Informe de Ciberpreparación de Hiscox 2023

HISCOX

Contenidos

Ilustración de portada: johnholcroft.com
Diseño de informes: somethingbrighter.com

Introducción

El informe de este año revela varios cambios en el panorama ciber que merece la pena destacar para cualquier persona que esté interesada en contrarrestar a los ciberdelincuentes.

Eddie Lamb
Director de Formación y Asesoramiento Cyber Hiscox

Una de las estadísticas más escalofriantes de este año es el claro aumento de la proporción de pequeñas empresas atacadas: hasta el 36%. Esto supone un aumento de la mitad en los últimos tres años. Ser una empresa pequeña no implica ser invisible a los ojos de los ciberdelincuentes. Sin embargo, lo más alentador es que el informe también muestra que las empresas más pequeñas han aumentado el gasto a un ritmo mucho más rápido que las demás, lo que puede ayudar a contrarrestar los crecientes ataques.

En la parte más alta del grupo encuestado, aumentó el número de empresas que sufrieron pérdidas de siete cifras este año. Pero la buena noticia es que los costes medianos de todo el grupo encuestado fueron contenidos. Esto refleja en parte una tendencia cada vez mayor al fraude, como el desvío de pagos a través del correo electrónico corporativo, que suele requerir menos conocimientos técnicos pero produce recompensas menores. La creciente prevalencia de los seguros ciber también puede haber desempeñado su papel aquí, y es que casi tres cuartas partes de las empresas atacadas contaban con algún tipo de cobertura ciber.

Los ataques con ransomware se han mantenido estables y la proporción de los que pagan un rescate ha disminuido ligeramente este año. En los casos en los que se pidió un rescate, la principal razón por la que las empresas pagaron fue para impedir que se divulgaran datos confidenciales. Esto marca un sutil cambio del cifrado de datos a la exfiltración de datos por parte de los ciberdelincuentes, algo que se refleja en nuestros propios datos de siniestros. Cada vez hay más pruebas de que el trato con los extorsionadores es un asunto de aciertos y errores, ya que menos de la mitad de las empresas que pagaron recuperaron todos sus datos.

A pesar del continuo aumento de los ciberataques, hay algunos aspectos positivos que se pueden extraer del informe de este año. Justificado o no, se observa una notable mejora en la actitud con un descenso en la proporción de empresas que ven la ciberseguridad como el reto número uno para su negocio. Esto puede deberse al aumento de otros problemas, en particular, la recesión económica; pero también es un reflejo del aumento de los presupuestos de ciberseguridad, de una mejor aplicación de las medidas de seguridad y de una mayor implicación de los consejos de administración, o simplemente que la ciberseguridad se ha convertido en un peligro que hay que gestionar de manera adecuada como cualquier otro riesgo empresarial.

Aumentar los niveles de concienciación y comprensión del desafío de la ciberseguridad es uno de los objetivos de este informe y también es una parte esencial de nuestro papel como aseguradora. La Hiscox CyberClear Academy ofrece formación online en materia de ciberseguridad para los empleados de nuestros clientes, con alrededor de 36.000 personas de 7.000 organizaciones que han realizado el curso desde 2017. Dado el número de personas que siguen siendo víctimas de correos electrónicos de phishing (que sigue siendo la principal vía de entrada de los ataques de ransomware), la formación de concienciación reiterada debe ser una prioridad para todas las empresas con presencia material en Internet.

También esperamos que este informe ayude a las empresas a medir su propia resiliencia a la ciberamenaza y a comparar su nivel de preparación con el de sus homólogas. Para hacerlo de manera más formalizada, te invitamos a visitar nuestro modelo interactivo de ciberpreparacion. Puede comparar su organización por tamaño, sector y país con más de 16.000 empresas. La batalla contra los ciberdelincuentes es interminable, pero la preparación es la clave para defenderse de los ataques y limitar los posibles daños a la empresa.

Resumen ejecutivo

La mayoría denuncian ataques

Los ciberataques aumentaron por cuarto año consecutivo: un 53% de las empresas sufrieron ciberataques, frente a un 48% que los sufrieron el año pasado.

Cambio de actitud

Sólo cinco de ocho países consideran ahora la amenaza cibernética como el principal riesgo empresarial. Las cuestiones económicas y la competencia adquieren mayor protagonismo.

El coste de los ataques disminuye

La mediana de los costes para las empresas atacadas disminuyó ligeramente, de casi 15.640€ a poco más de 14.766€.

Los grandes ataques aún suceden

Una de cada ocho empresas atacadas sufrió costes de 230.000€ o más.

Las empresas más pequeñas son las más afectadas

En tres años, el porcentaje de empresas atacadas con menos de diez empleados aumentó más de la mitad, hasta un 36%.

El fraude, principal amenaza

Una de cada tres empresas atacadas sufrió pérdidas económicas debido a fraude por desvío de pagos.

Resistencia al ransomware

Una de cada cinco empresas recibió una petición de rescate, pero aquellas que lo pagaron cayeron de un 66% a un 63%; menos de la mitad de las que pagaron recuperaron todos datos.

El gasto en seguridad aumenta

La mediana del gasto en ciberseguridad ha crecido un 39% en los últimos tres años, hasta alcanzar los 142.600€. En las empresas con menos de diez empleados esta cifra se ha cuadruplicado en dos años.

El eslabón más débil

Los ciberdelincuentes prefirieron atacar a través del correo electrónico de la empresa, seguido de un servidor corporativo o en la nube.

Cibersensibilidad

El riesgo ciber continúa siendo la principal preocupación para las empresas, pero comienzan a vislumbrarse atisbos de optimismo.

El factor miedo disminuye

¿Están las empresas aprendiendo a convivir con la amenaza ciber? La exposición a los ciberataques continúa primera en la lista de preocupaciones de las empresas entre nuestros encuestados, pero este año se ha producido un cambio visible para mejor en la percepción de amenaza. El porcentaje de empresas que identifican la amenaza ciber como de alto riesgo ha descendido este año de un 45% a un 40%, aunque esto debe contrastarse con una mejora general de la confianza en todas las categorías de riesgo empresarial. La amenaza ciber queda por delante de problemas económicos como la recesión, la inflación o los tipos de cambio (38%) y la aparición de un nuevo competidor (36%).

Aunque la amenaza ciber continúa siendo percibida como el principal peligro en la mayoría de sectores empresariales, varias industrias (servicios empresariales, construcción, transporte, alimentación y bebidas y ocio y turismo) ahora consideran más importantes las cuestiones económicas.

Siete de cada ocho países consideraron la amenaza cibernética como el mayor riesgo el año pasado. La cifra ha caído a la quinta posición este año, aunque esta sigue estando entre los principales tres riesgos en todos los países excepto en Bélgica. Allí, riesgos como la escasez de talento, la pérdida económica y la competencia tienen prioridad. Este es otro indicador que sugiere que algunas empresas sienten ahora mismo que existen otros riesgos que suponen una amenaza igual o mayor que la ciber.

Principales riesgos empresariales (%)

		2023	2022
1.	Exposición a un ciberataque	40	45
2.	Pérdidas debidas a problemas económicos (por ejemplo, inflación)	38	40
3.	Aparición de nuevos competidores	36	36
4.	Escasez de personal cualificado	35	40
5.	Escasez de personal cualificado	35	37
6.	Cambios normativos o legislativos	34	37
7.	Pandemias o enfermedades infecciosas	33	42
8.	Conflictos geopolíticos que alteran las operaciones	33	–
9.	Fraude y delitos de guante blanco	32	38
10.	Clima extremo y catástrofes naturales	29	33

Mas empresas consideran estar a la altura del reto
El porcentaje de empresas que afirman que su riesgo ciber ha disminuido creció de un 12% a un 16%. Opinan que esto se debe a una mejor ejecución de sus procesos de ciberseguridad y a presupuestos más elevados. Este año, un mayor número de grandes empresas han señalado también una mayor sensibilización por parte de los consejos de administración. Más de dos de cada cinco (41%) de los que afirman que su exposición a los ataques ha disminuido mencionan una mayor implicación del consejo de administración, lo que se traduce en una mejora en la gestión o transferencia de riesgos (es decir, seguros ciber).

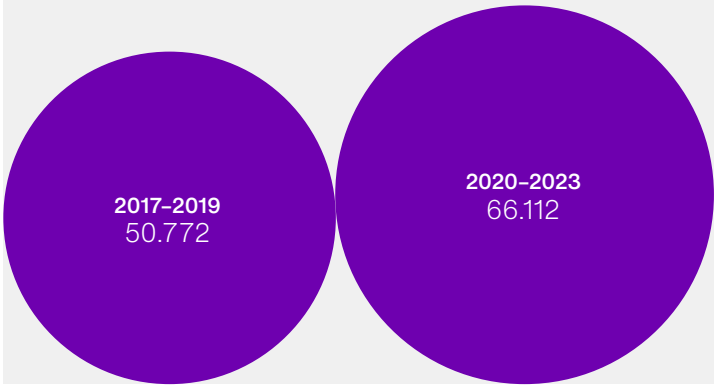
Pero el riesgo ciber sigue muy presente, sobre todo para quienes perciben que este va en aumento. Casi un tercio (32%) de los que consideran que la exposición al riesgo ha aumentado en los últimos 12 meses opinan que el motivo es el incremento del número de empleados que trabajan de manera remota. Esta preocupación fue mayor entre las grandes empresas con más de 250 trabajadores (35%) que entre las pequeñas (30%), aunque las últimas fueron ligeramente más propensas a preocuparse por que sus empleados hicieran uso de sus propios dispositivos (un 27% mencionaron esto frente a un 26% de las compañías más grandes). Por ello, los controles son más importantes que nunca.

El aumento de los parches genera preocupación
También preocupa cada vez más la capacidad de seguir el ritmo del volumen de parches de proveedores que son necesarios implementar. Más de una de cada cinco (22%) empresas grandes lo consideran un motivo de mayor riesgo cibernético, frente a un 16% el año anterior. El parcheado es necesario para corregir las brechas de seguridad del software u optimizar el rendimiento. Las vulnerabilidades y exposiciones comunes (CVE) han aumentado un 30% si se compara la media de los últimos tres años frente a los tres años anteriores.

Si bien es cierto que las vulnerabilidades del software han existido siempre, durante los últimos cinco a diez años los escáneres automáticos, los programas de detección de errores, los investigadores y el crowdsourcing han mejorado la detección y las notificaciones públicas.

Una vez detectados, las compañías de software deben proporcionar parches: los organismos reguladores y/o las compañías de seguros exigen entonces a las empresas que utilicen el software expuesto que apliquen los parches correspondientes. El parcheado constante y las actualizaciones de sistema son especialmente desafiantes para las grandes empresas, en las que la gestión de parches es, a menudo, compleja.

Vulnerabilidades ciber y exposiciones totales
Media de tres años



Confianza impulsada por la experiencia de ataques
Casi la mitad (48%) de los que sufren ciberataques consideran la amenaza como de alto riesgo. Sin embargo, de manera similar al año pasado, las grandes empresas y aquellos que han sufrido ataques confían más en la capacidad de sus empresas de lidiar con un ataque, así como en el enfoque del gobierno frente a la amenaza. Creen más tanto en los factores internos (como su tecnología, la participación del consejo administrativo) como en los externos (autoridades reguladoras, gobierno) para aportar un ambiente seguro o ayudar a minimizar los daños.

Las empresas pequeñas dudan más de su preparación
Las empresas pequeñas se quedan atrás en lo que se refiere a niveles de confianza. Solo tres de cada cinco empresas (61%) con menos de 250 empleados dicen sentirse seguras de su preparación en temas de ciberseguridad. La cifra equivalente para las empresas más grandes es de un 71%. Además, los encuestados de empresas más pequeñas están menos seguros de que su dirección ejecutiva dé prioridad a la ciberseguridad y tienden más a cuestionar si su tecnología informática está a la altura de las circunstancias.

La menor brecha entre las empresas grandes y pequeñas se da en la cuestión del daño a la marca si los datos de los clientes y socios no se gestionan de manera segura. En esto coinciden inequívocamente, con un 72% de las grandes empresas y un 70% de las pequeñas de acuerdo o muy de acuerdo.

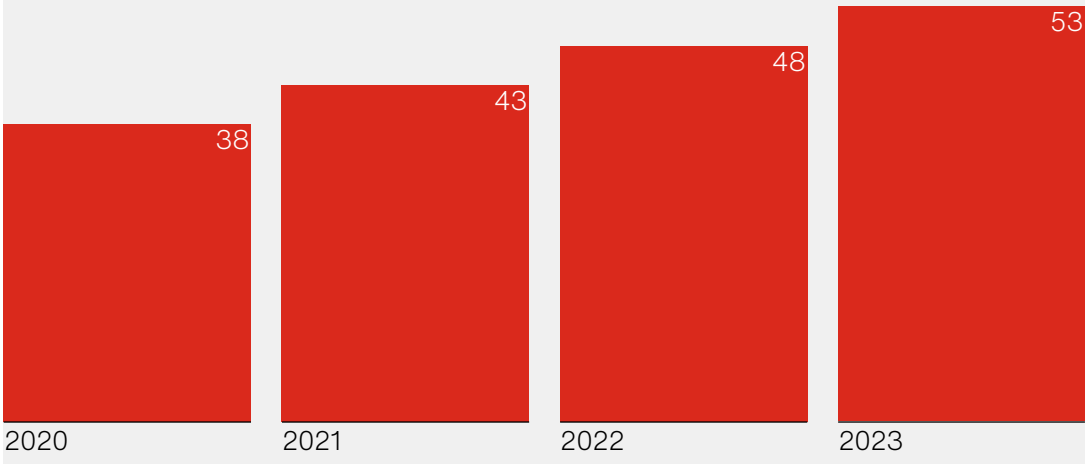
La realidad de la amenaza ciber

El alcance y la intensidad de los ataques aumenta, pero el impacto económico permanece bajo control.

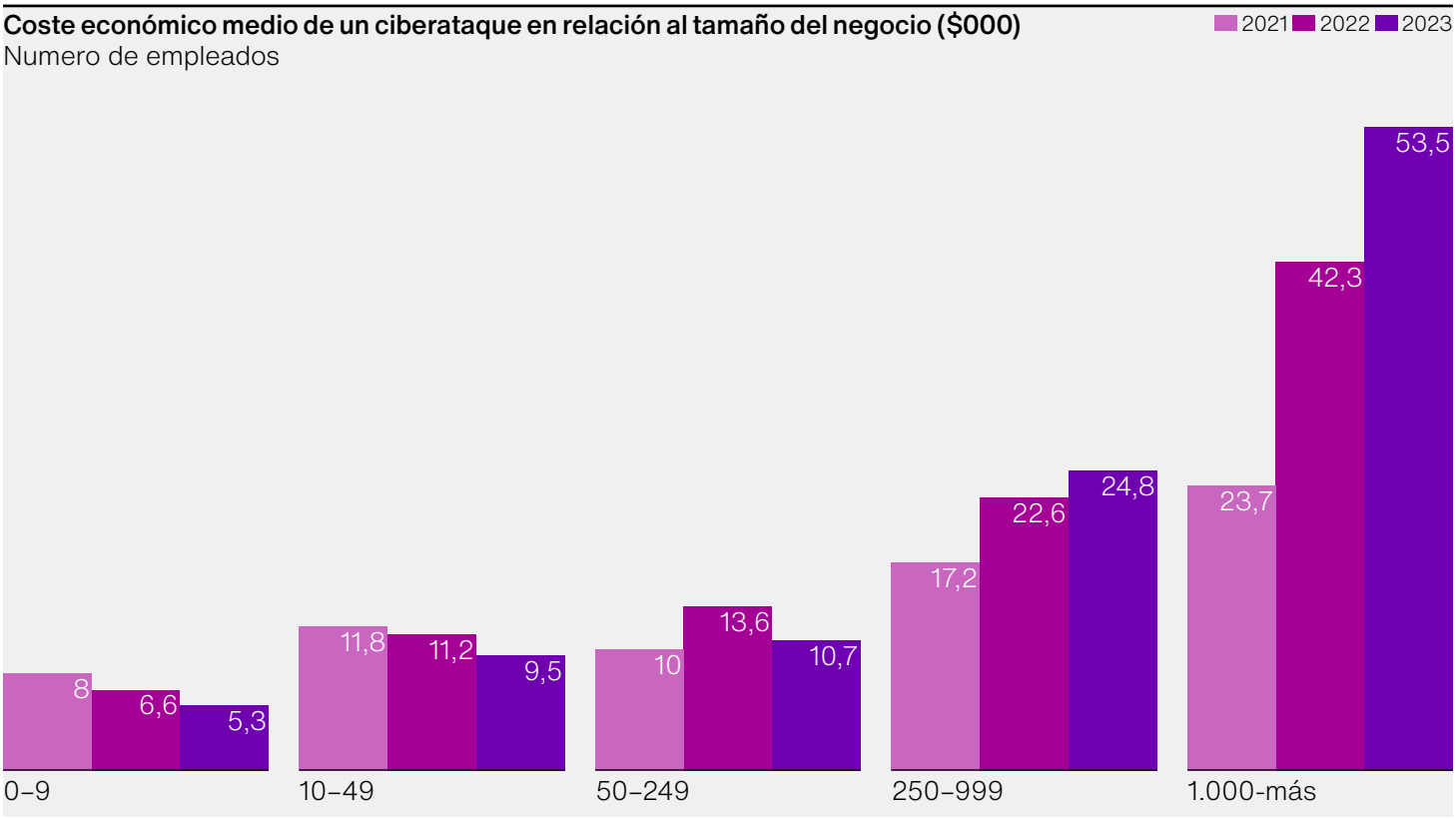
Las empresas más pequeñas quedan atrapadas en la red
El porcentaje de firmas que denuncian uno o más ciberataques ha crecido por cuarto año consecutivo, hasta un 53%, con respecto al 48% del año pasado, a la vez que la intensidad de los ataques ha aumentado radicalmente. Las empresas declaran una mediana de siete ataques, una subida con respecto a los cuatro del año pasado.

Esas cifras solo cuentan parte de la historia. Para las empresas más grandes (aquellas con 1.000 o más empleados) los ciberataques se han convertido en el día a día: siete de cada diez (70%) denuncian al menos uno, con respecto al 62% hace un año. Sin embargo, este no es un problema exclusivo de las grandes compañías. En los últimos tres años, el número de empresas con menos de diez empleados que experimentaron ataques ha aumentado de un 23% a un 36%. Aunque los pequeños negocios pueden manejar los costes de manera más efectiva y están empezando a invertir más en ciberseguridad, existe un riesgo claramente en aumento que las pequeñas empresas deben tomar en serio.

Empresas que sufrieron al menos un ciberataque (%)



Coste económico medio de un ciberataque en relación al tamaño del negocio ($000)
Numero de empleados



El impacto económico se mantiene
A pesar de esto, el impacto económico de los ciberataques ha caído ligeramente año tras año, lo que sugiere que las empresas siguen mejorando a la hora de identificar y frenar los ataques. Hubo un ligero aumento en el número de empresas que consiguieron defenderse con éxito frente a un ataque (un 8% comparado con un 7% el año anterior).

Considerando las cifras de la mediana, el coste de los ataques ha descendido de algo menos de 15.640€ a poco más de 14.720€ por cada empresa atacada. La mediana del mayor ataque individual también cayó de 6.118€ a 4.922€. Sin embargo, estas cifras ocultan una amplia gama de resultados: desde 1.968€ para empresas con hasta nueve empleados hasta 9.844€ para empresas con más de 1.000 empleados.

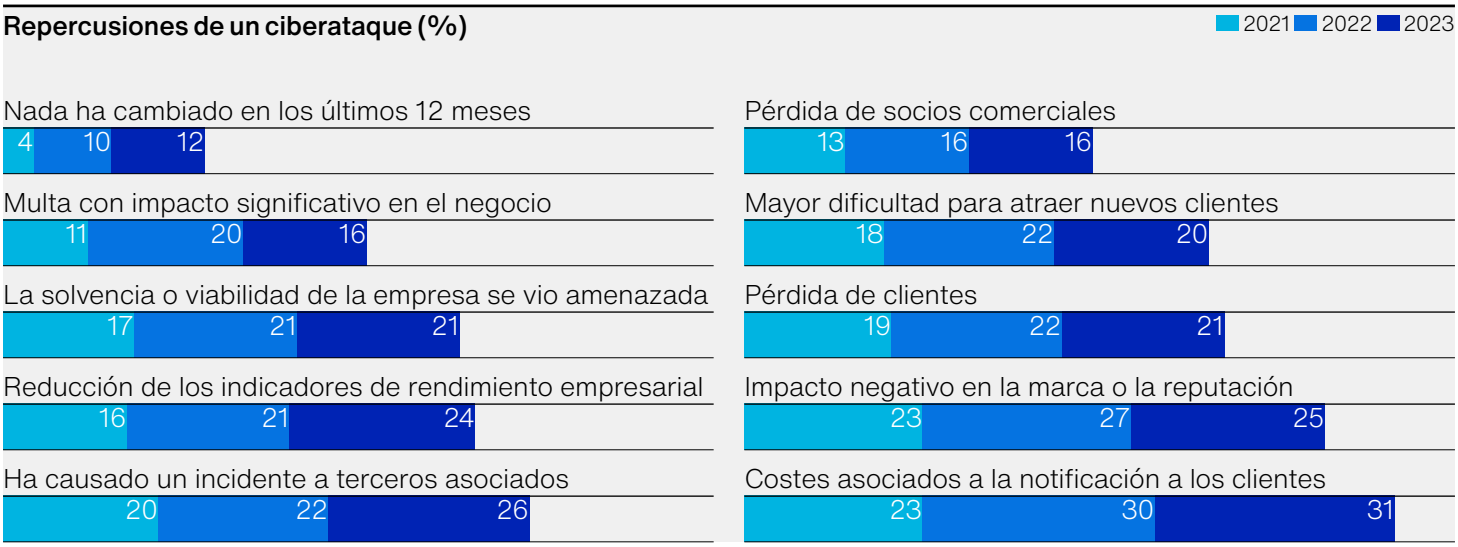
En nuestro informe de 2022, tan solo cuatro empresas reportaron costes de ciberataques por encima de los 4,6 millones de euros. Este año encontramos ocho empresas en ese rango y tres en el de 9,2 millones de euros o más. Una de cada ocho empresas (12%) sufrieron costes de 230.000€ o más.

Las empresas pequeñas son mejores gestionando los costes
Las cifras de este año son alentadoras. Las empresas más pequeñas están haciendo un buen trabajo a la hora de gestionar los costes de los ciberataques. Las empresas de las dos categorías de tamaño más bajo han visto caer los costes medianos dos años seguidos. Es tanto más notable en cuanto que la incidencia de los ataques ha aumentado para las pequeñas empresas en los últimos tres años, al igual que para las grandes. Sin embargo, los costes continúan aumentando para las empresas en las dos primeras categorías. Para los negocios con más de 1.000 empleados, los costes de los ciberataques han aumentado un 125% en dos años, quedando en torno a los 49.220€.

Los costes varían mucho en función del sector
Cuatro sectores asumieron costes medianos de 18.400€ o más: fabricación, transporte y distribución, energía (que ha figurado entre los tres objetivos principales en cada uno de los tres últimos años) y gobierno y organizaciones sin ánimo de lucro. Tanto el sector de transporte y distribución como el de gobierno y organizaciones sin ánimo de lucro vieron un incremento significativo de los costes año a año (28% y 83% respectivamente). Los fabricantes informaron del mayor coste mediano de pérdidas para el peor ataque individual, que alcanzó los 6.587€.

Las buenas noticias son que la mayoría de industrias han conseguido controlar o reducir el coste mediano del mayor ataque individual que sufrieron. Para las compañías energéticas, la cifra disminuyó de más de 10.120€ a poco menos de 6.440€ en dos años. Para la industria de la alimentación y bebidas, ha disminuido en más de la mitad, hasta 4.140€.

Repercusiones de un ciberataque (%)



Vulnerabilidades e impactos

El punto de entrada favorito de los ciberdelincuentes fue, una vez más, el correo electrónico corporativo, según mencionan un 35% de las empresas atacadas (y un 40% de los encuestados del gobierno y organizaciones sin ánimo de lucro). Los servidores corporativos, tanto de empresa (mencionado por un 31%) como en la nube (mencionado por un 29%) obtuvieron el segundo y tercer puesto. Pero en ambos casos, estos porcentajes fueron bastante más bajos que el año anterior, lo que sugiere que el trabajo de prevención está surtiendo efecto.

El sector energético parece ser particularmente propenso a las infiltraciones en un servidor de empresa. El sector de la construcción encabeza la lista de industrias golpeadas por infiltraciones en servidores en la nube, junto con el sector de ocio y turismo y el tecnológico. El resultado más común de un ciberataque fue la pérdida económica debido al fraude por desvío de pagos (mencionado por un 34% de las firmas atacadas, con respecto al 28% de hace dos años). La pérdida de datos y los ataques de virus bajaron por segundo año consecutivo.

Algunas de las repercusiones de los ciberataques se han dejado sentir este año más que nunca. Cerca de un tercio (31%) de las empresas atacadas informaron de un aumento de costes por notificar a los clientes de un ataque, una cifra que aumenta por segundo año consecutivo. Lo mismo ocurre con aquellos que informan de una infiltración para terceras partes (en ascenso durante dos años de un 20% a un 26%).

Cabe destacar que el escenario catastrófico no está tan lejos como podríamos creer. Una de cada cinco empresas (21%) atacadas dijo que el impacto fue suficiente para amenazar la viabilidad del negocio. Este fue también el caso para una quinta parte de las empresas muy pequeñas (aquellas con menos de diez empleados).

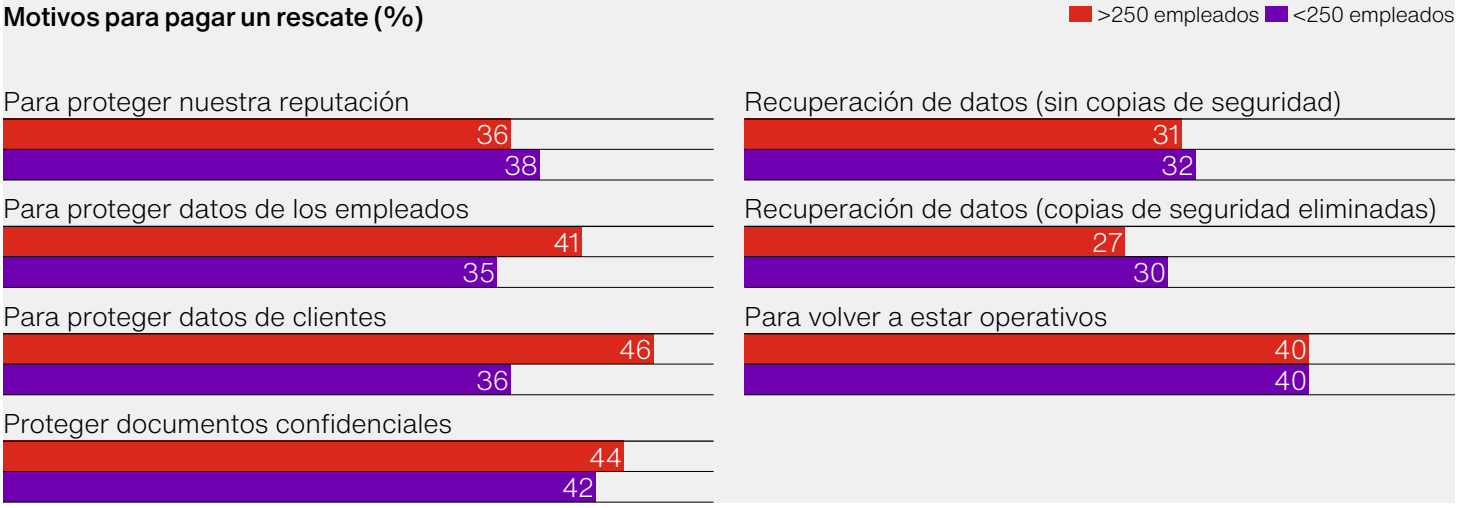
Datos por país: Irlanda destaca

¿Qué países fueron los más vulnerables? En términos de número de empresas atacadas, Irlanda destaca este año con más de siete de cada diez empresas (71%) como objetivo, una tercera parte más que la media del grupo de estudio en su totalidad. Las empresas irlandesas también fueron atacadas casi tres veces más a menudo que la mediana, y fueron mucho más propensas a ser atacadas con ransomware (30% comparado con un 20% de media en el grupo de estudio). Culpa del servidor: más de la mitad de los encuestados en Irlanda afirmaron que el primer punto de entrada fue el servidor de la empresa (57%) o el servidor en la nube (50%).

En términos financieros, los países peor parados fueron el Reino Unido (con costes medianos por empresa de 22.264€), los Países Bajos (19.688€) y Estados Unidos (18.400€). Para las empresas estadounidenses y británicas, la infiltración en el correo electrónico empresarial encabezó la lista (mencionado por un 38% y un 37% respectivamente).

Hubo un despunte significativo del número de empresas alemanas que denunciaron ataques, de un 46% a un 58%, con un número mediano de ataques por empresa que subió de seis a diez. En contraste, dos países (Bélgica y Países Bajos) vieron una caída en la mediana de ataques. Puede ser relevante el hecho de que Países Bajos fuera el único país en nuestro estudio que aumentó su puntuación media en ciberpreparación en nuestro modelo de madurez de este año.

Motivos para pagar un rescate (%)



Ransomware: una amenaza constante

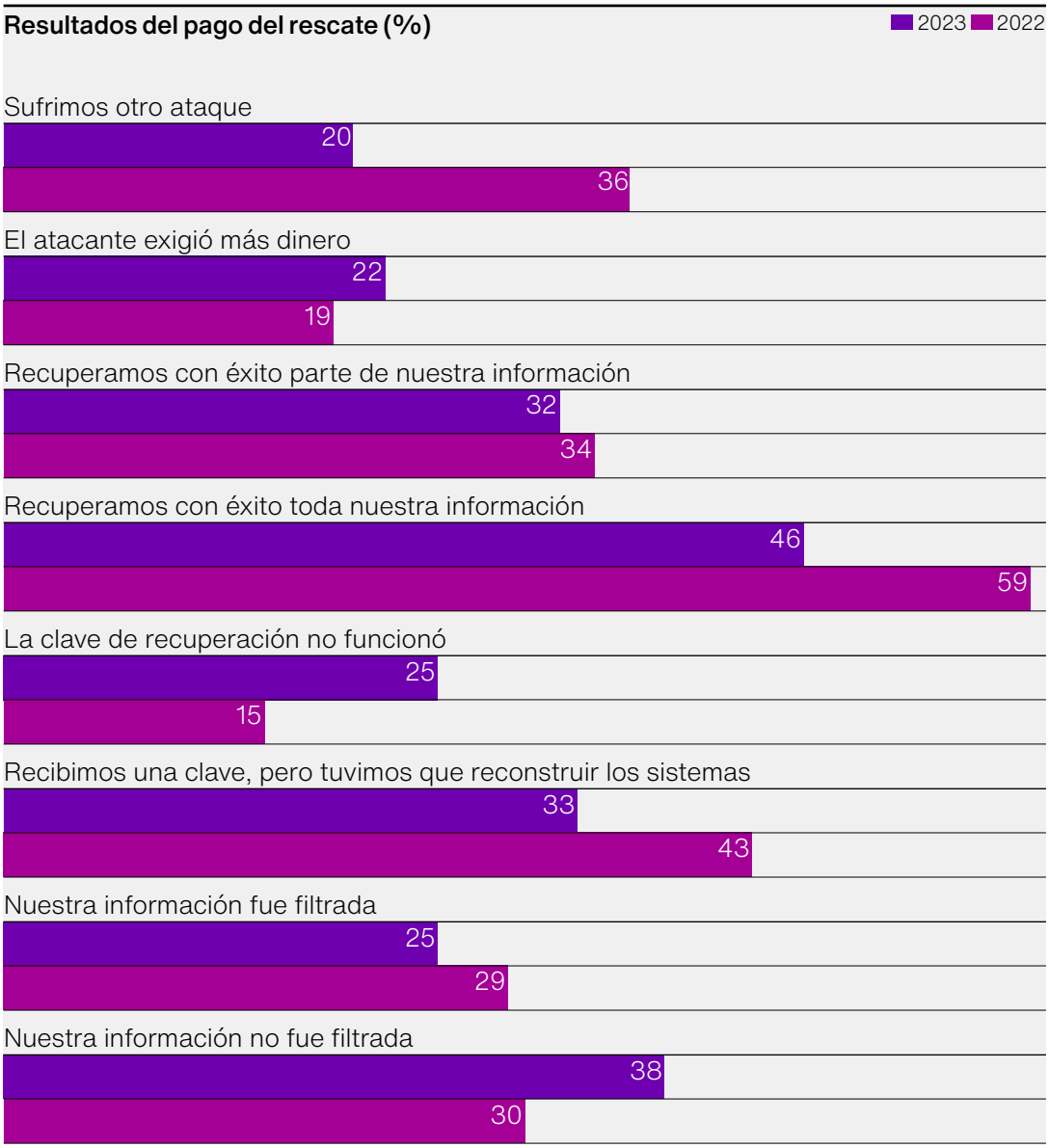
Una de cada cinco empresas atacadas (20%) recibieron una petición de ransomware, cifra ligeramente superior al 19% del año anterior. El porcentaje que pagó por el rescate cayó de un 66% a un 63%, pero el rescate mediano creció un 13% hasta alcanzar los 9.844€. Sobre esta misma base, el coste medio de las recuperaciones cayó ligeramente, hasta los 4.968€. La cantidad máxima pagada fue de 492.200€, aunque la cifra mediana para el mayor ataque individual fue de 4.922€, por lo que creció con respecto a los 3.680€ del año anterior. Los principales motivos aportados para el pago del rescate fueron la protección de información interna confidencial (43%) o de los datos de clientes (42%). Esta última fue la razón más destacada entre las grandes empresas para pagar el rescate.

La principal vía de entrada de los hackers fue, una vez más, mediante correos electrónicos de phishing (mencionados por un 63% de las víctimas). Por tercer año consecutivo, el phishing ha sido de lejos la fuente principal de los ataques de ransomware, y el segundo método más común de entrada sigue siendo el robo de credenciales. La defensa frente a ambos comienza con la formación de los empleados: el ransomware nunca es algo sencillo, pero formar a los empleados para que utilicen contraseñas complejas, protejan sus credenciales mediante la autenticación de múltiples factores (MFA) y la formación sobre phishing resultan ser formas relativamente sencillas y baratas de mitigar el riesgo para las empresas de cualquier tamaño.

¿Fue rentable el pago?

En muchos casos, no. El porcentaje de víctimas que afirman haber recuperado con éxito todos sus datos tras pagar fue tan solo de un 46%, una cifra inferior con respecto al 59% del año anterior. Alrededor de un tercio (32%) dijeron haber recuperado parte de sus datos, pero en una cuarta parte de los casos, los datos fueron filtrados o la clave de recuperación no funcionó. Además, una de cada cinco empresas (20%) volvió a sufrir otro ataque.

Resulta alentador que este año hayan sido más las empresas que han recuperado sus datos a partir de copias de seguridad (46%), aunque casi un tercio de las atacadas (32%) declararon que pagaron porque no tenían una. Esta cifra es superior al 26% del año anterior. Para aquellos con notas bajas en nuestro modelo de madurez, la principal razón para pagar un rescate fue el volver a estar operativos (44%), lo que significa que aquellos menos preparados tienen pocas opciones además de pagar. Es fundamental para que su negocio vuelva a funcionar. Pero mientras que tan solo un 46% de las empresas recuperaron toda su información después de pagar y un 22% recibieron una demanda mayor por parte de los atacantes, ¿es este un riesgo que merezca la pena correr? Cuando se trata de ciberseguridad, tener mayor madurez nos permite recuperarnos del ransomware sin pagar o al menos mitigar el ataque desde el inicio.


Resultados del pago del rescate (%)
2023
2022
Sufrimos otro ataque
20
36
El atacante exigió más dinero
22
19
Recuperamos con éxito parte de nuestra información
32
34
Recuperamos con éxito toda nuestra información
46
59
La clave de recuperación no funcionó
25
15
Recibimos una clave, pero tuvimos que reconstruir los sistemas
33
43
Nuestra información fue filtrada
25
29
Nuestra información no fue filtrada
38
30

Caso real
Paralización instantánea del negocio

Ataque ransomware
Comenzó como un día de trabajo normal en Autobedrijf de Pee, un taller de reparación de vehículos alemán. La persona encargada de la recepción no se encontraba en la empresa, por lo que el propietario, Arjan de Pee, se estaba encargando de revisar los correos electrónicos. Vio un e-mail de KPN, la empresa de telefonía móvil, con una factura adjunta y lo abrió con la intención de imprimirla. De pronto, todo se volvió negro.

"*Todos los sistemas fallaron*", cuenta. "*Todo lo que se veía era una pantalla negra con texto blanco, como en la época inicial de DOS.*"

Siguientes pasos
Arjan intentó reducir el daño y desconectó el cable de red de inmediato. No surtió efecto, todos los archivos habían sido encriptados de forma permanente. "*En cada carpeta había un archivo de texto que decía que todos los documentos estaban bloqueados y que solo se desbloquearían con un pago en Bitcoin*", explica.

Arjan llamó a su compañía de TI. Actuaron de inmediato y pudieron reinstalar los programas, por lo que en tan solo una hora el negocio estaba funcionando otra vez.

El coste
El daño económico se limitó a tener que pagar por la ayuda de la compañía informática y a la instalación de algunas medidas de ciberseguridad adicionales. Pero el daño emocional fue considerable. "*Nuestra empresa existe desde hace 34 años y he perdido todas las fotos del día de la apertura. Nunca las recuperaré*", declara.

Aprendizajes clave
Todo esto ha hecho llegar un mensaje que Arjan considera importante para otros empresarios: "*Es inteligente tomar medidas extraordinarias para proteger tus pertenencias*", incluidas las digitales.

Ahora, Arjan protege los datos de sus clientes con controles de acceso y se asegura de que la información crítica tenga copia de seguridad y esté guardada por separado. Los cibercriminales todavía pueden atacar, pero al menos existe otra barrera que protege la información personal de los clientes. "*Además, ahora les pido a los clientes que solo proporcionen la información personal necesaria*."

Más información
Arjan tiene más consejos para los empresarios. Uno, planifica qué ocurre si fallan todos tus ordenadores. ¿Cómo puedes conseguir que tu negocio vuelva a estar operativo lo más rápido posible? ¿Qué hace falta para ello? ¿Y cómo pueden iniciarse los procesos operativos offline? Dos: aprende a prevenir un ciberataque y compártelo con todos tus empleados, u ofréceles formación en temas cibernéticos. Empieza por cosas pequeñas, como utilizar contraseñas largas y complejas en todos los ordenadores.

Construyendo resiliencia
Prepara una estrategia proactiva – y apóyala con inversión.

¿Cómo deberían las empresas fortalecerse contra un ciberataque?
Existen dos maneras de abordar la gestión del riesgo ciber. La primera es una actitud proactiva y la segunda es una actitud reactiva o defensiva. Las empresas de nuestro grupo de estudio se sitúan mayoritariamente en el primer bando. Casi la mitad (48%) están motivadas principalmente por impulsores positivos, mientras que solo el 6% se inclina más por los impulsores reactivos o negativos. Las motivaciones positivas principales incluyen querer asegurar a los clientes que la empresa se toma la ciberseguridad en serio (27%) y evitar las interrupciones operacionales (26%). Las motivaciones negativas se centran en cumplir con los requisitos regulatorios (25%) o actuar porque los clientes lo exigen (17%).

La misma actitud proactiva se extiende a las empresas más pequeñas (las que tienen menos de 50 empleados), pero en este caso el factor más destacado es el deseo de evitar la interrupción de la actividad. Las empresas que no sufrieron ningún ataque este año son más propensas a estar motivadas de manera positiva, con un 56% de las firmas no atacadas actuando con proactividad, comparado con un 42% de las firmas atacadas. Entonces, si la mentalidad proactiva es la mejor, ¿en qué deberían centrarse las empresas?

¿Qué factores predicen un ciberataque?

Una evaluación de la madurez ciber indica cómo de efectivos son los controles de seguridad a la hora de gestionar los riesgos a los que se enfrenta la empresa. Cuanto más maduras sean las defensas de una empresa, mejor equipada está para prevenir un ciberataque o minimizar su impacto.

Aunque un ciberataque no es totalmente predecible, si analizamos los ámbitos clave de la ciberseguridad dentro del modelo de madurez ciber de Hiscox de este año, la falta de atención a estos diez atributos de madurez puede indicar un posible ataque.

- Realización de pruebas de penetración y evaluaciones de vulnerabilidad.
- Comprobación de vulnerabilidades en el nuevo software.
- Aplicación de la autenticación multifactor (AMF).
- Agregación/almacenamiento centralizado de datos de incidentes de seguridad.
- Inspección de las comunicaciones cifradas.
- Proporcionar redes privadas virtuales (VPN).
- Identificación de nuevos activos de hardware/software y datos en la red.
- Detección de comunicaciones sospechosas.
- Arreglo de vulnerabilidades de seguridad.
- Supervisión/análisis de datos sobre incidentes de seguridad.

¿Qué hacen las expertas?

Las ciberexpertas son empresas que obtienen una puntuación superior a cuatro sobre cinco en el modelo. Siguen siendo pocas las que alcanzan la cifra: solo el 3% este año (Ver los resultados completos de la evaluación de este año en la página 14). Las compañías energéticas poseen proporcionalmente más expertas (6%), seguidas por servicios financieros y el gobierno (4%).

Las empresas más grandes son las que menos probabilidades tienen de encontrarse en el grupo con menor puntuación (las novatas). Tan solo un 20% de las empresas con 1.000 o más empleados son novatas, frente a un 42% de las pequeñas (1 a 9 empleados). Además, hay un 1% menos de trabajadores remotos en las empresas expertas.

Cabe destacar que una de las diferencias principales de las empresas clasificadas como expertas es la implicación a nivel del consejo administrativo en el esfuerzo de ciberseguridad. Un 86% afirman que la administración superior posee una visión clara de cómo gestionar la ciberseguridad, mientras que tan solo un 57% de las novatas hace la misma afirmación.

Principales acciones de nuestras empresas ciberexpertas

Menos de 250 empleados

✓	Asegurar la autenticación multifactorial para el acceso sensible o privilegiado a los sistemas informáticos, como el acceso a información personal identificable (PII), el acceso remoto y las funciones de administración de sistemas.
✓	Control de las comunicaciones entre dispositivos conectados en red, por ejemplo, usando un cortafuegos basado en host como Windows Defender.
✓	Asistencia en la identificación y eliminación proactivas de software malicioso, usando antivirus (AV) o detección y respuesta de puntos finales (EDR).
✓	Realizar copias de seguridad para asegurar una fuente remota que elimine la posibilidad de una pérdida irrecuperable de información.
✓	Gestionar el ciclo vital de los parches de software y las actualizaciones necesarias para los sistemas y programas informáticos.

Más de 250 empleados

✓	Identificación y eliminación proactivas de software malicioso, como antivirus (AV) o detección y respuesta de puntos finales (EDR).
✓	Centralizar y almacenar la información sobre eventos de seguridad.
✓	Apoyar, permitir o reforzar la codificación de datos guardados en dispositivos portátiles tales como smartphones y ordenadores portátiles.
✓	Revisar las comunicaciones codificadas que entran y salen de los sistemas, por ejemplo, bloqueando contenido potencialmente peligroso.
✓	Asegurarse de que cada usuario tiene una identificación y/o nombre de usuario consistente y única en todos los sistemas informáticos.

Gasto mediano derivado en ciberseguridad (€)
Número de empleados

	1-9	10–49	50–249	250–999	1.000-más
2023	7.452	44.068	135.884	848.424	4.592.732
2022	4.232	32.476	55.384	863.696	5.060.000
2021	1.840	18.400	54.556	327.336	2.300.000

El vínculo con los presupuestos de ciberseguridad
Naturalmente, el dinero también se considera importante. Los presupuestos más elevados para riesgos ciber son razones de peso para sentirse más animados ante una ciberamenaza. Un 45% de las empresas grandes que afirman que su exposición a los ciberataques ha disminuido señalan a los presupuestos más elevados y las mejores soluciones para la reducción de riesgo como el motivo. Esto es frente a un 36% el año anterior.Esto plantea una pregunta obvia: ¿existe un vínculo entre el tamaño de los presupuestos y la reducción de los ciberataques? Este año, existen razones para creerlo.

Como mencionábamos antes, las empresas más pequeñas habían conseguido controlar el coste mediano de los ciberataques a pesar de su mayor intensidad. Al mismo tiempo, las compañías más pequeñas en los rangos de 1-9, 10-49 y 50 a 249 empleados han aumentado su gasto mediano de forma material: en un 77%, 36% y 145% respectivamente. En un plazo de dos años, las empresas con menos de diez empleados han cuadruplicado su gasto mediano en ciberseguridad. En contraste, en la cabeza de la lista (empresas con 250 o más empleados), el gasto mediano se ha recortado este año. Aquí, el impacto financiero de los ataques ha seguido aumentando.

Si echamos un vistazo a los datos por países, podemos ver que las empresas belgas gastaron menos en ciberseguridad que cualquier otro grupo (55.986€ de mediana, con respecto a los 132.480€ del año anterior). Las pérdidas medianas por ciberataques casi se duplicaron y un 62% de los encuestados afirmaron tener costes de 9.200€ o más (casi el doble de la media del grupo de estudio). Por el contrario, las empresas alemanas son las que más invierten (con una mediana de 196.880€) y vieron sus pérdidas reducidas de 19.320€ a 14.766€ ese periodo. Una cosa es segura: las expertas en nuestra encuesta tienden a invertir una parte más grande de sus presupuestos informáticos en ciber: 25% de media, frente al 23% de media de las ciberintermedias y menos del 22% de las novatas.

El dinero es solo una parte de la ecuación de los recursos
El número de personas que se necesitan para contrarrestar una amenaza ciber también es relevante. Las empresas belgas, irlandesas y estadounidenses encabezan esta sección con una media de 97, 95 y 84 personas en su equipo de ciberseguridad, respectivamente. Están muy por delante de los demás. Sin embargo, tras estas medias se esconde una estadística interesante: un 15% de las empresas estadounidenses y británicas carecen de puestos de gestión dedicados a la ciberseguridad. Esto puede compararse con un 8% de las empresas alemanas, por ejemplo. EE. UU y el Reino Unido resultan ser dos de los tres países más perjudicados en la encuesta de este año.

La existencia de un responsable dedicado a la ciberseguridad es una de las diferencias clave entre las expertas y las demás. Tan solo un 4% de las empresas expertas de este año carecían de un puesto dedicado a ciberseguridad. Esto contrasta con más de una cuarta parte (27%) de las novatas. Muchas de ellas son empresas más pequeñas para las que esto es claramente un problema de recursos. Más de un tercio (34%) de las empresas con menos de diez empleados afirmaron no tener un puesto definido para la ciberseguridad. Esta cifra cayó hasta un 9% entre las empresas de 10 a 49 empleados. Sin embargo, y lo que quizá sea más preocupante, las empresas más pequeñas también se quedan atrás en áreas como colocar seguridad adicional o formar a sus empleados tras un ataque.

La importancia de la transferencia de riesgos

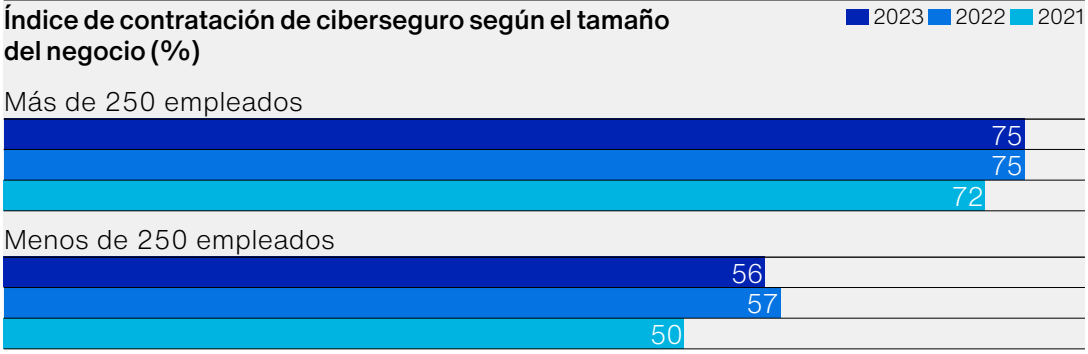
Una de las grandes diferencias entre expertas y novatas en nuestro grupo de estudio es la voluntad de responder a ataques con acciones positivas, tales como implementar mejores procesos o procedimientos (44% de las expertas dicen haberlo hecho el año pasado, frente a un 30% de las novatas). Una de las acciones clave es transferir el riesgo contratando un seguro ciber.

Hay una correlación cercana entre el experimentar un ataque y decidir asegurarse. Casi tres cuartos de los atacados (73%) poseen una póliza única de seguro ciber o cobertura dentro de otra póliza. Esto contrasta con algo más de la mitad (52%) de las que no han sufrido ataques. Las empresas con ciberseguro también son más propensas a tomar nuevas medidas para mejorar la seguridad tras un ataque: 36% comparado con el 29% de las no aseguradas.

Un 42% de las expertas aseguran tener una póliza de seguro ciber, mientras que un 36% adicional afirman tener coberturas dentro de otra póliza. En contraste, las cifras equivalentes para las novatas son tan solo un 24% y 26%. Más de una de cada cinco de las novatas dicen no tener planes de contratar un ciberseguro. Las empresas más pequeñas (hasta 250 empleados) se quedan atrás con respecto a las grandes en lo que se refiere a contratación de seguros.

Existe un amplio abanico de motivos para contratar una póliza única, pero entre las expertas, la razón principal es una: demostrarles a los clientes presentes y futuros que la empresa es cuidadosa con la ciberprotección. Casi la mitad de las expertas (46%) citan esta razón (la mitad que la media, una vez más).

Índice de contratación de ciberseguro según el tamaño del negocio (%)



Evaluación global de cibermadurez 2023

Nuestro modelo de ciberpreparación mide la alineación de las empresas con las mejores prácticas en seis ámbitos a lo largo de tres áreas funcionales. El sistema de puntuación es sobre cinco, y cualquier puntuación por encima de cuatro clasifica a las empresas como 'ciberexpertas'. Entre 2,51 y 3,9, se consideran 'ciberintermedias' y por debajo del 2,5, se consideran 'cibernovatas'.

	Personas	Proceso	Tecnología	Media
Gestión de la resiliencia empresarial	2,90	2,93	3,00	2,94
Criptografía y gestión de claves	2,78	2,73	2,86	2,79
Gestión de identidades y accesos	2,99	2,81	2,85	2,87
Seguridad y gestión de eventos	2,86	2,78	2,69	2,85
Gestión de amenazas y vulnerabilidades	2,89	2,91	3,28	3,03
Gestión de la confianza	2,93	2,98	3,02	2,98
Media	2,89	2,85	2,94	2,90

Caso real
El seguro juega un papel esencial

Paralización total
No se aprecia por completo la importancia de un ciberseguro hasta que no se sufre un ciberataque. Esta fue la lección clave aprendida por los propietarios de Schäfer Trennwandsysteme GMBH, una empresa mediana del pintoresco Westerwald alemán, después de que sus sistemas informáticos dejaran de funcionar un jueves cualquiera por la mañana.

Mientras todo estaba paralizado, encontraron un archivo de lectura en cada carpeta indicándoles que todos sus archivos de datos habían sido encriptados. Los administradores de la empresa estaban anonadados, cómo podían imaginar que podrían ser objetivo de los ciberdelincuentes. La empresa no contaba con ninguna patente ni con información confidencial, pero, lo que es más importante, tenían contratado un ciberseguro con Hiscox.

Siguientes pasos
El socio de respuesta de Hiscox intervino con dos coaches de crisis y, con la ayuda de este equipo, la actividad de la empresa pudo reanudarse rápidamente.

Además, el socio de respuesta contactó con un equipo de expertos forenses informáticos que trabajaron en averiguar por dónde había accedido el atacante. ¿Dónde estaba el malware? El equipo de respuesta se adentró en las profundidades del sistema de la firma y fueron capaces de entender qué había pasado mirando en los archivos de registro.

Este ejemplo cuenta la experiencia de un asegurado de Hiscox. Schäfer Trennwandsysteme GMBH no formó parte de los datos de investigación para el Informe de Ciberpreparación de Hiscox.

Obligaciones legales
La protección de datos era un problema porque era imposible saber si se había filtrado información personal o no.

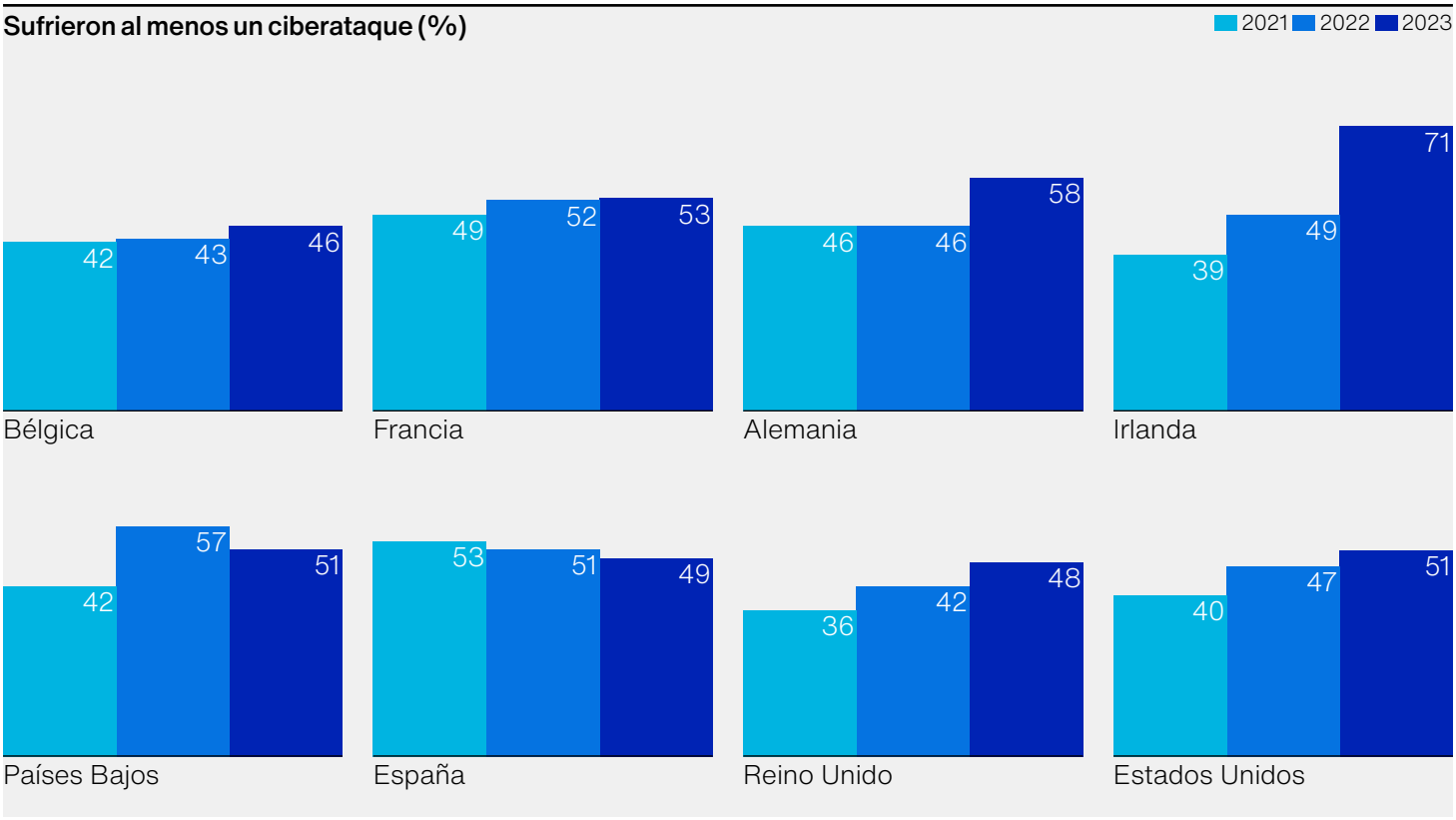
Hiscox puso a disposición de la empresa un bufete de abogados que colaboró con el responsable externo de protección de datos de la propia empresa, quien a continuación presentó un informe ante el responsable de protección de datos del estado de Renania-Palatinado.

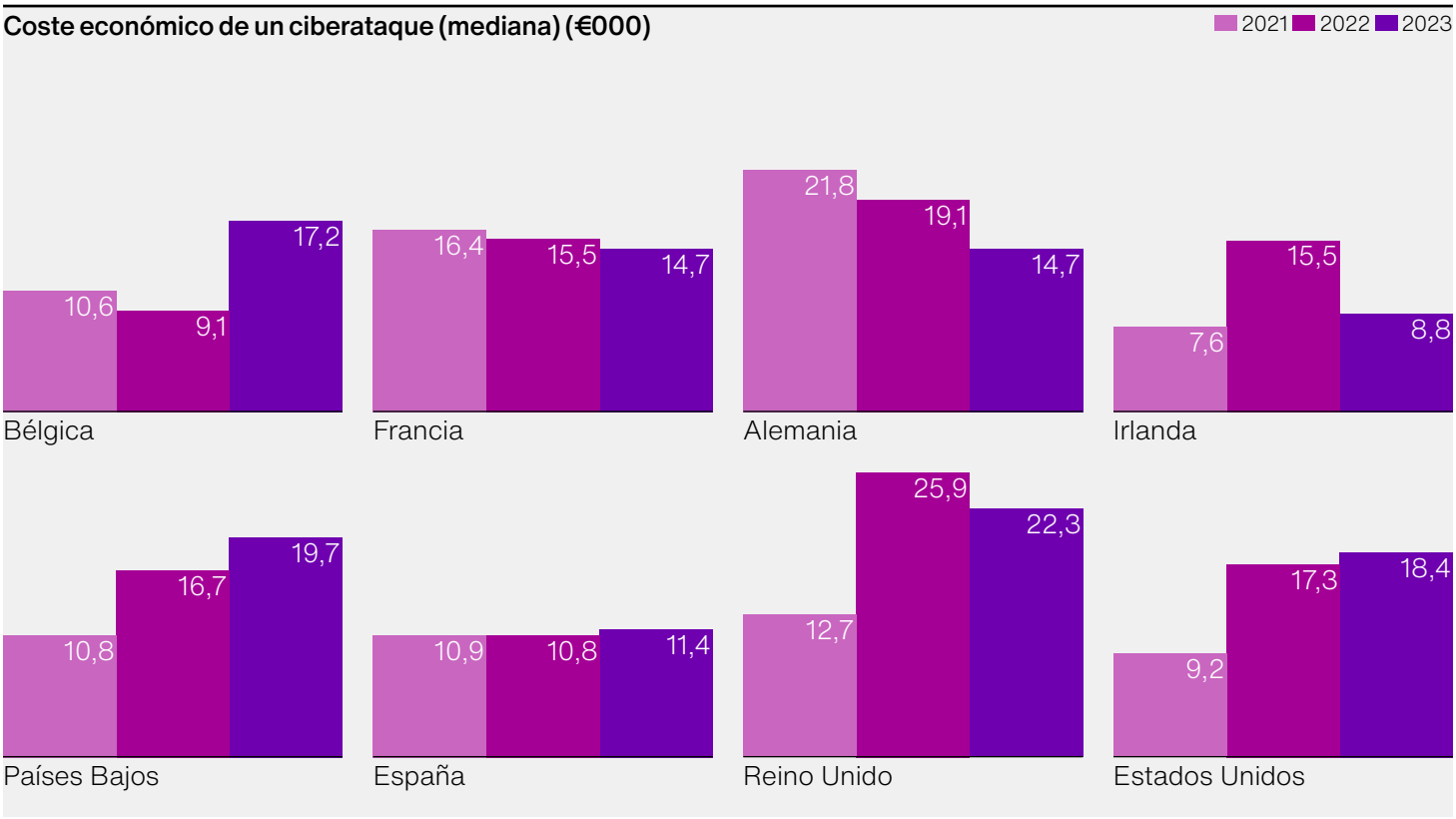
Había una obligación legal de hacerlo, pero "*fue agradable contar con un socio competente a nuestro lado*", afirmó Martin Schäfer, de GF Schäfer Trennwandsysteme GMBH.

Relaciones públicas
La comunicación también fue importante. Hiscox trajo a un experto en comunicación para dar consejo, estaba claro que la noticia sobre este incidente iba a salir a la luz. Había que gestionar de manera activa las comunicaciones, y para ello, la empresa lo hizo público rápidamente, para ayudar a aumentar la confianza y el entendimiento entre los empleados, proveedores y, sobre todo, los clientes.

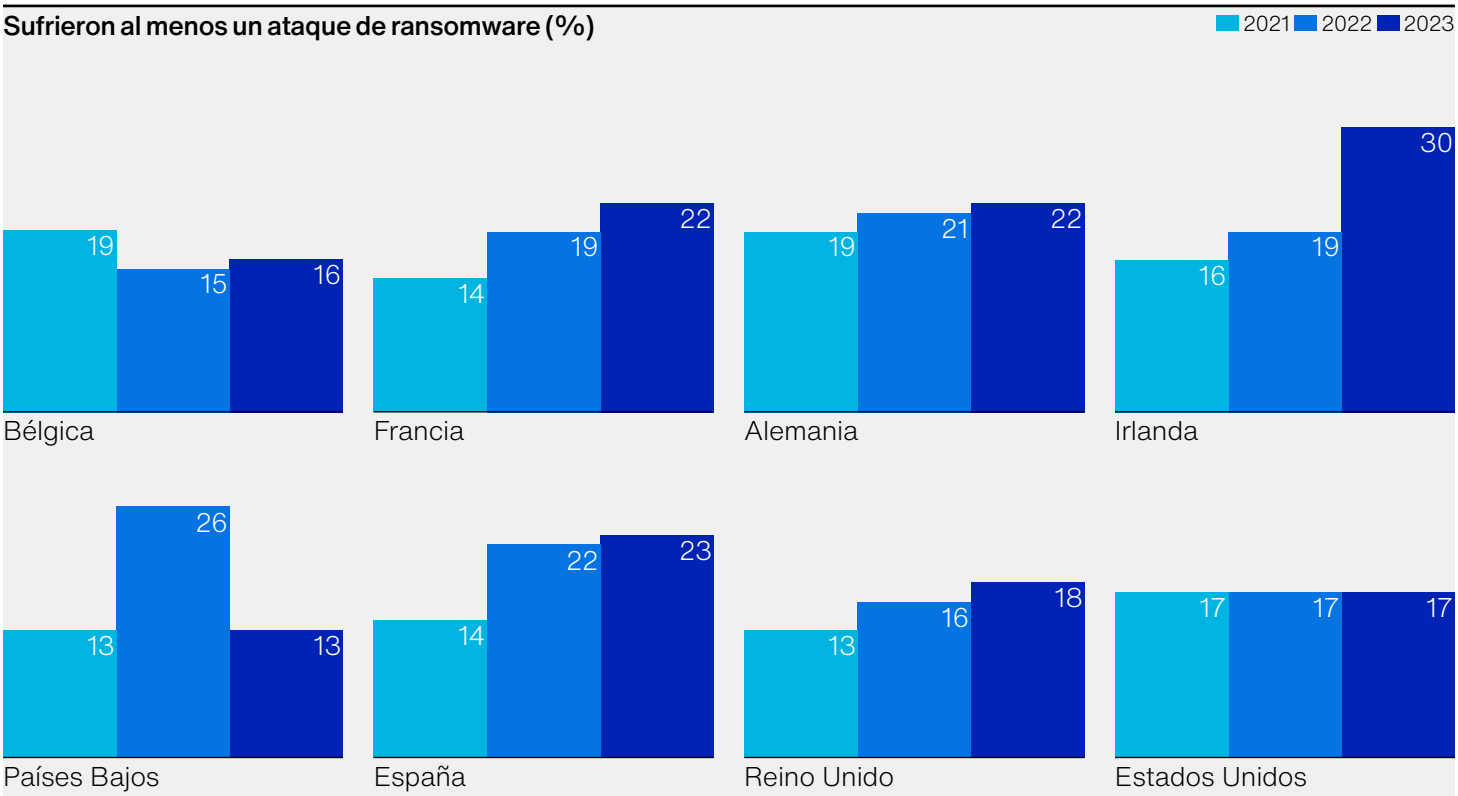
En un principio, pensaron que todos los datos habían desaparecido, pero con la ayuda de la agencia de respuesta, la empresa recuperó una gran cantidad en un plazo de cuatro a cinco días. El ataque demostró el valor del seguro. Los proveedores de servicio de Hiscox ayudaron a los clientes de forma rápida y efectiva en las áreas de gestión de crisis, forense y protección de datos. "*Si echamos la vista atrás, fue bueno contar con tantos asesores a nuestro lado*", declaró uno de los directores.

Datos por países

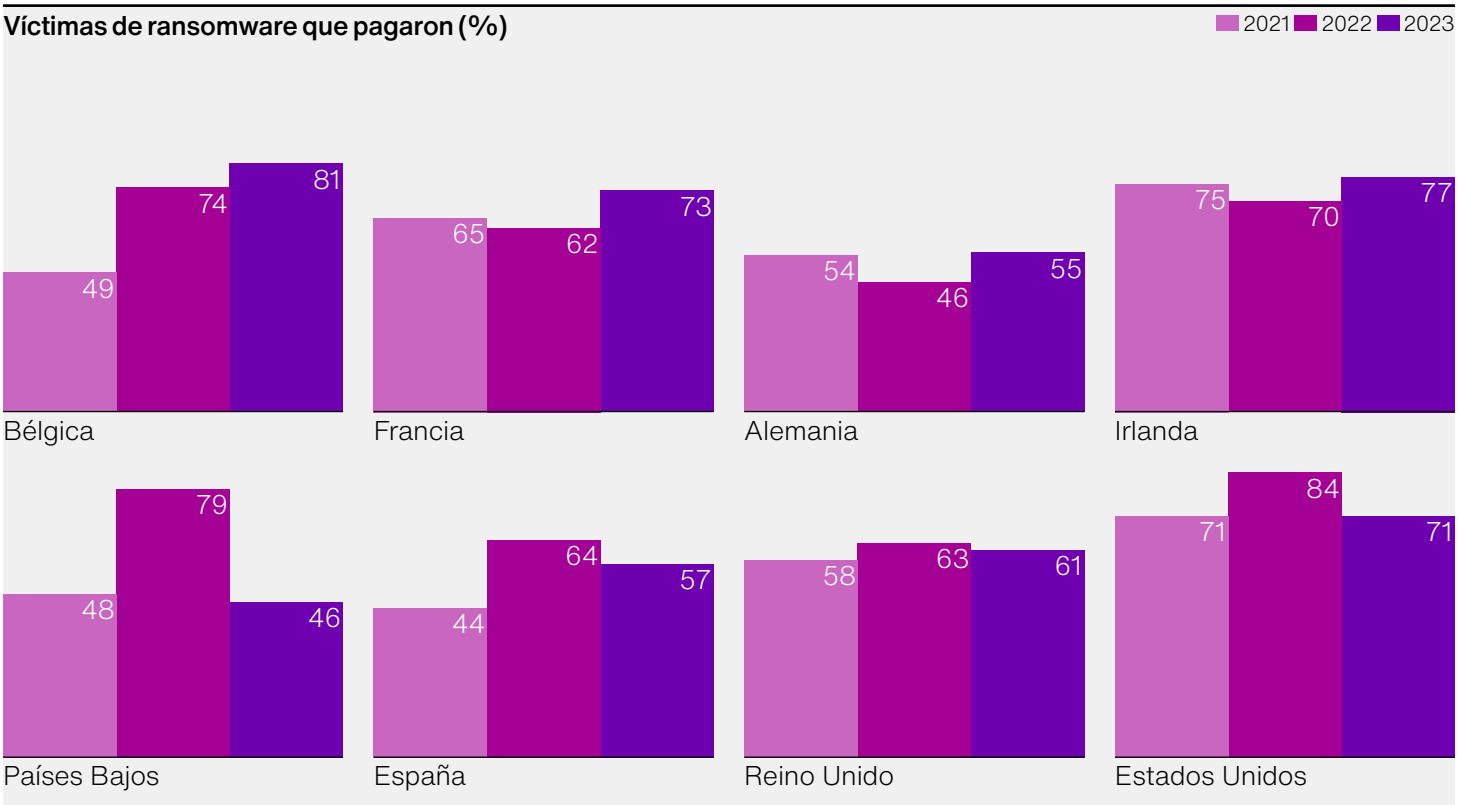




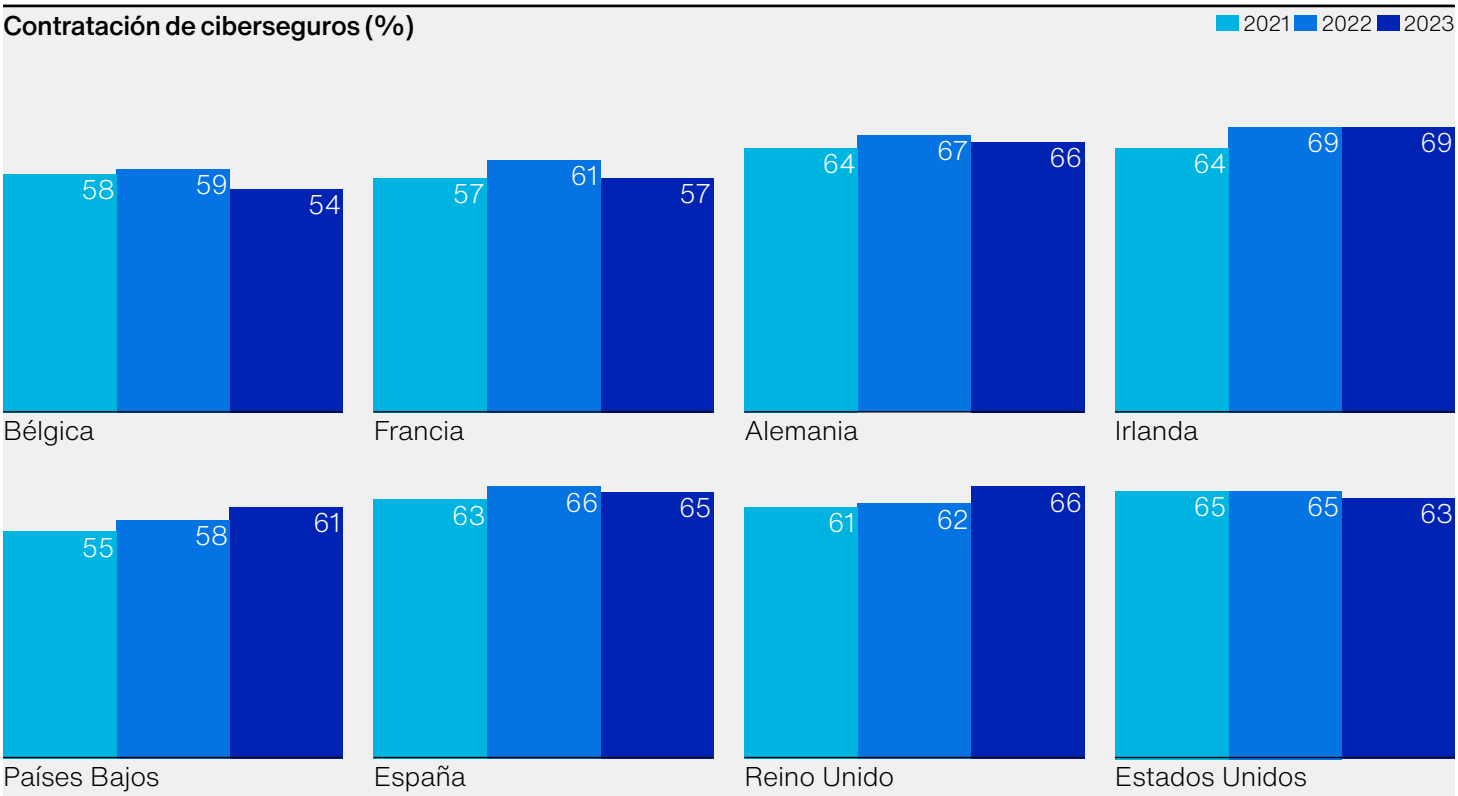
Sufrieron al menos un ataque de ransomware (%)



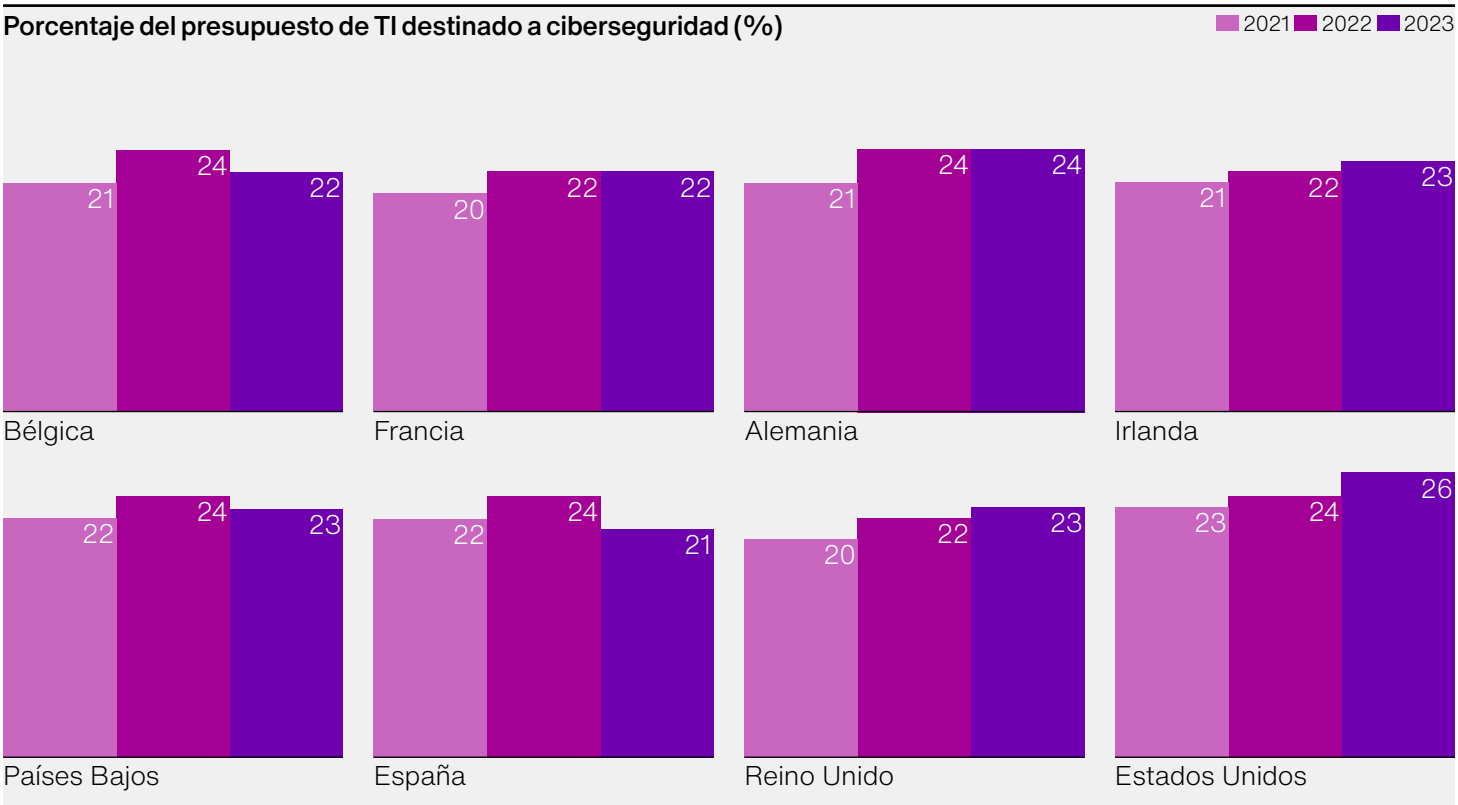
Víctimas de ransomware que pagaron (%)



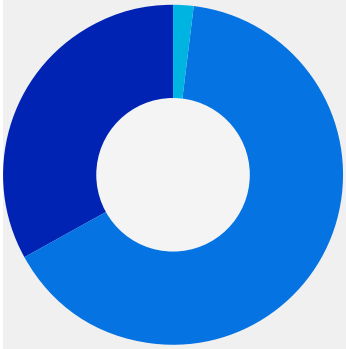
Contratación de ciberseguros (%)



Porcentaje del presupuesto de TI destinado a ciberseguridad (%)



Bélgica

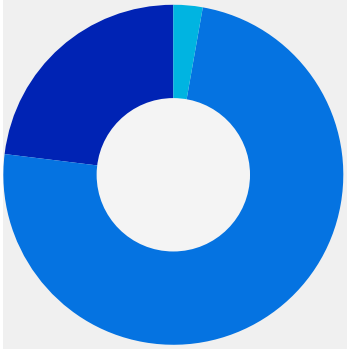


Madurez ciber	%
Expertas	2
Intermedias	65
Novatas	33

Único país del grupo de estudio en el que la ciberseguridad no es uno de los tres principales riesgos empresariales.

El gasto en formación ciber y cambio cultural de los empleados casi se ha duplicado en tres años.

Francia

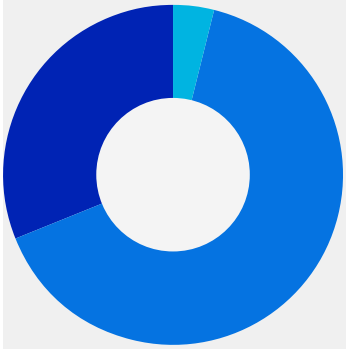


Madurez ciber	%
Expertas	3
Intermedias	74
Novatas	23

El 41% experimentó fraude por desvío de pagos debido a un ciberataque.

Razón principal para contratar un seguro: preocupación por la seguridad de los datos.

Alemania

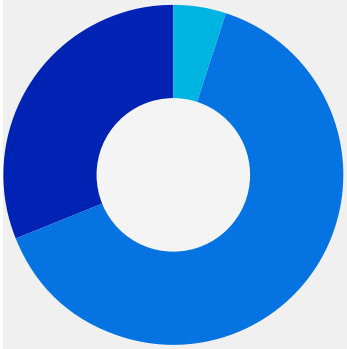


Madurez ciber	%
Expertas	4
Intermedias	65
Novatas	31

Aumento del 26% en la incidencia de ciberataques con respecto al año pasado.

Aumento del 40% del fraude por desvío de pagos a raíz de un ciberataque.

Irlanda

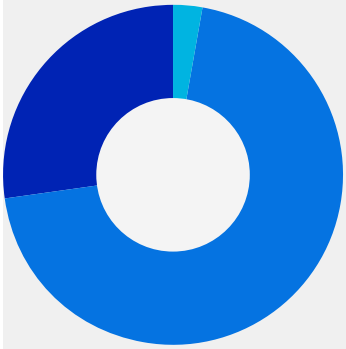


Madurez ciber	%
Expertas	5
Intermedias	64
Novatas	31

El 69% de los encuestados tenía un ciberseguro, el porcentaje más alto del grupo de estudio.

Aumento del 50% de los atacantes que exigen más dinero tras el pago de un rescate.

Países Bajos

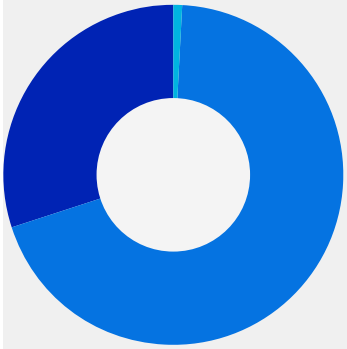


Madurez ciber	%
Expertas	3
Intermedias	70
Novatas	27

Unico país del estudio que aumenta su puntuación en ciberpreparación.

Descenso de los ataques ransomware en un 50% con respecto al año pasado.

España

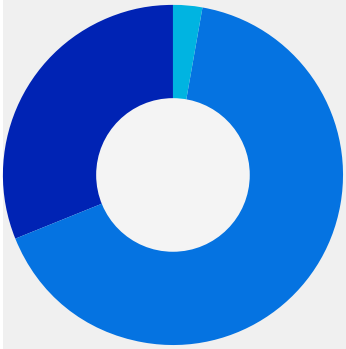


Madurez ciber	%
Expertas	1
Intermedias	69
Novatas	30

El punto de entrada más común fue el servidor corporativo en la nube.

Aumento del 25% en la creencia de que el riesgo ciber se está reduciendo debido al aumento de los presupuestos destinados a ciberseguridad.

Reino Unido

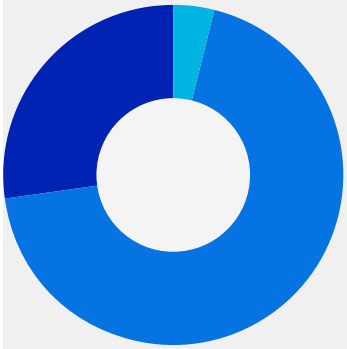


Madurez ciber	%
Expertas	3
Intermedias	66
Novatas	31

Casi tres cuartos de las empresas creen que la marca se verá perjudicada si los datos de los clientes no se gestionan de forma segura.

País con la segunda puntuación más baja (48%) en número de ciberataques.

Estados Unidos



Madurez ciber	%
Expertas	4
Intermedias	69
Novatas	27

Más de uno de cada cinco empresas vio amenazada su solvencia tras un ciberataque.

La razón número uno para gestionar proactivamente el ciberriesgo: tranquilizar a los clientes.

Metodología

Un total de 5.005 profesionales responsables de la estrategia de ciberseguridad de sus empresas fueron encuestados (más de 900 de EE.UU., Reino Unido, Francia y Alemania; más de 400 de España y 200 o más de Bélgica, República de Irlanda y Países Bajos). Los encuestados completaron el cuestionario online entre el 9 de Enero de 2023 y el 2 de Febrero de 2023.

A continuación, se detalla la composición completa de los encuestados.

Encuestados

Empleados	%	Nivel	%
1–9	26	Ejecutivo de nivel C	29
10–49	19	Vicepresidente	24
50–249	15	Director	32
250–999	15	Gerente	15
1.000-más	25		

Sector	%	Departamento	%
Servicios empresariales	7	Dirección ejecutiva	9
Construcción	8	Comercio electrónico	4
Energía	4	Finanzas	9
Servicios financieros	10	Asesoramiento jurídico	4
Alimentación y bebidas	4	Recursos humanos	7
Gobierno y organizaciones sin ánimo de lucro	5	TI y tecnología	18
Fabricación	8	Marketing y comunicaciones	5
Farmacia y sanidad	9	Operaciones	10
Servicios profesionales	8	Propietarios	14
Inmobiliarias	3	Adquisiciones	4
Minorista y mayorista	8	Gestión de productos	5
Tecnología, medios y telecomunicaciones (TMT)	18	Gestión de riesgos	5
Transporte y distribución	5	Ventas	5
Ocio y turismo	4		

La historia de un cliente de Hiscox fue utilizada en la página 15.

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 apoyo directo y ayuda 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, en colaboración con varios proveedores expertos.

Compartir nuestra experiencia y generar concienciación
Hemos creado herramientas gratuitas para todos, como nuestro modelo de autoevaluación de madurez ciber online para ayudar a las empresas a entender sus fortalezas y debilidades en el ámbito de la ciberseguridad. Gracias al modelo de madurez de Hiscox, pueden comparar el rendimiento de su empresa con el de más de 16.000 compañías.

Mantenerte al día sobre el panorama de la ciberseguridad
Hemos creado por séptimo año consecutivo el Informe de Ciberpreparación de Hiscox. Cada año, este informe presenta una imagen actualizada 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.

¿Cuál es la puntuación de tu ciberpreparación?
Nuestro modelo de madurez ciber es una herramienta interactiva, sin coste, que te ayudará a conocer la preparación en materia de ciberseguridad que tiene tu empresa utilizando marcos establecidos por el sector.

www.hiscoxgroup.com/cyber-maturity

Hiscox España
c/ Miguel Ángel, 11 4º planta
28010 Madrid

+34 915 15 9900
info_spain@hiscox.com
www.hiscox.es

22594 10/23