Informe del estudio internacional sobre seguridad

La ciberseguridad en la encrucijada

Por qué las empresas se enfrentan a un dilema en torno a la ciberseguridad y qué pueden hacer para resolverlo

fastly

Índice

Resumen ejecutivo

Los incidentes de ciberseguridad siguieron aumentando el año pasado. Se robaron datos de llamadas de casi todos los clientes de AT&T.[1] Un ataque a UnitedHealth dejó expuestos los datos personales de salud de «una parte considerable de la población de Estados Unidos».[2] Se dice que el grupo chino Salt Typhoon hackeó redes de telecomunicaciones estadounidenses con el objetivo de perjudicar a Donald Trump y su entorno.[3] El mundo fue testigo del que posiblemente haya sido el mayor incidente de ciberseguridad hasta la fecha, cuando una actualización mal configurada de CrowdStrike dejó sin servicio a millones de ordenadores con Windows.

Ante este panorama, la ciberseguridad y la resiliencia digital son más importantes que nunca, pero los programas de seguridad terminan 2024 en una posición muy precaria. Las adversidades a las que se enfrentan las iniciativas de ciberseguridad son mayores que el año pasado. Muchas de ellas no son de carácter técnico, sino que están relacionadas con el ajuste de los presupuestos y la confusión en torno a quién se responsabiliza de la ciberseguridad en las organizaciones.

La ciberseguridad está en una encrucijada. Para entender mejor qué están haciendo las empresas para gestionar los problemas de ciberseguridad y qué rumbo está siguiendo el sector, en septiembre de 2024, Fastly colaboró con Sapio, una agencia de estudios de mercado sobre empresas y consumidores, para encuestar a 1800 responsables de IT con influencia en la ciberseguridad. El resultado es un informe con información muy valiosa sobre las dificultades que plantea la ciberseguridad y sus planes para salir adelante. Estos son algunos de los principales hallazgos:

- **Las iniciativas de seguridad pasan por un momento de incertidumbre.** Aunque muchas personas (87 %) esperan que el gasto en ciberseguridad aumente el año que viene, los resultados de este incremento se mirarán con lupa. A los equipos de seguridad les costará convencer a los cargos directivos de que hace falta ese presupuesto extra. Esto se debe a que estos cargos tienen otras prioridades, sobre todo en los campos de la transformación digital y la modernización de IT, y creen que las iniciativas de ciberseguridad pueden frenarlas.
- **La escalabilidad de las operaciones de ciberseguridad plantea obstáculos a las organizaciones.** No es fácil justificarlas ante la junta directiva, y las ineficiencias en materia de ciberseguridad resultan preocupantes. Casi un tercio de las personas encuestadas no tienen claro cómo asignar los recursos de ciberseguridad y creen que se está invirtiendo en exceso.
- **El mercado no proporciona los profesionales que las empresas necesitan.** También hay indicios que apuntan a la incapacidad para llevar más allá las iniciativas de ciberseguridad a medida que aumenta el nivel de exigencia en cuanto a capacidad y complejidad. Hasta ahora, las empresas invertían en ampliar el personal para seguir el ritmo a las necesidades de ciberseguridad, pero este año hay una considerable falta de satisfacción con los profesionales disponibles. Esto requiere poner al día las prácticas relativas a la gestión de las habilidades para satisfacer las nuevas necesidades en términos de ciberseguridad.
- **La complejidad tecnológica pone trabas a las iniciativas de ciberseguridad.** Las tecnologías que usan las organizaciones para plantar cara a las ciberamenazas suponen un problema cuando estas quieren ampliar sus iniciativas de ciberseguridad. Además, siguen haciendo uso de herramientas complejas y con funciones similares que dificultan la respuesta ante incidentes y otras operaciones de ciberseguridad. El incidente de CrowdStrike de 2024 ha puesto en entredicho los productos y los servicios de seguridad, y los responsables de ciberseguridad están empezando a analizar las ventajas y los riesgos de sus herramientas.

---

1 Whittaker, Zack. «AT&T says criminals stole phone records of 'nearly all' customers in new data breach | TechCrunch». TechCrunch, 12 de julio de 2024, techcrunch.com/2024/07/12/att-phone-records-stolen-data-breach.

2 UnitedHealth Group. «UnitedHealth Group Updates on Change Healthcare Cyberattack». UnitedHealth Group, 22 de abril de 2024, www.unitedhealthgroup.com/newsroom/2024/2024-04-22-uhg-updates-on-change-healthcare-cyberattack.html.

3 Barrett, Devlin. «What to Know About the Chinese Hackers Who Targeted the 2024 Campaigns». N.Y. Times, 26 de octubre de 2024, www.nytimes.com/2024/10/26/us/politics/salt-typhoon-hack-what-we-know.html.

La realidad no se ajusta a las expectativas en lo relativo a la recuperación de incidentes de ciberseguridad

El año 2024 ha marcado un antes y un después para los incidentes de ciberseguridad. El de CrowdStrike, que dejó inutilizados aproximadamente 8,5 millones de sistemas con Windows en todo el mundo,[4] provocó interrupciones en empresas de distintos sectores, desde las finanzas hasta el transporte aéreo, pasando por la fabricación. Tarde o temprano volverá a ocurrir algo así. La pregunta es hasta qué punto estaremos preparados cuando llegue el momento.

A las organizaciones no se les da tan bien recuperarse de los incidentes de ciberseguridad como creen. De media, esperan tardar 5,85 meses en recuperarse. Sin embargo, tardan 7,34 meses, aproximadamente un 25 % más.

Cuanto menor es la inversión en ciberseguridad, mayor es el tiempo de recuperación. Las empresas que pretenden gastar menos durante el próximo año esperan que su recuperación tarde más de 8 meses, pero esto tampoco se ajusta a la realidad: cuando una empresa invierte menos en ciberseguridad, tarda casi 11 meses en recuperarse o, lo que es lo mismo, un tercio más de lo que prevé. Las empresas que se preocupan de invertir en ciberseguridad se recuperan más rápido de los incidentes en comparación con aquellas que recortan el gasto.

La prevención encabeza la lista de medidas de recuperación

Cuando se produce un incidente de ciberseguridad, se suelen tomar dos medidas: poner en marcha mecanismos de seguridad más estrictos (43 %) y dar más formación a los empleados (41 %). Ambas son el resultado de lecciones aprendidas para evitar futuros incidentes. Las personas encuestadas también dan más prioridad a los parches de software. Es más, el 86 % de ellas van a cambiar sus estrategias de pruebas y despliegue de parches tras el incidente de CrowdStrike.

Un menor número mencionan actividades concretas, como la restauración desde copias de seguridad (38 %) y la comunicación con las partes interesadas (34 %), para facilitar la recuperación tras un incidente. Y el análisis forense, algo útil a la hora de emprender acciones legales contra intrusos y atacantes externos o informar a los organismos reguladores, goza de menos popularidad con un 25 %. Una buena noticia es que el 32 % van a destinar más presupuesto a manuales y herramientas de apoyo para la respuesta ante incidentes.*(Figura 1)*

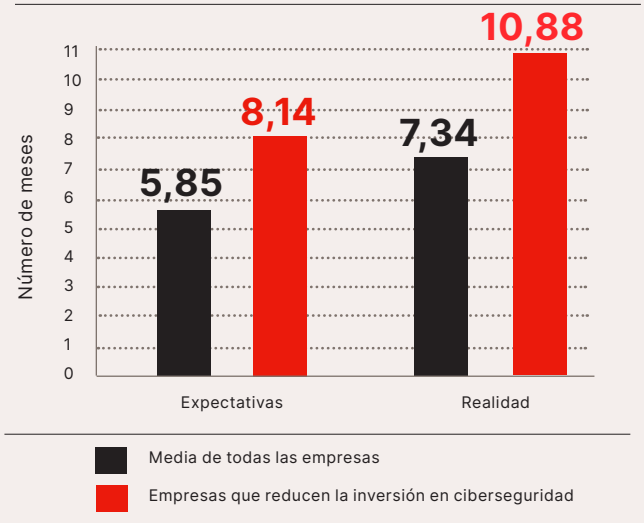
Las empresas dan prioridad a sus equipos internos. El 61 % confían en sus equipos de IT y el 39 % acuden a agencias de ciberseguridad externas para recuperarse. Por su parte, menos de un tercio de las personas encuestadas dicen hacer uso de seguros para cubrir los costes. Los datos del mercado indican que será más difícil conseguir ciberseguros, puesto que el coste medio de una fuga de datos se ha disparado hasta la cifra récord de 4,88 millones de USD.[5]

Las organizaciones también desconfían de los partners externos que contribuyen a estos incidentes de ciberseguridad. El 29 % estudiarían cambiar de proveedor de ciberseguridad debido a problemas relacionados con la calidad del software e incidentes de seguridad a gran escala, como el que se produjo el verano pasado. Casi la mitad (48 %) se están replanteando el uso que hacen de sus herramientas de ciberseguridad.

Lo que está claro es que cada vez se le da más importancia a la prevención; al fin y al cabo, la ciberseguridad debe ser proactiva. No obstante, responder de una manera oportuna y coordinada a los incidentes sigue siendo fundamental en caso de que un ataque supere las defensas.

Figura 1

Tiempo de recuperación tras un incidente de ciberseguridad



4 Weston, David. «Helping our customers through the CrowdStrike outage». Microsoft, 20 de julio de 2024, https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/

5 «Cost of a data breach 2024 | IBM». 4 de noviembre de 2024, www.ibm.com/reports/data-breach.

¿Cuánto confían las organizaciones en sus infraestructuras de seguridad y cuánto deberían hacerlo?

Casi ninguna empresa se libra de los incidentes de ciberseguridad. Las empresas sufrieron una media de 40 incidentes de ciberseguridad conocidos a lo largo del año pasado, y menos del 10 % tuvieron la suerte de no experimentar ninguno. Las organizaciones de Estados Unidos estuvieron a la cabeza, con una media de un incidente por semana. Y las organizaciones de gran envergadura se llevaron la peor parte, con una media de 64 incidentes al año, lo cual se debe a su mayor superficie de ataque.

Hasta los errores más insignificantes pueden traducirse en amenazas. Los activos de TI mal configurados han causado problemas al 25 % de las personas encuestadas. Otros problemas incluyen los errores de software (33 %). Sin embargo, los parches y otros cambios de TI para detener las amenazas no son lo suficiente rápidos y dan problemas al 18 % de las empresas. El DevOps seguro (SecDevOps) puede ayudar a prevenir los errores y agilizar los cambios de TI con la finalidad de poner fin a las vulnerabilidades.

Destaca especialmente el antagonismo entre los procesos manuales y la automatización. Los procesos manuales intervienen en el 24 % de los incidentes. Muchas empresas siguen dependiendo de que sus empleados sigan los procesos y las políticas de seguridad en lugar de integrar la seguridad en sus soluciones tecnológicas. Esto ha causado problemas al 16 % de las personas encuestadas.

Los incidentes de ciberseguridad hacen estragos

Los incidentes de ciberseguridad han causado pérdidas de ingresos a casi un cuarto (23 %) de las personas encuestadas, cuyas empresas perdieron una media del 3 % tras cada incidente en 2024. Los periodos de inactividad también están entre las consecuencias más graves, como demuestran los últimos incidentes, seguidos de las pérdidas de datos.

Las multas impuestas y las acciones legales emprendidas por los organismos reguladores también están entre los riesgos que entrañan los incidentes de ciberseguridad. El incumplimiento normativo ha sido problemático para el 17 % de las personas encuestadas, y en el 19 % de los casos se han puesto en riesgo cuentas de clientes, con el posible incumplimiento de leyes en materia de privacidad.

Los daños de imagen son otro factor importante que afecta al 22 % de las empresas. El 18 % y el 19 % de las mismas han visto cómo se reducían la confianza y la satisfacción de los clientes, respectivamente. Esto también pasa factura a la retención de los clientes, que se ha reducido para el 14 % de las empresas tras un incidente.

Se avecina otro año lleno de amenazas

Las ciberamenazas son cada vez más preocupantes. La perspectiva de que aumenten los ataques automatizados quita el sueño al 42 % de las personas encuestadas. A muchas les preocupa que sus tecnologías de ciberseguridad se estén quedando obsoletas: un 29 % se lamentan de que sus defensas no estén automatizadas y un cuarto mencionan la lentitud en la gestión de cambios como algo negativo. Con un 21 %, la automatización de la ciberseguridad es la segunda mayor prioridad durante los próximos doce meses para las personas encuestadas.

Las preocupaciones en torno a las ciberdefensas afectan a la búsqueda de la innovación en otros frentes. La transformación digital abre las puertas a nuevas oportunidades de crecimiento, pero al 40 % les preocupa que ampliar la arquitectura digital y el software haga a sus empresas más vulnerables a los ataques, sobre todo si tenemos en cuenta que el 32 % no se ven lo suficientemente preparadas como para proteger arquitecturas de software modernas y complejas.

Más de la mitad (52 %) creen que no serían capaces de hacer frente a una amenaza sofisticada, mientras que el 46 % dicen que no disponen de tecnologías de ciberseguridad sólidas a nivel interno.

Los ataques de DDoS, a fondo

Aunque lleven existiendo un cuarto de siglo, los ataques de denegación de servicio distribuido (DDoS) siguen siendo una amenaza muy presente. Estos ataques son una preocupación para el **23 %** de las empresas con vistas al año que viene.

Los daños provocados por los periodos de inactividad fueron un problema para el **62 %** de las empresas que sufrieron ataques de DDoS en 2024, más de la mitad (**52 %**) dicen haber perdido una cantidad considerable de ingresos, y los costes operativos se dispararon para un **70 %** de ellas.

A pesar de todo, la protección contra DDoS solo ocupa el noveno puesto en las prioridades de inversión con un **25 %**, y eso que el **45 %** de quienes los consideran una amenaza durante el año que viene dicen no contar con la preparación necesaria para hacerles frente. Existen numerosas opciones para mitigar estos ataques. La más popular, con un **71 %**, consiste en adoptar mecanismos de protección basados en la nube, mientras que el **56 %** acuden a sus proveedores de servicios de internet en busca de ayuda. La mitigación en el entorno local es una solución para el **54 %**. Los firewalls de aplicaciones web (WAF) en la nube o el entorno local son una medida muy extendida que se adopta en el **66 %** de los casos.

¿El gasto en ciberseguridad se está estancando?

La inversión es la clave de todo, y esto incluye la ciberseguridad. Ahora que el número y el nivel de sofisticación de los atacantes están aumentado, hay que dedicar más recursos económicos a la protección de los activos. Y aunque quienes se encargan de las defensas tienen buenas intenciones, la realidad es que hay graves problemas.

En 2023, tres cuartos de las personas encuestadas decían que iban a invertir más ciberseguridad. Un año después, la mitad de las empresas creen que no han invertido lo suficiente en aspectos clave de la ciberseguridad y que eso puede hacerlas vulnerables a los ataques. Esto preocupa especialmente a las empresas de Estados Unidos (61 %), algo lógico si tenemos en cuenta que han recibido el mayor número de ataques.

En líneas generales, las empresas creen que están apostando por las áreas de la ciberseguridad adecuadas. De hecho, el 71 % afirman que sus inversiones están en sintonía con sus estrategias. La pregunta es por qué tantas empresas creen que invierten de menos en seguridad.

Las inversiones son difíciles de justificar

La desconexión va más allá de la falta de concienciación en torno a la ciberseguridad, algo relativamente sencillo de resolver. El mayor problema es que la ciberseguridad se considera un obstáculo para otras prioridades. Sin ir más lejos, al 45 % de los cargos directivos de las personas encuestadas les preocupa que ponga trabas a la innovación. La modernización de IT es un componente importante de la trasformación digital, y el 43 % de las personas encuestadas cree que invertir en ciberseguridad resulta perjudicial en este aspecto.

Los profesionales de la ciberseguridad deben justificar el gasto a los cargos directivos superiores, pero el 44 % no lo consiguen. Si bien el 72 % de las personas encuestadas creen que sus inversiones han respaldado sus objetivos de ingresos y crecimiento, solo el 62 % consideran que el gasto en ciberseguridad ha producido un retorno de la inversión. Parte del problema es saber cómo invertir el dinero: el 36 % dicen haber invertido demasiado y sin tener un plan real para asignar los recursos.

Quienes más recortan son quienes no deben

En el lado positivo, el 87 % de las empresas tienen la intención de aumentar su inversión en ciberseguridad, más que el año pasado. Sin embargo, el 76 % de las empresas querían invertir más en ciberseguridad el año pasado y la mitad dicen haberse quedado cortas, por lo que la realidad puede ser muy diferente.

Solo el 4 % van a reducir su inversión en ciberseguridad, pero esto no significa que vayan a perder funcionalidades, como explica Jay Coley, Director of Technical Strategy de Fastly. «Es posible que se pasen a soluciones más económicas, que consoliden contratos para ser más eficientes o que estudien opciones de código abierto», comenta.

Exprimir cada céntimo no tiene nada de malo, pero el relativamente bajo rendimiento del grupo que ha realizado recortes da que pensar. Sus integrantes sufrieron una media de 68 incidentes de seguridad el año pasado, un 70 % más que el promedio general de 40.

El análisis de riesgos como pieza clave de la inversión

Invertir en los mecanismos de prevención y respuesta adecuados puede aportar mucho a las empresas. Conviene enfocar el análisis de riesgos con madurez, saber qué tipo de ciberamenaza es el que más afecta a una organización concreta y concentrar la inversión en las mitigaciones correspondientes.

La clave consiste en hablar de riesgos a los cargos directivos. Los profesionales de la ciberseguridad deben mostrarles métricas de mitigación de riesgos a alto nivel para que comprendan por qué la ciberseguridad hace que la innovación y la transformación sean más seguras. También pueden colaborar con los equipos de producción para adoptar medidas de seguridad en las fases tempranas del desarrollo y utilizar la automatización siempre que sea posible para que estas sean más efectivas y planteen menos obstáculos.

Así están cambiando las responsabilidades

Si se produce un incidente de ciberseguridad, ¿quién es responsable? Los organismos reguladores apuntan cada vez más al Chief Information Security Officer (CISO). En octubre de 2023, la Comisión de Bolsa y Valores (SEC) de Estados Unidos acusó de fraude y errores de control interno no solo a SolarWinds, sino también a Timothy G. Brown, el CISO de la empresa, que finalmente fue absuelto de casi todos los cargos.[6] La pregunta es si la SEC y otros organismos reguladores han modificado el lenguaje que utilizan para aclarar las responsabilidades de los CISO.

Casi todo sigue igual para los CISO

Las personas encuestadas son conscientes de cómo están cambiando las responsabilidades, y el 93 % de las empresas están modificando las políticas pertinentes. Sin embargo, esto apenas tiene relevancia en la práctica. La medida más extendida, que consiste en dar a los CISO voz y voto en las decisiones estratégicas (41 %), no es precisamente revolucionaria.

Algunas medidas son defensivas o se limitan a marcar determinadas casillas. El 38 % se comprometen a analizar más a fondo la documentación de seguridad proporcionada por los organismos reguladores, pero eso no es más que leer las reglas. La misma proporción promete más apoyo legal para su personal de ciberseguridad en caso de que alguno de estos organismos llame a sus puertas. Y apenas una quinta parte (21 %) destacan que los CISO deben cumplir la ley en materia de ciberseguridad.

«Estas medidas están muy bien, pero sirven para poco más que cubrirse las espaldas», dice Marshall Erwin, CISO de Fastly. «No mejoran la seguridad de por sí».

¿Hasta dónde llegan las responsabilidades?

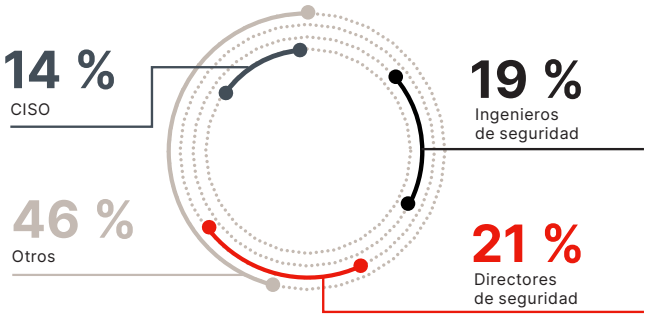
Parte del problema reside en que no termina de estar claro quién es el responsable cuando se produce un incidente de ciberseguridad. No hay una cara visible, por lo que personas que ocupan puestos de distintos niveles se sienten responsables. Dicho sea de paso, los CISO ocupan el tercer lugar (14 %), por detrás de los ingenieros de seguridad (19 %) y los directores de seguridad (21 %). (*Figura 2)*

Por suerte, también hay datos que invitan al optimismo. Como la responsabilidad cada vez está más repartida entre los desarrolladores de aplicaciones (10 %), los ingenieros de plataforma (8 %) y los ingenieros de fiabilidad del sitio (7 %), todo parece indicar que ya no se atribuye a puestos concretos.

En la teoría, esto quiere decir que todo el mundo es responsable. Sin embargo, en la práctica, significa que nadie lo es. Solo el 36 % de las personas encuestadas indican claramente cuáles son los puestos con responsabilidades en el ámbito de la ciberseguridad. Por tanto, casi dos tercios no saben a quién atribuir las responsabilidades, y el 46 % opinan que no se sabe a ciencia cierta quién se responsabiliza de los incidentes de ciberseguridad. En última instancia, alguien debe dar la cara.

Figura 2

Quién es responsable de los incidentes de ciberseguridad



Los empleados, en el punto de mira

Para que la seguridad sea una responsabilidad compartida en toda una empresa, todos los empleados deben saber en qué consiste y verse capaces de cumplir las políticas. Los ataques de ingeniería social, que son los más temidos por las personas entrevistadas de cara al año que viene con un **37 %**, están dirigidos a los empleados. El auge del trabajo híbrido también ha afectado a la seguridad: el **70 %** de las empresas temen que los empleados a distancia sufran un ataque.

Muchas de ellas (**77 %**) creen que comunican la importancia de cumplir las políticas de seguridad a todos sus empleados. Y parece ser así, porque el **70 %** afirman que los empleados ajenos a IT conocen su impacto en la ciberseguridad y el 69 % dicen que todos sus empleados cumplen las normas de ciberseguridad. Pero no todo el monte es orégano, ya que el **55 %** consideran que falta formación interna sobre las prácticas recomendadas en materia de ciberseguridad.

Una cosa es conocer las reglas, pero otra muy distinta es disponer de los recursos necesarios para cumplirlas. Un **72 %** de las empresas afirman dar acceso a estos recursos, pero eso significa que más de una cuarta parte de ellas no lo hacen. Los procedimientos para avisar de incidentes no siempre están claros. Aunque el **73 %** de las personas encuestadas dicen contar con un proceso universal y bien definido para informar de los incidentes, solo el **63 %** creen que el personal ajeno a TI tiene la confianza necesaria para identificar las posibles amenazas y actuar en consecuencia.

6 Becky Bracken, Senior Editor. «Sizable Chunk of SEC Charges Against SolarWinds Tossed Out of Court». Dark Reading, 18 de julio de 2024, www.darkreading.com/application-security/solarwinds-charges-tossed-out-of-court-in-legal-victory-against-sec.

Suplir las carencias del personal de ciberseguridad

El 30 % de las personas encuestadas mencionan la falta de conocimientos para hacer frente a amenazas modernas como uno de los mayores obstáculos para la ciberseguridad. Casi la mitad de las empresas (47 %) no han invertido lo suficiente en contrataciones y aumentos salariales para el personal de ciberseguridad. La formación y la contratación son las principales prioridades para el año que viene, con un 28 %.

Algunas empresas buscan profesionales en los lugares equivocados. La mitad de ellas (51 %) no encuentran personas con las habilidades necesarias en sus respectivas canteras. Por su parte, solo el 13 % creen que no hay problemas graves con el personal al que tienen acceso los responsables de contratación para puestos de ciberseguridad.

Lograr que una nueva incorporación se convierta en un buen fichaje para el equipo de seguridad requiere mucho tiempo y esfuerzo. Una persona recién graduada en ciberseguridad debe adquirir distintos conocimientos técnicos, como los necesarios para trabajar con las herramientas específicas de una empresa y familiarizarse tanto con sus procesos como con su cultura.

Cuanto más grande es una empresa, mayores son estos retos. Trabajar en un entorno grande y en constante evolución plantea dificultades a los empleados. El 17 % de las personas encuestadas consideran que la falta de experiencia de los empleados con tecnologías y empresas a gran escala supone un problema.

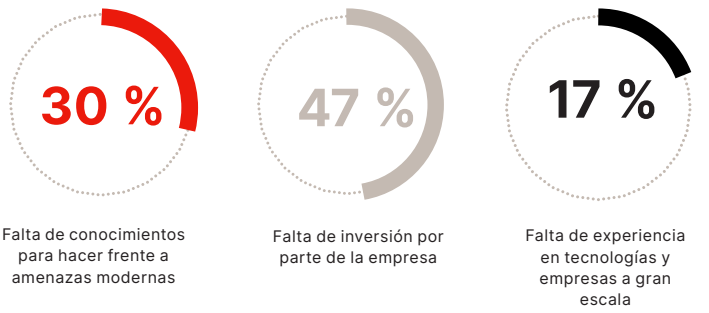
Alternativas a la contratación externa

A la vista de todos estos retos, ¿deberían las empresas centrarse en el desarrollo del personal interno? Para ello, disponen de varias opciones:

- **Mejora de habilidades.** Como ya conocen la cultura de la empresa y, en mayor o menor medida, los sistemas y los procesos, puede ser una buena idea formar a los empleados actuales para que adquieran nuevas responsabilidades.
- **Orientación.** Recibir formación de personas con más experiencia es una forma fantástica de asentar los conocimientos de una nueva incorporación y ayudarla a hacer bien su trabajo.
- **Colaboración entre equipos.** Fomentar la comunicación entre el personal de seguridad y otros equipos, como los de IT, cumplimento normativo, asistencia y desarrollo de productos, ayuda a sus integrantes a desenvolverse mejor y a entender cómo encaja la seguridad con las demás funciones. Incluso puede que se les presente la oportunidad de hacer un traslado temporal. Lo ideal es que también aumenten los conocimientos y las responsabilidades de quienes no trabajan en seguridad. Cuando alguien que se dedica a desarrollar productos entiende cómo funciona la seguridad, puede seguir los principios del desarrollo seguro en su día a día, por poner un ejemplo.

Buscar profesionales dentro de la empresa tiene varias ventajas, sobre todo si estos desempeñan distintas funciones. Ayuda a transmitir la idea de que la seguridad es responsabilidad de todo el mundo e impulsa la transformación digital. Al 40 % de las empresas les preocupa que las iniciativas de transformación digital las hagan más vulnerables a los ataques, por lo que una cultura basada en la integración de la seguridad puede contribuir a impulsarla durante este proceso.

Figura 3
Carencias del personal existente



Elegir las herramientas adecuadas para unas amenazas que evolucionan

Las ciberamenazas cambian constantemente, por lo que las herramientas que utilizamos para protegernos de ellas deben hacer lo mismo.

Las amenazas de ingeniería social son las que más preocupan a un 37 % de las empresas, que se dice pronto. Esto engloba otras amenazas tan comunes como la suplantación de identidades, un elemento clave de ataques como los que afectan a las cuentas de correo de empresa y el ransomware (este último es la segunda amenaza más temida, con un 34 %).

Además, muchas amenazas van de la mano, lo cual no hace sino aumentar su complejidad. La apropiación de cuentas, algo que el 20 % de las personas encuestadas consideran una amenaza, suele ser una consecuencia directa de la suplantación de identidades, y la exfiltración de datos, muy preocupante para el 28 %, suele ser el resultado del ransomware.

Las fugas de datos a través de terceros, mencionadas por el 20 %, han empezado a dar quebraderos de cabeza a las empresas tras incidentes como el hackeo de SolarWinds en 2020 y el ataque de ransomware a Kaseya en 2021. Hace poco, las tarjetas de crédito de Amex quedaron expuestas en una fuga de estas características, y la que afectó a UnitedHealth provocó la paralización de partes importantes de su ecosistema sanitario.*(Figura 4)*

Invertir en protección

Las organizaciones están haciendo inversiones de todo tipo para protegerse y adquiriendo productos o servicios para mantener a raya las amenazas. Nos alegra que las funcionalidades de autenticación modernas estén entre las dos principales inversiones, con un 35 %. El uso de herramientas para la gestión de identidades y accesos, así como la autenticación multifactor, ayudan a mitigar los ataques de ingeniería social en los que se basan numerosas amenazas.

El auge de las amenazas que se aprovechan de vulnerabilidades de las API ha puesto en alerta a las organizaciones, razón por la cual el 29 % de ellas invierten en seguridad para las puertas de enlace de las API. Además, la misma proporción de organizaciones invierten en firewalls de aplicaciones web. Este porcentaje supera al 21 % de empresas a las que les preocupa que los atacantes se aprovechan de vulnerabilidades de las aplicaciones web. En cualquier caso, los WAF son un método común de defensa por capas ante otros ataques, como los de DDoS de bajo volumen. De media, las organizaciones invierten 1,58 millones de USD al año en soluciones de seguridad para aplicaciones web y API.

Nos sorprende que las inversiones en protección contra DDoS hayan bajado hasta el noveno puesto, con un 25 %, y que la mitigación de bots esté casi al final de la lista, con un 15 %. Los bots se utilizan mucho en los ataques de relleno de credenciales, que suelen estar presentes en las apropiaciones de cuentas.

Las organizaciones de las personas encuestadas también han invertido en servicios para mitigar los incidentes de ciberseguridad. Uno de ellos es la transferencia de riesgos: los ciberseguros empatan con la autenticación moderna como principales inversiones, con un 35 %. Otra estrategia consiste en externalizar la prevención de riesgos de ciberseguridad y la respuesta ante incidentes a un proveedor de servicios de seguridad gestionados, cosa que hacen el 29 % de las personas encuestadas.

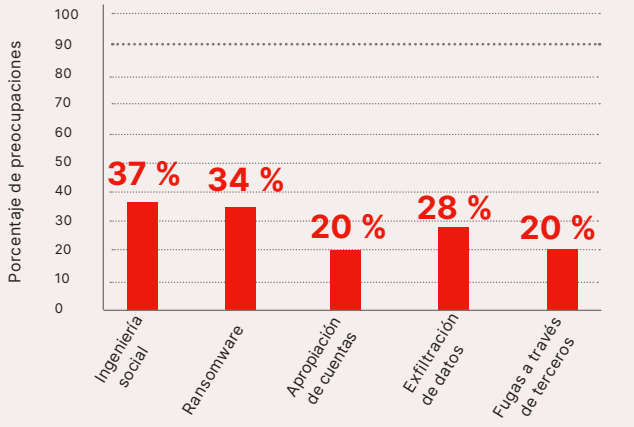
Entre quienes externalizan la seguridad, el 27 % cuentan con varios proveedores, mientras que el 32 % confían su respuesta de seguridad a un único proveedor. El 17 % prefieren consolidar la respuesta de seguridad en un equipo interno y el 18 % combinan ambas estrategias.

Las herramientas siguen fragmentadas

El solapamiento entre las herramientas es un problema para las personas encuestadas. De media, las organizaciones utilizan 7,85 soluciones enfocadas a la seguridad de redes y aplicaciones, cifra que asciende hasta nada menos que 9,4 en los países nórdicos. Más de un tercio (37,7 %) de estas herramientas se solapan, lo cual supone una pequeña mejora con respecto al año pasado (41 %).

Figura 4

Principal motivo por el que consolidar herramientas



Por qué es el momento de consolidar, centralizar e integrar la seguridad desde el principio

El dato clave de nuestro estudio de 2024 es que las empresas se enfrentan a un aumento de las ciberamenazas y limitaciones en las inversiones en ciberseguridad. El 75 % están de acuerdo en que la ciberseguridad es fundamental y el 50 % creen que la falta de inversión las hace más vulnerables, así que no es de extrañar que muchas de ellas esperen gastar más en mecanismos de protección. Sin embargo, los hechos demuestran que no siempre lo acaban haciendo. Esto se debe en cierta medida a lo complicado que resulta justificar estos gastos ante las directivas. Los cargos ejecutivos consideran que este dinero está mejor invertido en otra parte.

El uso de herramientas fragmentadas y con funciones similares agravan el problema, puesto que estos stacks tipo Frankenstein son caros y difíciles de integrar. También son una consecuencia natural de las estrategias de ciberseguridad reactivas que cambian de forma heterogénea para adaptarse a unas amenazas en constante evolución.

Hora de adoptar la seguridad por diseño

Las organizaciones deben innovar para hacer frente a las ciberamenazas de una forma más eficiente, todo ello sin que los costes y la complejidad se vayan de las manos. Esto significa que conviene adoptar un mecanismo para identificar y mitigar las amenazas que se pueda aplicar a toda una empresa.

Una de las claves es la consolidación de las herramientas, ya que contribuye a reducir los costes y la complejidad. Para ello hacen falta una gestión de riesgos avanzada y la asignación de las funcionalidades de las herramientas a las amenazas según su impacto y su probabilidad. Esto depende de factores como el sector y el tamaño de la empresa (ver el apartado «Pensar en vertical»).

El otro requisito es contar con un conjunto de principios universales de seguridad y tener la voluntad de aplicarlos en todo momento, desde el desarrollo de productos y servicios dirigidos a clientes hasta los procesos internos. Si se ponen en práctica desde la fase de diseño en adelante, contribuyen a reforzar la seguridad desde el primer momento.

Aplicar el concepto de la seguridad por diseño a la arquitectura del software solo es una prioridad para el 18 % de las personas encuestadas y ocupa el sexto lugar entre otras mitigaciones, algo comprensible si tenemos en cuenta que no solo exige cambios técnicos, sino también cambios en la cultura, y eso no se consigue de la noche a la mañana.

Otro problema es que el 34 % de las personas encuestadas creen que la ciberseguridad es una pérdida de tiempo y que este presupuesto estaría mejor invertido en otra parte. Quienes comparten esta opinión tienen más probabilidades de reducir las inversiones en ciberseguridad (55 %).

En palabras de Erwin, el problema está en la falta de visibilidad de la ciberseguridad por parte de los cargos directivos. «Si un programa de seguridad es eficaz, puede mitigar muchos riesgos y reducir las probabilidades de que se produzcan incidentes. Sin embargo, este valor no es evidente para los altos cargos», explica.

Cambiar esta actitud no es tarea fácil, pero asociar las inversiones en ciberseguridad con resultados cuantificables sobre la mitigación de riesgos es un buen punto de partida.

Pensar en vertical

Las ciberamenazas campan a sus anchas, pero no se distribuyen de una manera uniforme. Cada sector vertical se enfrenta a unos riesgos determinados. Este año nos hemos fijado en seis sectores, dos más que el año pasado.

Finanzas Dos de cada cinco profesionales de la ciberseguridad (41 %) que trabajan en empresas de servicios financieros y contabilidad prevén que los ataques de ingeniería social (como la suplantación de identidades, incluida la que se realiza a través de mensajes de texto), estarán detrás de la mayoría de las amenazas. Quienes toman decisiones financieras tienen un 8 % más de probabilidades de considerarlos una amenaza grave en comparación con sus equivalentes de otros sectores.

Servicios públicos Las organizaciones gubernamentales son especialmente susceptibles a los ataques de DDoS. El 15 % sufren interrupciones causadas por estos ataques, sobre todo ahora que están aumentando las tensiones geopolíticas. No obstante, esto no significa que los atacantes hayan perdido interés en los datos de las administraciones. Casi la mitad (47 %) han experimentado periodos de inactividad o interrupciones y más de un tercio (35 %) han perdido datos debido a incidentes de seguridad.

Continúa en la siguiente página

Pensar en vertical *Continuación*

Sanidad Los ciberdelincuentes atacan a las empresas de finanzas para apropiarse de su dinero y al sector sanitario para hacerse con datos de los pacientes, que pueden alcanzar un alto precio en la internet oscura. Por este motivo, el 39 % de las organizaciones de servicios sanitarios y ciencias de la vida han sufrido pérdidas de datos tras un incidente de seguridad, un 7 % más que la media de los otros sectores. Por tanto, no es de extrañar que la exfiltración de datos sea una de las mayores amenazas para estas organizaciones durante los próximos doce meses.

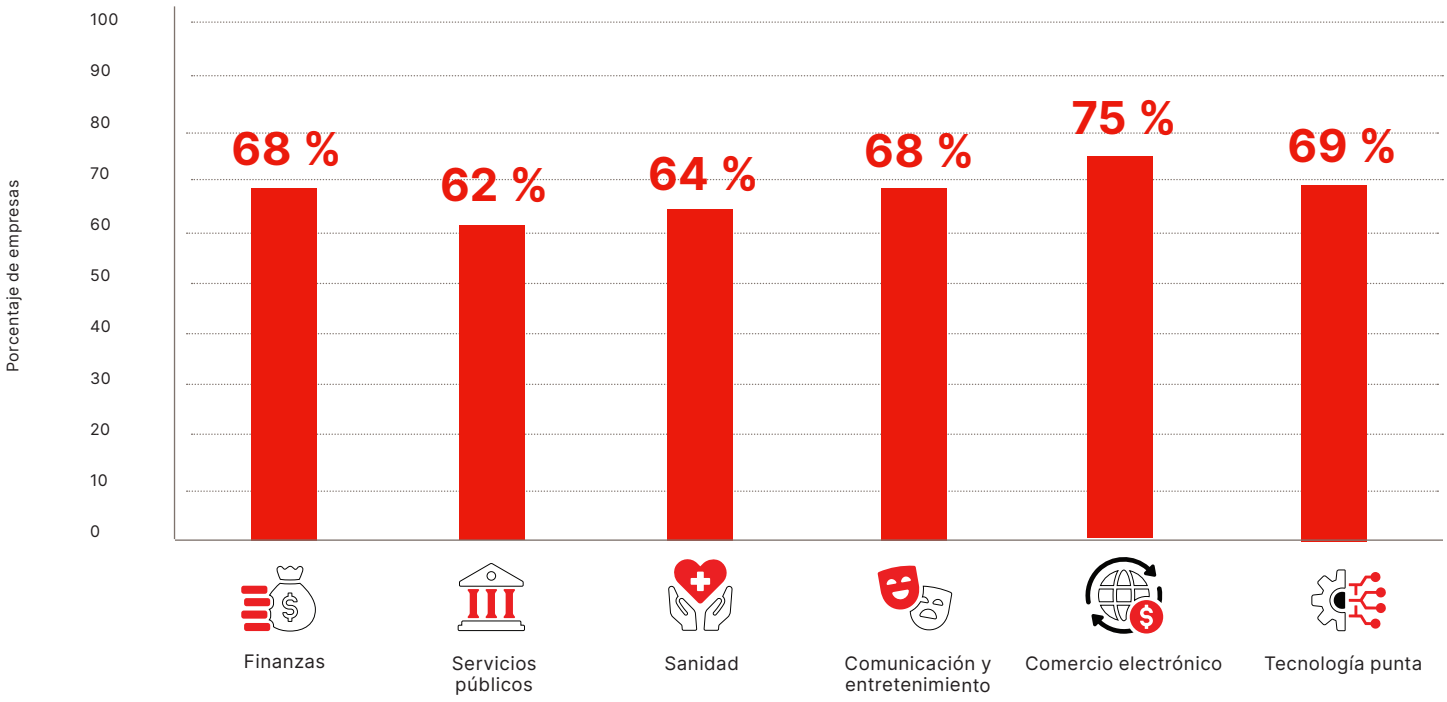
Comunicación y entretenimiento Los contenidos son la piedra angular de este sector. De hecho, los profesionales de la ciberseguridad que trabajan en él tienen un 36 % más de probabilidades de pensar que la extracción no autorizada de contenidos sea una de las mayores amenazas durante los próximos doce meses en comparación con otros sectores.

Comercio electrónico Los retailers deben lidiar con todo tipo de ataques, desde el robo de datos de tarjetas de crédito hasta fraudes en los envíos y la apropiación de cuentas de clientes. Más de una quinta parte (22 %) de los retailers prevén que la apropiación de cuentas será su mayor ciberamenaza, lo cual pone de relieve la necesidad de adoptar sistemas de autenticación seguros.

Tecnología punta Las propiedades intelectuales son el principal objetivo de los hackers que ponen las empresas de tecnología punta en la diana, pero las cuentas de usuarios también son fáciles de monetizar, por eso el 22 % de las empresas del sector creen que la apropiación de cuentas será su mayor ciberamenaza durante los próximos doce meses. Por otra parte, el ransomware y la extorsión no les preocupan tanto.

Aunque todos los sectores se enfrentan a riesgos determinados, la mitad de las personas encuestadas (52 %) coinciden en que sus empresas no están preparadas para hacer frente a unas amenazas cada vez más sofisticadas.

Porcentaje de empresas que han sufrido un incidente de seguridad durante los últimos doce meses



Acerca del estudio

Para este estudio hemos encuestado a 1800 responsables de IT con influencia en la ciberseguridad de empresas de gran tamaño y distintos sectores ubicadas en Norteamérica, Centroamérica, Sudamérica, Europa, Asia-Pacífico y Japón.

Sapio Research llevó a cabo las entrevistas en septiembre de 2024 mediante invitaciones por correo electrónico y una encuesta online. Los resultados están sujetos a la variación de las muestras.

La magnitud de las variaciones se puede calcular y afecta tanto al número de entrevistas como a los porcentajes que expresan los resultados. En este estudio concreto, hay un 95 % de probabilidades de que un resultado no varíe más de un 2,6 %, ya sea alza o a la baja, con respecto a una muestra hipotética que incluyera a todas las personas del mundo.

Acerca de Sapio

Sapio ha sido finalista en la categoría de mejor nueva agencia y es una empresa experta en encuestas de opinión (con acceso a más de 80 millones de personas de todo el mundo), grupos de estudio, entrevistas cara a cara, entrevistas telefónicas, investigación online, investigación de fuentes secundarias y modelado estadístico, entre otras técnicas. Nos encanta la consultoría y el estudio de empresa a empresa. Nuestro negocio se basa en principios de colaboración inspirados en organizaciones sociales.

Acerca de Fastly, Inc.

La plataforma de edge cloud potente y programable de Fastly ayuda a las marcas más importantes del mundo a ofrecer experiencias online rápidas, seguras y dinámicas, todo ello gracias a una oferta de informática en el edge, distribución, seguridad y observabilidad que mejora el rendimiento de los sitios web, refuerza la protección e impulsa la innovación a escala global. En comparación con otros proveedores, la arquitectura de plataforma potente, moderna y de alto rendimiento de Fastly permite a los desarrolladores crear aplicaciones y sitios web seguros con una rápida comercialización y el mayor ahorro del sector. Organizaciones de todo el mundo confían en Fastly para mejorar las experiencias que ofrecen en internet, entre ellas Reddit, Neiman Marcus, Universal Music Group y SeatGeek. Infórmate sobre Fastly en https://www.fastly.com y síguenos en @fastly.