HISCOX

Informe de Ciberpreparación de Hiscox 2022

Contenidos

Cover illustration
www.johnholcroft.com

Introducción

Gareth Wharton
Cyber CEO, Hiscox

Uno de los hallazgos más reveladores del informe de este año es que la amenaza ciber se considera ahora el principal riesgo para las empresas en siete de los ocho países encuestados, por delante de la pandemia, la recesión económica, la escasez de personal cualificado y otros problemas. Si tenemos en cuenta que la concienciación del peligro es el primer paso para afrontarlo, seguramente esta es una señal alentadora. Sin embargo, la parte negativa es que han aumentado tanto el número de empresas que notifican ataques como la gravedad de los mismos, por lo que no cabe duda de la magnitud del desafío.

Si bien los ciberdelincuentes han dirigido ataques durante mucho tiempo a organizaciones de alto valor, está claro que ahora están descendiendo en la 'cadena alimentaria'. Las agencias de seguridad internacionales han advertido recientemente que un mayor número de medianas y pequeñas empresas recibe ataques y esto se confirma en el informe de este año.

Las empresas con ingresos de €90.000 a €450.000 pueden esperar ahora tantos ciberataques como las que ganan entre €900.000 y €8,1m anuales. Sin embargo, aunque las grandes empresas han aumentado su inversión para crear estrategias de ciberdefensa, el gasto de las empresas más pequeñas se ha reducido este año, como parte de una disminución en el gasto total en TI en el extremo inferior del espectro empresarial. Pero esto no llega en un buen momento.

La pandemia bien puede haber jugado su papel aquí. El paso al trabajo remoto ha llevado a muchas empresas más pequeñas a adoptar soluciones en la nube en lugar de desarrollar sus propios servicios remotos. Eso, a su vez, ha alentado a más ciberdelincuentes a explotar las vulnerabilidades existentes en las aplicaciones en la nube y a dirigir ataques también a los proveedores de servicios en la nube.

En medio de estas problemáticas, una buena señal: hay pruebas evidentes en el informe de que las empresas están respondiendo a los ataques con más fortaleza. Muchas más empresas están tomando medidas decisivas y esto lo vemos claramente en la calidad de los planes de ciberresistencia que se nos presentan en el ámbito asegurador. La mayor concienciación que se observa en el tejido empresarial se manifiesta en una mayor comprensión por parte de los directivos de las empresas tanto del problema como de los estándares de ciberpreparación frente al mismo.

Creemos que tenemos un papel importante que desempeñar en el apoyo a ese proceso y, por ello, brindamos formación online sobre ciberseguridad para los empleados de nuestros clientes a través de Hiscox CyberClear Academy. Sin ir más lejos, el continuo número de vulneraciones creadas por simples correos electrónicos de phishing que se destacan en el informe muestra la necesidad apremiante de que los trabajadores sean conscientes de los riesgos.

Del mismo modo, el propósito del informe no es solo señalar la magnitud y la naturaleza del desafío que supone la ciberseguridad, sino también ayudar a las empresas a estar a la altura de la situación, identificando y adoptando las mejores prácticas. Para ello, les invitamos a visitar nuestro modelo interactivo de ciberpreparación y comparar la 'madurez' ciber de su empresa con la de empresas similares. El modelo está destinado a ayudarle a identificar sus fortalezas y debilidades y a elaborar una agenda para acciones futuras. Esperamos que estas herramientas en conjunto con el informe les ayuden a construir defensas más sólidas contra las ciberamenazas y una mayor resiliencia para afrontar los problemas a medida que ocurran.

Hay señales de que las empresas están respondiendo de manera más decisiva al desafío de la ciberseguridad.

Hiscox y la ciberseguridad

Cuando se trata de ciberseguridad, Hiscox ofrece experiencia
Contamos con una trayectoria de más de 20 años de experiencia en privacidad y seguros ciber, y durante este periodo hemos suscrito cientos de miles de pólizas y gestionado miles de siniestros en todo el mundo. Comprender los riesgos y los desafíos en términos de ciberseguridad a los que se enfrentan las empresas es fundamental para nuestro éxito, y por eso, en 2017, Hiscox creó un equipo de ciberseguridad central con presencia en todo el mundo para proporcionar productos sólidos, información coordinada y servicios colaborativos.

El seguro de nueva generación incluye un conjunto de herramientas y servicios
Más allá de la clásica transferencia de riesgos, el seguro ciber de Hiscox ofrece a las empresas apoyo directo de verdaderos expertos: gestores de crisis, especialistas en TI, abogados de protección de datos y consultores de relaciones públicas. Además, Hiscox ofrece desde 2018 formación gratuita para los empleados de todas las empresas aseguradas pequeñas y medianas de todo el mundo a través de Hiscox CyberClear Academy, una plataforma de formación que cuenta con casi 30.000 usuarios.

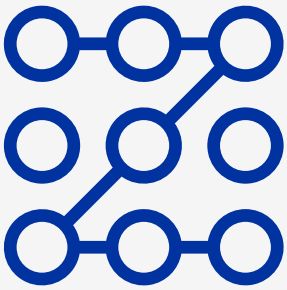
Compartir nuestra experiencia y generar concienciación
Hemos creado herramientas gratuitas para todos, como la Calculadora de Ciberriesgo de Hiscox, que ayuda a las empresas a comprender el impacto financiero que un ciberataque podría tener en su organización. Para completar este servicio, en 2021 presentamos nuestro modelo de autoevaluación de madurez ciber online para ayudar a las empresas a comprender las fortalezas y debilidades de su estrategia de ciberseguridad. En esta plataforma pueden comparar de forma gratuita su desempeño con otras más de 11.000 empresas.

Mantenerte al día sobre el panorama de la ciberseguridad
Hemos elaborado por sexto año consecutivo el Hiscox Cyber Readiness Report ('Informe de ciberpreparación de Hiscox'), que brinda una fotografía actualizada del panorama de la ciberpreparación de las empresas y ofrece un modelo de las mejores prácticas en la prevención para contrarrestar una amenaza en constante evolución. Partiendo de una muestra representativa de organizaciones seleccionadas por tamaño y sector en ocho países, el informe refleja la experiencia directa de quienes están en la primera línea de la batalla empresarial contra la ciberdelincuencia.

Resumen ejecutivo

Los ataques se intensifican
El 48% de las empresas informaron de un ciberataque en los últimos 12 meses, frente al 43% del año pasado.

El riesgo percibido es alto
Siete de los ocho países clasifican los ciberataques como la amenaza número uno para su negocio.



Presión sobre la cuenta de resultados
Una de cada cinco empresas atacadas dice que su solvencia se vio amenazada, lo que supone un aumento del 24% respecto al año pasado.

Riesgos del trabajo a distancia
El covid hizo que las empresas aceleraran su viaje a la nube, lo que provocó un gran salto en los ataques a través de servidores en la nube.

Vale la pena tener experiencia
Los costes medianos de los ciberataques, expresados como porcentaje de los ingresos, son dos veces y media más altos para las empresas calificadas como 'cibernovatas'.

Más pólizas ciber
El 64% de las empresas tienen actualmente coberturas ciber, con un seguro ciber específico o como parte de otra póliza, frente al 58% de hace dos años.

Más ataques de ransomware
El 19% de las empresas encuestadas notifica un ataque de extorsión, frente al 16% del año pasado. Dos tercios pagaron el rescate.

Aumento del gasto
El gasto medio en ciberseguridad de todos los encuestados ha aumentado un 60% en el último año hasta los €4,8 millones y ha aumentado un 250% desde 2019.

Impacto más grave
El coste mediano de los ataques ha aumentado un 29%, hasta algo menos de €15.300.

Comparaciones entre países

Aspectos destacados	
Bélgica Una de cada siete empresas belgas (14%) despidió a trabajadores como resultado de un ciberataque.	**Francia** Dos de cada cinco empresas que fueron víctimas de ataques sufrieron fraude de desvío de pagos (el 41%), situándose con la proporción más alta en el ranking por país.
Alemania Si bien es menos probable que las empresas alemanas paguen un rescate después de un ataque, son las que tienen los pagos de rescate más altos.	**Irlanda** Las empresas irlandesas pagaron rescates con más regularidad que el resto, en concreto una cuarta parte pagó cinco veces o más para recuperar datos (el 25%), pero los costes de rescate estuvieron entre los más bajos.
Países Bajos Las empresas neerlandesas son ahora los objetivos número uno de nuestro grupo de estudio. El porcentaje que sufrió ataques en los últimos 12 meses pasó del 41% al 57%.	**España** España es el único país donde ha disminuido la proporción de empresas atacadas en el último año, del 53% al 51%.
Reino Unido Por tercer año consecutivo, el Reino Unido cuenta con la menor proporción de empresas que sufrieron ataques, con un 42%, pero el coste mediano de los ataques se duplicó hasta alcanzar más de €25.200.	**Estados Unidos** El número de empresas estadounidenses que notificaron uno o más ciberataques el último año aumentó considerablemente (+7%), mientras que las empresas que asumieron costes de €22.500 o más aumentaron también del 34% al 40%.

Comparaciones entre países
continuación

Experimentaron un ciberataque (%)

	2021	2022	+/-
Bélgica	42	**43**	+1
Francia	49	**52**	+3
Alemania	46	**46**	–
Irlanda	39	**49**	+10
Países Bajos	41	**57**	+16
España	53	**51**	-2
Reino Unido	36	**42**	+6
Estados Unidos	40	**47**	+7

Coste mediano de todos los ciberataques (€000)

	2021	2022	+/-
Bélgica	11	**9**	+2
Francia	16	**15**	-1
Alemania	22	**19**	-3
Irlanda	7	**15**	+9
Países Bajos	11	**16**	+6
España	11	**11**	–
Reino Unido	13	**25**	+14
Estados Unidos	9	**17**	+9

Experimentaron un ataque de ransomware (%)

	2021	2022	+/-
Bélgica	19	**15**	-4
Francia	14	**19**	+5
Alemania	19	**21**	+2
Irlanda	16	**19**	+3
Países Bajos	13	**26**	+13
España	14	**22**	+8
Reino Unido	13	**16**	+3
Estados Unidos	17	**17**	–

Las víctimas del ransomware que pagaron (%)

	2021	2022	+/-
Bélgica	49	**74**	+25
Francia	65	**62**	-3
Alemania	54	**48**	-6
Irlanda	75	**80**	+5
Países Bajos	48	**79**	+31
España	44	**64**	+20
Reino Unido	58	**63**	+5
Estados Unidos	71	**84**	+13

Adopción del seguro ciber (%)

	2021	2022	+/-
Bélgica	58	**59**	+1
Francia	57	**61**	+4
Alemania	64	**67**	+3
Irlanda	64	**69**	+5
Países Bajos	55	**58**	+3
España	63	**66**	+3
Reino Unido	61	**62**	+1
Estados Unidos	65	**65**	–

Porcentaje del presupuesto de TI destinado a ciberseguridad (%)

	2021	2022	+/-
Bélgica	21	**24**	+3
Francia	20	**22**	+2
Alemania	21	**24**	+3
Irlanda	21	**22**	+1
Países Bajos	22	**24**	+2
España	22	**24**	+2
Reino Unido	20	**22**	+2
Estados Unidos	23	**24**	+1

Percepción frente a realidad

La experiencia nos hace más cautos: parece que no hay nada como un incidente con los ciberdelincuentes para ir con más cuidado. Por eso es mucho más probable que las empresas que sufrieron un ataque en el último año clasifiquen la amenaza de un ciberataque como de 'alto riesgo' que aquellas que no lo sufrieron.

La amenaza ciber ya es considerada como el riesgo número uno para las empresas. Desde la perspectiva por países, solo las empresas irlandesas relegaron la ciberamenaza al puesto número dos, por detrás de la pandemia. Pero hay un gran abismo de percepción entre las empresas que han sufrido realmente un ataque y las que no. Más de la mitad de las víctimas de ciberataques ven la ciberamenaza como un área de alto riesgo (el 55%), mientras que entre las que no fueron víctimas, la cifra es solo del 36%. Mantener los datos seguros, independientemente del riesgo ciber, parece ser importante para todas las empresas: el 72% está de acuerdo en que su reputación podría verse dañada si no gestionan los datos de los clientes y socios de manera segura.

Este abismo en la percepción se refleja en el número de empresas que dicen que han aumentado los riesgos en el último año. Más de dos de cada cinco de las empresas que sufrieron ataques (el 41%) dicen que ha aumentado su exposición al riesgo. Entre las que no sufrieron ataques, la cifra se acerca más a una de cada cinco (el 23%).

Hay algunas excepciones. Por ejemplo, es más probable que las empresas de servicios financieros consideren que la ciberamenaza supone un alto riesgo (el 55% de ellas), a pesar de que el número que sufrió ataques el año pasado es de menos de la mitad (el 36%). Sin embargo, estuvieron muy cerca de la parte superior del ranking por ataques el año anterior. Por el contrario, las empresas encuestadas del sector de alimentación y bebidas, que fue el que sufrió más ataques este año, clasifican la pandemia, la escasez de habilidades y el aumento de competencia como los desafíos de mayor riesgo.

Otro indicador de la percepción del riesgo es la cantidad de dinero que las empresas de diferentes sectores gastan en ciberseguridad. Las empresas de servicios empresariales son las que más gastan con diferencia, con un promedio de €31 millones. Eso supone más de seis veces el promedio, mientras que el sector de ocio y turismo es el que menos gasta.

Las empresas expertas y los asegurados ven los riesgos

La mayoría de las empresas que obtienen la calificación de ciberexpertas muestran una conciencia elevada del peligro, al igual que el 49% de los que tienen algún tipo de cobertura ciber (para una completa comprensión de cómo funciona nuestro modelo para evaluar las personas, los procesos y la tecnología necesarios para una ciberseguridad eficaz, visite www.hiscoxgroup.com/cyber-maturity). La cantidad de empresas expertas que consideran que su exposición a los ciberataques es alta o muy alta es casi el doble que las novatas: el 59% frente al 32%. Esto se da a pesar del hecho de que han construido mejores defensas.

Es de señalar que cuatro de cada cinco empresas que no tienen cobertura ciber y que dicen que no tienen previsto obtenerla, no sufrieron un ataque en el último año. Más de la mitad son novatas (el 51%). No han pasado todavía por el cambio de percepción que experimentan por lo general las víctimas de ciberataques.

La confianza para hacer frente a los ataques de manera eficaz es mayor entre las grandes empresas y las que han sido víctimas de ataques, mientras que las empresas más pequeñas tienen que ponerse al día.

En general, el 62% de los encuestados están de acuerdo en que su organización es más vulnerable a los ataques al tener más empleados que trabajan desde casa. Entre las empresas con más de 250 empleados la cifra asciende hasta el 69%, mientras que entre las empresas expertas es del 76% y entre las novatas solo del 49% de media.

Y, ¿cuál es la realidad?

Existe cierta correlación entre la exposición al riesgo que se percibe y la incidencia de ciberataques. Como se ha mencionado anteriormente, las empresas que obtienen la calificación de expertas tienen más probabilidades de ver el alto riesgo que supone una ciberamenaza. Y tienen razón en hacerlo, porque reciben la atención de los hackers con más frecuencia que las demás, probablemente porque son objetivos más tentadores dado su tamaño relativo.

¿Qué relación guarda la percepción de las personas sobre la ciberamenaza con la probabilidad real de sufrir un ataque?

Parece ser que el paso al trabajo remoto ha cambiado el foco de los ataques. La forma principal de entrada de los hackers son los servidores de empresa, aunque también ha habido un gran aumento en el número de notificaciones de entrada a través del servidor en la nube. Esta realidad está en consonancia con la advertencia que hacen las agencias internacionales de que los ciberdelincuentes dirigen ataques cada vez más a la infraestructura de la nube.

Percepción frente a realidad
continuación

Aunque existe una percepción bastante uniforme de los diferentes tipos de ataques, la realidad enseña a las empresas dónde deben poner su foco de atención. Así, el uso indebido de recursos de TI (el 32%) y el fraude de desvío de pagos (el 31%) se posicionan como los dos tipos principales de ataques y, por tanto, parecen contar con más riesgos que la extorsión cibernética (el 19%). La conclusión, por tanto, es que las empresas puede que no estén prestando la atención necesaria para evitar los dos primeros.

Los hackers amplían su grupo de ataques

La cantidad media de ciberataques por empresa ha aumentado este año solo moderadamente: de 179 a 190. Para las grandes empresas, en cambio, ha disminuido levemente (aunque las mayores, con ingresos de más de €4.5 millones, notifican un promedio de más de 1,100). En la mayoría de los grupos de otros tamaños, ha aumentado a medida que los hackers han dirigido más su atención a las empresas medianas y pequeñas.

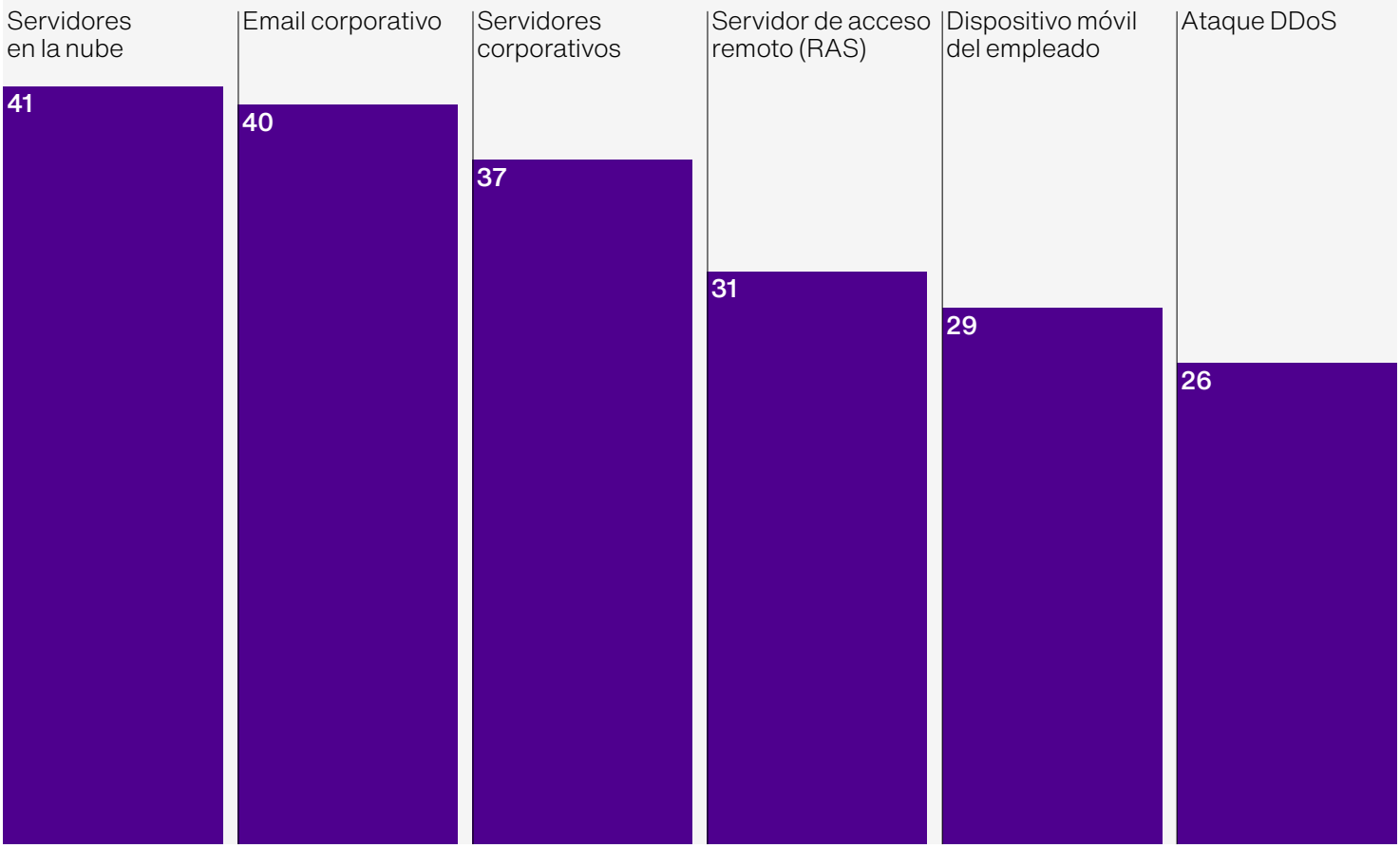
Por lo tanto, las empresas que tenían entre 250 y 999 empleados vieron aumentar el número medio de ataques de 45 a 69. Las que tenían de 10 a 49 empleados sufrieron un promedio de 56 ataques, frente a 31 del año anterior, y las más pequeñas, con menos de 10 empleados, vieron cómo se multiplicaban casi por cuatro los ataques, pasando de 11 a 40.

En las empresas con ingresos de hasta €90,000 cabe esperar aproximadamente tantos ataques como las empresas que son 100 veces mayores, en línea con las advertencias de las agencias internacionales acerca de que los extorsionadores están trasladando su foco de atención para dirigirse cada vez menos a objetivos de 'primer orden' y más a los de tamaño mediano.

También ha habido un cambio en el enfoque sectorial. Los sectores que sufrieron más ataques fueron los de ocio y turismo (en el que el 61% notificaron uno o más ataques), los servicios profesionales (el 58%) y el comercio minorista/mayorista (el 56%). Los principales objetivos del año anterior, energía y transporte/distribución, experimentaron una marcada caída en los ataques.

Método de entrada más común (%)

Los servidores en la nube son ahora la principal vía de entrada de los ciberataques.



Percepción frente a realidad
continuación

Los costes siguen aumentando
El coste mediano de todos los ciberataques sufridos por cada empresa aumentó un 30% en el último año, hasta situarse en los €15.300. Pero este porcentaje esconde una amplia gama de resultados, entre un mínimo de €8.910 en Bélgica y un máximo de €25.290 en el Reino Unido, donde los costes se duplicaron con creces. También las empresas irlandesas vieron duplicarse sus costes, hasta alcanzar los €15.120.

Una empresa del Reino Unido sufrió costes totales por ataques por importe de €6 millones. En las compañías más afectadas de Alemania, Irlanda y los Países Bajos, los costes superaron los €4,5 millones. Por el contrario, Bélgica, Francia, Alemania y España registraron costes medianos estables o más bajos.

El número de encuestados que despidieron personal tras un ataque se duplicó, pasando del 5% al 11%. A su vez, una de cada cinco empresas pagó una sanción administrativa sustancial, casi el doble que el año anterior, y una proporción similar dijo que el impacto supuso una amenaza para su solvencia (el 21%).

Las empresas inmobiliarias registraron el mayor número de ataques (319), seguidas de cerca por el sector de servicios empresariales (304). Pero las pérdidas medianas más altas las sufrió el sector minorista y mayorista, con €27,000. Les siguieron el sector energético (€21,150) y el sector farmacéutico/sanitario (€19,170).

Ransomware en aumento
Más empresas fueron víctimas de ataques por extorsión: el 19% en comparación con el 16% del año anterior. Dos tercios pagaron rescates en una ocasión (el 66%) y más de la mitad los pagaron en varias ocasiones (el 53%). Las empresas estadounidenses e irlandesas tenían más probabilidades de pagar, pero las alemanas menos. El mayor rescate que se pagó fue de poco menos de €90.000 ligeramente superior a los €85.000 del año pasado. Una anomalía extraña: el sector de alimentación y bebidas fue el que sufrió menos ataques de extorsión (solo el 14% de las empresas notificaron un ataque), pero tenía más probabilidades de pagar un rescate (el 62% de las empresas afectadas cedieron).

Algunas buenas noticias: la mediana del total de rescates pagados ha bajado un 20% y los costes de recuperación se han reducido casi a la mitad. Más empresas recuperaron o reconstruyeron sus datos a partir de copias de seguridad en varias ocasiones. Las grandes empresas (con más de 1.000 empleados) tienen más probabilidades de recuperar sus datos satisfactoriamente (el 68% en comparación con el 59% de media) y muchas menos probabilidades de que se filtren sus datos (el 20% en comparación con el 29% de media). Las firmas de servicios profesionales, que son de lejos las que más gastan en ciberseguridad (con un promedio de €30,1 millones), fueron las menos propensas a pagar (solo lo hizo el 18%).

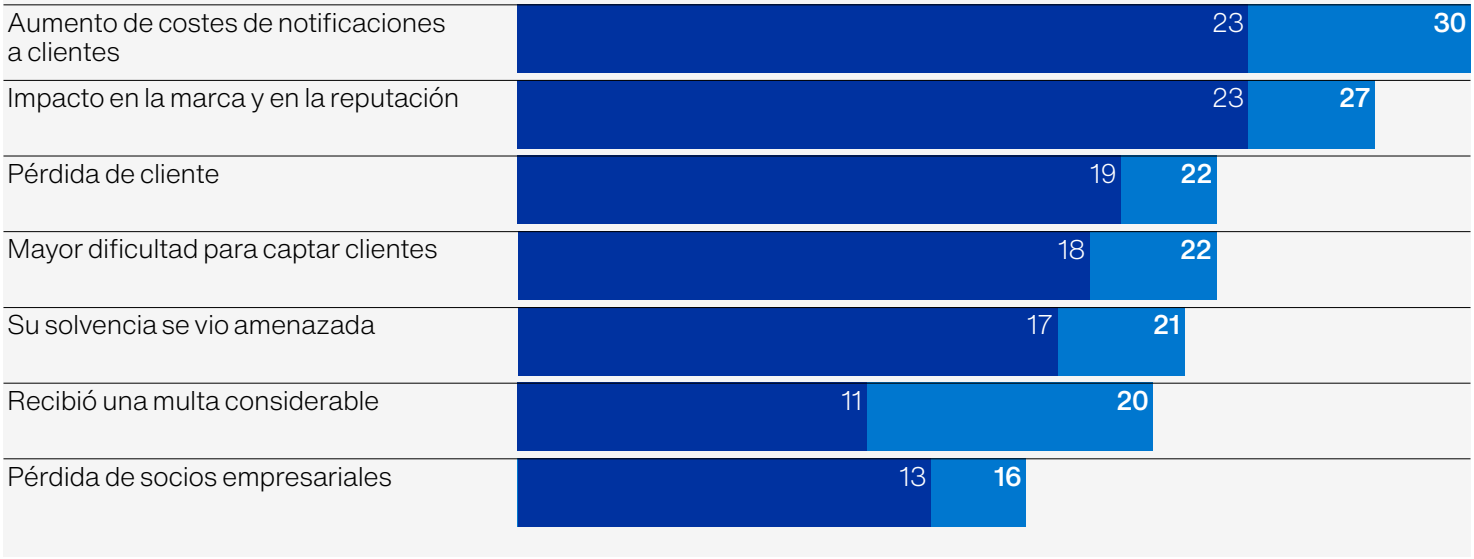
Nuevo aumento en el gasto en ciberseguridad
El gasto medio en ciberseguridad de todos los encuestados aumentó un 60% el año pasado, hasta alcanzar los €4,8 millones, experimentando un aumento del 250% desde 2019. Las firmas alemanas, las que más gastaron el año pasado, han sido sustituidas por las irlandesas, con un promedio de €12,5 millones por empresa (frente a €1,9 millones).

Sin embargo, existe una gran división entre empresas grandes y pequeñas. El gasto medio de las empresas de 250 a 999 empleados se ha duplicado en el último año. Para las grandes empresas de más de 1.000 empleados, es un 65% superior. Con casi €18 millones, su gasto medio se ha multiplicado casi por cinco en tres años.

En el otro extremo de la escala, la historia es diferente. Las empresas que tienen entre 10 y 49 empleados han reducido casi a la mitad sus presupuestos de ciberseguridad, desde €369.900 hasta €229.500. Entre aquellas que tienen menos de 10 empleados, el gasto se ha desplomado, de un promedio de €135.000 hasta solo €26.100. Es probable que esto guarde relación con la pandemia, ya que las empresas tienen menos recursos para gastar en TI. Sin embargo, ha aumentado ligeramente el porcentaje del presupuesto de TI que han gastado en ciberseguridad las compañías de este tamaño, del 17% del año pasado al 20%. Aunque tienen menos recursos disponibles, no renuncian por completo a la importancia de la ciberseguridad.

Percepción frente a realidad
continuación

Impactos de un ciberataque (%)
Los efectos de un ciberataque van mucho más allá de las consecuencias financieras directas. Más empresas descubren hasta qué punto.



¿Qué hacen las empresas expertas?

Responder a la pregunta diciendo que invierten dinero en el problema es tentador, pero eso es solo cierto parcialmente y no es la respuesta completa, porque la realidad es que hay muchos pasos que pueden seguir sin disparar su presupuesto.

Las empresas más grandes de nuestro grupo de estudio constituyen sin duda la mayor parte de las empresas que obtienen la calificación de ciberexpertas en nuestro modelo de madurez. Como tales, disfrutan de recursos sustancialmente mayores, sobre todo en la prevención contra el ciberdelito.

Sin embargo, el tamaño comporta desafíos adicionales. La empresa experta media tiene que lidiar con 41 servidores diferentes, de los cuales más de 20 probablemente estén en la nube. Como se ha indicado en varias ocasiones a lo largo del informe, esa puede ser un área de vulnerabilidad. Del mismo modo, las grandes empresas son los principales objetivos y sufren ataques con más frecuencia que las pequeñas, y eso provoca sus propias respuestas. Las empresas que experimentaron 30 o más ataques en el último año tenían presupuestos medios de ciberseguridad de más de €9 millones.

Pero la brecha de gasto existente entre las expertas y el resto se ha reducido drásticamente en el último año. Las empresas que obtienen la calificación de novatas han aumentado el gasto medio en ciberseguridad más del triple (hasta €2.9 millones), mientras que las que obtienen la calificación de intermedias han aumentado el suyo en un 63% de media. Con €5.6 millones, gastan ahora más de €900,000 que la empresa experta media.

No todo es cuestión de dinero

Afortunadamente no lo es. Las expertas lo han dejado patente en lo que respecta a la ciberseguridad. No la inventan a medida que avanzan, sino que tienen una o más funciones definidas claramente para gestionar el desafío de la ciberseguridad, y cuentan con el aval del consejo de administración o de la Dirección. La gran mayoría (el 87%) dice que los altos ejecutivos tienen una visión clara de cómo se gestiona la ciberseguridad (en comparación con el 69% en todo el grupo de estudio).

Y se abren camino por lo general a través del marco Instituto Nacional de Normas y Tecnología (NIST) del gobierno de Estados Unidos, distribuyendo la inversión y el tiempo en las cinco funciones: identificar, proteger, detectar, responder y recuperar.

Las dos iniciativas que han aumentado más fueron la creación de un plan de respuesta a incidentes y la simulación periódica de un ciberataque para probar el plan de respuesta a incidentes de la empresa. Estas actividades son especialmente sensibles en estos tiempos inciertos de conflicto europeo y sanciones occidentales. La lista de prioridades de las expertas incluye también evaluaciones periódicas de la infraestructura tecnológica y de datos de la empresa, brindando al personal formación efectiva en ciberseguridad y asegurando que los socios empresariales cumplan los requisitos de seguridad de la empresa. Hay otras muchas medidas recomendadas cuya implantación cuesta relativamente poco, y precisamente esas son las oportunidades que necesitan aprovechar las empresas. De hecho, unos dos tercios o más de las expertas afirman que implantan alguna de ellas.

Y no todo es cuestión de tamaño. Dentro de las ciberexpertas hay el mismo número aproximadamente de empresas más pequeñas (las que tienen menos de 50 empleados) que de empresas grandes (con más de 1,000). Las empresas más pequeñas no tienen previsto hacer todo lo necesario como sí han hecho las grandes, pero tampoco se quedan muy atrás. Un ejemplo: el 44% del contingente más pequeño dice que simula periódicamente un ciberataque para probar el plan de respuesta a incidentes de la empresa en comparación con lo que afirma el 58% de las grandes empresas, y en contraste con lo que dice solo el 37% de las empresas novatas.

Dedicar esfuerzos refuerza la confianza. Una de cada seis expertas dice que ha disminuido su exposición a los ciberataques en el último año. ¿Por qué? Los dos motivos principales son una mejor implantación de procesos o procedimientos de ciberseguridad, como por ejemplo parches o pruebas de penetración (según el 62% de este grupo), y el nombramiento de funciones clave de ciberseguridad o el refuerzo del equipo de personas (según el 46%).

Todas las empresas deben adoptar el enfoque metódico y estructurado de las expertas. Las respuestas coyunturales no funcionarán.

¿Qué hacen las empresas expertas?
continuación

Fuerte caída en el número de expertas
Las puntuaciones de ciberpreparación han caído un 2,6% en general, con un fuerte deterioro en la gobernanza/garantía (función de proceso) y en la presencia de personal cualificado y experimentado adecuadamente (personas). Se han realizado mejoras en herramientas y tecnología (tecnología).

Esta disminución global ha llevado a una fuerte caída en la cantidad de empresas que obtienen la calificación de expertas en nuestro modelo de ciberpreparación desde el 20% a solo el 4,5% este año. Estados Unidos y el Reino Unido siguen a la cabeza, con un 6% de las empresas con la calificación de expertas. La proporción de empresas con la calificación de novatas se ha reducido también drásticamente, dejando un gran grupo de intermedias.

Nuestro modelo de madurez ciber se basa en que las empresas evalúen ellas mismas su preparación. Dos factores parecen haber contribuido a la caída de la confianza. El principal es el descubrimiento de que la biblioteca de registro de Log4j que se utiliza ampliamente en aplicaciones y servicios en Internet era vulnerable a los ataques, hecho al que se dio mucha publicidad el 9 de diciembre del año pasado. Tras esa noticia, la proporción de los encuestados que calificaron sus mecanismos de ciberseguridad de “optimizados” cayó del 18% al 2,9% y la de aquellos encuestados que dijeron que tenían mucha confianza en su preparación en materia de ciberseguridad cayó del 73% al 67%.

Un factor que contribuye a ello puede ser la dificultad cada vez mayor de contratar a personas debidamente cualificadas, lo que se desprende de las bajas puntuaciones de las personas en nuestro modelo de ciberpreparación.

¿Qué hacen las empresas expertas? continuación

Hacer lo básico
Si tenemos en cuenta la publicidad que se ha hecho de algunos ciberataques recientes, sorprende que casi la mitad de los encuestados consideran que utilizan herramientas 'optimizadas' o 'adecuadas' para realizar copias de seguridad de datos (el 49%).

Entre las novatas, la cifra es mucho más baja (solo el 21%) y solo el 17% estaban organizadas de forma adecuada para recuperar los sistemas y datos de TI en caso de fallo del sistema.

Mientras que cuatro de cada cinco expertas tenían un planteamiento adecuado u optimizado para los controles de selección previos al trabajo, prohibiendo el uso de nuevas cuentas genéricas o el intercambio de credenciales entre los usuarios, la cifra equivalente para las novatas fue de uno de cada cinco, o menos. Hacer bien lo básico es crucial y tiene un coste relativamente bajo, especialmente en comparación con el coste que supone hacer frente a un ataque de extorsión cibernética.

Reforzar las defensas tras los ataques
Cuando se les preguntó sobre cómo respondieron a los ciberataques, dos de cada cinco expertas dicen que implantaron requisitos adicionales de auditoría y ciberseguridad (el 41%), que intensificaron la formación de los empleados (el 39%) y que mejoraron su preparación para ciberataques (el 39%). Las cifras son generalmente más altas entre las empresas grandes.

Las pequeñas empresas que obtienen la calificación de expertas están a la cabeza en lo que respecta a la primera de estas medidas: más de la mitad dice que han implantado requisitos adicionales de ciberseguridad después del ataque. Del mismo modo, la mayoría de ellas han contratado un proveedor de respuesta a incidentes, aunque esto es una evidencia del hecho de que las grandes empresas ya cuentan con ayuda externa o no necesitan más.

Protección del seguro ciber
Tomando todo el grupo de estudio, más de un tercio de las empresas con 250 o más empleados tienen una póliza de ciberseguridad independiente (el 35%), y el 40% tiene cobertura de ciberseguridad como parte de otra póliza. Por debajo de ese umbral, las cifras equivalentes son del 28% y el 29%. La pertinencia de la protección es obvia para las empresas más pequeñas que no pueden emplear grandes equipos de especialistas en ciberseguridad, sobre todo porque la evidencia pone de manifiesto que las empresas pequeñas están cada vez más en la línea de fuego, como se ha expuesto en otras partes del informe.

Considerando el grupo de estudio en su conjunto, los tres motivos principales para obtener cobertura de ciberseguridad son la capacidad de adquirir experiencia, la gestión de crisis y el análisis pericial de TI (por detrás de las preocupaciones sobre la seguridad de los datos y un poco por delante de la necesidad de mostrar a los clientes que la empresa se toma la protección de ciberseguridad en serio). Pero entre las expertas, que son las que tienen generalmente experiencia interna, el segundo motivo es la preocupación de que en el caso de sufrir un ataque los clientes podrían presentar una reclamación en su contra. En total, el 46% de las expertas tiene actualmente una póliza de seguro ciber independiente (en comparación con el 31% de media y el 29% de las novatas).

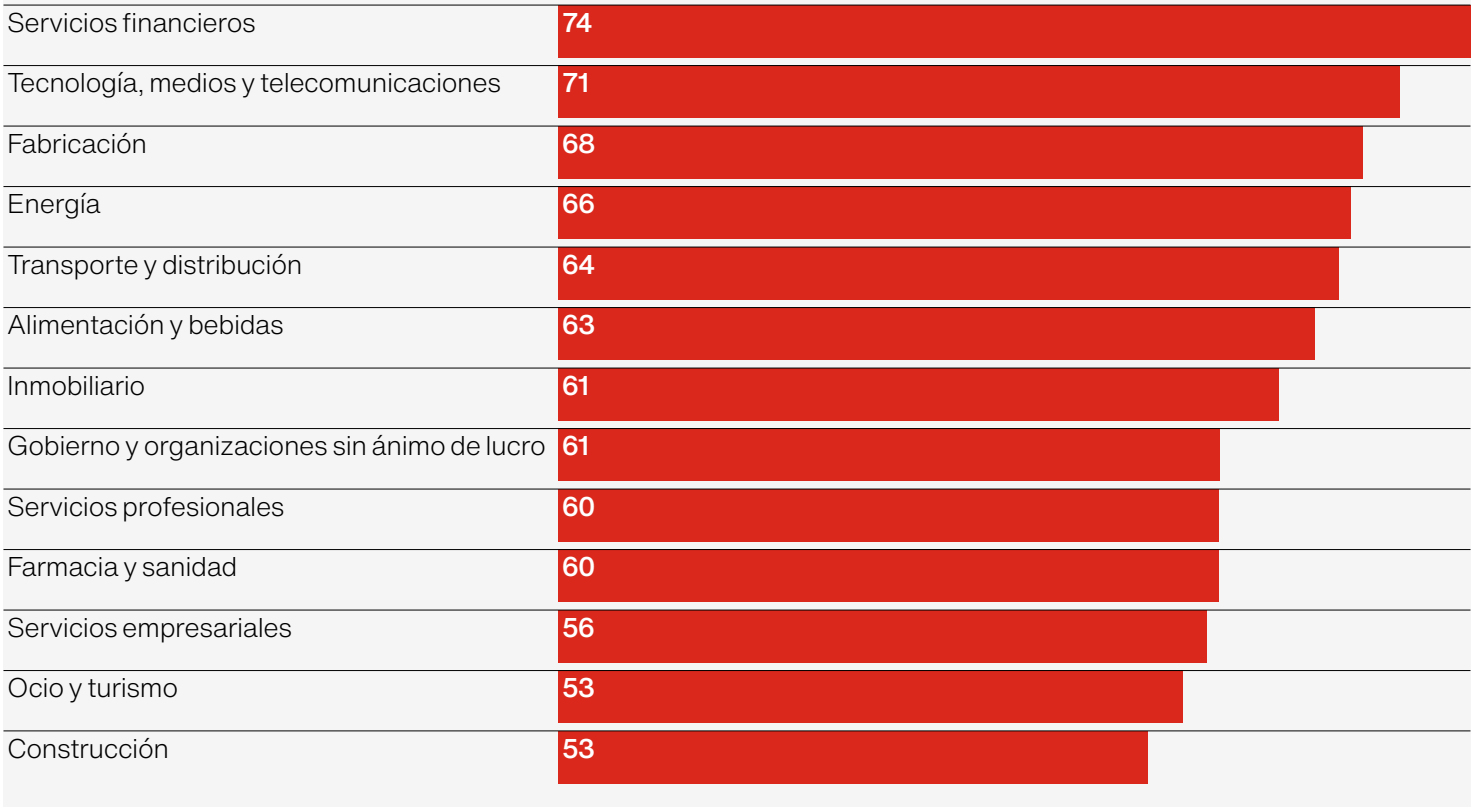
No es de extrañar que la adopción de seguros ciber sea más alta en el sector de servicios financieros, en el que el 74% tienen cobertura a través de una póliza independiente o como parte de una póliza más amplia, y otro 18% dice que tiene previsto obtener cobertura pronto. Las empresas de construcción y turismo se encuentran en el otro extremo del espectro: el 53% de ambos sectores tiene algún tipo de cobertura ciber.

Cabe destacar que las empresas aseguradas tienen más probabilidades de responder a un ciberataque aumentando sus defensas que las empresas no aseguradas. Uno de los motivos que explica esta diferencia es el hecho de que la propia aseguradora que les respalda les pregunte si han mitigado ciertas amenazas o si les han ayudado a solucionar un problema tras un ataque anterior.

Las expertas han respondido también de forma más decidida a los desafíos de la pandemia. Es mucho más probable que hayan aumentado el trabajo remoto, adoptado tecnologías colaborativas y basadas en la nube, cambiado los pagos en línea y acelerado sus planes de transformación digital.

¿Qué hacen las empresas expertas?
continuación

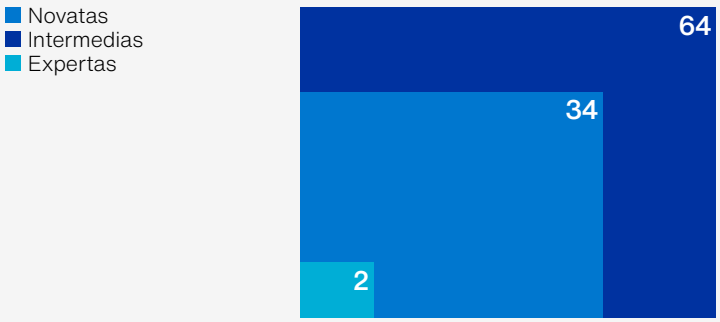
Adopción del seguro ciber por sector (%)
Como una póliza independiente o como parte de otra póliza.



Datos por países

Bélgica

Madurez ciber (%)

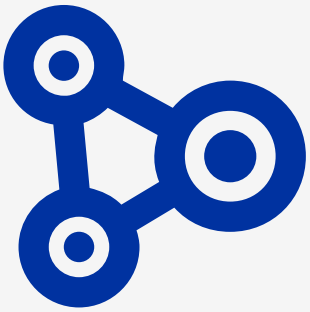


+10%

Mala publicidad e impacto negativo en la marca incrementó un 10% en los dos últimos años.

x2

Las empresas que pusieron en peligro la seguridad de terceros se duplicaron desde el año pasado hasta alcanzar el 24%.

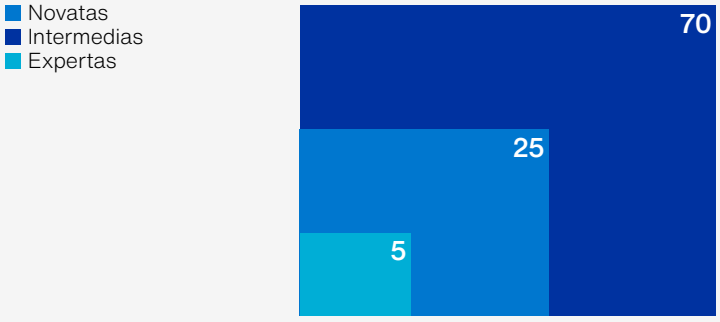


Las tres prioridades de gasto principales

1. Abordar las amenazas y vulnerabilidades existentes.
2. Lograr o mantener el cumplimiento normativo.
3. Mejorar la seguridad del servicio y las aplicaciones orientadas al cliente.

Francia

Madurez ciber (%)



24%

El porcentaje de las empresas cuya solvencia se vio amenazada gravemente por un ataque.

#1

Motivo principal para invertir en ciberseguridad: preocupación por la seguridad de los datos.

Las tres prioridades de gasto principales

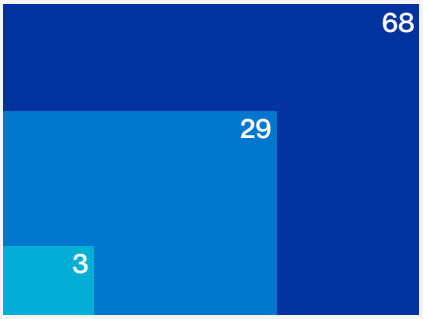
1. Abordar las amenazas y vulnerabilidades existentes.
2. Lograr o mantener el cumplimiento normativo.
3. Mejorar la seguridad de los servicios y aplicaciones orientados al cliente.

Datos por países
continuación

Alemania

Madurez ciber (%)

- Novatas
- Intermedias
- Expertas

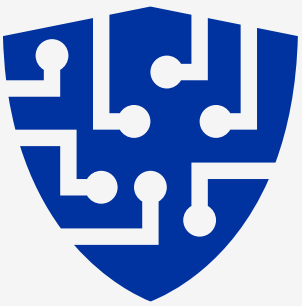


€3,1m

El mayor ciberataque sufrido el año pasado.

27%

El porcentaje de empresas que compraron o mejoraron un seguro ciber después de un ataque.



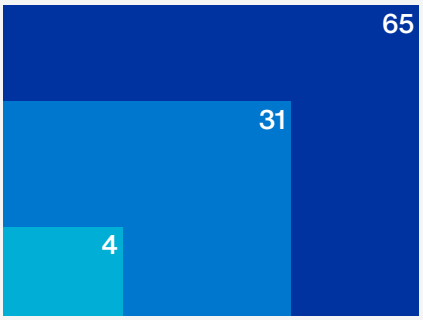
Las tres prioridades de gasto principales

1. Formación y concienciación efectivas sobre ciberseguridad para los empleados.
2. Mejorar la seguridad de los servicios y aplicaciones orientados al cliente.
3. Políticas y procedimientos internos de ciberseguridad.

Irlanda

Madurez ciber (%)

- Novatas
- Intermedias
- Expertas



#1

Motivo principal para invertir en ciberseguridad: el miedo al coste de una posible infracción.

34%

El porcentaje de las empresas que compraron o mejoraron un seguro ciber después de un ataque (un 24% más que el año pasado).

Las tres prioridades de gasto principales

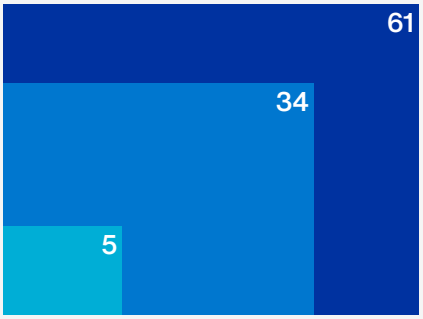
1. Formación y concienciación efectivas sobre ciberseguridad para los empleados.
2. Implantar escaneos de vulnerabilidad del entorno.
3. Cumplir los requisitos de seguridad de los socios.

Datos por países
continuación

Países Bajos

Madurez ciber (%)

- Novatas
- Intermedias
- Expertas

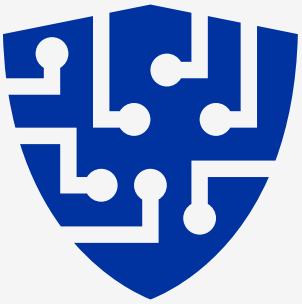


€2m

El mayor ciberataque sufrido el año pasado.

x3

Las empresas neerlandesas que compraron o mejoraron un seguro ciber después de un ataque en comparación en los últimos 12 meses se triplicaron.



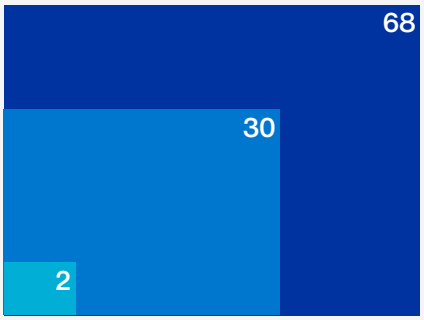
Las tres prioridades de gasto principales

1. Abordar las amenazas y vulnerabilidades existentes.
2. Garantizar que los socios cumplan los requisitos de seguridad.
3. Mejorar la seguridad del servicio y las aplicaciones orientadas al cliente.

España

Madurez ciber (%)

- Novatas
- Intermedias
- Expertas



#1

Motivo principal para invertir en ciberseguridad: preocupación por la seguridad de los datos.

x2

Las empresas que han perdido clientes como consecuencia de ataque se duplicó con creces en los últimos dos años.

Las tres prioridades de gasto principales

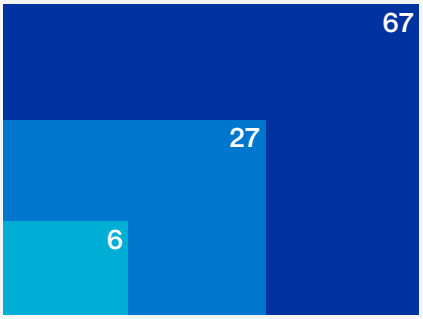
1. Abordar las amenazas y vulnerabilidades existentes.
2. Mejorar la seguridad del servicio y las aplicaciones orientadas al cliente.
3. Conseguir o mantener el cumplimiento normativo.

Datos por países
continuación

Reino Unido

Madurez ciber (%)

- Novatas
- Intermedias
- Expertas



x2

Las empresas que tuvieron una sanción sustancial por una infracción se duplicaron con creces en el último año.

20%

Porcentaje de empresas cuya solvencia se vio amenazada gravemente tras un ataque.

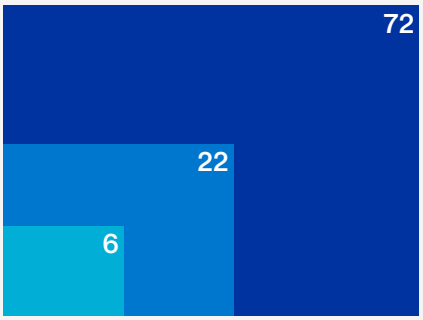
Las tres prioridades de gasto principales

1. Abordar las amenazas y vulnerabilidades existentes.
2. Lograr o mantener el cumplimiento normativo.
3. Cumplir los requisitos de seguridad de los socios.

Estados Unidos

Madurez ciber (%)

- Novatas
- Intermedias
- Expertas



29%

El porcentaje de las empresas tuvieron mayores dificultades para atraer nuevos clientes tras un ataque.

#1

Motivo principal para invertir en ciberseguridad: mitigar las reclamaciones de los clientes tras un ataque.

Las tres prioridades de gasto principales

1. Abordar las amenazas y vulnerabilidades existentes.
2. Realizar evaluaciones de ciberseguridad de la infraestructura de datos y tecnología.
3. Cumplir los requisitos de seguridad de los socios.

Principales prioridades de gasto

Las empresas parecen estar volviendo a lo básico tras dos años de pandemia y varias vulnerabilidades a gran escala. Se están centrando en las amenazas existentes (asegurándose de que los dispositivos estén parcheados y actualizados), además de garantizar que las políticas y los procedimientos estén actualizados, en especial probando los planes de respuesta a incidentes. Por último, están combatiendo los ataques de phishing (el método de entrada más frecuente para los ataques de extorsión cibernética) impartiendo formación en ciberseguridad en sus organizaciones.

Grandes empresas (más de 1 000 empleados)
✓ Abordar las amenazas y vulnerabilidades existentes
✓ Lograr y/o mantener el cumplimiento normativo
✓ Revisar las políticas y procedimientos internos de ciberseguridad
✓ Mejorar la seguridad de los servicios y aplicaciones orientados al cliente
✓ Establecer o implantar un marco formal de gestión de ciberseguridad de tecnología/TI

Pequeñas empresas (de 0 a 49 empleados)
✓ Abordar las amenazas y vulnerabilidades existentes
✓ Lograr y/o mantener el cumplimiento normativo
✓ Implantar sistemas para detectar personal, conexiones, dispositivos o software no autorizados
✓ Garantizar que los socios empresariales/terceros cumplan los requisitos de seguridad
✓ Implantar escaneos de vulnerabilidad del entorno

La lista no es exhaustiva y en ella se indican únicamente algunas de las prioridades principales de las empresas de acuerdo con la investigación realizada. Dicha lista de verificación no constituye una recomendación por parte de Hiscox, ni garantiza que si una empresa completa la misma sea completamente cibersegura.

Hiscox encargó a Forrester Consulting que evaluara la ciberpreparación de las empresas. En total, se encuestó a 5.181 profesionales responsables de la estrategia de ciberseguridad de sus organizaciones respectivas (a más de 900 de Estados Unidos, de Reino Unido, de Francia y de Alemania; a más de 400 de Bélgica, de España y de Países Bajos; y a más de 200 en Irlanda). Los encuestados completaron la encuesta online entre el 30 de noviembre de 2021 y el 21 de enero de 2022.

La composición completa de los encuestados se detalla a continuación.

Nivel (%)	
Fundador/Ejecutivo de nivel C	32
Vicepresidente	23
Director	34
Gerente	12

Sector (%)	
Servicios empresariales	9
Construcción	7
Energía	4
Servicios financieros	9
Alimentación y bebidas	4
Gobierno y organizaciones sin ánimo de lucro	5
Fabricación	8
Farmacia y sanidad	8
Servicios profesionales	9
Inmobiliarias	4
Minorista y mayorista	8
Tecnología, medios y telecomunicaciones (TMT)	18
Transporte y distribución	5
Ocio y turismo	3

Departamento (%)	
Dirección ejecutiva	12
Comercio electrónico	3
Finanzas	9
Asesoramiento jurídico	4
Recursos humanos	5
TI y tecnología	19
Marketing y comunicaciones	5
Operaciones	10
Propietarios	18
Adquisiciones	3
Gestión de productos	4
Gestión de riesgos	4
Ventas	4

Número de empleados (%)	
1,000+	25
250-999	15
50-249	15
10-49	19
1-9	26

Hiscox España

c/ Miguel Ángel, 11 4º planta
28010 Madrid

+34 915 15 9900
info_spain@hiscox.com
hiscox.es/hiscox-cyber-readiness-report-2022

22054 05/22