Estudio

Radiografía de la ciberseguridad en Directorios de Chile

Noviembre 2023

IdD Instituto de Directores Chile

Agenda

01 Introducción

Grupo de la muestra
Metodología
Técnica utilizada

02 Resultados

03 Observaciones y recomendaciones

Introducción

La ciberseguridad ha emergido como uno de los pilares fundamentales en la era digital, donde la interconexión y la dependencia de la tecnología son cada vez más pronunciadas. Reconociendo la vital importancia de salvaguardar la integridad, confidencialidad y disponibilidad de la información en el entorno empresarial, el Instituto de Directores de Chile, en estrecha colaboración con el Centro de Investigación de Ciberseguridad IOT, ha llevado a cabo un exhaustivo análisis de la situación actual de la ciberseguridad en los directorios de Chile.

Este esfuerzo conjunto se centra en el levantamiento de información crucial sobre la ciberseguridad en los directorios empresariales, evaluando su nivel de madurez frente a las crecientes amenazas cibernéticas. Ante el panorama dinámico y complejo de las amenazas digitales, este estudio no solo busca identificar vulnerabilidades, sino también proporcionar un panorama integral que permita a los directores y líderes empresariales adoptar estrategias proactivas para fortalecer las defensas cibernéticas y garantizar la continuidad segura de las operaciones corporativas. En un mundo interconectado, la seguridad cibernética en los directorios no solo es una responsabilidad corporativa, sino un imperativo estratégico para salvaguardar la confianza de los stakeholders y el futuro sostenible de las organizaciones.

Grupo muestral

La encuesta fue enviada a la base de datos del Instituto de Directores de Chile a través de correo electrónico y LinkedIn, resultando en una cantidad correspondiente a 99 respuestas.

Metodología

El cuestionario utilizado para la evaluación comprende un conjunto de 20 preguntas en total.

PREGUNTA FILTRO

¿Es usted director, gerente general o gerente con reporte directo al Directorio?

- ◯ SÍ
- ◯ No

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

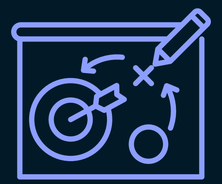
- ◯ SÍ, regularmente.
- ◯ Sí, pero solo en caso de solicitud.
- ◯ No se presenta.
- ◯ No lo sabe.

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

- ◯ Si cuenta con una metodología de riesgo de seguridad.
- ◯ No cuenta con una metodología de riesgo de seguridad.
- ◯ No lo sabe.

Metodología

El cuestionario utilizado para la evaluación comprende un conjunto de 20 preguntas en total.



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

- ◯ Se conoce la existencia de la metodología.
- ◯ No conoce la existencia de la metodología.
- ◯ No lo sabe.

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

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

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

Metodología

El cuestionario utilizado para la evaluación comprende un conjunto de 20 preguntas en total.

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

- ◯ Se cuenta con un presupuesto estratégico de seguridad robusto.
- ◯ Se cuenta con un presupuesto estratégico de seguridad limitado.
- ◯ Se cuenta con un presupuesto de seguridad básico.
- ◯ Se cuenta con un presupuesto estratégico de seguridad priorizado por un Business Impact Analysis (BIA) de la organización.
- ◯ No se cuenta con un presupuesto de seguridad.
- ◯ No lo sabe.

.

¿La organización dispone de una protección adecuada que permite resguardar y proteger la operación en el escenario que sea objeto de un ataque que intente vulnerar las unidades más valiosas de una empresa u otros datos confidenciales?

- ◯ Cuenta con una protección adecuada a escenarios de seguridad.
- ◯ Cuenta con una protección solo en un caso básico específico.
- ◯ Solo se cuenta protección a un escenario básico general.
- ◯ No se cuenta con protección.
- ◯ No lo sabe.

Metodología

El cuestionario utilizado para la evaluación comprende un conjunto de 20 preguntas en total.

¿El Directorio conoce la existencia de un plan de protección mencionado en la pregunta anterior?

- ◯ Sí, conoce la existencia.
- ◯ No conoce la existencia.
- ◯ No sabe.

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?

- ◯ La evaluación de la ciberseguridad es parte regular del ciclo de decisión.
- ◯ Se realiza solo en caso de una solicitud.
- ◯ No se realiza.
- ◯ No lo sabe.

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

- ◯ Se cuenta con una estrategia de comunicación segmentada, aplicable a un escenario de incidente de seguridad y según el potencial receptor.
- ◯ Se cuenta con una estrategia de comunicación estándar, aplicable a un escenario de incidente de seguridad, el cual facilita una respuesta a diversos receptores.
- ◯ No se cuenta con una estrategia de comunicación.
- ◯ No lo sabe.

.

Metodología

El cuestionario utilizado para la evaluación comprende un conjunto de 20 preguntas en total.

¿La organización participa en alguna asociación y/o grupo técnico especializado de seguridad, generando un intercambio de información entre los sectores público o privado?

- ◯ Participa en agrupaciones especializadas de seguridad nacionales e internacionales.
- ◯ Participa en agrupaciones especializadas de seguridad nacionales.
- ◯ No participa.
- ◯ No lo sabe.

¿El Directorio tiene conocimiento de la participación en la pregunta anterior?

- ◯ Sí, tiene conocimiento.
- ◯ No tiene conocimiento.
- ◯ No lo sabe.

¿La organización está verificando adecuadamente la legislación, las regulaciones y las normativas técnicas actuales y potenciales relacionadas con la seguridad, al igual que el cumplimiento de estándar, políticas y marcos nacionales de seguridad?

- ◯ Se cuenta con supervisión adecuada de la legislación, las regulaciones y las normativas técnicas de ciberseguridad.
- ◯ Se cuenta con supervisión básica de la legislación, las regulaciones y las normativas técnicas de ciberseguridad.
- ◯ No se cuenta con supervisión adecuada de la legislación, las regulaciones y las normativas técnicas de ciberseguridad.
- ◯ No lo sabe.

Metodología

El cuestionario utilizado para la evaluación comprende un conjunto de 20 preguntas en total.

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

- ◯ Sí, el Directorio supervisa.
- ◯ El Directorio no supervisa.
- ◯ No lo sabe.

.

¿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 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.

Metodología

El cuestionario utilizado para la evaluación comprende un conjunto de 20 preguntas en total.

¿El Directorio ha habilitado el uso de una póliza de seguro que considere la cobertura de los directores y colaboradores, en actividades que tengan como foco resguardar la operación de la empresa de posibles incidentes de seguridad?

- ◯ Se cuenta con una póliza que cubre escenarios críticos de ciberseguridad.
- ◯ Se cuenta con una póliza básica de ciberseguridad.
- ◯ No se cuenta con una póliza.
- ◯ No lo sabe.

¿El Directorio cuenta con punto de control que facilite la supervisión del estatus de la seguridad?

- ◯ El Directorio cuenta con un punto de control.
- ◯ El Directorio no cuenta con un punto de control.
- ◯ No lo sabe.

En caso de que contar con un punto de control de seguridad, por favor indique en qué estructura del Directorio asigna esta responsabilidad.

- ◯ Comité de Seguridad.
- ◯ Comité de Riesgo.
- ◯ Comité de Auditoría.
- ◯ Comite Hibrido (ejemplo, Comité de Riesgo - Comité de Auditoria).
- ◯ No se cuenta con la asignación de responsabilidades.
- ◯ No lo sabe.

Metodología

El cuestionario utilizado para la evaluación comprende un conjunto de 20 preguntas en total.

¿El Directorio cuenta con algún integrante calificado en materias de Ciberseguridad?

- ◯ Se cuenta con una póliza que cubre escenarios críticos de ciberseguridad.
- ◯ Se cuenta con una póliza básica de ciberseguridad.
- ◯ No se cuenta con una póliza.
- ◯ No lo sabe.

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 31 de octubre hasta el 15 de noviembre, permitiendo a los participantes tener un período adecuado para compartir sus respuestas.

3

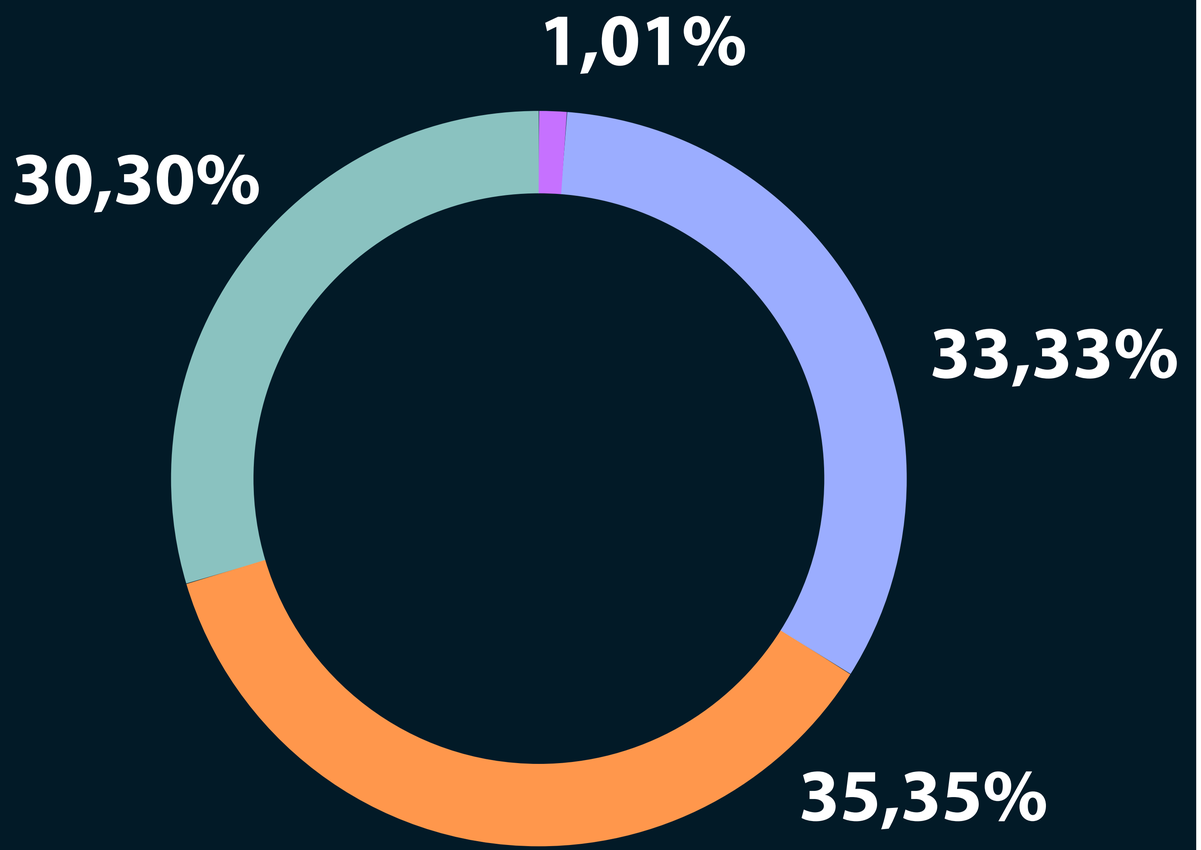
El tiempo promedio necesario para finalizar la encuesta fue de 6 minutos, asegurando una experiencia eficiente para los encuestados.

4

El análisis exhaustivo de los datos se llevó a cabo entre el 20 de noviembre y el 30 de noviembre, 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.

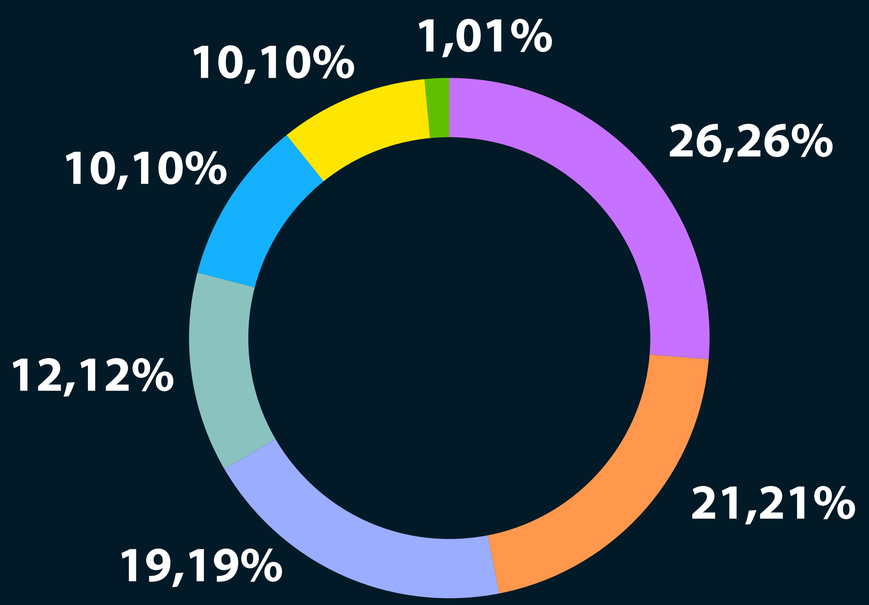
Resultados

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



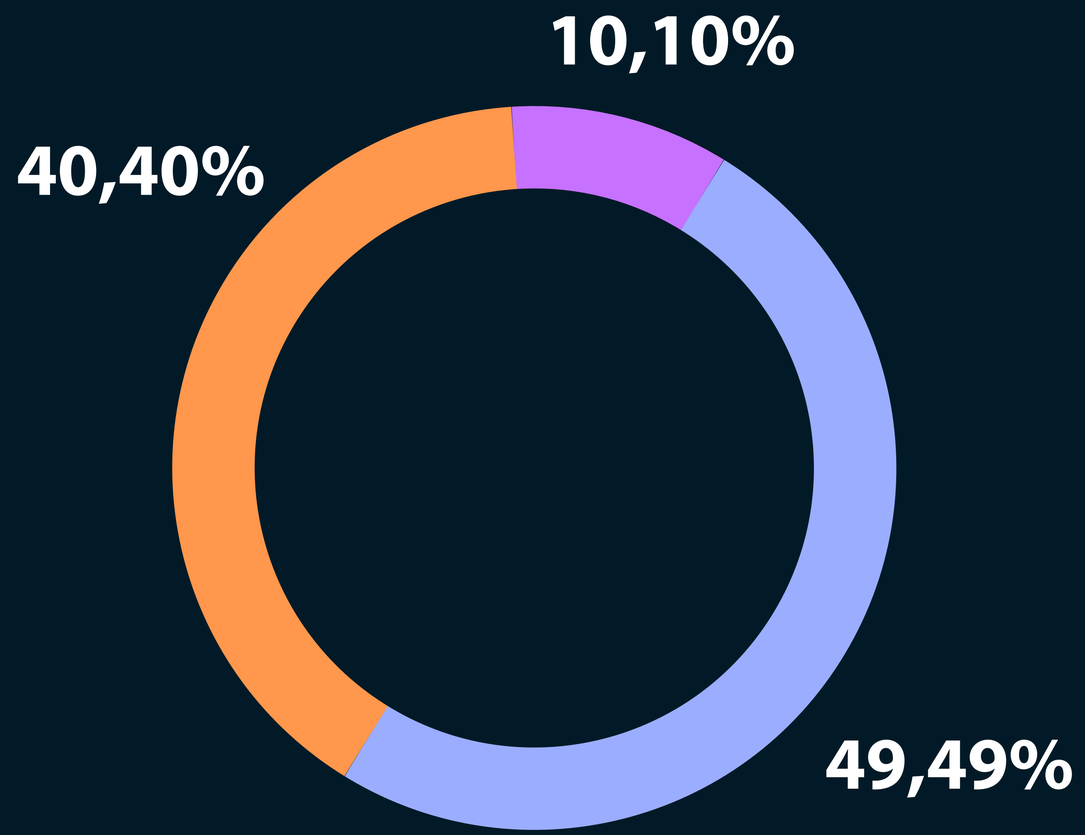
¿Su organización cuenta con una metodología de riesgo de seguridad?

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



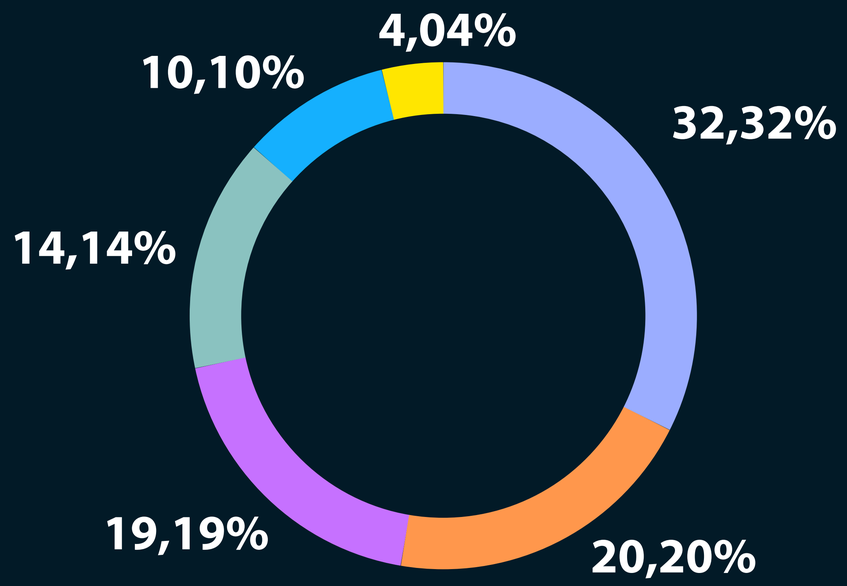
- No lo sabe.
- No se presentan informes
- Trimestral y cada vez que se produce un incidente considerado crítico.
- Solo cuando se produce un incidente considerado crítico.
- Mensual y cada vez que se produce un incidente considerado crítico.
- Anual y cada vez que se produce un incidente considerado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

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



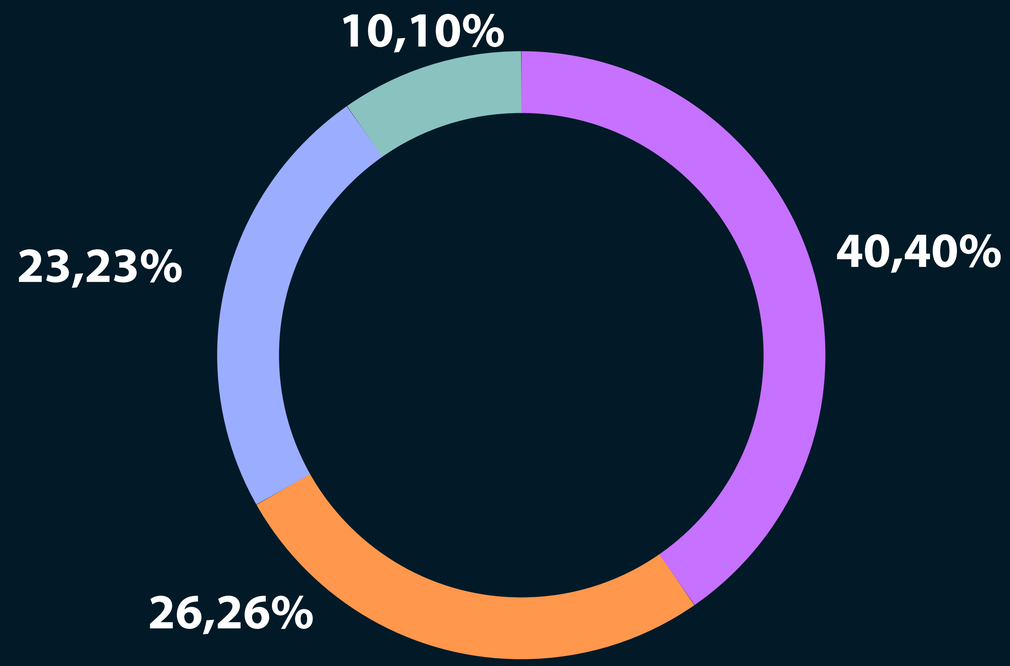
- No lo sabe
- No conoce la existencia de la metodología.
- Sí, conoce la existencia de la metodología.

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



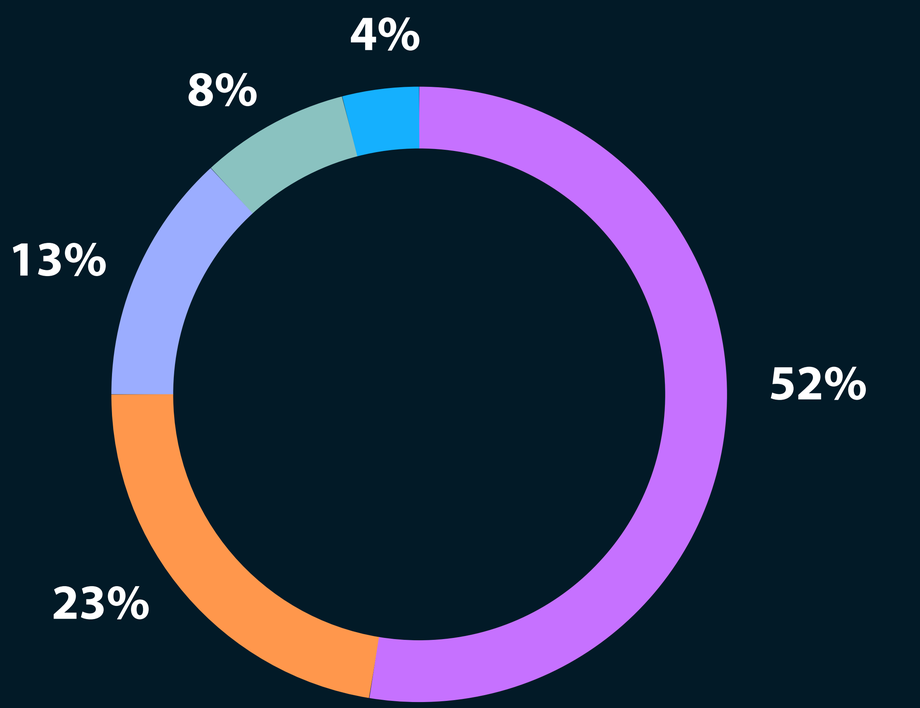
- No lo sabe.
- No se cuenta con un presupuesto de seguridad
- Se cuenta con un presupuesto estratégico de seguridad robusto
- Se cuenta con un presupuesto estratégico de seguridad limitado.
- Se cuenta con un presupuesto de seguridad básico.
- Se cuenta con un presupuesto estratégico de seguridad priorizado por un Business Impact Analysis (BIA) de la organización.

¿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?

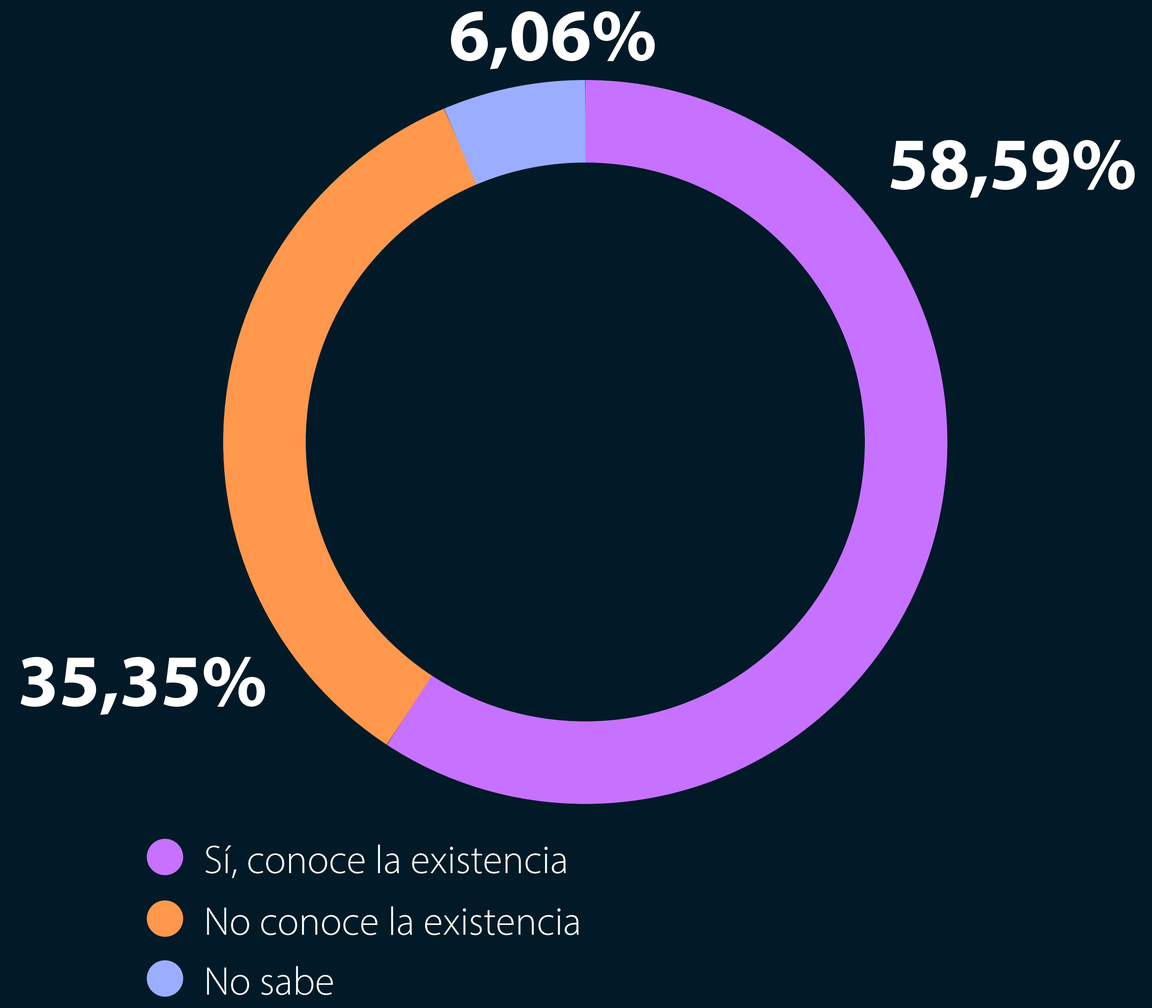


- Se realiza solo en caso de una solicitud
- No se realiza
- La evaluación de la ciberseguridad es parte regular del ciclo de decisión.
- No lo sabe

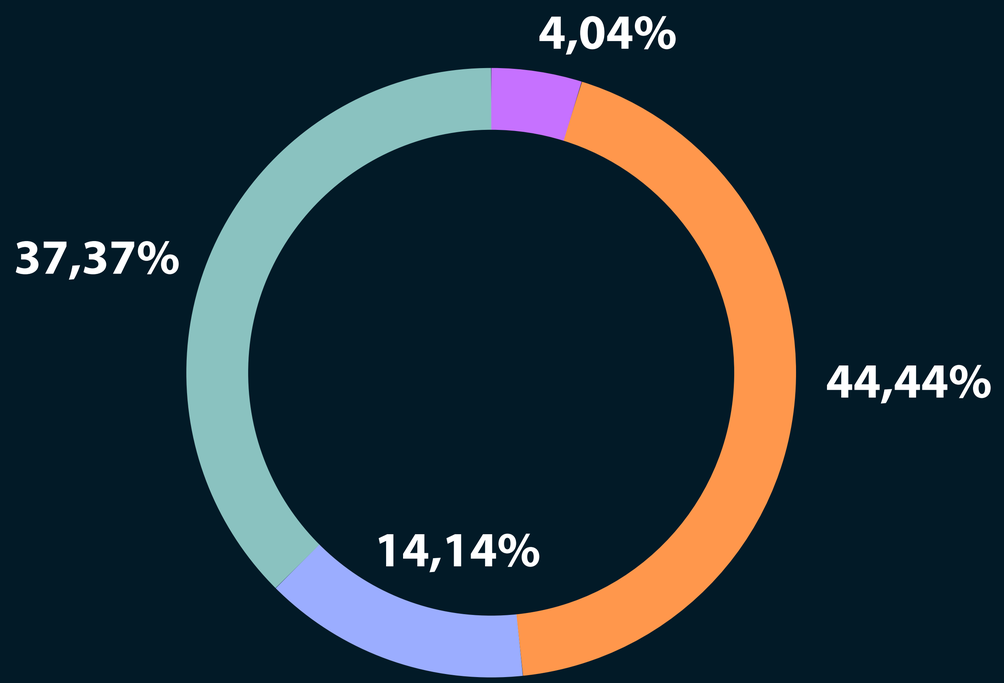
¿La organización dispone de una protección adecuada que permite resguardar y proteger la operación en el escenario que sea objeto de un ataque que intente vulnerar las unidades más valiosas de una empresa u otros datos confidenciales?



¿El Directorio conoce la existencia de un plan de protección mencionado en la pregunta anterior?

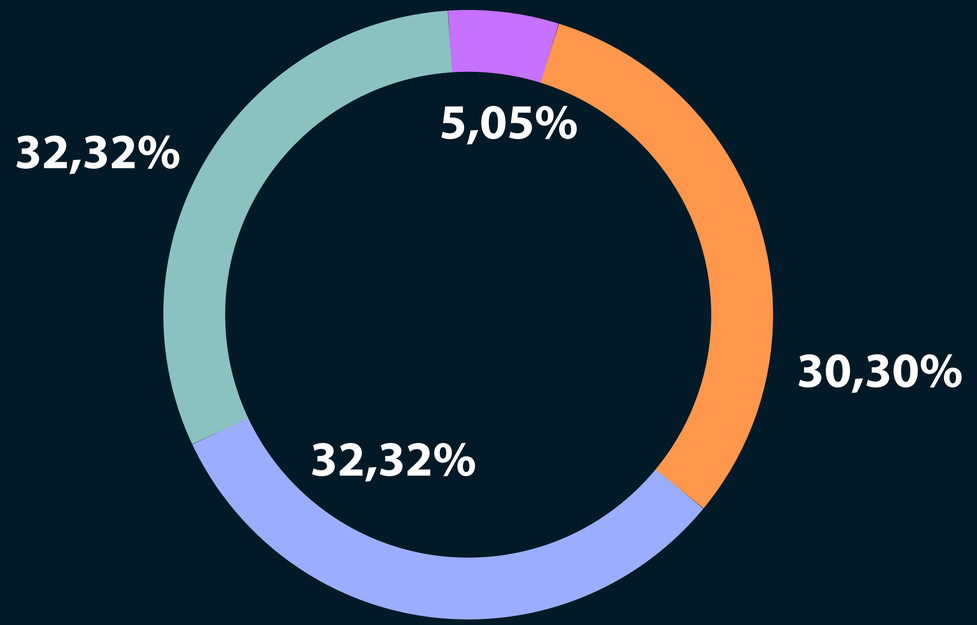


¿El Directorio cuenta con una estrategia de comunicación segmentadas para el público, reguladores, agencias de calificación, que estén alineados a los escenarios de ciberseguridad de su organización?



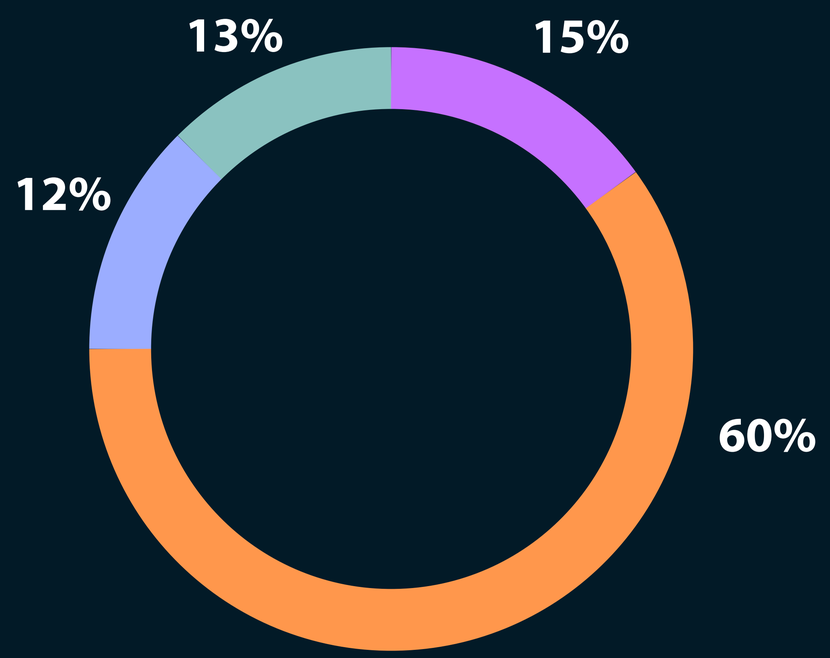
- No lo sabe
- No se cuenta con una estrategia de comunicación
- Se cuenta con una estrategia de comunicación segmentada, aplicable a un escenario de incidente de seguridad y según el potencial receptor.
- Se cuenta con una estrategia de comunicación estándar, aplicable a un escenario de incidente de seguridad, el cual facilita una respuesta a diversos receptores.

¿La organización está verificando adecuadamente la legislación, las regulaciones y las normativas técnicas actuales y potenciales relacionadas con la seguridad, al igual que el cumplimiento de estándar, políticas y marcos nacionales de seguridad?



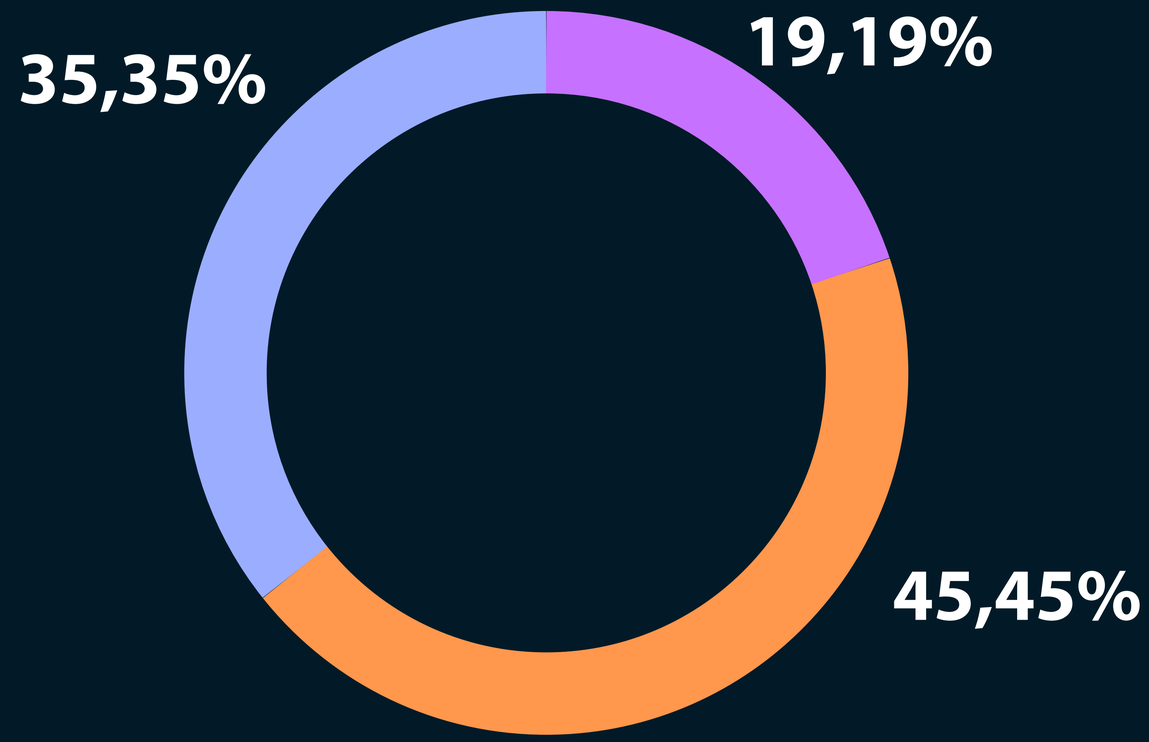
- No lo sabe
- No se cuenta con supervisión adecuada de la legislación, las regulaciones y las normativas técnicas de ciberseguridad.
- Se cuenta con supervisión adecuada de la legislación, las regulaciones y las normativas técnicas de ciberseguridad.
- Se cuenta con supervisión básica de la legislación, las regulaciones y las normativas técnicas de ciberseguridad.

¿La organización participa en alguna asociación y/o grupo técnico especializado de seguridad, generando un intercambio de información entre los sectores público o privado?



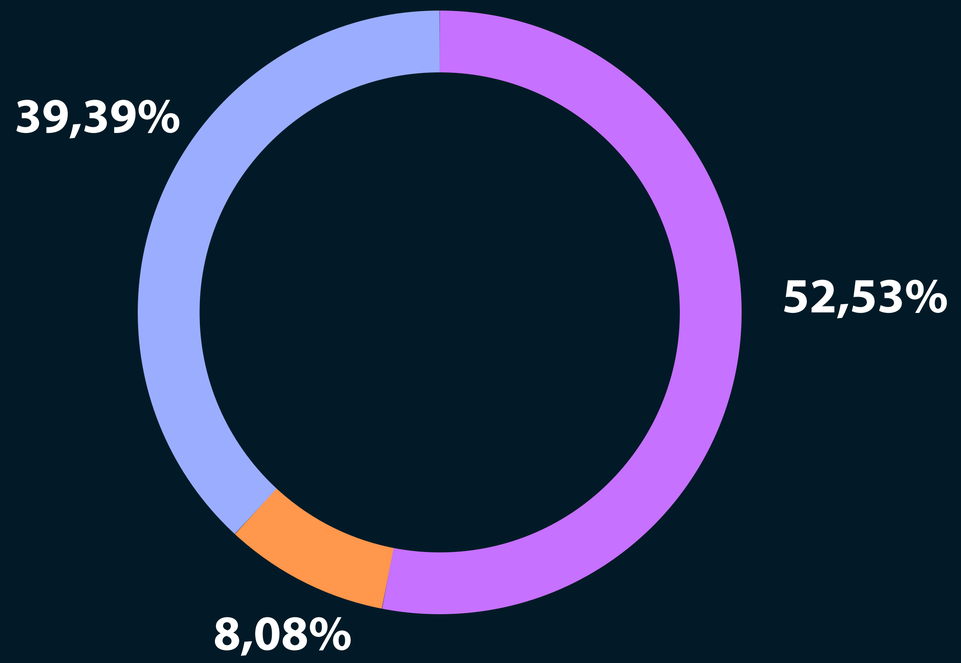
- No lo sabe
- No participa
- Participa en agrupaciones especializadas de seguridad nacionales e internacionales.
- Participa en agrupaciones especializadas de seguridad nacionales.

¿El Directorio tiene conocimiento de la participación en la pregunta anterior?



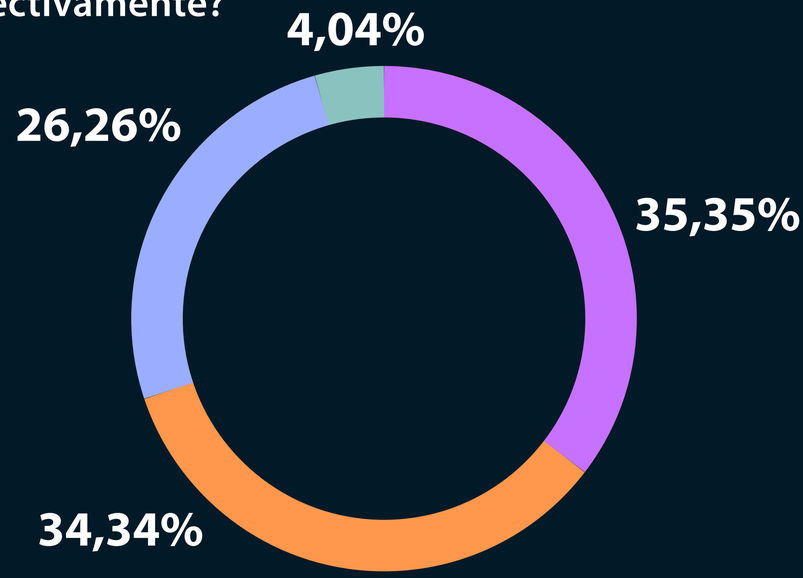
- No lo sabe
- No tiene conocimiento
- Sí, tiene conocimiento.

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



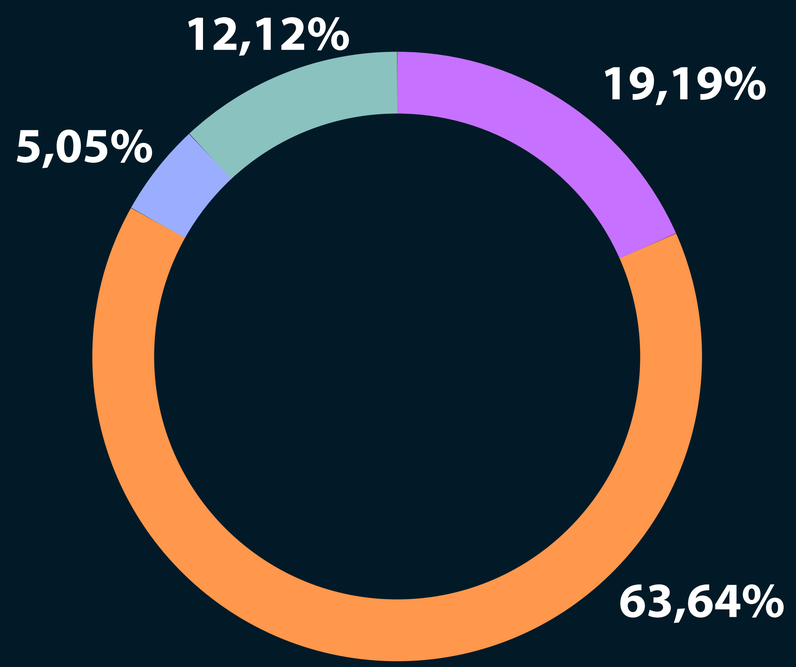
- El Directorio no supervisa
- No lo sabe
- Sí, el Directorio supervisa.

¿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?



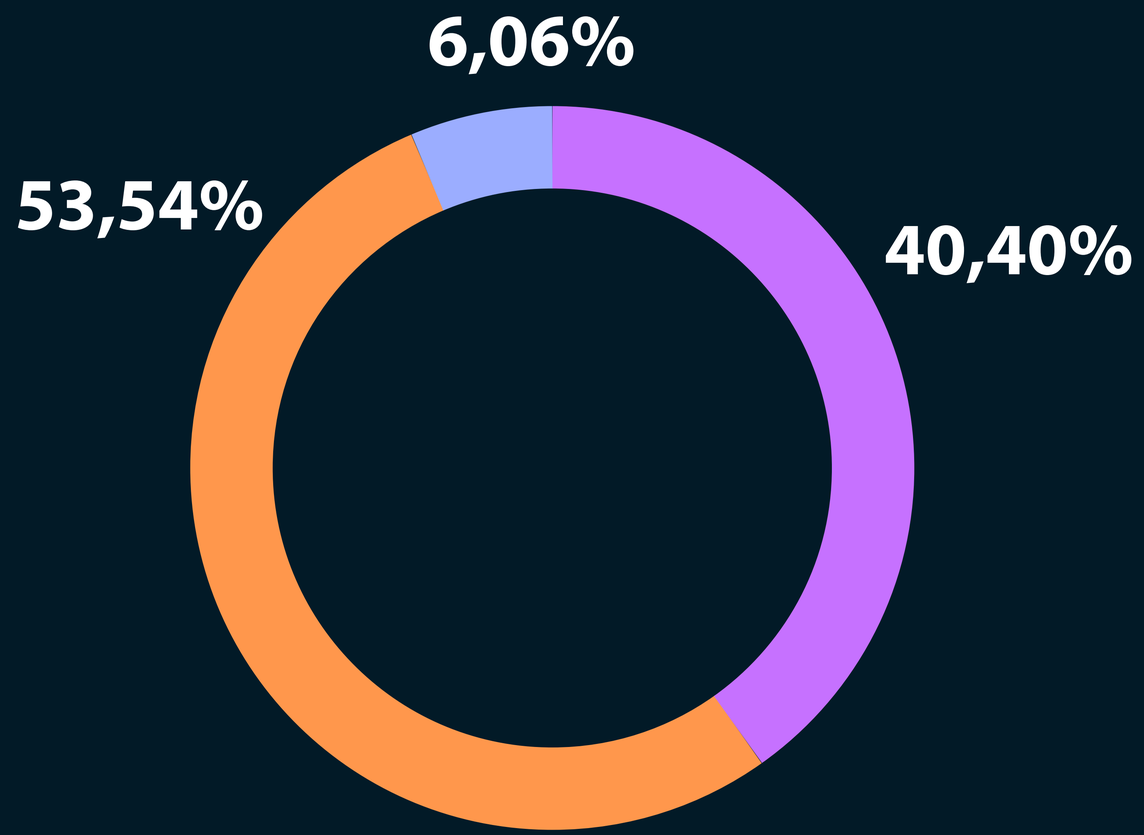
- El Directorio facilita una estructura de gobernanza de seguridad básica (solo seguridad de la información)
- El Directorio facilita una estructura de gobernanza de seguridad integral (seguridad de la información, seguridad informática, ciberseguridad y protección de los datos).
- El Directorio no facilita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

¿El Directorio ha habilitado el uso de una póliza de seguro que considere la cobertura de los directores y colaboradores, en actividades que tengan como foco resguardar la operación de la empresa de posibles incidentes de seguridad?



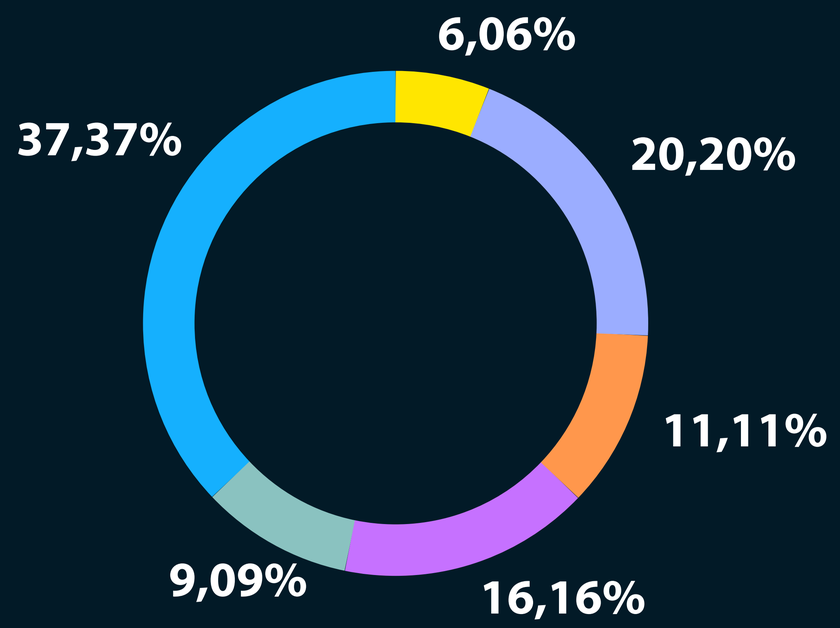
- No lo sabe
- No se cuenta con una póliza
- Se cuenta con una póliza básica de ciberseguridad
- Se cuenta con una póliza que cubre escenarios críticos de ciberseguridad

¿El Directorio cuenta con punto de control que facilite la supervisión del estatus de la seguridad?



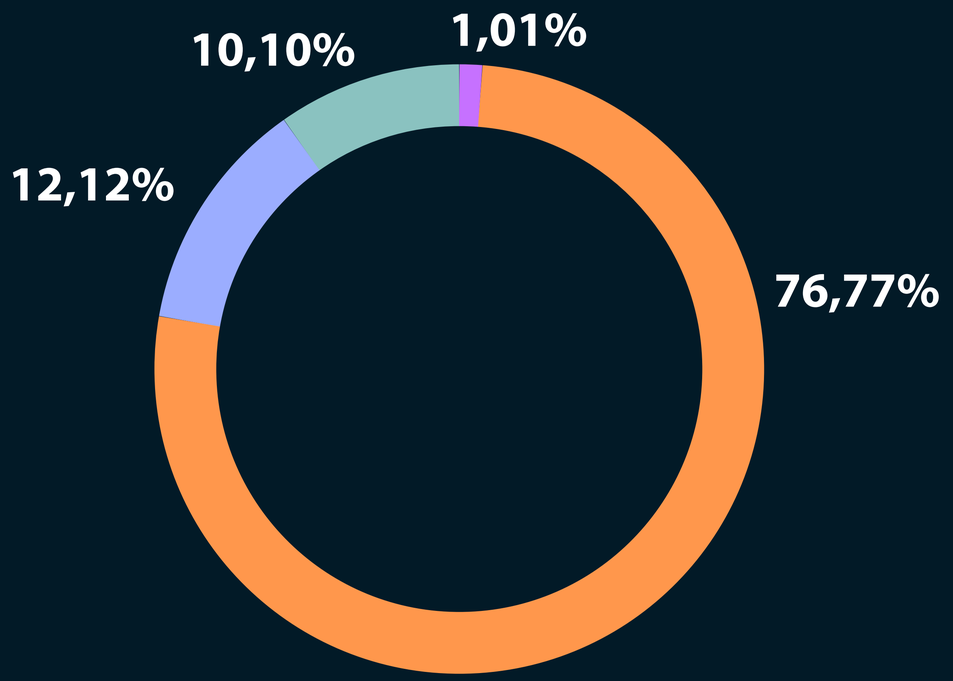
- El Directorio cuenta con un punto de control
- El Directorio no cuenta con un punto de control
- No lo sabe

En caso de que contar con un punto de control de seguridad, por favor indique en qué estructura del Directorio asigna esta responsabilidad.



- Comité de Auditoría
- Comité de Riesgo
- Comité de Seguridad
- Comite Hibrido (ejemplo, Comité de Riesgo - Comité de Auditoria)
- No lo sabe
- No se cuenta con la asignación de responsabilidades

¿El Directorio cuenta con algún integrante calificado en materias de Ciberseguridad?



- No lo sabe
- No se cuenta con un integrante calificado con el Rol Estratégico de Ciberseguridad como parte del Directorio
- Se cuenta con un Asesor Estratégico de Ciberseguridad como parte del Directorio
- Se cuenta con un integrante calificado con el Rol Estratégico de Ciberseguridad como parte del Directorio

Observaciones y recomendaciones

Basado en las respuestas proporcionadas, se identifican varios puntos clave para mejorar el enfoque de la ciberseguridad en el estudio de radiografía en directorios:

2 CREAR CONCIENCIA Y EDUCACIÓN CONTINUA

Dado que una parte significativa del Directorio no está familiarizada con aspectos fundamentales de la ciberseguridad, se debe enfatizar la importancia de la educación continua sobre las amenazas cibernéticas emergentes y los riesgos asociados. Implementar programas de capacitación para los miembros del Directorio puede mejorar su comprensión y toma de decisiones.

1 IMPLEMENTAR METODOLOGÍAS DE RIESGO DE SEGURIDAD

Aunque una proporción considerable tiene una metodología de riesgo de seguridad, existe un número significativo que carece de ella o desconoce su existencia. Es crucial establecer y aplicar metodologías de evaluación de riesgos específicas para la ciberseguridad para ayudar al Directorio a comprender y gestionar los riesgos de manera más efectiva.

Observaciones y recomendaciones

Basado en las respuestas proporcionadas, se identifican varios puntos clave para mejorar el enfoque de la ciberseguridad en el estudio de radiografía en directorios:

3

REPORTES REGULARES Y ACTUALIZADOS

Considerando la variedad de respuestas sobre la regularidad de los informes de riesgo cibernético presentados al Directorio, se debe establecer un calendario anual para presentar informes detallados que aborden tanto los riesgos existentes como los incidentes críticos recientes.

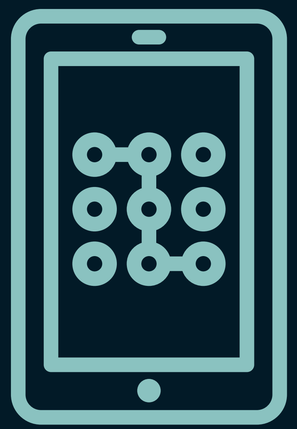
4

PRESUPUESTO ESTRATÉGICO DE SEGURIDAD

Fomentar la asignación estratégica del presupuesto para herramientas, soluciones, servicios de seguridad y capacitación, priorizando las inversiones según un análisis de impacto comercial (BIA) para fortalecer la postura de seguridad de la organización.

Observaciones y recomendaciones

Basado en las respuestas proporcionadas, se identifican varios puntos clave para mejorar el enfoque de la ciberseguridad en el estudio de radiografía en directorios:



5

IMPLEMENTAR ESTRATEGIAS DE PROTECCIÓN Y COMUNICACIÓN

Desarrollar e implementar estrategias integrales de protección que aborden diferentes escenarios de ataques y establecer planes de comunicación adaptados a varios públicos en caso de incidentes de seguridad.

6

PARTICIPACIÓN EN REDES ESPECIALIZADAS EN CIBERSEGURIDAD Y SUPERVISIÓN LEGAL

Incentivar la participación en grupos especializados de seguridad para el intercambio de información y asegurar una supervisión adecuada de las leyes, regulaciones y normativas relacionadas con la ciberseguridad.

Observaciones y recomendaciones

Basado en las respuestas proporcionadas, se identifican varios puntos clave para mejorar el enfoque de la ciberseguridad en el estudio de radiografía en directorios:

7

ESTRUCTURA DE GOBERNANZA Y PÓLIZAS DE SEGURO

Establecer una estructura de gobernanza de seguridad integral que abarque la seguridad de la información, seguridad informática, ciberseguridad y protección de datos. Además, considerar la adquisición de pólizas de seguros que cubran escenarios críticos de ciberseguridad.

8

PUNTO DE CONTROL Y ASIGNACIÓN DE RESPONSABILIDADES

Implementar un punto de control efectivo para la supervisión continua del estatus de la seguridad y asignar claramente responsabilidades dentro del Directorio para su supervisión.

Observaciones y recomendaciones

Basado en las respuestas proporcionadas, se identifican varios puntos clave para mejorar el enfoque de la ciberseguridad en el estudio de radiografía en directorios:

9

PRESENCIA DE EXPERTOS EN CIBERSEGURIDAD EN EL DIRECTORIO

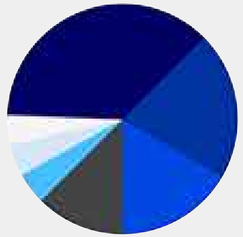
Se recomienda contar con al menos un miembro del Directorio con experiencia y conocimiento en ciberseguridad para garantizar una toma de decisiones más informada y estratégica en este campo.

Al enfocarse en estos aspectos, las organizaciones pueden mejorar significativamente su postura de ciberseguridad y fortalecer su capacidad para mitigar riesgos y responder eficazmente a posibles amenazas.

Estudio
Radiografía de la ciberseguridad en Directorios de Chile

Noviembre 2023

IdD Instituto de Directores Chile



CONOCE NUESTRO PROGRAMA

Actualización para Directores de Empresas

ADE 2024

DIRIGIDO A DIRECTORES Y GERENTES DE PRIMERA LÍNEA

Actualiza tus conocimientos de gobernanza en Chile y complementa con una semana de **experiencia en España, el aprendizaje y reflexión sobre nuevas macrotendencias emergentes**, que amplían nuestra visión de negocios para hacer las empresas más competitivas y conectadas globalmente.

Una experiencia única de networking y vivencia internacional que por primera vez brinda el IdDC en alianza con el IE de España.

Para más información:
+56965242210
contacto@iddc.cl

IdD Instituto de Directores Chile

ie University