FTI CONSULTING

REDEFINIENDO AL CISO

NAVEGANDO LAS PERCEPCIONES Y EXPECTATIVAS DE LA ALTA DIRECCIÓN

REDUCIENDO LOS RIESGOS Y CERRANDO LA BRECHA EN LAS COMUNICACIONES DE CIBERSEGURIDAD

Introducción de Meredith Griffanti. - Senior Managing Director Globlal Head of Cybersecurity & Data Privacy Communications

A medida que nuestro equipo de Comunicaciones de Ciberseguridad y Privacidad de Datos sigue expandiéndose por todo el mundo, he tenido la oportunidad de pasar tiempo en distintos países con ejecutivos de empresas y de ciberseguridad cuyas empresas tienen formas muy diferentes de hacer negocios, así como normas culturales y de comunicación distintas, dependiendo de dónde tengan su sede. El estudio de redefinición del CISO (director de seguridad de la información) es una ventana a lo que nuestro equipo considera un punto débil común en la gobernanza y gestión de la ciberseguridad: independientemente de la región geográfica en la que opere la organización, al CISO le cuesta comunicarse de forma adecuada y con confianza con la Junta Directiva y la alta dirección.

Dado que la ciberseguridad sigue siendo uno de los principales problemas de riesgo y gobernanza para las organizaciones a nivel mundial, recomiendo a todos los directores, líderes de la alta dirección y CISO por igual que lean esta investigación para entender mejor cómo encontrar un terreno común y dónde se encuentran las desconexiones. A menudo oímos hablar de “potenciar el rol” de la Junta y de los altos directivos en lo que respecta a la ciberseguridad, pero buscar oportunidades de formación específicas para los CISO, como el programa Secure Your Seat de FTI Consulting, también es una parte importante para reducir el riesgo y cerrar la brecha en las comunicaciones de ciberseguridad.

Espero que esta investigación, realizada por nuestro equipo de Digital & Insights, anime a las organizaciones a tomar medidas.

.

Preparar el terreno

El riesgo que plantean las vulnerabilidades de ciberseguridad nunca ha sido más grande. A medida que los altos ejecutivos se enfrentan a una mayor responsabilidad por los riesgos de ciberseguridad frente a los reguladores, inversores y otras partes interesadas, FTI Consulting se propuso basarse en nuestro barómetro inaugural CISO (que encuestó a diversos CISO y líderes de seguridad de la información sobre las crecientes presiones en sus funciones, liderazgo y operaciones) para comprender las percepciones y expectativas de los ejecutivos de la alta dirección sobre sus CISO. Mientras que la encuesta inicial reveló una brecha en la comunicación entre los CISO y los ejecutivos, estos nuevos resultados indican que la brecha percibida es aún mayor en la alta dirección.

Parte I: **Resumen de la encuesta a los CISO de 2022**

Metodología

165 CISO encuestados

Solo **EE.UU.**

Hallazgos:

- Ha aumentado el control interno y externo
- Los CISO reportaron una desconexión de comunicaciones con los altos líderes en lo que respecta a las prioridades en ciberseguridad
- Los CISO dijeron que experimentaron dificultades para comunicarse con los altos líderes internos
- Los CISO afirmaron que hacen que las cosas suenen mejor de lo que son para la Junta

Parte II: **Introducción a la encuesta de ejecutivos de la alta dirección de 2024**

Metodología

787 ejecutivos de alta dirección

Audiencia Global 5 continentes

Principales preguntas del estudio:

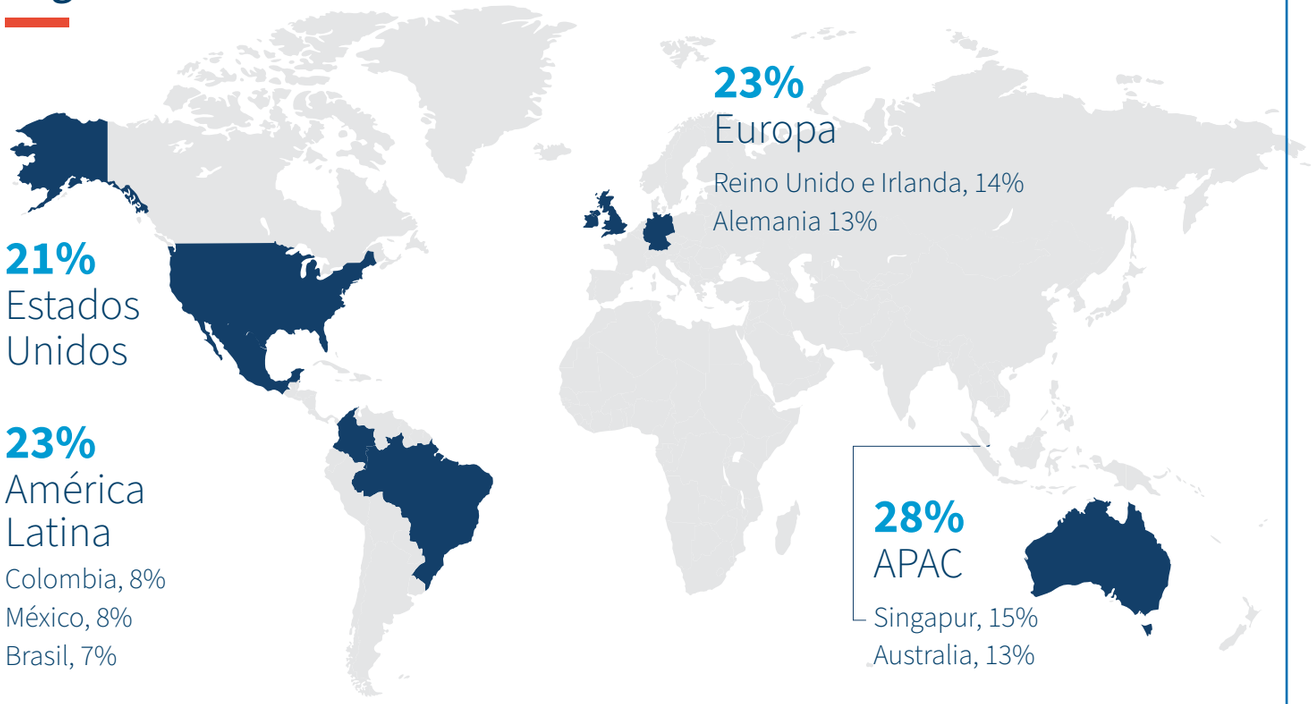
- ¿Perciben los ejecutivos la misma desconexión en las comunicaciones que los CISO? ¿Es quizás esta brecha aún más pronunciada?
- ¿Existe una desalineación constante?
- ¿Qué piensan los ejecutivos sobre las prioridades clave de ciberseguridad?
- ¿Hay necesidad de formación adicional?

CISO — Desconexión de comunicaciones entre los CISO y los líderes — Alta dirección

Metodología Global

El equipo de Digital & Insights de FTI Consulting realizó una encuesta en línea entre n=787 ejecutivos de alta dirección en organizaciones con más de 500 empleados en las industrias clave de FTI. Fue realizada en línea en noviembre de 2023. La investigación previa* se llevó a cabo entre n=165 CISO (indicados por el símbolo en el resto del informe). Si tiene alguna pregunta sobre la metodología, póngase en contacto con James.Condon@fticonsulting.com.

Regiones Globales



21% Estados Unidos

23% América Latina

Colombia, 8%
México, 8%
Brasil, 7%

23% Europa

Reino Unido e Irlanda, 14%
Alemania 13%

28% APAC

Singapur, 15%
Australia, 13%

Ingresos Anuales

$21.5 Billones
Suma de ingresos agregados

$27 millardos
Ingreso promedio

Número de empleados

3,690,000
Total de empleados

4,700
Número promedio de empleados

Sectores de la industria

18% Minoristas

14% Industrias

13% Salud y ciencias de la vida

13% Servicios financieros

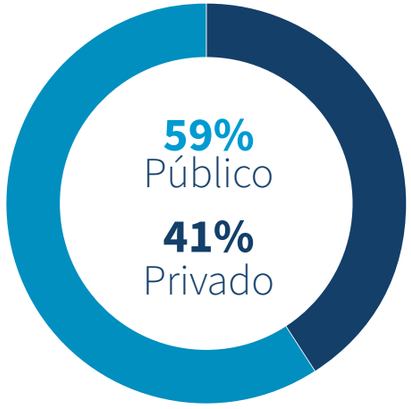
13% Tecnología, medios y telecomunicaciones (TMT)

12% Asuntos públicos y relaciones gubernamentales (PAGR)

11% Energía (ENR)

5% Otros

Publico/Privado



Posición

19% CEO

10% VP

23% CFO

21% Otra alta dirección

27% Director/Gerente

[1]"CISO Communications Redefined," FTI Consulting (2022), https://fticommunications.com/ciso-communications-redefined/

Hallazgos clave

Las empresas siguen siendo vulnerables a los ataques de ciberseguridad mientras aumentan las expectativas sobre los CISO.

Los incidentes están aumentando y **9 de cada 10 encuestados** afirman que han sufrido un ciberincidente en los últimos 12 meses.

El 87% de los ejecutivos afirma haber aumentado la responsabilidad de toma de decisiones de su CISO en los últimos 12 meses, probablemente para responder a la evolución de los retos de la ciberseguridad.

Los CISO no están totalmente preparados para comunicarse con los líderes.

Uno de cada tres altos ejecutivos percibe que sus CISO dudan en alertar a la alta dirección sobre vulnerabilidades potenciales, y una proporción similar cree que sus CISO hacen que las cosas parezcan más optimistas de lo que son en realidad.

Casi **cuatro de cada diez** ejecutivos creen que su CISO no está 100% preparado para comunicarse con las principales partes interesadas internas y externas, y más de un tercio no está totalmente preparado para comunicarse con las directivas.

A los CISO les cuesta demostrar liderazgo a los ejecutivos

El **31% de los ejecutivos** no entiende por completo conceptos técnicos utilizados por los CISO.

El **58% de los CISO** tiene dificultades para comunicar el lenguaje técnico de forma que los altos directivos entiendan (de la Encuesta CISO 2022).

El **62% de los ejecutivos** reportaron que las habilidades de comunicación directa de sus CISO no superan sus expectativas.

El **66% de los CISO** considera que a la alta dirección le cuesta comprender su función (de la Encuesta CISO 2022).

Los ejecutivos apoyan los programas de formación para los CISO, y muchos dicen que es una necesidad inmediata.

El **98% de los ejecutivos** apoya más financiamiento para mejorar las habilidades de comunicación de los Ciso.

El **45%** afirma que existe una necesidad inmediata, especialmente para empresas con más de 2500 empleados.

Los ejecutivos afirman que las mayores carencias en formación están relacionadas con **la anticipación de amenazas, concienciación de los empleados, ROI de comunicación y el ciberriesgo.**

A medida que aumentan los incidentes, el escrutinio y las presiones que vienen desde todas las fuentes, las organizaciones se ven obligadas a priorizar la ciberseguridad y a resaltar el papel del CISO.

Cambios en la organización en los últimos 12 meses*

*Indica la opinión de n=165 CISO en el estudio de FTI de 2022, Redefinición de Comunicaciones de CISO, https://fticommunications.com/ciso-communications-redefined/

La seguridad de la información y la ciberseguridad ocupan un lugar destacado en la lista de prioridades de la alta dirección en 2024.

El 94% de los ejecutivos afirman que la seguridad de la información ha aumentado en importancia en los últimos 12 meses, y la mayoría considera la ciberseguridad una prioridad crítica o alta.

Curiosamente, este porcentaje fue mayor que el de los CISO en la encuesta de octubre de 2022, ya que solo el 85% de los CISO dijeron que la importancia de la seguridad de la información y la ciberseguridad en la agenda de la junta directiva ha aumentado. Está claro que tanto los ejecutivos de la alta dirección como los CISO sienten enormemente las crecientes presiones internas y externas sobre los programas de ciberseguridad. En particular, la ciberseguridad se sitúa un 6% por encima de la experiencia del cliente y la satisfacción entre las prioridades de una organización.

Es probable que estas presiones se deban a la evolución del panorama de las amenazas, la regulación, la importancia de los incidentes de ciberseguridad, y la atención y prioridad que reciben los programas por parte de la junta directiva se nivelan con el escrutinio externo de los medios de comunicación y de las partes interesadas.

De hecho, los ejecutivos de la alta dirección perciben incluso un mayor escrutinio por parte de las directivas, los miembros de la junta y los medios de comunicación sobre la preparación en ciberseguridad en comparación con la opinión de los CISO que encuestamos en 2022.

94% dice que la seguridad de la información ha aumentado en importancia en los últimos 12 meses.

Nivel de prioridad de la ciberseguridad

Prioridades principales de las organizaciones

1. **39%** Información y ciberseguridad.
2. **36%** Eficiencia operativa y optimización de procesos.
3. **33%** Satisfacción y experiencia del consumidor.
4. **32%** Optimización de la cadena de suministros y gestión de proveedores.
5. **31%** Iniciativas ambientales, sociales y de gobernanza.

A medida que aumentan los presupuestos de ciberseguridad, se espera que los CISO comuniquen el retorno de la inversión (ROI).

A medida que la ciberseguridad avanza en el registro de riesgos, los altos directivos esperan realizar inversiones significativamente mayores en sus programas de ciberseguridad, y se espera que las inversiones aumenten en una serie de áreas, incluyendo garantizar que se disponga de la infraestructura de TI adecuada, programas de formación de empleados y preparar a la organización para incidentes de ciberseguridad a través de planes de respuesta a incidentes, proyectos de preparación y capacitación de la alta dirección.

Cabe destacar que los ejecutivos informaron que los presupuestos de ciberseguridad aumentarán una media de 23% en los próximos uno o dos años, con un aumento previsto del 36% más que los presupuestos actuales en los próximos tres a cinco años.

Este aumento del gasto -aunque sin duda es bienvenido por los CISO- conducirá probablemente a un mayor escrutinio de la estrategia de ciberseguridad de la organización y del papel del CISO en ella. Los CISO tendrán que comprometerse con la alta dirección para garantizar que las inversiones se asignen con precisión en línea con las expectativas de la alta dirección y de la junta directiva, así como vincular los resultados de esta inversión a resultados empresariales reales que resuenen entre los altos directivos.

En particular, la formación de los empleados y los programas de concienciación sobre seguridad son la segunda prioridad más alta para las organizaciones este año, ya que los ejecutivos de la alta dirección esperan que sus equipos de seguridad de la información inviertan tiempo y dinero en el uso compartido de información interna.

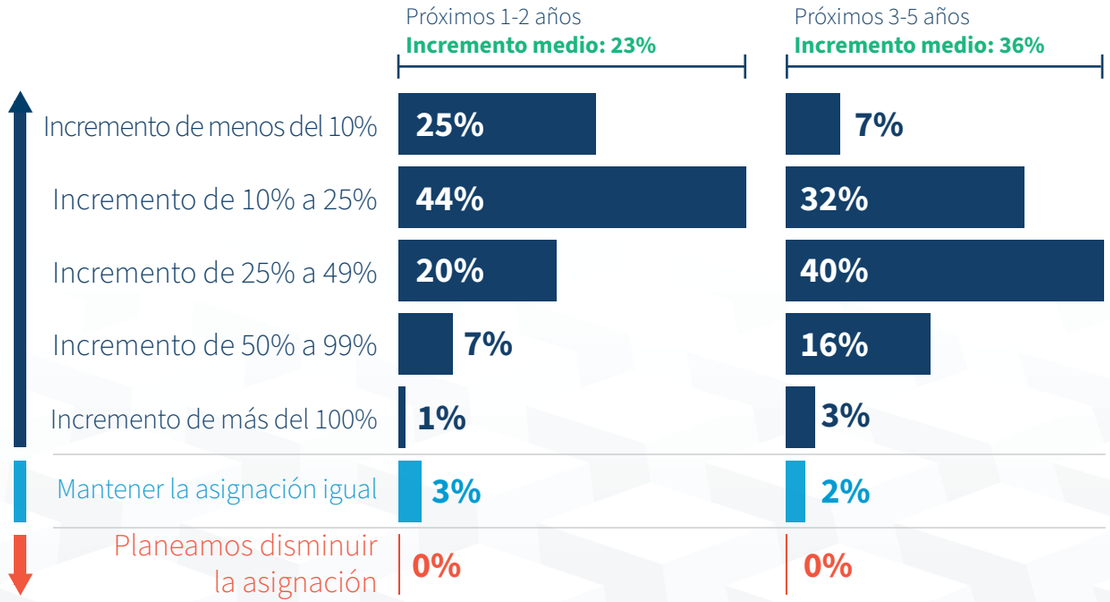
"La ciberseguridad es una prioridad y un gasto cada vez mayor para las organizaciones, y con ello, los CISO se ven obligados a salir de detrás del teclado y situarse en el centro de atención"

Orla Cox - Senior Director
Cybersecurity & Data Privacy Communications

Las 5 principales inversiones esperadas

1. **43%** Actualización o mejora de infraestructura de TI.
2. **42%** Formación de empleados y programas de concienciación en seguridad.
3. **40%** Actualización de la continuidad del negocio y recuperación ante desastres, respuesta a incidentes y planes de comunicación de crisis.
4. **38%** Evaluación de crisis cibernéticas. Preparación y desarrollo de ejercicios de mesa o simulaciones.
5. **37%** Preparación de equipo directivo para gestionar crisis inesperadas.

Incremento esperado del gasto



A medida que crece la supervisión de la ciberseguridad y sus presupuestos, se espera que los CISO articulen mejor el riesgo cibernético y sus planes estratégicos para mitigarlo, pero a menudo se quedan cortos.

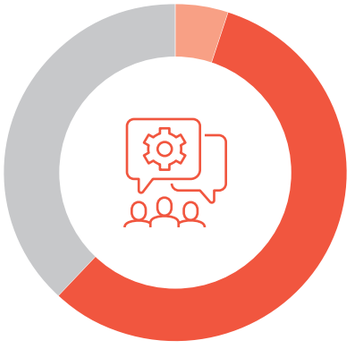
La combinación del aumento de los presupuestos, la ampliación de las responsabilidades de los CISO y un impulso por mayor supervisión de las directivas sobre la ciberseguridad significa que los ejecutivos de la alta dirección desean una mayor visibilidad del rendimiento de la inversión en programas de ciberseguridad.

Sin embargo, muchos ejecutivos creen que sus CISO tienen dificultades para comunicar el retorno de la inversión, son más optimistas con sus evaluaciones de lo que quizá la realidad demuestra, y a menudo no logran traducir sus planes en términos que resuenen en la empresa en general.

Uno de cada tres ejecutivos indica que no entiende del todo los conceptos técnicos utilizados por los CISO y sugiere que el nivel de comunicación directa en torno a la ciberseguridad no supera sus expectativas.

Al igual que en 2022, el 66% de los CISO informaron que a los altos directivos les cuesta comprender plenamente su papel dentro de la organización, lo que significa que los CISO también parecen ser conscientes de esta brecha en la comprensión. En particular, con los aumentos de presupuesto, esta desconexión se observó con más fuerza entre los directores financieros (CFO).

Aunque hay mayores expectativas puestas en los CISO, conceptos de comunicación como la aceptación del riesgo, el rendimiento de las inversiones cibernéticas y el progreso con respecto a los planes estratégicos a largo plazo para la madurez de la seguridad son complicados y pueden resultar difíciles de entender (pero es fundamental que la dirección y la junta direcitva los comprendan). Por lo tanto, existe una necesidad aún mayor de que los CISO perfeccionen sus habilidades de comunicación y ofrezcan una actualización a la junta directiva de forma clara, concisa y nítida cada trimestre.

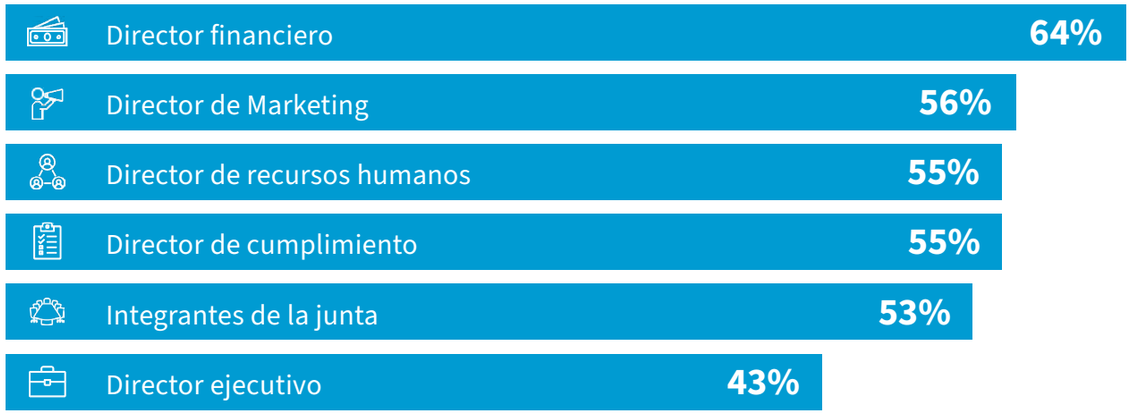


62%
dicen que el nivel de comunicaciones directas del CISO **no supera las expectativas**

▲ América latina, 65%

31%
no entiende por completo los conceptos técnicos usados por el CISO

Posiciones que no entienden por completo el papel del CISO



Los CISO no parecen estar demostrando las principales competencias en liderazgo que esperan los ejecutivos. Les cuesta gestionar las dinámicas de las relaciones internas y externas que pueden afectar directamente a los resultados y la reputación de una organización.

A medida que a los CISO se les da más responsabilidad y hay mayores expectativas de que sean líderes empresariales, hay una presión para que las organizaciones construyan una "cultura" de ciberseguridad de arriba hacia abajo para elevar el perfil e influencia de los CISO, tanto dentro como fuera de las organizaciones.

El 100% de los cinco atributos principales que necesita un CISO, según los ejecutivos, se centran en cualidades de liderazgo; en particular, 4 de cada 5 atributos presentan claramente la necesidad de que los CISO aprovechen las competencias básicas de las comunicaciones. Sin embargo, estas mismas habilidades son aquellas que más les cuestan a los CISO actualmente, a pesar de que los ejecutivos quieren que sus CISO sean más visibles para las directivas y para toda la organización.

Si bien el 36% de los ejecutivos espera que sus CISO sean expertos en construir y gestionar relaciones externas, en 2022 el 52% de los CISO afirmó que gestionar las comunicaciones con las partes interesadas internas y externas es el mayor desafío al responder a un incidente. En última instancia, esta brecha en la comunicación resalta la importancia y el valor de gestionar las relaciones tanto internas como externas antes, durante y después de un incidente en vivo.

Además, el 36% de los ejecutivos también informó que esperan que los CISO establezcan y gestionen las relaciones internas, pero el 23% de los ejecutivos cree que existe un enfoque aislado de la seguridad de la información. Esta mentalidad de aislamiento puede conducir a la desinformación y causar confusión y falta de comunicación en torno a la ciberseguridad en toda la organización.

En general, los CISO deben enfocar ahora su papel como líderes empresariales y no solo como expertos técnicos.

Los 5 principales atributos que necesita un CISO

1. **45%** Gestionar eficazmente los presupuestos y recursos de seguridad.
2. **38%** Traducir fácilmente la jerga técnica a términos comprensibles.
3. **38%** Liderar hábilmente en tiempos de crisis.
4. **36%** Ser experto en construir y gestionar relaciones externas.
5. **36%** Ser capaz de desarrollar y mantener relaciones internas.

"En medio del panorama de riesgos actual, nuevas regulaciones y el creciente escrutinio, los CISO deben trabajar para dominar un conjunto de habilidades centradas en la empresa para satisfacer las nuevas demandas de su función en evolución"

Jamie Singer - Senior Managing Director
Cybersecurity & Data Privacy Communications

Los ejecutivos tampoco se sienten alineados estratégicamente con los líderes de ciberseguridad, lo que significa un riesgo organizativo adicional.

A pesar de este aumento del poder de decisión, del gasto presupuestario y de las expectativas de que los CISO asuman funciones de liderazgo, casi la mitad de los encuestados de la alta dirección no consideran que sus prioridades de liderazgo estén completamente alineadas con las de quienes trabajan en sus departamentos de seguridad de la información y ciberseguridad. El 53% de los CISO también señalaron que sus prioridades no están completamente alineadas con las de la alta dirección.

Además, en 2022, el 82% de los CISO afirmaron que sentían la necesidad de exagerar positivamente frente a la junta directiva, y curiosamente, el 31% de los ejecutivos encuestados también reconoce que este es un de los retos más importantes de un CISO. Esto ocurre probablemente porque los líderes en ciberseguridad y seguridad de la información no saben cómo comunicar adecuadamente el riesgo y temen que esto se refleje negativamente en sus programas.

Además, el 30% de los ejecutivos sintieron que su CISO dudaba en mostrar preocupaciones sobre las vulnerabilidades de la organización, perpetuando así el escepticismo dentro del programa de ciberseguridad.

Esta falta de alineación y la incapacidad y vacilación para comunicar adecuadamente el riesgo de ciberseguridad plantea un reto importante para las organizaciones. Con los reguladores y otras partes interesadas responsabilizando cada vez más a los altos cargos por la ciberseguridad, es fundamental que estos tengan una imagen clara y precisa del nivel de riesgo cibernético de la organización y de que se estén aplicando las medidas adecuadas. Aunque tanto los ejecutivos como los CISO coinciden en que existe una falta de alineación de prioridades, muchas organizaciones aún no han identificado un plan para abordar esta brecha.

Prioridad organizacional versus acciones de ciberseguridad

46%
de los ejecutivos no se sienten completamente alineados con sus CISO

53%
de los CISO no se sienten completamente alineados con su equipo ejecutivo

Retos comunes

"Lo vemos muy a menudo cuando los CISO tienden a pintar un panorama más optimista que la realidad. Este es un gran problema: los líderes de las empresas DEBEN comprender con precisión los riesgos cibernéticos que enfrentan; de lo contrario, no podrán dirigirlas de manera efectiva y se verán sorprendidos cuando se produzca un incidente"

Meredith Griffanti - Senior Managing Director
Global Head of Cybersecurity & Data Privacy Communications

Curiosamente, tanto los CISO como los ejecutivos reconocen la desalineación y los retos a los que se enfrenta los CISO dentro de una organización.

Los desafíos de los CISO al comunicarse con la alta dirección

66%
Siente que los altos directivos no comprenden completamente el papel del CISO dentro de la organización.

82%
Siente que tienen que hacer que las cosas suenen mejor de lo que realmente son para la junta directiva.

58%
Tiene dificultades para comunicar el lenguaje técnico a los altos directivos de una manera que estos lo puedan entender.

Los desafíos de los altos directivos al comunicarse con los CISO

30%
Los CISO tienen dificultades para expresar el riesgo de ciberseguridad en términos financieros/materiales.

31%
Los CISO hacen que las cosas parezcan más optimistas de lo que realmente son.

31%
Dificultad para comprender el retorno tangible de la inversión cibernética.

28%
Los CISO tienen dificultades para traducir términos técnicos a términos comerciales.

30%
Los CISO dudan en plantear preocupaciones sobre las vulnerabilidades de la organización.

19%
No hay suficiente tiempo para discutir con los CISO.

Al mismo tiempo, una pluralidad de ejecutivos siente que los CISO no están completamente preparados para comunicarse con la junta o los altos directivos.

En caso de un incidente cibernético, muchos ejecutivos encuestados creen que los CISO no están completamente preparados para comunicarse con las partes interesadas internas y externas más importantes de su empresa. En particular, los ejecutivos hablan de una falta de preparación entre una variedad de partes interesadas internas y externas críticas, quienes sirven como portavoces de la respuesta de una organización a un incidente o cuya opinión impacta directamente los resultados de la organización. Aunque los CISO necesitan evolucionar hasta convertirse en líderes empresariales y desarrollar nuevas habilidades en el panorama actual, los ejecutivos en gran medida no sienten que ellos estén preparados para comunicarse con las partes interesadas clave, lo que podría tener un impacto significativo en la empresa.

Además, los ejecutivos citaron una falta de preparación para comunicar eficazmente los problemas a las fuerzas policiales y a los responsables políticos.

Con este nuevo poder de toma de decisiones, en la actualidad es fundamental para los CISO articular su respuesta, los puntos de decisión y responder preguntas ejecutivas (especialmente relacionadas con las acciones tomadas durante un incidente en vivo). Esto se convertirá en un problema mayor en los próximos años a medida que los reguladores observen críticamente a los CISO y su papel como asesores de ciberseguridad de sus juntas directivas. Conocer los riesgos y vulnerabilidades es una de sus tareas, pero no resolver el problema o, en ocasiones, no poder plantearlo lo suficiente dentro de la empresa, crea una responsabilidad inherente para el CISO y el equipo directivo de su organización. Esto puede tener consecuencias dramáticas para una empresa, incluida la pérdida de clientes, pérdida de ingresos, acciones legales y daños duraderos a la reputación de la organización.

Desafíos de preparación para las comunicaciones con las partes interesadas

"Existe un claro punto de fricción entre las expectativas de comunicación de la alta dirección y la realidad operativa de un CISO. A los CISO se les pide que actúen como portavoces de la empresa, pero muchos simplemente no están preparados para hacerlo"

James Condon - Managing Director
Head of Research, Digital & Insights

Para cerrar esta brecha percibida de comunicación y abordar el riesgo organizacional resultante, los ejecutivos apoyan más presupuesto para las comunicaciones de los CISO y su capacitación en presentaciones. Muchos muestran esto como una necesidad inmediata para los CISO como parte de la preparación en materia de ciberseguridad de su organización.

Ante estas mayores responsabilidades y expectativas, los ejecutivos están más que dispuestos a invertir en sus CISO y respaldar programas de capacitación que, en última instancia, conducirán a comunicaciones internas fluidas en torno a la ciberseguridad y tendrán un impacto en los resultados.

Debido a que no abordar estos problemas podría traer mayores implicaciones para la empresa, casi todos los encuestados apoyan una mayor financiación de las comunicaciones y la capacitación de presentaciones de los CISO, y casi la mitad caracteriza esto como una necesidad inmediata.

Actualmente, los ejecutivos sienten que existen varias brechas importantes que podrían abordarse con capacitaciones de expertos, incluido un énfasis en mejores métodos de comunicación y cuantificación de riesgos para las partes interesadas. A medida que el papel del CISO continúa evolucionando, los CISO siguen teniendo una responsabilidad de comunicación, tanto como defensores internos como portavoces externos.

Los ejecutivos quieren preparar a los CISO para el éxito, entendiendo que tener la capacidad de cuantificar los riesgos y retornos cibernéticos es un conjunto de habilidades que ahora se requieren para los líderes en ciberseguridad. La capacitación y el coaching en comunicaciones no solo facilitarán la vida del CISO, sino que, en última instancia, prepararán a la empresa para el éxito y la conducirán a decisiones más inteligentes y rápidas en el futuro.

98% Apoya más fondos para la presentación y capacitación en comunicación de sus CISO.

Nivel de prioridad de seguridad cibernética

- **45%** Necesidad inmediata
- **44%** Necesidad eventual
- **11%** No hay necesidad

55% APAC

37% EE.UU.

48% 2500 + Empleados

40% <2500 Empleados

Los 5 temas principales para la capacitación en comunicaciones de los CISO

1. **31%** Estrategias para anticipar y contrarrestar futuras amenazas y tendencias cibernéticas
2. **27%** Enfoques colaborativos para la capacitación de empleados en concientización sobre la seguridad
3. **27%** Métodos para cuantificar y comunicar los riesgos de ciberseguridad a las partes interesadas
4. **27%** Orientación sobre la comunicación de información técnica de manera clara y precisa
5. **26%** Enfoques para construir una cultura de ciberseguridad proactiva y adaptable

"Sus dos mayores aliados [en caso de incidente] son la comunicación y la opcionalidad. La comunicación es poder contar la historia de cómo están las cosas y asegurarse de que todos remen en la misma dirección. Es poder comunicar el estado actual y sus planes a los reguladores y, al mismo tiempo, poder tranquilizar a sus clientes y asegurarse de que tengan confianza en que podrán salir adelante"

Evan Roberts - Senior Managing Director
Co-Head, Cybersecurity & Data Privacy Communications

Invierta en enfrentar la brecha en las comunicaciones a través del programa de capacitación en comunicaciones CISO de FTI

SECURE YOUR SEAT

COMMUNICATIONS TRAINING PROGRAM

La práctica de Comunicaciones de Ciberseguridad y Privacidad de Datos de FTI Consulting tiene una capacidad inigualable para tomar cuestiones complejas de ciberseguridad y dividirlas en conceptos fáciles de entender. A menudo escuchamos de los CISO después de un incidente que quieren nuestra ayuda continua para perfeccionar sus presentaciones trimestrales a la Junta o sus habilidades de comunicación general para que resuenen mejor entre los directivos de la empresa. Damos la bienvenida a los CISO para que aprovechen nuestra experiencia tanto en ciberseguridad como en comunicaciones con el lanzamiento de Secure Your Seat (SYS), un programa de capacitación en comunicaciones y preparación para juntas directivas basado en investigaciones y creado exclusivamente para CISO.

El programa de seis semanas guía a los CISO a través de sesiones de capacitación individuales semanales personalizadas que les permiten comunicarse mejor con los altos directivos, conocer las expectativas de la junta directiva, traducir el lenguaje técnico y los KPI a términos sencillos y mejorar sus presentaciones trimestrales y anuales ante la junta directiva. Los participantes también reciben capacitación práctica personalizada en comunicación de mensajes y presentaciones, con la oportunidad de practicar sus presentaciones a la junta directiva frente a nuestro consejo asesor, que reúne a un grupo diverso de ejecutivos de alta dirección y directores en funciones de la junta directiva con conocimientos de ciberseguridad.

Presentamos Secure Your Seat: un programa de capacitación en comunicaciones para CISO

- Estudio para identificar áreas por mejorar
- Establecimiento de metas
- Análisis de marca
- Vocería
- Taller de definición de mensajes y presentaciones
- Mejora trimestral/anual de la plataforma Cyber Board
- Desarrollo de CV listo para la junta directiva
- Sesión simulada de presentación y comentarios de la junta (frente a nuestro consejo asesor de SYS)

Para obtener más información sobre Secure Your Seat, comuníquese con **SYS@fticonsulting.com** y un miembro del equipo se comunicará con usted.

"El programa Secure Your Seat de FTI está dirigido por un equipo de expertos de talla mundial que viven y respiran las comunicaciones cibernéticas. Bien si es un CISO nuevo en el puesto o un CISO experimentado como yo, este programa es esencial para preparar a los líderes de ciberseguridad para articular claramente los objetivos, riesgos y oportunidades de ciberseguridad a los altos ejecutivos de su organización"

Jesse Whaley
Chief Information Security Officer, Amtrak

MEREDITH GRIFFANTI
Senior Managing Director
Global Head of Cybersecurity & Data Privacy Communications
meredith.griffanti@fticonsulting.com

ANA HEEREN
Senior Managing Director
ana.heeren@fticonsulting.com

JORGE DEL CASTILLO
Managing Director
jorge.delcastillo@fticonsulting.com

ANA MARÍA MUÑOZ
Senior Director
anamaria.munoz@fticonsulting.com

ADRIANA PRADO
Managing Director
adriana.prado@fticonsulting.com

KELLY SOUZA
Senior Director
kelly.souza@fticonsulting.com

ISAAC MORALES
Director Sénior
isaac.morales@fticonsulting.com

Sobre FTI Consulting

FTI Consulting es una firma independiente de asesoría empresarial global dedicada a ayudar a las organizaciones a gestionar el cambio, mitigar riesgos y resolver disputas: financieras, legales, operativas, políticas y regulatorias, reputacionales y transaccionales. Los profesionales de FTI Consulting, ubicados en los principales centros de negocios del mundo, trabajan en estrecha colaboración con los clientes para anticipar, identificar y superar desafíos y oportunidades comerciales complejos.

FTI Consulting, Inc., incluidas sus subsidiarias y afiliadas, es una firma de consultoría y no es una firma de contadores públicos certificada ni una firma de abogados.

Las opiniones expresadas en este artículo son de los autores y no necesariamente las opiniones de FTI Consulting, su administración, sus subsidiarias, sus afiliados u otros profesionales.

Acerca de las Comunicaciones Estratégicas de FTI

Altos directivos, juntas directivas y líderes empresariales de todo el mundo acuden a FTI Consulting con sus problemas más complejos y críticos para su negocio que requieren diversos conjuntos de habilidades y disciplinas integradas.

Nuestra división de comunicaciones estratégicas apoya a docenas de altos ejecutivos y personas de alto perfil con sus estrategias de redes sociales, contenido y gestión de canales, ayudándolos a mitigar el riesgo y mejorar su reputación al combinar décadas de profunda experiencia en la materia con experiencia funcional y disciplinaria.

Acerca de las comunicaciones sobre ciberseguridad y privacidad de datos de FTI

Nuestra oferta de Comunicaciones de Ciberseguridad y Privacidad de datos es uno de los principales grupos de comunicaciones de ciberseguridad de la industria. Nombrada Firma de Relaciones Públicas Cibernéticas del Año por los Premios a la Excelencia en Ciberseguridad en 2021, 2022 y 2023 y reconocida por Chambers & Partners como uno de los principales proveedores de comunicaciones de crisis a nivel mundial, el grupo brinda asesoramiento experto en comunicaciones de crisis y apoyo en la preparación para la ciberseguridad y durante todo el proceso de un incidente, ayudando a organizaciones de todo el mundo a mitigar riesgos, mejorar la continuidad y proteger sus relaciones con las partes interesadas antes, durante y después de un incidente.

En pocas palabras, ayudamos a nuestros clientes a comunicarse de manera efectiva (a través de cualquier canal) para proteger y mejorar sus intereses con las partes interesadas clave.

Acerca de FTI Digital & Insights

La práctica de Digital & Insights se encuentra en el centro de la oferta multifacética de FTI Consulting. Al reunir a expertos en ciencia de datos e investigación primaria, así como en integrada.estrategia y ejecución digital y creativa, trabajamos junto con nuestros colegas en la materia para ofrecer un enfoque integral que dé prioridad a la audiencia. Estos conocimientos se convierten en la base sobre la que se construyen las campañas de comunicación.

Para más información y para contactar a nuestro equipo, visite nuestra **página web de Redefiniendo al CISO** ▶

FTI CONSULTING™