Marsh | Microsoft

Estado de la resiliencia cibernética

Un nuevo informe de Marsh y Microsoft para ayudarle a los líderes de todas las áreas a alinear y priorizar sus estrategias cibernéticas para el 2022 y años posteriores

May 2022

Contenido

Introducción

Hoy en día, las empresas siguen aumentando la inversión en una serie de soluciones tecnológicas, opciones de financiación de riesgos, talento calificado y otras medidas en su enfoque de riesgo cibernético, para crear resiliencia. Sin embargo, el costo de casi tres años de interrupción en el lugar de trabajo, transformación digital y ataques de ransomware significa que la mayoría de los líderes no confían más que hace dos años en su capacidad para gestionar el riesgo cibernético. Este es uno de los hallazgos de la Encuesta de riesgo cibernético de Marsh y Microsoft 2022, la tercera colaboración de este tipo que nuestras empresas han llevado a cabo en los últimos cuatro años.

Uno de los aspectos que está frenando la confianza, es que la mayoría de las empresas no han adoptado un enfoque de riesgo cibernético para toda la empresa; un enfoque que, en esencia, se basa en una estrategia de amplia comunicación y fomenta la colaboración, así como la armonización, entre las partes interesadas durante los momentos clave en la toma de decisiones en su travesía de resiliencia cibernética. Por ejemplo, todos los departamentos que abordan el riesgo cibernético deben participar en la gestión de incidentes cibernéticos y los conocimientos cibernéticos deben compartirse en toda la empresa para resolver adecuadamente los puntos débiles de la seguridad cibernética en la organización.

Este año, nuestro informe examina cómo las distintas funciones y líderes de la empresa ven el riesgo cibernético, específicamente los de seguridad cibernética y TI, gestión de riesgos y seguros, finanzas y dirección ejecutiva.

Aunque todas estas funciones tienen intereses comunes en torno a los riesgos cibernéticos, descubrimos que a menudo actúan de forma independiente, perdiendo así los beneficios potenciales que ofrece un enfoque integral en la empresa. Sus diferentes puntos de vista y formas separadas de gestionar los riesgos cibernéticos se reflejan en nuestro hallazgo de que únicamente 41% de las organizaciones involucran a los departamentos jurídicos, de planificación corporativa, de finanzas, de operaciones o de gestión de la cadena de suministro en la elaboración de planes de riesgos cibernéticos.

En las siguientes páginas, encontrará ocho tendencias clave que los líderes cibernéticos de su empresa pueden discutir, mientras buscan una comprensión común del riesgo cibernético. El informe también examina las funciones y responsabilidades de su equipo cibernético empresarial para ayudarle a comprender las necesidades, responsabilidades y perspectivas de cada una. Y, por último, compartimos algunas de las mejores prácticas que su empresa puede utilizar para alinearse, para gestionar eficazmente el riesgo cibernético.

Queremos agradecer a los más de 650 líderes de riesgo cibernético de organizaciones de todo el mundo que se tomaron el tiempo de compartir sus opiniones sobre este importante tema. Esperamos que este informe integre a su organización y estimule las conversaciones mientras construye un enfoque de resiliencia cibernética en toda la empresa.

Únicamente 41 % de las organizaciones involucran a los departamentos jurídicos, de planificación corporativa, de finanzas, de operaciones o de gestión de la cadena de suministro en la elaboración de planes de riesgo cibernético.

Resumen ejecutivo

El riesgo cibernético está presente en la mayoría de las organizaciones. Un empleado o proveedor que enciende su computadora portátil desde casa conlleva un riesgo. Un usuario que conecta un nuevo producto a la Internet de las cosas genera un riesgo. Decidir no lanzar un producto nuevo por temor a las amenazas cibernéticas es un riesgo. Y la lista sigue. Para contrarrestar estos riesgos es necesario alinear a toda la empresa.

Tendencias principales en materia de riesgo cibernético

Al analizar las respuestas de la Encuesta de riesgo cibernético de Marsh y Microsoft 2022 , se destacan ocho tendencias:

1. Los objetivos cibernéticos específicos de la empresa, incluyendo las medidas de seguridad cibernética, los seguros, los datos y los análisis, y los planes de respuesta a incidentes, deben estar alineados con la creación de la resiliencia cibernética frente a la simple prevención de incidentes, ya que toda organización puede esperar un ataque cibernético. *73% de las empresas afirma haber sufrido* un ataque cibernético.

2. El ransomware (programas maliciosos que secuestran datos) es considerada la principal amenaza cibernética a la que se enfrentan las empresas, pero no es la única. Otras amenazas generalizadas son la suplantación de identidad electrónica (phishing)/ingeniería social, violaciones de la privacidad y la interrupción de negocios debido a un ataque a un proveedor externo.

3. Los seguros son una parte importante de la estrategia de gestión de riesgos cibernéticos e influyen en la adopción de mejores prácticas y controles. 61 % expresó que su empresa compra algún tipo de cobertura de seguro cibernético.

4. La adopción de más controles de seguridad cibernética resulta en una mayor calificación de higiene cibernética. *Sólo 3 % de los encuestados calificó como excelente la higiene* cibernética de su empresa.

5. Las organizaciones tienen cierto retraso en la medición del riesgo cibernético en términos financieros, lo que perjudica su capacidad para comunicar eficazmente las amenazas cibernéticas en toda la empresa. Sólo 26 % de los encuestados *dijo que su organización utiliza medidas financieras para medir el* riesgo cibernético.

6. Sigue aumentando la inversión en la mitigación de los riesgos cibernéticos, aunque las prioridades de gasto varían según la empresa. 64 % dijo que el estímulo para aumentar las inversiones en riesgos cibernéticos fue haber sufrido un ataque.

7. Las nuevas tecnologías deben ser evaluadas y supervisadas de forma continua, no sólo durante la exploración y análisis previos a su adopción. *54 % de las empresas afirma que no* amplía las evaluaciones de riesgo de las nuevas tecnologías más allá de su aplicación

8. Las empresas adoptan muchas medidas de seguridad cibernética, pero en general pasan por alto a sus proveedores/cadenas de suministro digitales. Sólo 43 % ha llevado a cabo una evaluación de riesgos de su proveedor/cadena de suministro.

Formando un equipo resiliente

Es importante entender cómo los profesionales de una empresa ven su función cuando se trata de seguros cibernéticos, gestión de incidentes cibernéticos, herramientas y servicios de seguridad cibernética, etc. ¿Consideran que su función es la de tomar decisiones? ¿Forman parte del equipo general, con un aporte a las decisiones? ¿O no están involucrados en absoluto? Las respuestas serán de gran ayuda para determinar los próximos pasos que debe seguir su empresa para desarrollar resiliencia cibernética.

Encontramos que el nivel de involucramiento en diversas áreas de la gestión de riesgos cibernéticos es una mezcla de funciones y responsabilidades. Por ejemplo, los profesionales de la gestión de riesgos y de los seguros, suelen estar en el equipo de gestión de incidentes cibernéticos, pero, por lo general, están ausentes de los debates acerca de las herramientas y servicios de seguridad cibernética. No existe un líder evidente para la toma de decisiones en torno al seguro cibernético. Además, más de una cuarta parte de los administradores de riesgos y de los profesionales de las finanzas, afirman que no participan en la gestión de los incidentes cibernéticos.

Aunque las respuestas reflejan un deseo generalizado de aumentar el gasto en riesgo cibernético, el lugar exacto en el que deben realizarse las inversiones varía según la función. El motivo por el que la claridad de las funciones y una autoridad evidente para la toma de decisiones son importantes, se debe a que ayuda a las organizaciones a maximizar la eficiencia de esas inversiones

Mejores prácticas

Un enfoque de mejores prácticas para la gestión de riesgos cibernéticos abarca todas las funciones de la organización. Esto incluye invertir y comprometerse con un conjunto amplio, equilibrado y continuamente actualizado de recursos y actividades para mitigar los riesgos cibernéticos, así como reforzar la resiliencia cibernética. Sin embargo, es poco probable que incluso las mejores herramientas y actividades, alcancen su potencial si no existe una comunicación eficaz en toda la empresa.

Entendiendo los riesgos cibernéticos: 8 tendencias clave que hay que conocer en la actualidad

Es importante que los líderes de toda la organización tengan una comprensión común de las tendencias generales de riesgo cibernético y de cómo pueden afectar a sus negocios. Tener un entendimiento común de los problemas de riesgo a los que se enfrenta la empresa, ayuda no solo a alinear a los responsables de la toma de decisiones y a dirigir la estrategia, sino que al mismo tiempo presenta un mensaje unido a otras partes interesadas, ya sean internas o externas.

Como ocurre con cualquier riesgo, las tendencias cibernéticas cambiarán con el tiempo. A continuación, se presentan ocho áreas clave en el entorno cibernético actual.

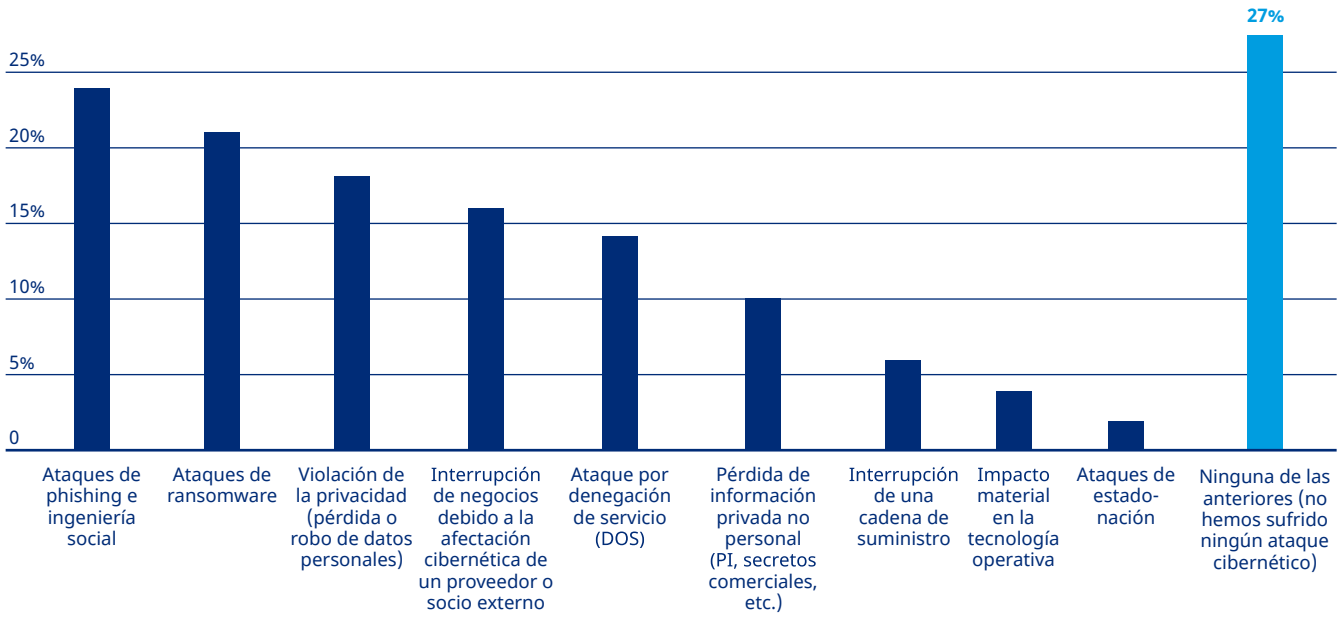
TENDENCIA CLAVE #1

Los objetivos cibernéticos específicos de la empresa deben alinearse con la creación de la resiliencia cibernética, ya que toda organización puede esperar un ataque cibernético.

En torno al riesgo cibernético se desarrolló un tema que vale la pena repetir: ¿qué haría el día de hoy, de manera diferente, si supiera que sufrirá un ingreso cibernético no autorizado? Entre los encuestados, casi tres cuartas partes dijeron que su organización había experimentado uno o más ataques cibernéticos en el último año, siendo los tipos más comunes el phishing/ingeniería social y el ataque cibernético tipo ransomware.

- Las empresas más grandes por ingreso, se enfrentaron a más ataques tanto en número como en variedad, ya que el 85 % afirma haber sido objeto de al menos un ataque, en comparación con 68 % de las organizaciones más pequeñas.
- A nivel regional, los negocios con sede en América Latina fueron las que menos reportaron haber sufrido algún tipo de ataque cibernético, en particular las violaciones a la privacidad. Los que se encontraban en la región del Pacífico tenían significativamente más probabilidades de haber sufrido violaciones a la privacidad que los de otras regiones.

Tipos de ataques cibernéticos sufridos por la organización



Casi

75%

de las organizaciones han sufrido ataques

TENDENCIA CLAVE #2

El ransomware se considera la principal amenaza cibernética a la que se enfrentan las empresas, pero no es la única.

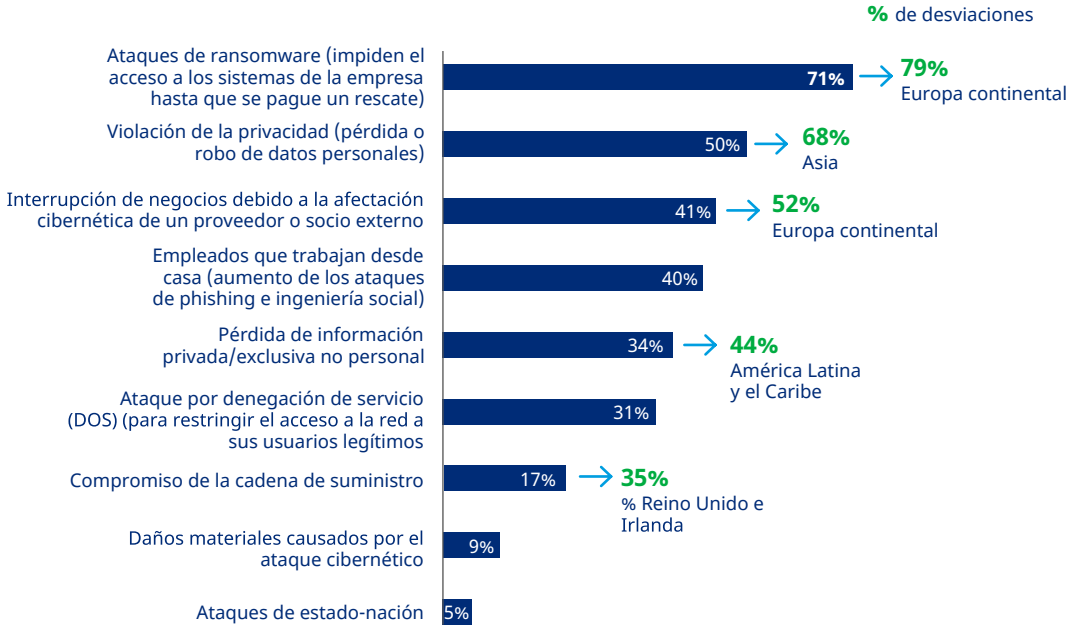
Hoy en día, muchas conversaciones acerca del riesgo cibernético comienzan con un debate sobre la omnipresencia del ransomware. Los encuestados situaron el ransomware en la cima de los riesgos cibernéticos a los que se enfrentan sus organizaciones, con más de un tercio diciendo que es la amenaza número uno, y casi tres cuartas partes lo sitúan entre los tres primeros.

- Las organizaciones consideran que la infinidad de vulnerabilidades, hace que sea casi imposible protegerse contra el ransomware. Esto subraya la importancia de desarrollar una organización con resiliencia cibernética.
- Los profesionales que desempeñan funciones de gestión de riesgos y de seguros son más propensos a señalar al ransomware como el motor clave de los ataques; los líderes de los consejos de administración y los Directores Generales son menos propensos a tener esa opinión.
- Más de la mitad de las empresas norteamericanas afirman que las compañías que pagan las demandas de rescate de los atacantes contribuyen a la creciente incidencia.

Mientras que el ransomware encabezó la lista de amenazas cibernéticas, las violaciones de la privacidad, las interrupciones de los proveedores y el phishing/ingeniería social le siguieron, a nivel mundial. Dejando a un lado el ransomware, las principales preocupaciones difieren según la región, por ejemplo, las organizaciones europeas fueron más propensas a señalar las interrupciones de los proveedores/socios, las organizaciones asiáticas mostraron una mayor preocupación en torno a las violaciones a la privacidad y las organizaciones latinoamericanas citaron con más frecuencia la pérdida de información comercial exclusiva.

El ransomware encabeza la lista de amenazas cibernéticas

Principales amenazas cibernéticas a la organización



TENDENCIA CLAVE #3

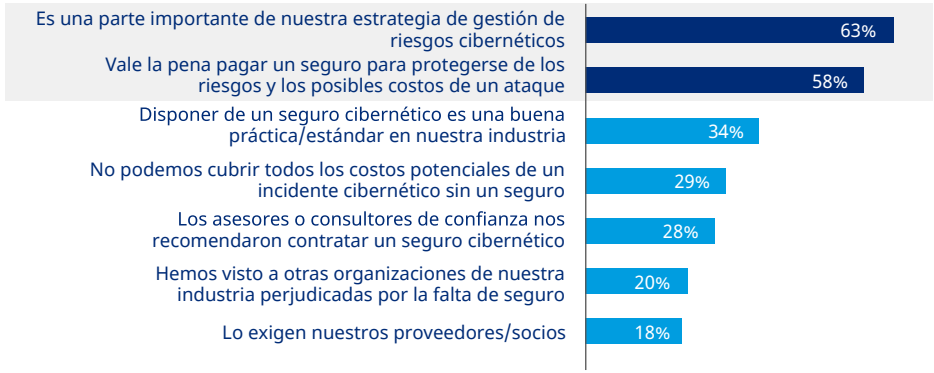
Los seguros son una parte importante de la estrategia de gestión de riesgos cibernéticos e influyen en la adopción de mejores prácticas y controles.

El seguro cibernético ha demostrado su resiliencia desde que se introdujo a finales de la década de 1990. Se ha convertido en un producto que aborda un conjunto de riesgos derivados de la tecnología digital y ha pagado eficazmente los siniestros según lo previsto, lo que ayuda a las empresas a gestionar los riesgos de forma más responsable e integral a medida que innovan y digitalizan sus negocios. También crea un valioso bucle de retroalimentación, ya que las aseguradoras aprenden de los siniestros y cambian la prioridad de sus requisitos de suscripción a aquellos controles que podrían haberlos mitigado.

- Entre los encuestados, 61 % dijo que su organización adquiere algún tipo de cobertura cibernética, casi un aumento del 30 % desde nuestra última encuesta en 2019. El seguro se citó con frecuencia como una parte importante de la estrategia general de riesgo cibernético, como una medida de protección contra los posibles costos de un ataque.
- La adopción de ciertos controles se ha convertido en un requisito mínimo para la mayoría de las aseguradoras, ya que la asegurabilidad potencial de las organizaciones está en juego. Se dice que esto tiene un efecto positivo en las posturas de seguridad cibernética, ya que el 41% de los encuestados afirma que los requisitos de las aseguradoras influyeron en las decisiones de aumentar los controles existentes o adoptar otros nuevos.
- Aunque estos controles se establecieron como mejores prácticas desde hace varios años, algunas organizaciones aún tienen dificultades para adoptarlos, la mayoría de las veces porque no han podido justificar el costo o no entendieron ni vieron la necesidad de dichos controles

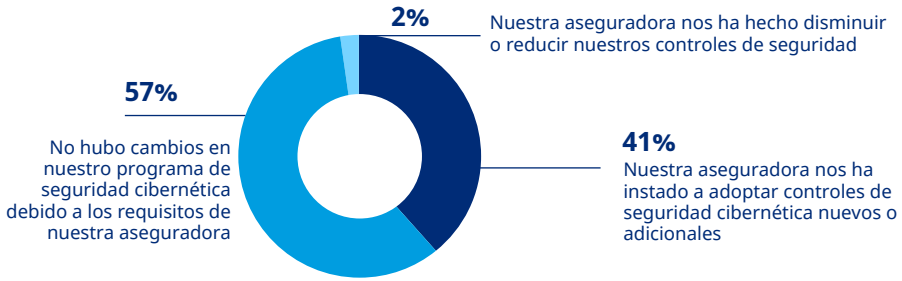
El seguro se considera ampliamente como una parte importante de la estrategia de gestión de riesgos cibernéticos

Motivos para contratar un seguro cibernético



Los requisitos de suscripción del seguro cibernético afectan la adopción de controles

Repercusiones de los requisitos de suscripción de seguros/controles de seguridad cibernética en las decisiones sobre seguridad cibernética



TENDENCIA CLAVE #4

La adopción de más controles de seguridad cibernética resulta en una mayor calificación de higiene cibernética.

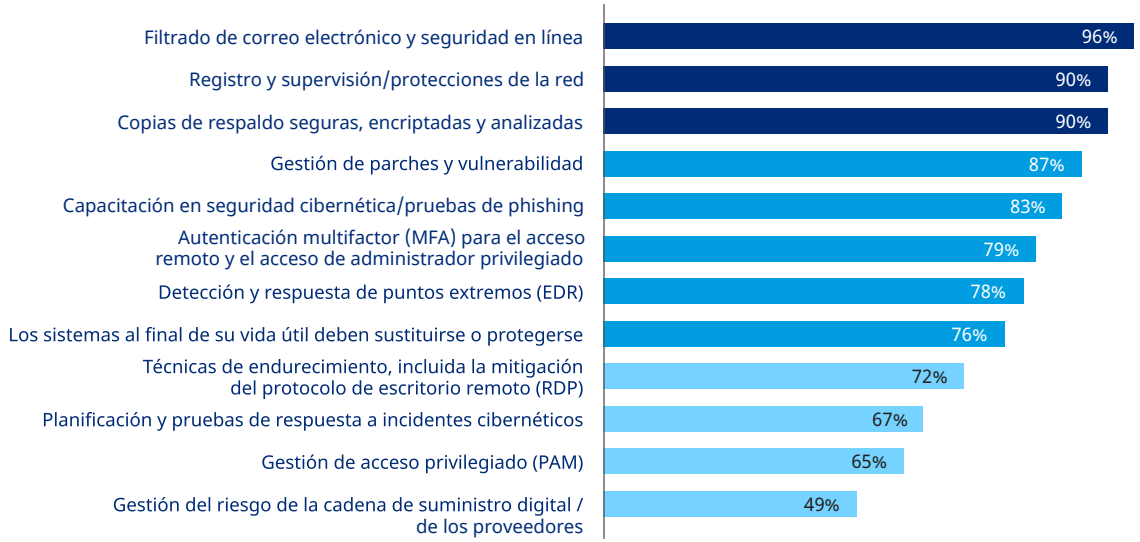
Las organizaciones que buscan abordar estratégicamente el riesgo cibernético y aumentar la higiene cibernética deben considerar la adopción de 12 controles de seguridad cibernética reconocidos por los expertos en seguridad cibernética para ayudar a prevenir, responder, minimizar y recuperarse de un ataque cibernético. Aunque estos controles se establecieron desde hace tiempo, últimamente se ha prestado más atención a ellos. Esto se debe, en parte, al aumento continuo de la frecuencia y gravedad de ataques de ransomware y, en parte, a la capacidad de las aseguradoras para identificar los efectos de determinados controles en los siniestros e incidentes cibernéticos correspondientes.

- Las organizaciones que utilizan todos o la mayoría de los 12 controles de seguridad cibernética fueron casi dos veces más propensas a calificar su higiene cibernética como “muy buena” o “excelente”
- Las empresas más grandes suelen estar por delante de las más pequeñas y tienen más probabilidades de tener casi todos los controles en orden, aunque incluso aquí algunas empresas se enfrentan a deficiencias.
- Es probable que las empresas con seguro cibernético hayan tomado más medidas para reforzar la seguridad y tengan controles más estrictos que las que no lo tienen.

66% **de los encuestados afirma que el trabajo en casa y a distancia encabeza la lista de tecnologías que se consideran propicias para los ataques cibernéticos.**

El filtrado del correo electrónico y la seguridad en línea se encuentran entre una docena de controles de higiene cibernética

Controles de seguridad cibernética utilizados actualmente



Cómo califican los encuestados la “higiene cibernética” general de su organización

40%

Necesita mejorar

34%

Satisfactoria

23%

Muy buena

3%

Excelente

TENDENCIA CLAVE #5

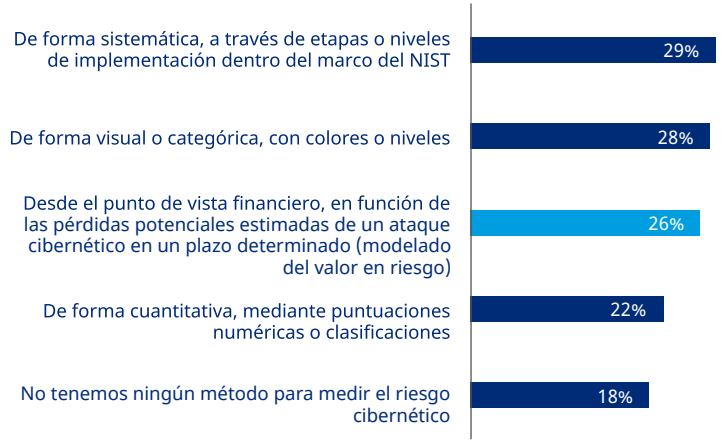
Muchas organizaciones tienen cierto retraso en la medición del riesgo cibernético en términos financieros, lo que perjudica su capacidad para comunicar eficazmente las amenazas cibernéticas a toda la empresa.

Poner los riesgos cibernéticos en términos financieros es fundamental para crear un enfoque de toda la empresa para su gestión. Parte de la resiliencia al riesgo cibernético implica entender cómo los ataques cibernéticos y otros eventos pueden crear volatilidad financiera, tanto a corto como a largo plazo. Sin embargo, la mayoría de los encuestados afirmaron que sus organizaciones no utilizan una medida financiera al evaluar el riesgo cibernético. Lo que nos lleva a preguntas tales como: ¿Cómo pueden saber cuánto riesgo, o qué riesgos, pueden permitirse? ¿Cómo lo reservan?

- Las grandes empresas son significativamente más propensas a utilizar métodos formales para evaluar la exposición al riesgo cibernético.
- A nivel regional, las organizaciones con sede en la región de América Latina y el Caribe son más propensas a utilizar métodos de evaluación cualitativos.
- Entre el 26% que utiliza cálculos de valor en riesgo, la mayoría (90%) utiliza la interrupción de negocios en sus cálculos, mientras que más de la mitad utiliza el robo de datos personales/ violación a la privacidad, posibles demandas de ransomware y los costos de los servicios para ayudar a los clientes tras un ataque.

La medición de la exposición al riesgo cibernético se beneficiaría de la incorporación de un método financiero

Método utilizado para medir la exposición al riesgo cibernético



Factores utilizados en los cálculos financieros

Sólo 26% de los encuestados afirmó que su organización utiliza medidas financieras para medir el riesgo cibernético

TENDENCIA CLAVE #6

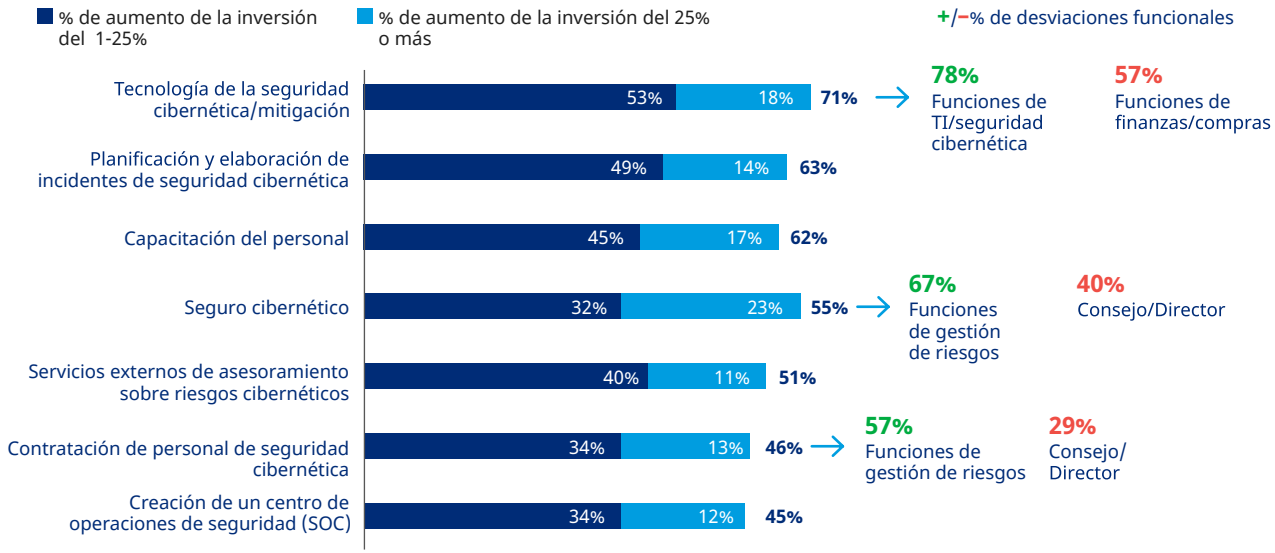
Sigue aumentando la inversión en la mitigación de los riesgos cibernéticos, aunque las prioridades de gasto varían según la empresa.

A nivel mundial, la mayoría de las organizaciones tienen previsto aumentar el gasto en tecnología de seguridad cibernética, planificación de incidentes, capacitación del personal, seguro cibernético y servicios de asesoramiento cibernético el próximo año. Los líderes de riesgos cibernéticos, en general, reconocen la necesidad de invertir en múltiples recursos internos y externos para reforzar la resiliencia cibernética general. Sin embargo, las ideas acerca de hacia dónde deben dirigirse las inversiones suelen variar dentro de una organización según el departamento y el líder de riesgos cibernéticos

- Haber sufrido un incidente cibernético fue el motivo principal citado para tomar la decisión de aumentar las inversiones. Otros motivos principales fueron las recomendaciones de asesores externos y la adopción de nuevas tecnologías / transformación digital.
- Casi una cuarta parte de las organizaciones afirmó que su gasto en el seguro cibernético aumentará un 25% o más en 2022.
- Las funciones de gestión de riesgos / seguros son las que respondieron, con mayor frecuencia, que buscarán dar prioridad a las inversiones en seguros cibernéticos y a la contratación de personal de seguridad cibernética.
- En general, los Directores Generales y los líderes del consejo de administración vieron aumentos en la tecnología/mitigación de la seguridad cibernética, la capacitación del personal, así como la planificación y preparación de incidentes de seguridad cibernética.
- Las organizaciones más grandes fueron más propensas a decir que utilizarán las inversiones para contratar talentos de seguridad cibernética y ampliar las capacidades del centro de operaciones de seguridad (SOC, por sus siglas en inglés).

La tecnología de la seguridad cibernética y mitigación es el área más común para aumentar la inversión

Cambio previsto en las inversiones de riesgos cibernéticos durante los próximos 12 meses



TENDENCIA CLAVE #7

Las nuevas tecnologías deben ser evaluadas y supervisadas de forma continua, no sólo durante la exploración y análisis previos a su adopción.

Mientras que 69% de las empresas encuestadas considera importante evaluar los riesgos de las nuevas tecnologías mientras se encuentran en la etapa de exploración y análisis del desarrollo, 54% afirma que no amplía las evaluaciones de riesgos de las nuevas tecnologías después de su implementación. La evaluación y la supervisión continuas de una nueva tecnología después de la fase de aplicación son necesarias, dado que la digitalización y los avances tecnológicos aumentan la exposición a nuevas y más intensas vulnerabilidades cibernéticas.

- La disminución en la evaluación de los riesgos tras la adopción puede estar relacionada con un problema más amplio en torno a los obstáculos que existen en la implementación de los métodos de evaluación de riesgos cibernéticos. Estos incluyen, la falta de talento, de datos relevantes y de consenso interno.

Obstáculos para la implementación de los métodos de evaluación de riesgos cibernéticos

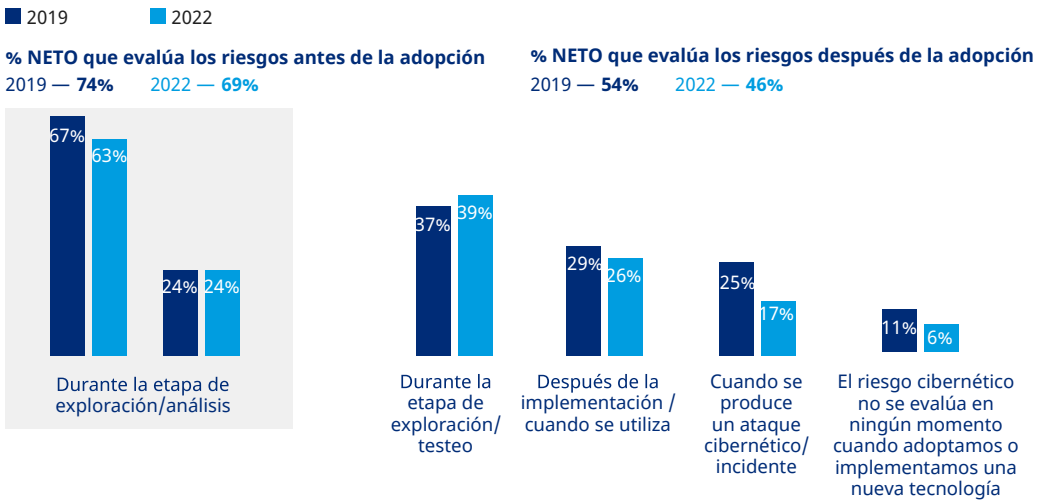
53% **de las organizaciones cree que el mayor obstáculo para la evaluación de los riesgos cibernéticos es la falta de empleados/talento adecuados para hacerlo**

33% **afirma que no tener los datos adecuados es un obstáculo para evaluar las nuevas tecnologías**

- Cuando se preguntó a los encuestados cuáles eran los mayores obstáculos para la evaluación de riesgos cibernéticos en su organización, 53% cree que el mayor obstáculo es no tener los empleados y el talento adecuados para hacerlo, mientras que 33% afirma que tener acceso a los datos adecuados fue un obstáculo.
- También puede haber problemas relacionados con el "traspaso" de una nueva tecnología del equipo de desarrollo a otras partes de la organización. Este es un ejemplo de las ventajas potenciales de enfocar el riesgo cibernético como un esfuerzo de toda la empresa; sería menos probable que aparecieran estas deficiencias si una mentalidad coordinada e interfuncional fuera la norma.

Muchas empresas dejan de evaluar el riesgo cibernético de las nuevas tecnologías en alguna etapa de su adopción

¿Cuándo se evalúa el riesgo cibernético durante la adopción e implementación de la tecnología?



TENDENCIA CLAVE #8

Las empresas adoptan muchas medidas de seguridad cibernética, pero en general pasan por alto a sus proveedores/cadenas de suministro digital.

En el caso de muchas organizaciones, comprender el alcance completo de la relación entre el riesgo cibernético y sus proveedores/vendedores externos puede ser un punto ciego. Sin embargo, es fundamental. Es parte del motivo, por ejemplo, por la que muchas aseguradoras cibernéticas han aumentado sus solicitudes de información, sobre el ecosistema de proveedores, ya que buscan identificar y asegurar las dependencias críticas más allá de los proveedores/vendedores de primer nivel.

- La auditoría y verificación de los proveedores y cadenas de suministro, es el área que menos han abordado las grandes organizaciones, aunque, en general, han sido bastante agresivas a la hora de adoptar medidas de seguridad cibernética.
- Las organizaciones más pequeñas tienen aún menos probabilidades de haber adoptado medidas en torno a las cadenas de suministro.
- Las empresas de servicios financieros van por delante de otros sectores en la realización de evaluaciones de proveedores.
- La mayoría de las empresas están adoptando medidas para mejorar algunas áreas “básicas” como la seguridad de las computadores, dispositivos y sistemas.

Los problemas de los proveedores y la cadena de suministro están rezagados, entre las medidas de seguridad cibernética adoptadas

Medidas de seguridad cibernética adoptadas en los últimos 12 meses

Creando el equipo de riesgos cibernéticos de su empresa

La gestión de riesgos cibernéticos debe ser una responsabilidad compartida en su empresa. Los administradores de riesgos, los directores financieros, los CISO, los líderes ejecutivos y sus equipos deberían debatir los principales riesgos cibernéticos y trabajar juntos para identificarlos, cuantificarlos y gestionarlos.

La realidad suele ser muy diferente, ya que las opiniones sobre los riesgos cibernéticos y los puntos fuertes y débiles de la organización difieren según la función. Esto a menudo resulta en una visión de túnel, en la que las empresas no pueden obtener la visión global necesaria para identificar y responder a los riesgos cibernéticos con la suficiente antelación para mitigarlos.

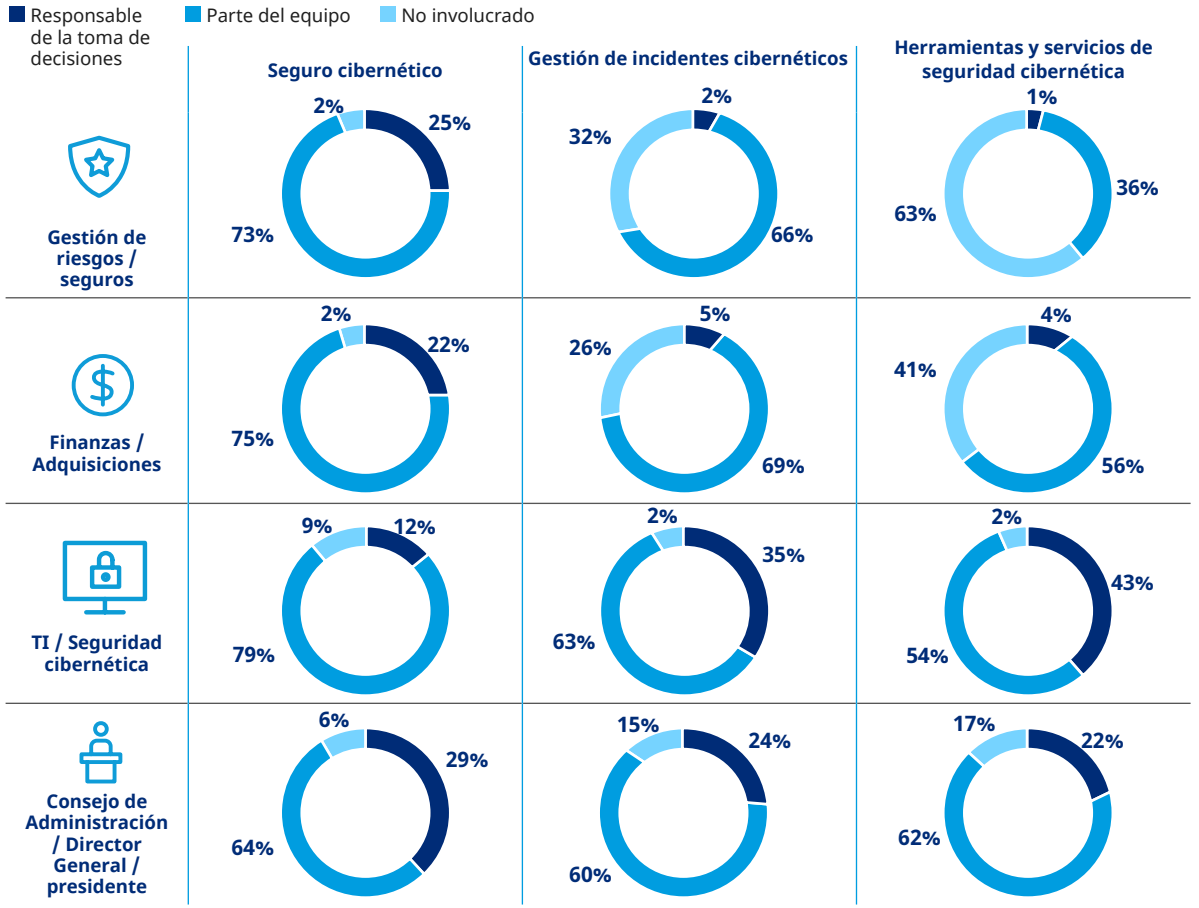
En esta sección, examinaremos la información que puede ayudarle a crear mejores alianzas en la empresa: entre los Directores Generales, los consejos de administración y los presidentes; los administradores de riesgos y los profesionales de los seguros; los departamentos de finanzas; así como las TI y la seguridad cibernética. Lograr sinergias contribuirá a reducir el riesgo, disminuir los costos y aumentar la resiliencia cibernética.

Entender las funciones, las responsabilidades y las perspectivas reforzará la resiliencia al riesgo cibernético

¿Cómo ven los profesionales de una empresa su papel en los seguros cibernéticos, la gestión de incidentes cibernéticos y las herramientas y servicios de seguridad cibernética? ¿Consideran que su función es la de tomar decisiones? ¿Forman parte del equipo general, con aportes a las decisiones? ¿O no están involucrados en absoluto?

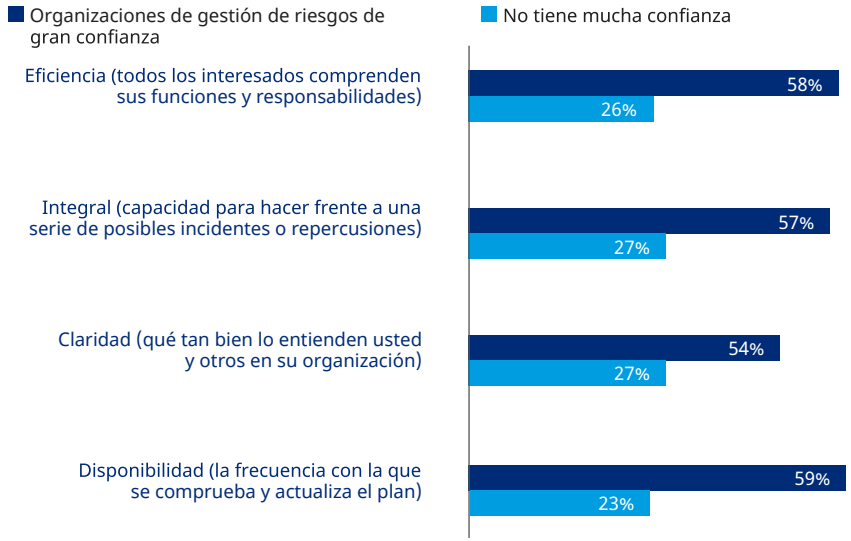
- Los profesionales de la TI/seguridad cibernética fueron los más implicados en general, de conformidad con los encuestados. En más del 90 % de las respuestas, eran quienes tomaban las decisiones o formaban parte del equipo en las tres áreas, y tenían el nivel más bajo, en general, de “no involucrados”. También fueron los más propensos a considerarse a sí mismos como los responsables de la toma de decisiones para la gestión de incidentes cibernéticos y las herramientas y servicios de seguridad cibernética.
- Los encuestados del consejo de administración/Director General/ presidente son los que más se consideran como últimos responsables de la toma de decisiones en materia de seguros cibernéticos, seguidos de cerca por la gestión de riesgos y las finanzas.
- Resulta interesante que 90% de los encuestados que son administradores de riesgos afirmen que existe un plan de respuesta a incidentes cibernéticos, mientras que sólo 60 % de los líderes de nivel ejecutivo lo afirman. Posiblemente, parte de la baja respuesta entre los ejecutivos tenía más que ver con la falta de compromiso con los responsables de la gestión de riesgos cibernéticos que con la falta de un plan real.
- Las decisiones sobre seguros cibernéticos muestran el nivel más alto de encuestados que dicen formar parte del equipo.
- Las herramientas y servicios de seguridad cibernética representan los niveles más bajos de colaboración, entre los profesionales de la empresa en comparación con otras áreas.

El nivel de involucramiento en las áreas cibernéticas varía según la función



El nivel de involucramiento en las áreas cibernéticas varía según la función

Calidad del plan de respuesta a los incidentes cibernéticos
(% que califica cada aspecto como “bueno” o “excelente”)



79%

de las organizaciones cuenta con un plan de respuesta

La confianza en las estrategias de gestión de riesgos cibernéticos es relativamente baja

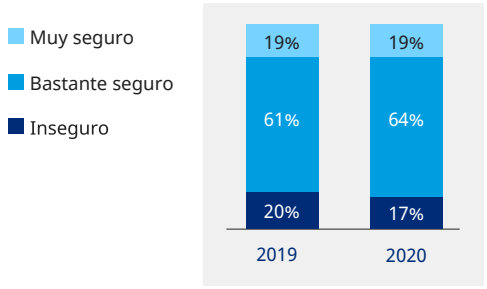
La confianza en la capacidad de la propia organización para evaluar, medir, mitigar y responder a las amenazas cibernéticas sigue siendo baja, sin que se observen cambios sustanciales en las respuestas de las encuestas recogidas en la Encuesta Cibernética de Marsh y Microsoft 2019 [hipervínculo]: solo el 19 % de los encuestados indicó que tienen gran confianza en su gestión de riesgos cibernéticos tanto en 2019 como en 2022.

En general, los líderes ejecutivos expresaron el menor nivel de confianza en estas áreas en comparación con los líderes de departamentos. Por ejemplo, en lo que respecta a la capacidad de la organización para gestionar y responder a los ataques cibernéticos, sólo 9% de los líderes ejecutivos dijo tener mucha confianza, en comparación con 19% de los líderes departamentales. Estas percepciones diferentes podrían afectar donde se implementan finalmente los recursos como parte de una estrategia de riesgo cibernético.

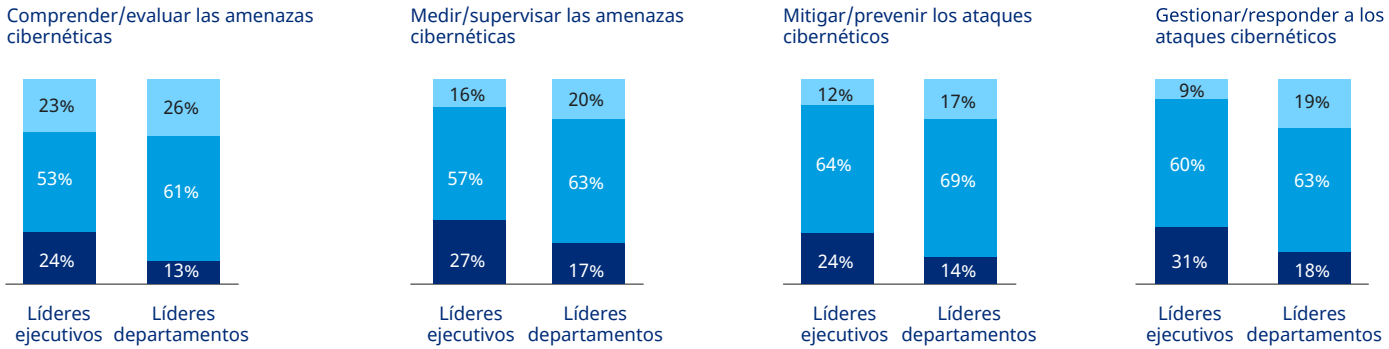
- Tanto los líderes ejecutivos como los líderes departamentales mostraron los niveles de confianza más altos en cuanto a la capacidad de las organizaciones para comprender y evaluar las amenazas cibernéticas. Esto refleja la creciente exposición a la información acerca del riesgo cibernético que experimentan la mayoría de las áreas de la sociedad.
- La mayor brecha en la percepción también estaba relacionada con la capacidad de gestionar y responder a los ataques cibernéticos, ya que casi un tercio de los líderes ejecutivos dijo no estar seguro, en comparación con el 18% de los líderes departamentales. Una comunicación interempresarial más eficaz tiene el potencial de subsanar esas deficiencias. A medida que la información se comparte entre las funciones, puede haber una mejor alineación en torno a las capacidades de la organización, y dónde hacer las inversiones.

Los líderes ejecutivos son los más propensos a no confiar en los programas de gestión de riesgos cibernéticos

Confianza general en la gestión de riesgos cibernéticos



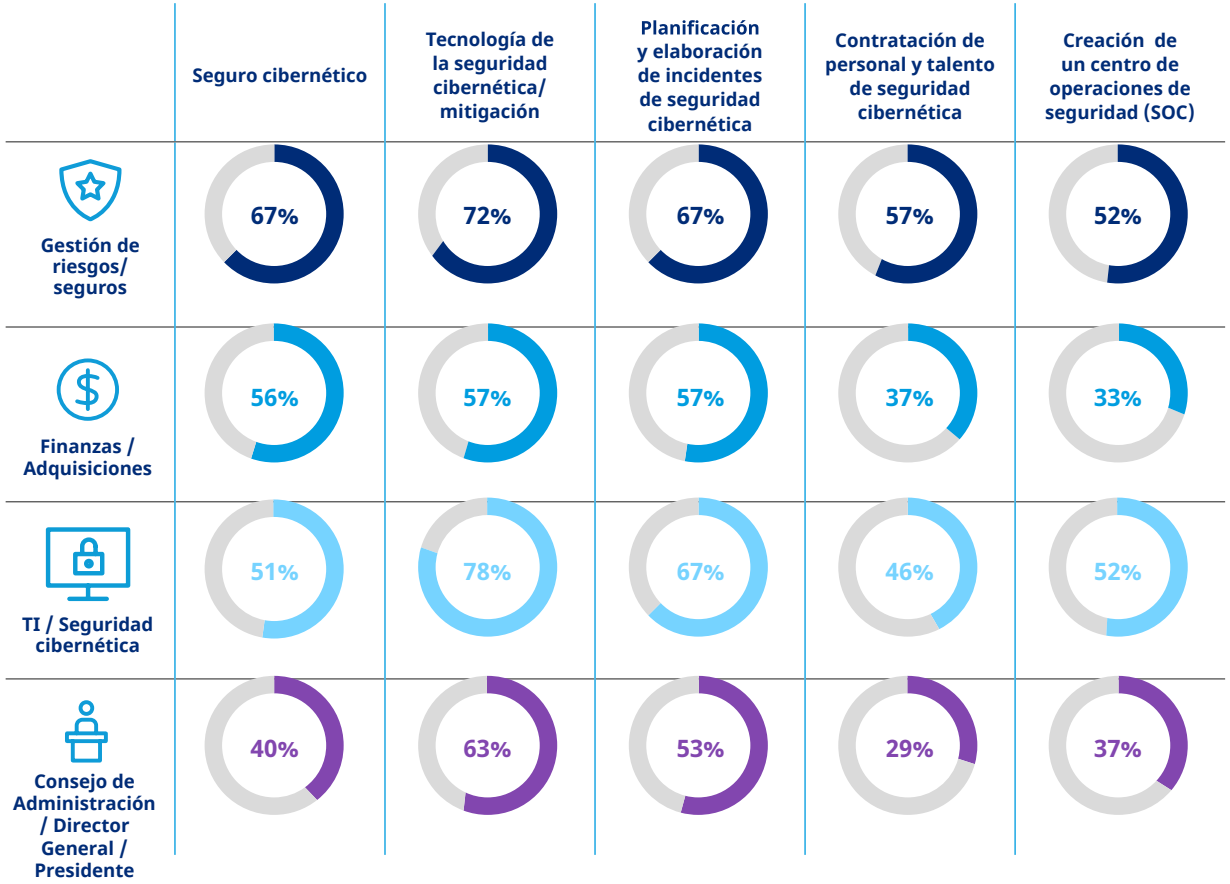
Confianza en la capacidad de la organización para...



Amplio consenso entre las funciones que las inversiones cibernéticas aumentarán en 2022

¿Cómo espera que evolucionen las inversiones de su organización en los próximos 12 meses?

% de cualquier aumento



A medida que aumentan las inversiones cibernéticas, se necesita una estrategia para toda la empresa.

Hubo un amplio consenso entre las funciones de la organización sobre la necesidad de aumentar las inversiones en recursos y capacidades de gestión de riesgos cibernéticos, en comparación con el 2019. Muy pocos encuestados esperan que las inversiones disminuyan, y más de la mitad dijeron que es probable un cierto nivel de aumento en la mayoría de las áreas. Como la mayoría de las decisiones presupuestarias, decidir dónde invertir puede ser una cuestión complicada y un proceso largo. Es probable que las organizaciones que comparten sus conocimientos sobre los riesgos cibernéticos en toda la empresa encuentren la tarea más eficaz y eficiente.

- Es de esperar que los líderes de los riesgos cibernéticos en diferentes funciones y departamentos tengan planes y prioridades variados para las inversiones futuras. Los encuestados de TI y seguridad cibernética fueron más propensos a planificar un mayor gasto en tecnología de seguridad cibernética; aquellos de finanzas y compras, los menos.
- Los líderes de gestión de riesgos y de seguros fueron más propensos a prever un mayor gasto en un seguro cibernético y en la contratación de más profesionales de la seguridad cibernética; los del Consejo de Administración y los Directores Generales fueron significativamente menos propensos. Por ejemplo, el 35 % de los líderes de la gestión de riesgos esperan ver aumentos del 25% o más en el gasto en seguros; sólo el 9% de los líderes ejecutivos esperan ese nivel de aumento.
- La falta de personal/talento pertinente se consideró uno de los principales obstáculos que impiden a las empresas aplicar métodos de evaluación de riesgos más formales y rigurosos. Al mismo tiempo, los líderes ejecutivos fueron los menos propensos a prever un aumento de la contratación de talento en seguridad cibernética; sólo el 29% espera algún incremento en esta área, en comparación con el 57% de los administradores de riesgos y el 46% de los líderes de seguridad cibernética y TI que lo esperan. ¿Esto representa una falta de comunicación entre las distintas funciones y los líderes? Si lo hace, esta es otra área que se beneficiaría de un enfoque de toda la empresa para la gestión de riesgos cibernéticos.

Mejores prácticas para crear una gestión de riesgos cibernéticos en toda la empresa

Un enfoque de mejores prácticas para la gestión de riesgos cibernéticos se basa en el compromiso de toda la empresa para compartir la responsabilidad. Esto incluye invertir y comprometerse con un conjunto amplio, equilibrado y continuamente actualizado de recursos y actividades para mitigar los riesgos cibernéticos y reforzar la resiliencia cibernética.

Estos elementos incluyen, de manera enunciativa mas no limitativa, la tecnología de seguridad cibernética y la adquisición de talento, la capacitación de respuesta a incidentes, los análisis de penetración, las evaluaciones de riesgo del proveedor/la cadena de suministro, el seguro cibernético y los servicios de consultoría en riesgos cibernéticos.

En esta sección, examinamos las ocho tendencias identificadas anteriormente, centrándonos en lo que significa para los líderes de riesgos cibernéticos, desarrollar un enfoque interinstitucional para cada una de ellas.

TENDENCIA CLAVE #1

Los objetivos cibernéticos específicos de la empresa deben alinearse con la creación de la resiliencia cibernética, ya que toda organización puede tener un ataque cibernético.

Líderes ejecutivos y de departamentos

- Se comprometen a una comunicación continua e interfuncional en relación con las amenazas de riesgos cibernéticos, la preparación y la estrategia.
- Participan en la planificación de la gestión de riesgos cibernéticos, incluyendo el ejercicio regular de los planes.
- Participan en las revisiones posteriores a los incidentes

TENDENCIA CLAVE #2

El ransomware es la principal amenaza cibernética a la que se enfrentan las empresas, pero no es la única.

Líderes ejecutivos

(Consejo de Administración/ Director General/Presidente)

- Reciben actualizaciones periódicas de las amenazas para reforzar la comprensión de dichos riesgos como el ransomware-como-servicio.
- Hacen preguntas y ofrecen orientación acerca de los vínculos entre el riesgo cibernético y la estrategia de crecimiento de la organización.
- Aprueban una estrategia de respuesta que incluye escenarios en los que se pagará o no el rescate.
- Participan en las pruebas anuales del plan de respuesta a incidentes cibernéticos.

Líderes de departamento

(gestión de riesgos/seguros, finanzas/adquisiciones, TI/seguridad cibernética)

- Supervisan, revisan y comparten periódicamente las actualizaciones de las evaluaciones de amenazas internas y externas de la organización.
- Conservan un plan de respuesta a incidentes cibernéticos que se revisa y analiza anualmente.
- Participan en ejercicios de capacitación para ayudar a todas las partes interesadas a comprender las funciones y responsabilidades de cada una y cómo actuar en caso de incidente.

TENDENCIA CLAVE #3

Los seguros son una parte importante de la estrategia de gestión de riesgos cibernéticos e influyen en la adopción de mejores prácticas y controles

Líderes ejecutivos (Consejo de Administración/ Director General/Presidentes)

- Involucran a los líderes departamentales en los debates relativos a cómo la financiación de riesgos cibernéticos encaja en la estrategia de crecimiento corporativo.
- Toman decisiones sobre la asignación del presupuesto.

Líderes de departamento (gestión de riesgos/seguros, finanzas/adquisiciones, TI/seguridad cibernética)

- Recurren a la ayuda del departamento de finanzas, así como de gestión de riesgos para cuantificar los riesgos cibernéticos en términos financieros y establecen métricas relativas a la tolerancia al riesgo corporativo.
- Evalúan las necesidades de financiación de riesgos de toda la empresa.
- Adquieren una amplia cobertura de seguro cibernético, como responsabilidad por errores y omisiones tecnológicas, defensa y sanciones regulatorias, daños físicos a los activos operativos, de seguridad de la red y otros, según las necesidades.
- Consideran la posibilidad de una financiación de riesgos alternativa, como las cautivas y la cobertura paramétrica.
- La gestión de riesgos/seguros adopta la iniciativa en las comunicaciones con las aseguradoras y comparte las opiniones/ solicitudes de las aseguradoras con respecto a la seguridad cibernética/TI, las finanzas, los líderes ejecutivos y otros.
- Los administradores de riesgos deberían considerar la posibilidad de implicar a su CISO (o equivalente) en los debates con las aseguradoras.

TENDENCIA CLAVE #4

La adopción de mayores controles de seguridad cibernética, resulta en una mayor calificación de higiene cibernética.

Líderes ejecutivos (Consejo de Administración/ Director General/Presidentes)

- Adoptan una estrategia organizacional que incluya una mentalidad de gestión de riesgos cibernéticos que incluya el desarrollo y el mantenimiento de la higiene cibernética entre todos los usuarios de tecnología de la organización.

Líderes de departamento (gestión de riesgos/seguros, finanzas/adquisiciones, TI/seguridad cibernética)

- Adoptan una mentalidad de gestión de riesgos que aproveche las sinergias entre las herramientas y tácticas de gestión de riesgos cibernéticos y refuerce un fuerte nivel de higiene cibernética diaria entre todos los usuarios de tecnología de la organización.
- La seguridad cibernética/TI lidera la implementación de una combinación amplia y equilibrada de tácticas y controles de tecnología de seguridad cibernética, incluidos el filtrado del correo electrónico y la seguridad de la web, la detección y la respuesta de los puntos extremos, las técnicas de endurecimiento, incluida la mitigación del protocolo de escritorio remoto, y la gestión de acceso privilegiado.
- La gestión de riesgos transmite a TI las perspectivas/requisitos de las aseguradoras.

TENDENCIA CLAVE #5

Las organizaciones tienen cierto retraso en la medición del riesgo cibernético en términos financieros, lo que perjudica su capacidad para comunicar eficazmente las amenazas cibernéticas en toda la empresa.

Líderes ejecutivos (Consejo de Administración/ Director General/Presidentes)

- Solicitan información que ponga los costos potenciales del riesgo cibernético en términos financieros.
- Solicitan actualizaciones periódicas con respecto al apetito y la tolerancia al riesgo cibernético.
- Incorporan esas medidas al establecimiento de las prioridades de la estrategia comercial.

Líderes de departamento (gestión de riesgos/seguros, finanzas/adquisiciones, TI/seguridad cibernética)

- Utilizan enfoques cuantitativos para evaluar y comprender las exposiciones a los riesgos cibernéticos.
- El departamento de finanzas toma la iniciativa, solicita información a otras áreas (operaciones, I+D, etc.) para ayudar a determinar la tolerancia al riesgo.

TENDENCIA CLAVE #6

Sigue aumentando la inversión en la mitigación de los riesgos cibernéticos, aunque las prioridades de gasto varían según la empresa.

Líderes ejecutivos

(Consejo de Administración/ Director General/Presidentes)

- Sintetizan las aportaciones de toda la empresa, hacen preguntas, asignan el presupuesto.

Líderes de departamento

(gestión de riesgos/seguros, finanzas/adquisiciones, TI/seguridad cibernética)

- Todas las áreas aportan información a los líderes de finanzas y ejecutivos con respecto a las prioridades de inversión.
- Los profesionales de la gestión de riesgos/seguros aportan información acerca de las prioridades de inversión, basándose en parte en los requisitos/opiniones de las aseguradoras cibernéticas.

TENDENCIA CLAVE #7

Las nuevas tecnologías deben ser evaluadas y supervisadas de forma continua, no sólo durante la exploración y análisis previos a su adopción.

Líderes ejecutivos

(Consejo de Administración/ Director General/Presidentes)

- Responsabilizan a los departamentos para que no existan deficiencias en la supervisión.

Líderes departamentales

(gestión de riesgos/seguros, finanzas/compras, TI/seguridad cibernética)

- Al evaluar las nuevas tecnologías, los líderes de tecnología deben trabajar con los líderes de riesgos cibernéticos en finanzas y compras, y potencialmente contratar a socios externos, como aseguradoras y servicios de asesoramiento acerca de riesgos cibernéticos.
- Evalúan los riesgos que plantean las nuevas tecnologías comerciales antes y después de su aplicación.
- La gestión de riesgos y la seguridad cibernética/TI trabajan conjuntamente para lograr una transición fluida de la I+D a las operaciones, en la forma de como se implementa y supervisa el riesgo cibernético.

TENDENCIA CLAVE #8

Las empresas adoptan muchas medidas de seguridad cibernética, pero en general pasan por alto a sus proveedores/cadenas de suministro digital.

Líderes ejecutivos

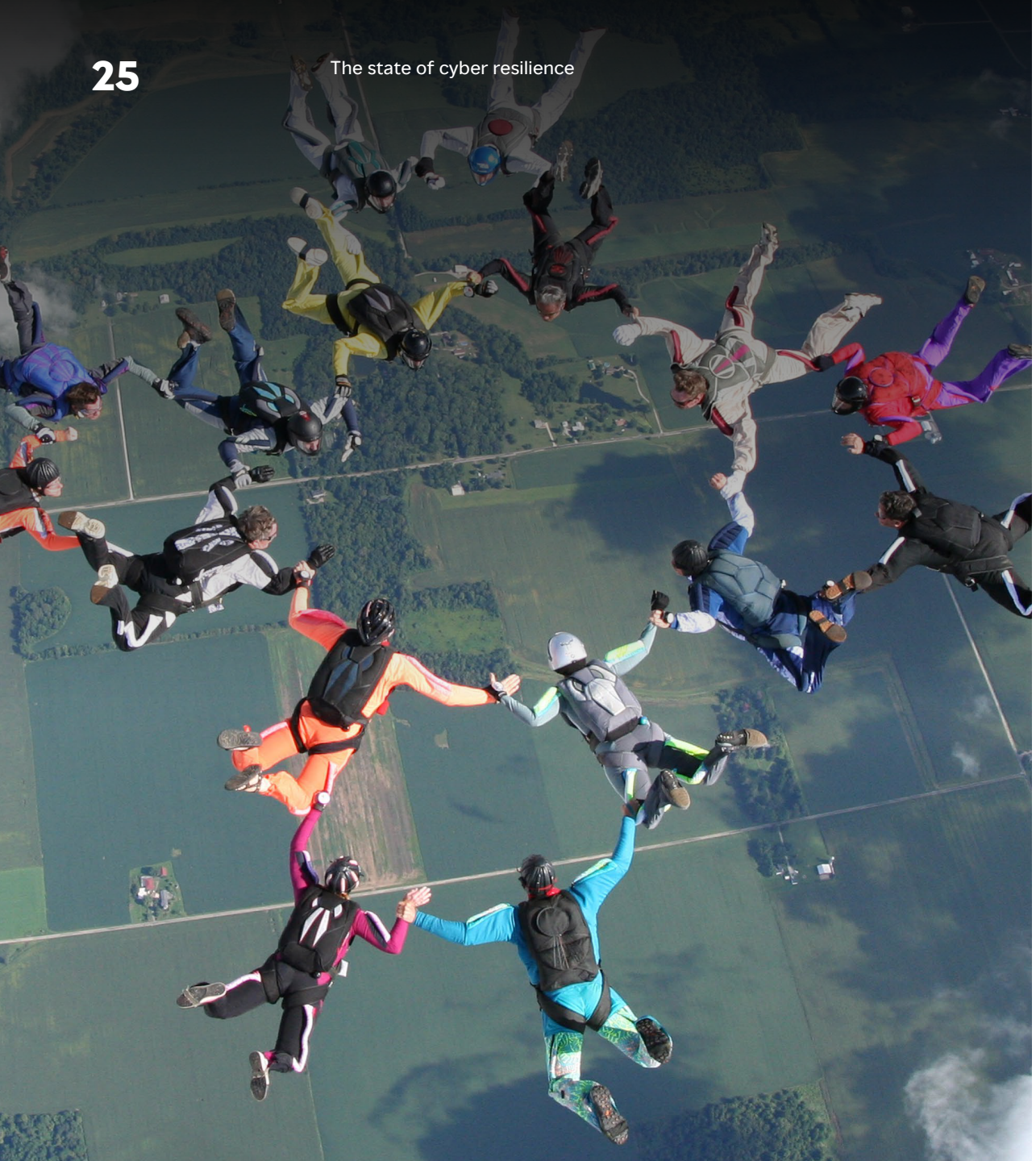
(Consejo de Administración/ Director General/Presidentes)

- Investigan minuciosamente a los proveedores y vendedores de terceros desde la perspectiva del riesgo cibernético.

Líderes de departamento

(gestión de riesgos/seguros, finanzas/adquisiciones, TI/seguridad cibernética)

- Evalúan a los proveedores y socios de la cadena de suministro, incluyendo auditorías de los controles y protocolos de seguridad cibernética.
- Los contratos con vendedores y proveedores contienen disposiciones relacionadas con la postura de seguridad cibernética.
- Colaboran con los departamentos jurídicos, de operaciones, de compras y otros, según proceda, para auditar y verificar las medidas técnicas y operativas de los proveedores.



Compartir la responsabilidad fomenta la confianza en la resiliencia cibernética

Hoy en día, no existe una solución única para los riesgos cibernéticos a los que se enfrentan las organizaciones. Las medidas de seguridad cibernética, los seguros, los datos y los análisis, y los planes de respuesta a incidentes desempeñan un papel importante. Sin embargo, un elemento crítico para hacer que estas y otras piezas funcionen en conjunto es desarrollar una armonización de toda la empresa en torno a la gestión de riesgos cibernéticos, fomentando una responsabilidad compartida.

Todas las partes interesadas, incluidos los administradores de riesgos, el departamento de finanzas, la seguridad cibernética/TI y la dirección ejecutiva, probablemente ganarán confianza en la postura de seguridad cibernética de la organización, al estar mejor conectados con la empresa en general.

Metodología

La investigación consistió en una encuesta global en línea de n=662 responsables de la toma de decisiones sobre riesgos cibernéticos.

Las encuestas se administraron en 16 idiomas y se recolectaron respuestas de 56 países.

El trabajo de campo de la encuesta se realizó a lo largo de noviembre y diciembre de 2021.

Todos los encuestados proceden de la base de datos de Marsh y de la divulgación en línea de 7DOTS.

Sobre Microsoft

Microsoft (Nasdaq “MSFT” @microsoft) facilita la transformación digital para la era de la nube y un entorno inteligentes. Su misión es empoderar a cada persona y organización en el planeta para que puedan lograr más.

Sobre Marsh

Marsh es el corredor de seguros y asesor de riesgos líder en el mundo. Con alrededor de 45,000 colegas que operan en 130 países, Marsh atiende a clientes comerciales y particulares con soluciones de riesgo basadas en datos y servicios de asesoramiento. Marsh es un negocio de Marsh McLennan (NYSE: MMC), la principal empresa de servicios profesionales del mundo en las áreas de riesgo, estrategia y personas. Con un ingreso anual de casi USD 20,000 millones, Marsh McLennan ayuda a sus clientes a desenvolverse en un entorno cada vez más dinámico y complejo a través de cuatro negocios líderes en el mercado: Marsh, Guy Carpenter, Mercer y Oliver Wyman. Para obtener información adicional, visite marsh.com, síganos en LinkedIn y Twitter o suscríbase a BRINK.

1166 Avenue of the Americas, New York 10036