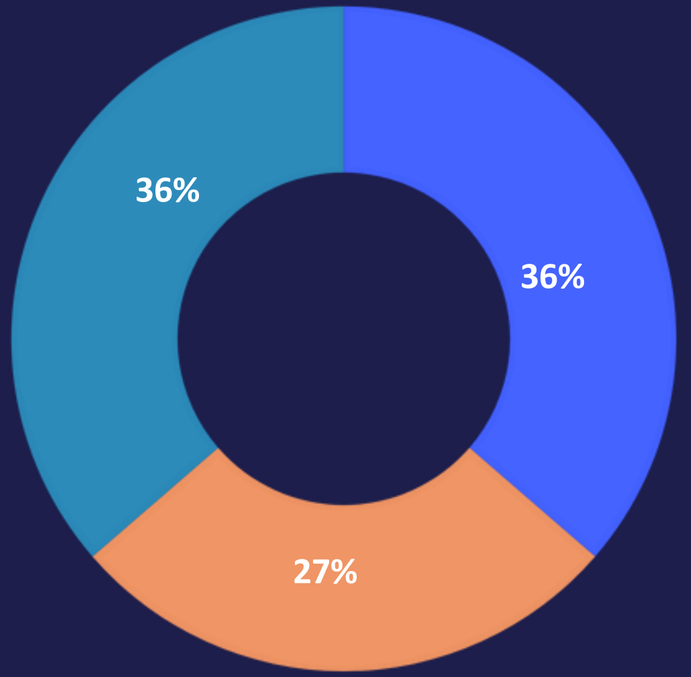
¿Ha sido su organización víctima de pérdidas de datos o filtración de actas de directorios?



- Sí
- No
- No lo sabe

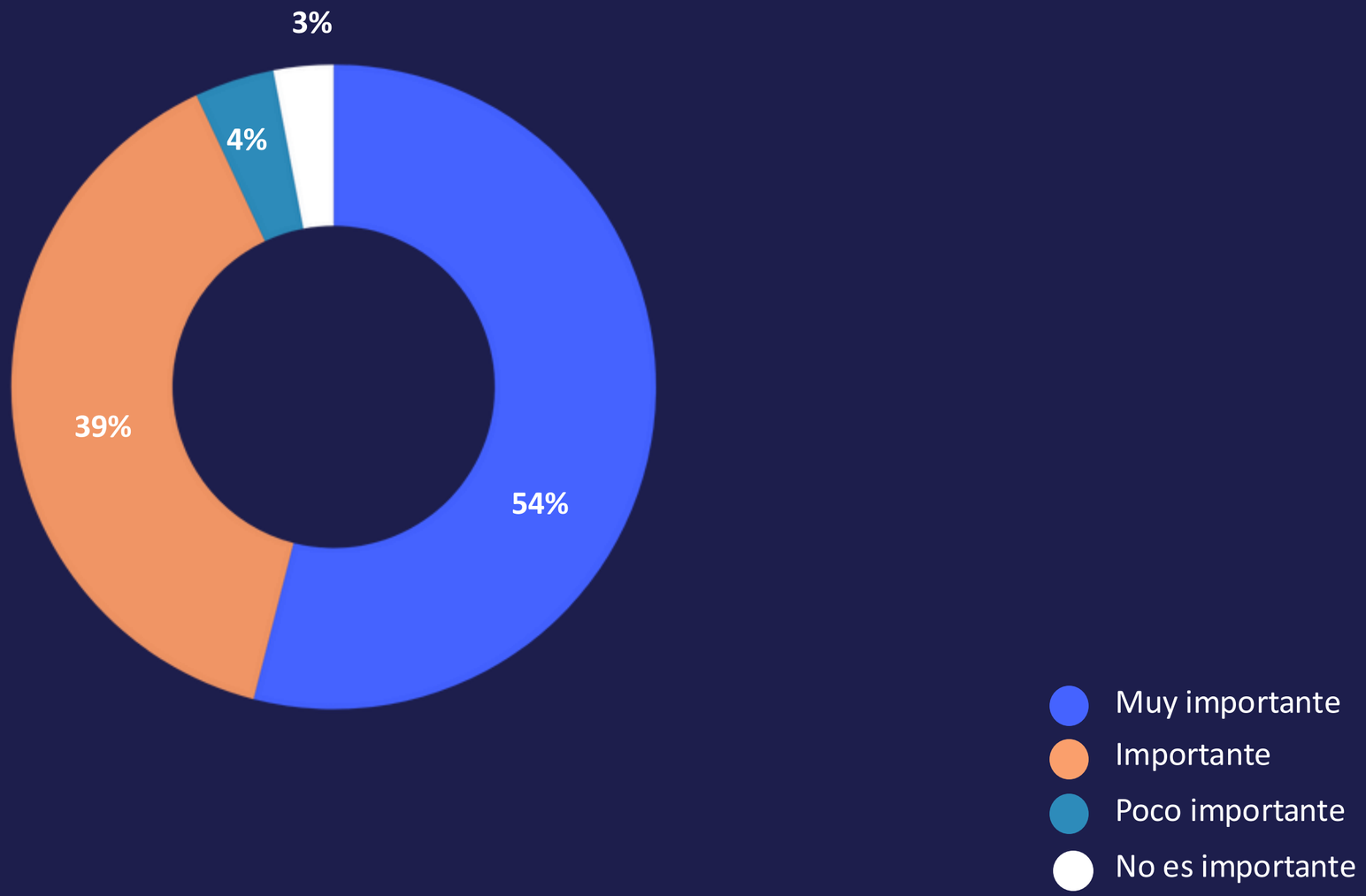
Al responder sí

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

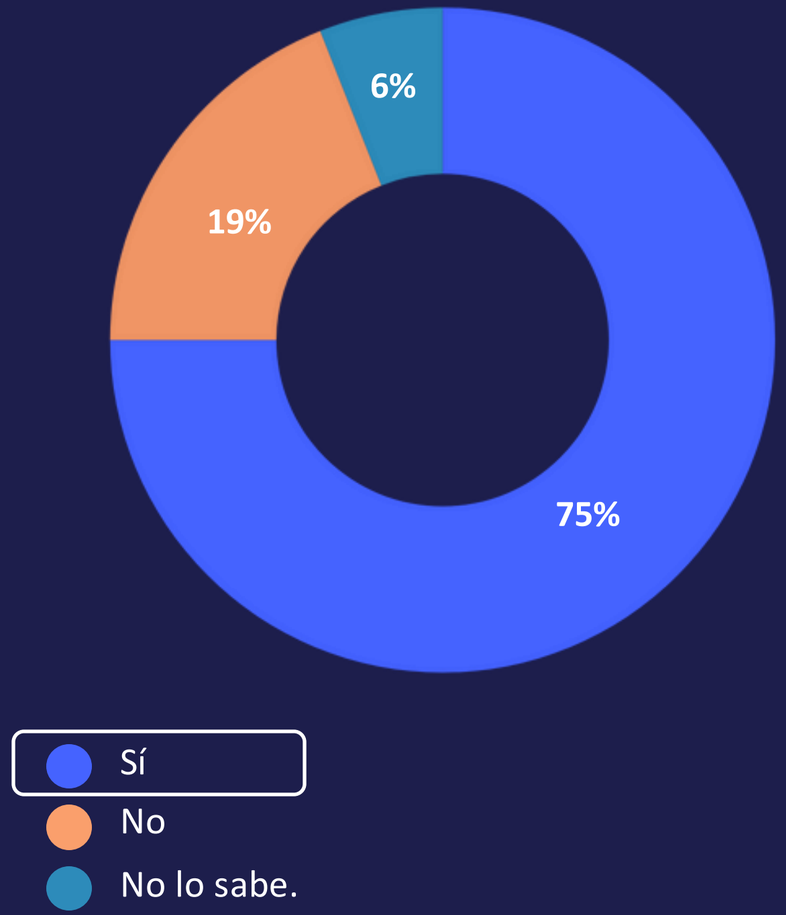


- Impacto crítico: afectó significativamente la operación y reputación de la empresa
- Impacto moderado: afectó algunas áreas, pero la empresa pudo continuar operando
- Impacto leve: hubo consecuencias mínimas, sin afectar la operación

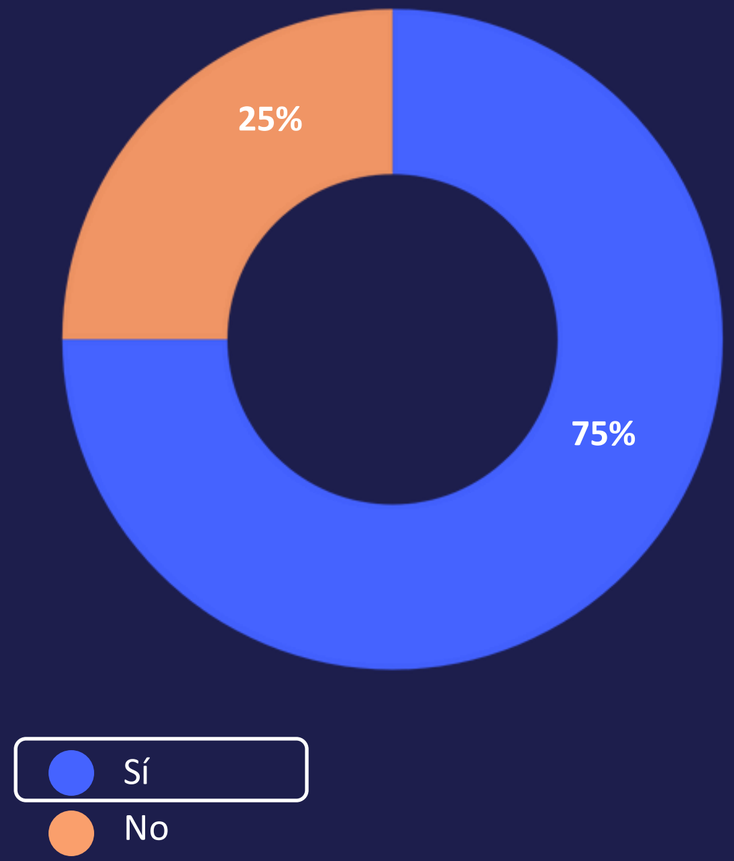
¿Qué importancia le asigna a tener toda la información en un solo lugar: seguro, remoto y permanente?



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



¿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

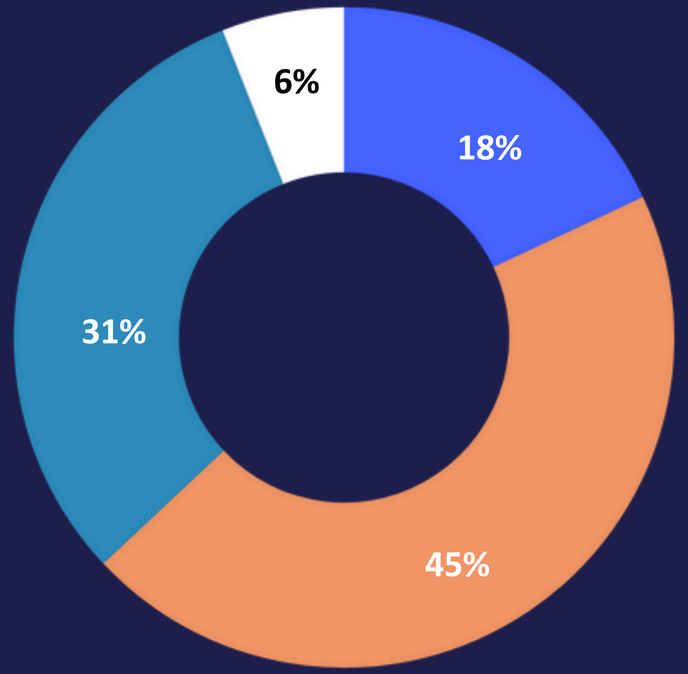
35%

¿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?

36% indicó que sí en 2024

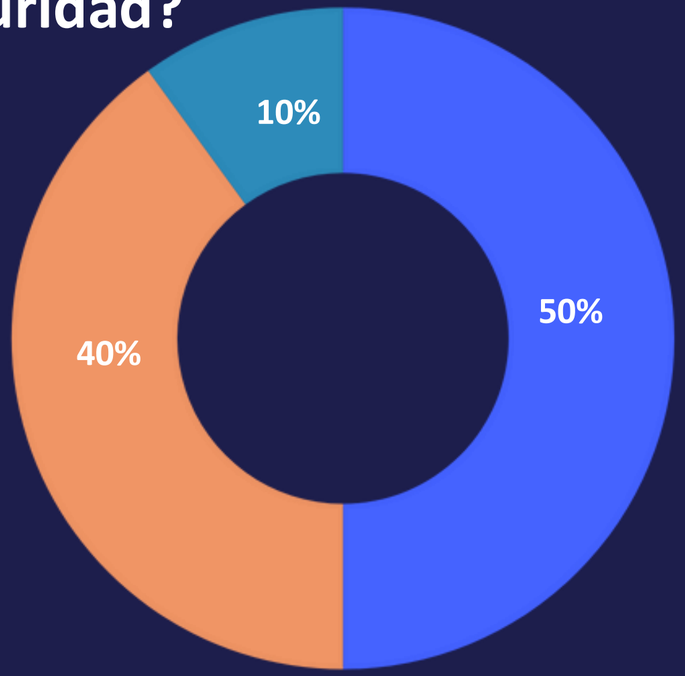
23% indicó que sí en 2023

¿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?

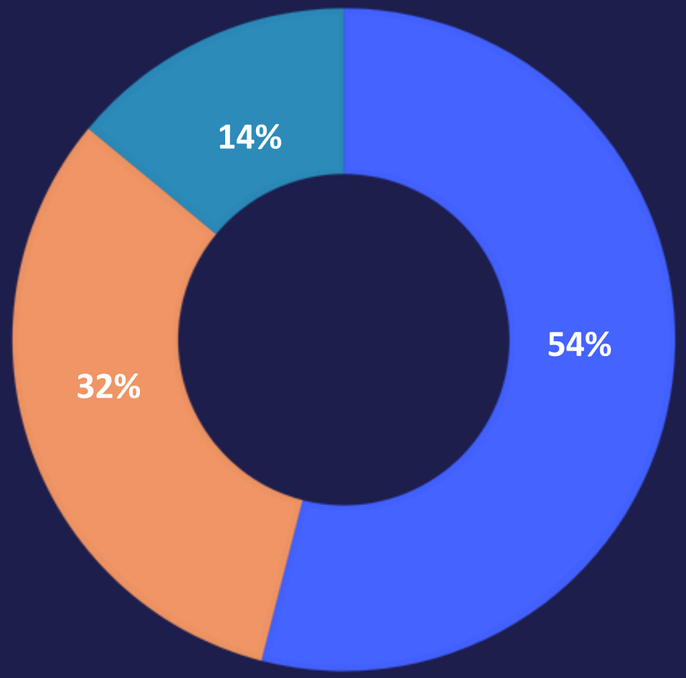


Nuevo marco regulatorio

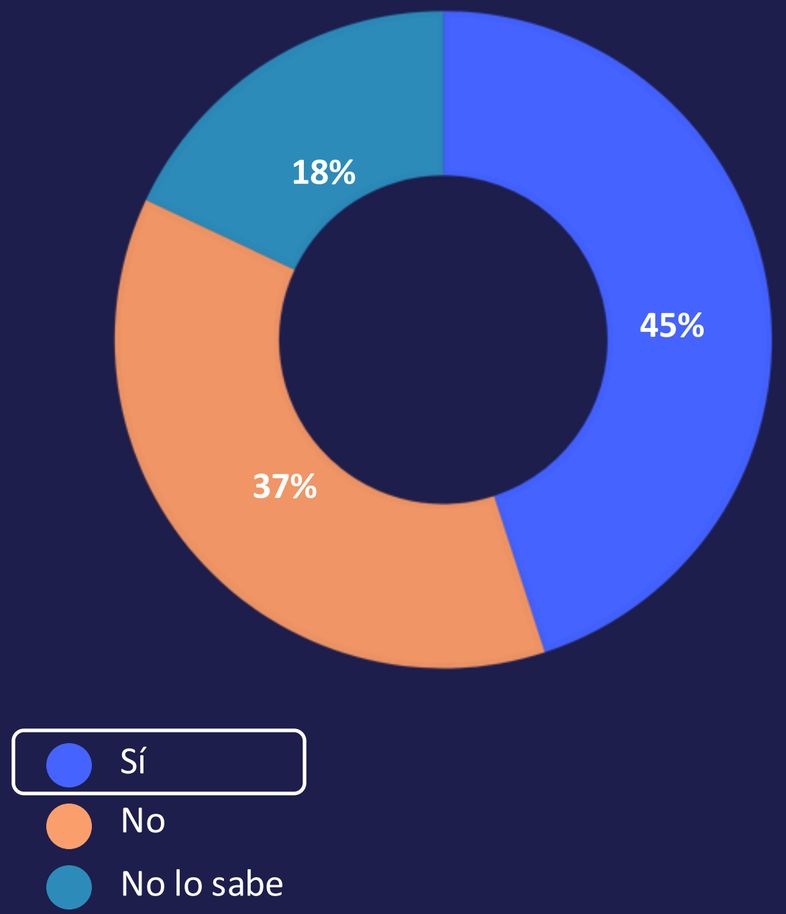
¿El Directorio supervisa que la organización esté verificando adecuadamente la legislación, las regulaciones y las normativas técnicas actuales y potenciales relacionadas con la seguridad?



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



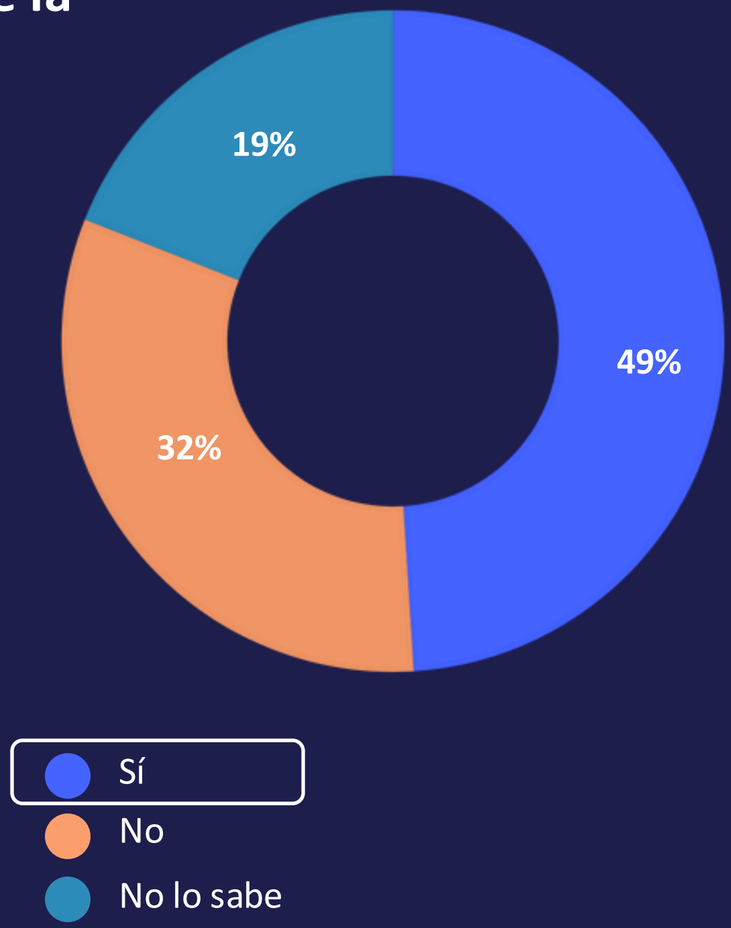
¿El Directorio conoce la existencia de las sanciones y multas consideradas en la nueva Ley Marco de Ciberseguridad de Chile?



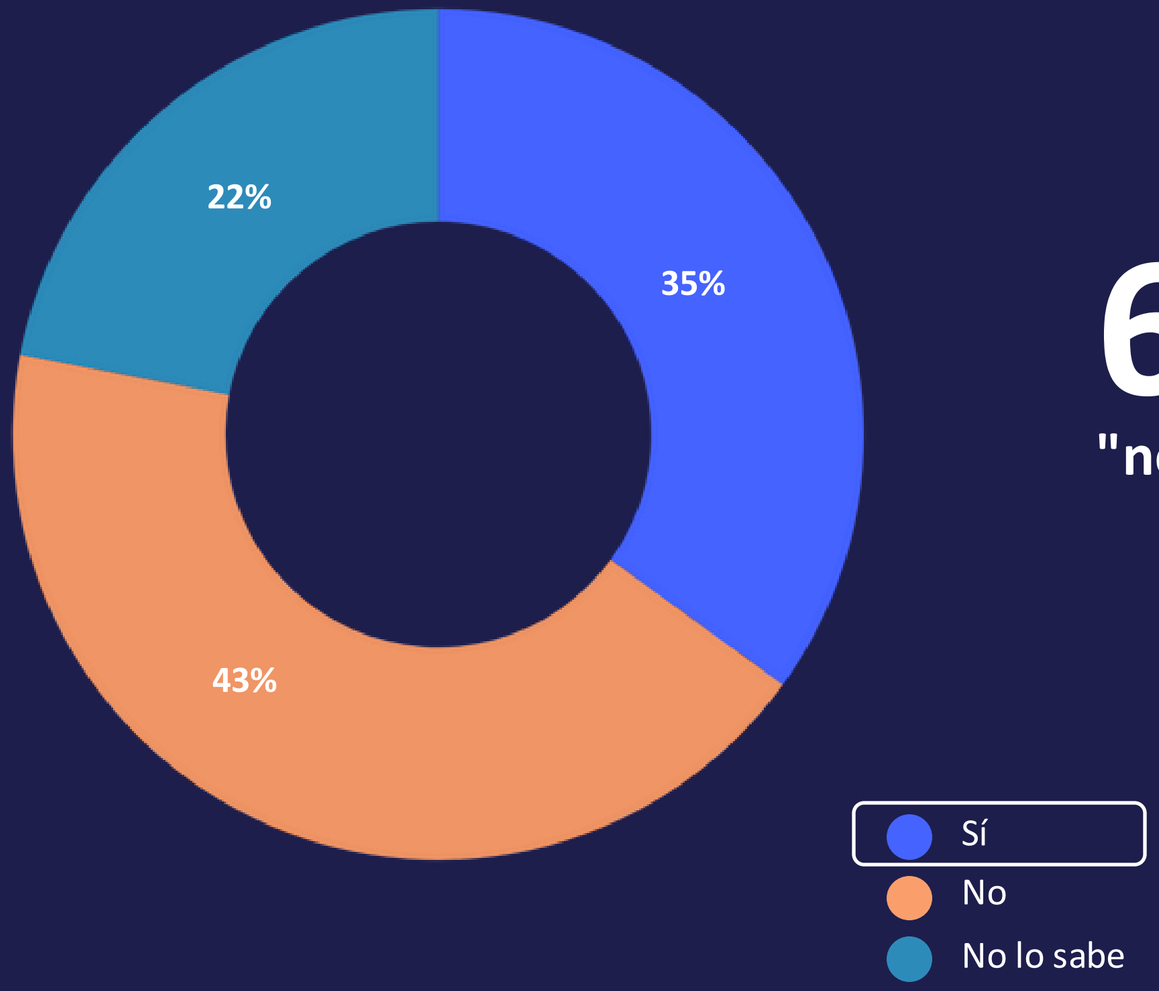
55%

"No conoce" o "no sabe" de las sanciones y multas consideradas en la nueva Ley Marco de Ciberseguridad de Chile

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



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



65% indicó que "no" o "no lo sabe"

Recomendaciones para el Directorio

Recomendaciones para el Directorio

1. Capacite a sus colaboradores

Los colaboradores pueden hacer que su empresa sea vulnerable a ataques. Si bien las estadísticas precisas varían según el país y el sector industrial, es indudable que una gran proporción de las brechas de ciberseguridad son causadas por personal interno que, de manera malintencionada o por negligencia, dan acceso a sus redes a los ciberdelincuentes.

Para protegerse contra las amenazas, invierta en capacitación en ciberseguridad para sus empleados. Establezca directivas claras que describan cómo manejar y proteger la información interna, de sus clientes y otros datos vitales.

Recomendaciones para el Directorio

2. Realice una evaluación de riesgos

Evalúe los riesgos potenciales que podrían comprometer la seguridad de las redes, los sistemas y la información de su empresa. Identificar y analizar posibles amenazas puede ayudarlo a diseñar un plan para cubrir las brechas de ciberseguridad. El directorio es el principal articulador e impulsador de que se instale en la organización una cultura de la evaluación del riesgo de ciberseguridad.

Como parte de su evaluación de riesgos, determine dónde y cómo se almacenan sus datos y quién tiene acceso a ellos. Identifique quiénes pueden querer acceder a los datos y cómo pueden intentar obtenerlos. Si los datos de su empresa están almacenados en la nube, puede pedirle a su proveedor de almacenamiento en la nube que facilite la evaluación de los riesgos. Establezca los niveles de riesgo de posibles escenarios de incidentes de ciberseguridad y cómo las brechas podrían afectar su empresa.

Una vez que este análisis esté completo y haya identificado las amenazas, use la información que ha recopilado para desarrollar o perfeccionar su estrategia de seguridad. Revise y actualice esta estrategia a intervalos regulares. Esto asegurará que sus datos estén siempre protegidos de la mejor manera que esté a su alcance.

Recomendaciones para el Directorio

3. Gobernanza de ciberseguridad

Es una prioridad contar con una estructura de gobernanza de ciberseguridad. Los actuales requerimientos de seguridad de la información sumados a los nuevos requerimientos de ciberseguridad demandaran equipos robustos y las regulaciones solicitaran como punto base contar con los perfiles necesarios para dar respuesta a las diversas acciones a realizar. La separación de funciones será determinante.

Los directorios debe facilitar las instancias para que las empresas cuenten con las estructura de gobernanza necesarias para soportar los distintos requerimientos de los entes reguladores.

Recomendaciones para el Directorio

4. Punto de control en ciberseguridad:

El directorio debe contar con un punto de control que facilite desarrollar escenarios claros de supervisión. El directorio podrá diseñar según su nivel de madurez como desea abordar la ciberseguridad en la mesa y para esto deberá definir cómo será abordado el tema de manera regular, ya sea en un único comité o por intermedio de comités híbridos si considera que esta en una etapa temprana del manejo de la ciberseguridad en su empresa. Esta definición es estratégica para saber llevar la supervisión de los riesgos cibernéticos de forma efectiva.

Recomendaciones para el Directorio

5. Expertos en ciberseguridad:

Las empresas tienen en este punto el mayor desafío para avanzar en la protección y resguardo de las organizaciones. Con una oferta académica ínfima, un déficit creciente de perfiles de ciberseguridad y con una constante demanda de un nivel de expertice cada vez más alto impulsado por el desarrollo de actividades en los ambientes del Internet de las cosas o el uso de la inteligencia artificial crean el escenario ideal para una tormenta perfecta.

Este desafío aumenta significativamente en la medida que se busca que este perfil tenga el debido conocimiento para poder sumar colaborativamente en el impulso del Gobierno Corporativo, el desarrollo de las actividades regulares de la mesa o en los aportes que la ciberseguridad puede proveer en las inversiones que las empresa proyecte para su desarrollo.

En este sentido la mejor recomendación es abordar este desafío lo antes posible ya que esta problemática no es solo del ámbito local sino que este mismo desafío de réplica de forma global, lo que se tendrá como consecuencia que se ampliara la demanda de perfiles

INSTITUTO DE DIRECTORES DE CHILE

CIC -IOT IIOT

Estudio

Radiografía de la ciberseguridad en Directorios de Chile