HISCOX

Informe de Ciberpreparación de Hiscox 2021

No dejes tu ciberseguridad en manos del azar

El riesgo ciber es demasiado importante como para dejarlo al azar.

Una de cada seis empresas afectadas el año pasado dijo que el ataque había supuesto un peligro para la viabilidad de su negocio. La amenaza es compleja. Pero, al igual que otros riesgos empresariales, se puede gestionar. La clave es desarrollar la ciberresiliencia.

Descubre cual es el nivel de resiliencia de tu empresa con nuestro modelo de madurez en hiscoxgroup.com/cyber-maturity.

Gestión de las ciberamenazas

Las empresas están dedicando más recursos que nunca a la ciberseguridad.

Gareth Wharton
CEO Cyber de Hiscox

Crece el número de empresas que sufren ciberataques, a menudo en repetidas ocasiones. El informe de este año subraya la magnitud de la ciberseguridad, pero ofrece también buenas noticias. A pesar de las dificultades que presenta la pandemia de la Covid-19, las empresas han intensificado su lucha dedicando más recursos y atención que nunca a su ciberresiliencia.

Al principio de la pandemia, la mayoría de las empresas antepusieron la simple necesidad de seguir funcionando a todo lo demás. La preocupación era que al reducirse los presupuestos de TI se recortara la inversión en ciberseguridad. Este informe demuestra que no fue así. El gasto en ciberseguridad se ha disparado.

Muchas empresas han trasladado eficazmente todo su negocio a Internet. Como aseguradora de riesgos ciber, sabemos que esto no solo ha aumentado la conciencia sobre el desafío ciber, sino que ha llevado la conversación sobre seguridad al frente de la toma de decisiones.

La incidencia creciente del ransomware debería poner de manifiesto la importancia empresarial de una buena ciberseguridad. Los ataques de ransomware no son un asunto tecnológico, tienen un impacto sobre el negocio a múltiples niveles.

No hay duda de que la ciberseguridad es un problema complejo, pero eso no significa que sea inmanejable. Hoy en día, el riesgo es demasiado alto y tangible para que las empresas y los particulares lo dejen en el cajón de "demasiado difícil". Existe una posibilidad real de que un ataque ponga en riesgo todo el negocio. Una de cada seis empresas afectadas el año pasado dijo que el ataque había amenazado la viabilidad de su negocio. Los pasos simples y prácticos pueden conducir a un nivel de ciberresiliencia en el que es menos probable que se produzca un ataque. Cuando ocurre uno, tu empresa tiene la formación, las herramientas y la protección financiera para recuperarse.

Como ex director de tecnología, siempre me estaba preguntando "¿qué están haciendo nuestros competidores?" y "¿cómo estamos nosotros?". Este año no solo hemos analizado los datos del informe, sino que hemos creado un nuevo modelo de ciberpreparación que mide las fortalezas de los encuestados en seis áreas clave de ciberseguridad abarcando personas, procesos y tecnología. Está diseñado para ser un modelo interactivo, por lo que te permite verificar y comparar la madurez de tu negocio con otras empresas en tu misma geografía, sector y banda de facturación. El modelo de madurez ilustra lo que hacen los ciberexpertos en cada área para ayudarte a planificar y desarrollar tu ciberresiliencia.

Nuestra experiencia aseguradora nos ha demostrado que es esencial contar con normas coherentes en todos los ámbitos de la seguridad para que los hackers no encuentren la manera de entrar en los sistemas. Esperamos que te brinde una nueva perspectiva sobre tus medidas actuales y quizás resalte áreas de mejora.

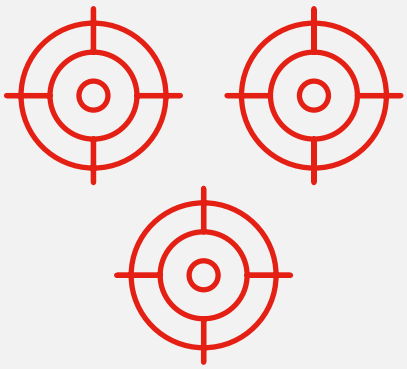
La amenaza ciber no va a desaparecer, pero las empresas podrán contener el impacto y minimizar los daños con una buena gestión del riesgo, complementada con un seguro ciber adecuado. Esperamos que este informe contribuya a que las empresas comprendan esta amenaza, ofrezca un modelo de buenas prácticas y ayude a desarrollar la preparación y la resistencia necesarias para hacer frente a los retos que se presenten.

Resumen ejecutivo

Las empresas centran el gasto de TI en la ciberresiliencia para gestionar los ataques crecientes.

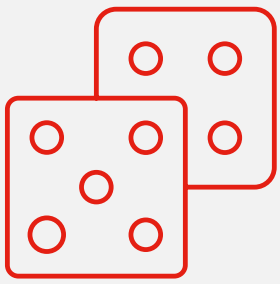
Más empresas en el punto de mira

La proporción de empresas que sufrieron ciberataques aumentó del 38% al 43%. Muchas fueron víctimas de ataques múltiples.



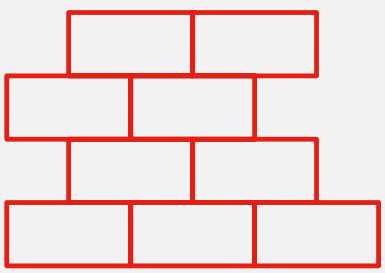
Una variedad de resultados aterradora

El coste de los ataques varía mucho. Una de cada seis empresas ciberatacadas dice que vio amenazada su supervivencia.



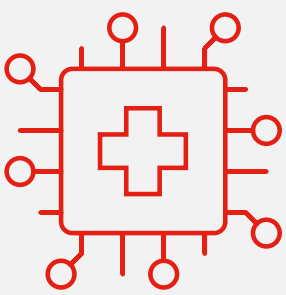
Los presupuestos de TI se reorientan hacia la ciberseguridad

La empresa media dedica ahora más de una quinta parte (el 21%) de su presupuesto de TI a la ciberseguridad, lo que supone un aumento del 63%.



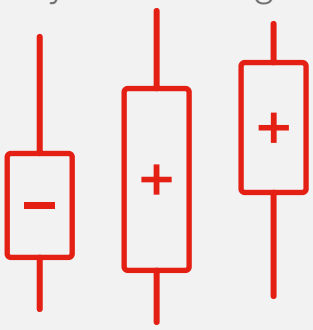
El ransomware se ha convertido en algo habitual

Aproximadamente una de cada seis víctimas fue extorsionada y más de la mitad pagó un rescate. Los correos electrónicos de phishing fueron el origen más habitual.



Personas, procesos y tecnología

Nuestro modelo de ciberpreparación muestra que las puntuaciones que obtiene el ámbito de las personas es inferior a las que obtienen los otros dos ámbitos, los correspondientes a los procesos y la tecnología.



A los expertos les fue mejor

Las empresas calificadas como ciberexpertas sufrieron menos ataques de ransomware, fueron menos propensas a pagar y se recuperaron más rápidamente.

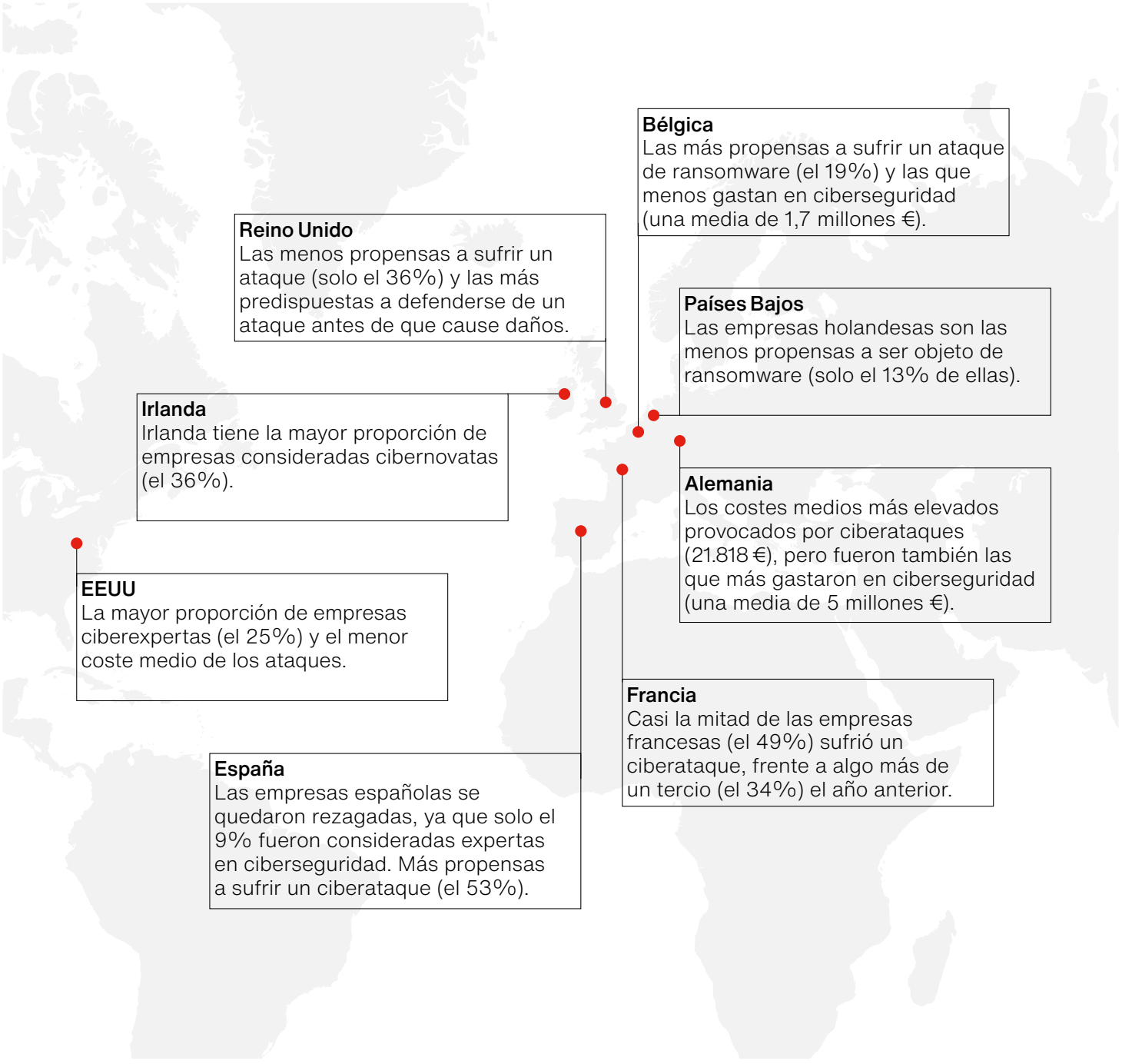
La contratación de seguros es lenta

La adopción de una cobertura independiente y especializada pasa del 26% al 27%; la penetración de mercado de estas pólizas es mayor entre las empresas ciberexpertas.

Grandes variaciones entre países

Las empresas estadounidenses encabezan el ranking de ciberexpertas, las españolas son las más atacadas y las alemanas pagan el precio más alto por incidentes sufridos.

Comparación por países



Bélgica
Las más propensas a sufrir un ataque de ransomware (el 19%) y las que menos gastan en ciberseguridad (una media de 1,7 millones €).

Reino Unido
Las menos propensas a sufrir un ataque (solo el 36%) y las más predispuestas a defenderse de un ataque antes de que cause daños.

Países Bajos
Las empresas holandesas son las menos propensas a ser objeto de ransomware (solo el 13% de ellas).

Irlanda
Irlanda tiene la mayor proporción de empresas consideradas cibernovatas (el 36%).

Alemania
Los costes medios más elevados provocados por ciberataques (21.818 €), pero fueron también las que más gastaron en ciberseguridad (una media de 5 millones €).

EEUU
La mayor proporción de empresas ciberexpertas (el 25%) y el menor coste medio de los ataques.

Francia
Casi la mitad de las empresas francesas (el 49%) sufrió un ciberataque, frente a algo más de un tercio (el 34%) el año anterior.

España
Las empresas españolas se quedaron rezagadas, ya que solo el 9% fueron consideradas expertas en ciberseguridad. Más propensas a sufrir un ciberataque (el 53%).

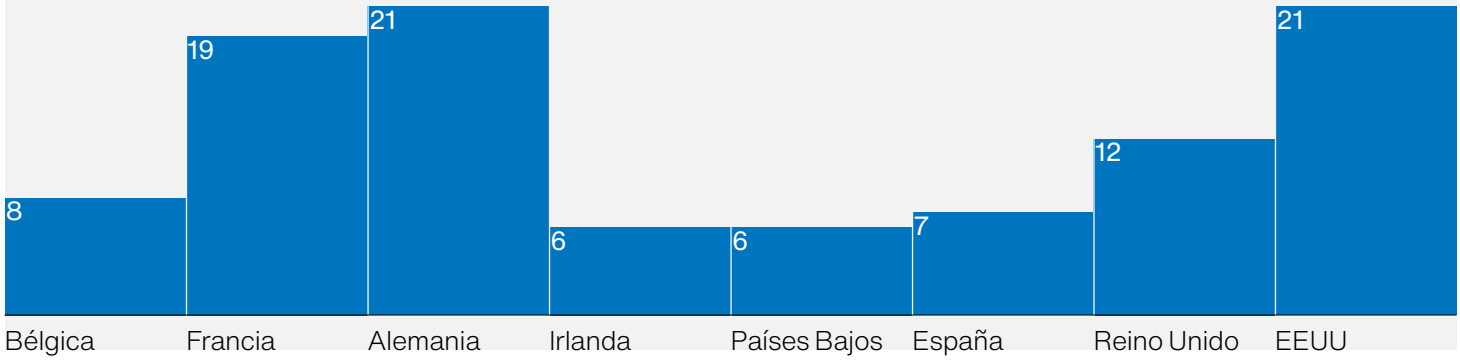
En cifras

Porcentaje del gasto en TI destinado a ciberseguridad

(%)

Pagó una demanda de rescate

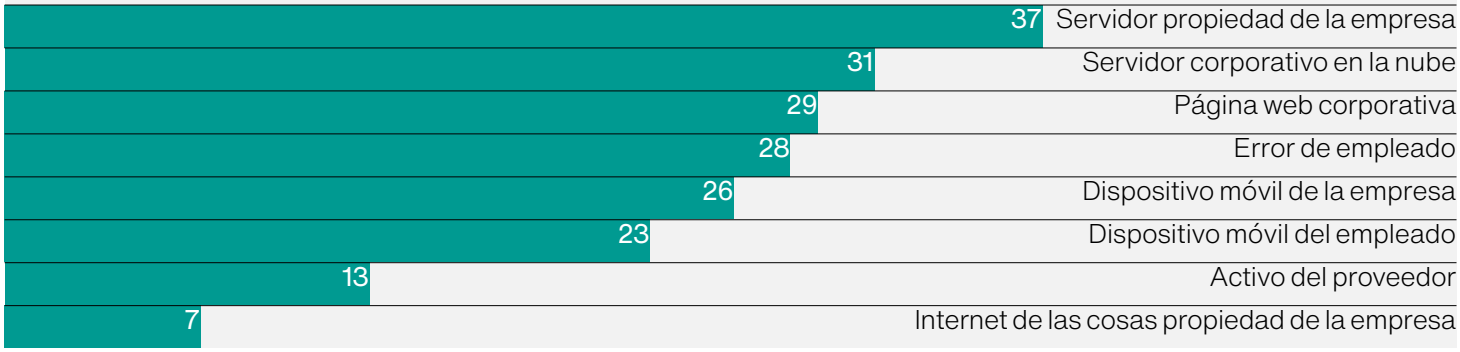
(%)



Primer punto de entrada para un ciberataque

Los encuestados eligieron todas las opciones que aplicaban para su caso

(%)



Magnitud del problema

Crece el número de empresas que informan de ciberataques a medida que aumenta la intensidad en sectores clave.

En la encuesta de este año ha aumentado considerablemente la proporción de empresas que han denunciado uno o más ciberataques, y los ciberdelincuentes han centrado sus esfuerzos en tres o cuatro sectores en particular y en muchas más empresas de gran tamaño.

¿Quién está siendo atacado?
La proporción de encuestados que declararon haber sufrido un incidente pasó del 38% en 2020 al 43%. Los objetivos favoritos de los hackers fueron los sectores de telecomunicaciones, medios y tecnología, (TMT), de servicios financieros y de energía. El porcentaje de empresas afectadas en estos sectores pasó de un nivel bajo o medio, en torno al 40% en nuestro estudio de 2020, a un nivel medio del 50% (ver Gráfico 1.).

Asimismo, este año había muchas más grandes empresas en la línea de fuego. Como se ha señalado en ediciones anteriores, la probabilidad de ser objeto de un ataque aumenta considerablemente según el tamaño de la empresa. Este año la pendiente de la curva se hizo más pronunciada, desde el 23% de las más pequeñas hasta el 61% de las grandes empresas (las que tienen más de 1.000 empleados). El año pasado, las cifras equivalentes eran del 31% para las empresas más pequeñas y del 51% para las empresas de mayor tamaño.

En general, las empresas españolas fueron las más propensas a informar de un ciberataque (el 53%). Casi la mitad de los encuestados franceses (el 49%) declararon haber sufrido un ataque, frente al 34% del año anterior. En cambio, solo el 36% de las empresas británicas declararon haber sido objeto de ataques.

Un gran número de empresas sufren ataques múltiples
Más de una cuarta parte (el 28%) de las empresas que sufrieron ciberataques fueron atacadas más de cinco veces en el último año. Casi la mitad (el 47%) de las empresas atacadas se enfrentaron a los hackers seis veces o más. Un tercio (el 33%) tuvo que hacerlo más de 25 veces. Más de una quinta parte (el 22%) de las empresas francesas y alemanas que fueron objeto de ataques se encontraban en la franja que superaba los 25 ataques.

Gráfico 1. Los cinco sectores principales que informan de al menos un ciberataque
(%)

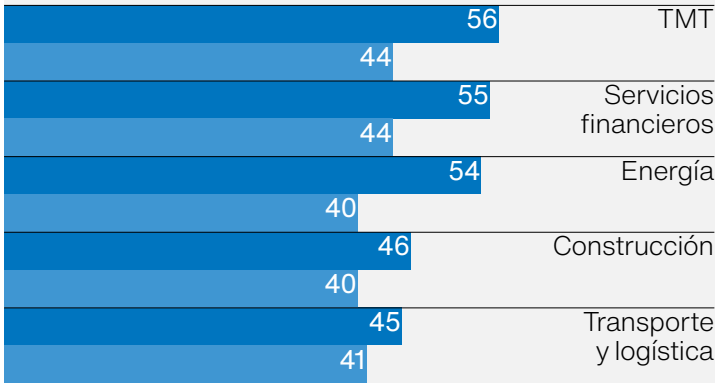


Gráfico 2. Número de ataques en el último año (por empresas que declararon al menos uno)
(%)

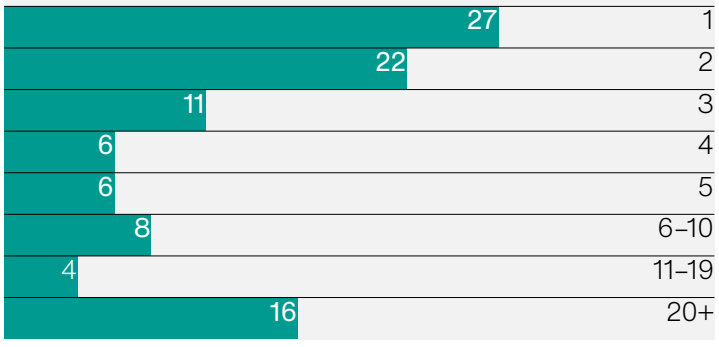
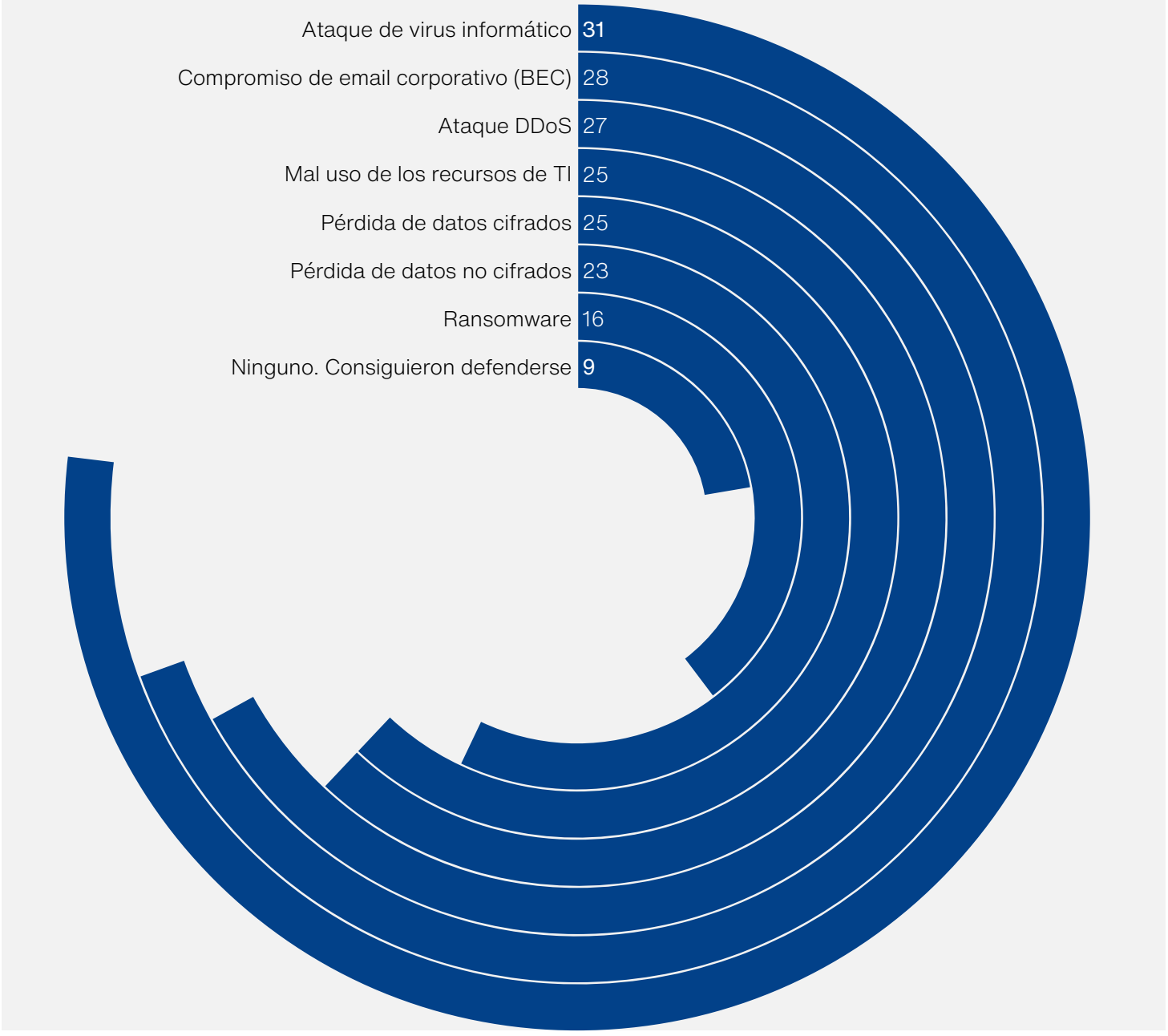


Gráfico 3. Las empresas tuvieron que hacer frente a una gran diversidad de ataques
(%)

Los encuestados eligieron todas las opciones que aplicaban para su caso



La visión de Hiscox

La tendencia de que las empresas más grandes estén en el punto de mira una pregunta: ¿son simplemente mejores en detectar ataques? También es notable que las empresas que obtuvieron la calificación de intermedias o expertas en nuestro modelo de ciberpreparación tenían más probabilidades de sufrir múltiples ataques. En 2020, vimos empresas de todos los tamaños trasladar su modelo de negocio online y su equipo a trabajar en remoto. Los puertos RDP (Protocolo de escritorio remoto) abiertos fueron responsables del 61% de las reclamaciones de ransomware gestionadas por Hiscox en 2020. Estas son algunas de las razones de los múltiples ataques.

Las empresas tuvieron que hacer frente a una amplia gama de ataques

Tres de cada diez empresas que fueron objetivo de los ataques (el 31%) tuvieron que hacer frente a un virus informático (diferente de un ransomware), el 28% a un fraude por desvío de pagos derivado de compromiso de email corporativo (BEC) y, el 27% a un ataque DDoS (ataque de denegación del servicio). Las empresas alemanas, francesas y estadounidenses fueron las más propensas a sufrir estos resultados.

Un dato significativo es que el 39% de las empresas estadounidenses tuvo que hacer frente a incidentes por un uso indebido de los recursos informáticos, como el alojamiento de malware o el secuestro de la infraestructura para minar criptomonedas, frente a únicamente el 25% total.

La rendija por la que colarse

Deja una puerta sin cerrar o una ventana sin el pestillo y los ladrones la encontrarán. Cuando pedimos a los encuestados que citaran el primer punto de entrada de los ciberdelincuentes, el 37% mencionó los propios servidores de la empresa. Los servidores alojados en la nube quedaron en segundo lugar (mencionados por el 31%), seguidos por los sitios web de la empresa (el 29%) y, los errores de los empleados, como el phishing o spoofing (el 28%). En 2020, el phishing fue la primera causa, mencionado por el 45% de los encuestados. El estudio de este año ofrece una mayor variedad de respuestas.

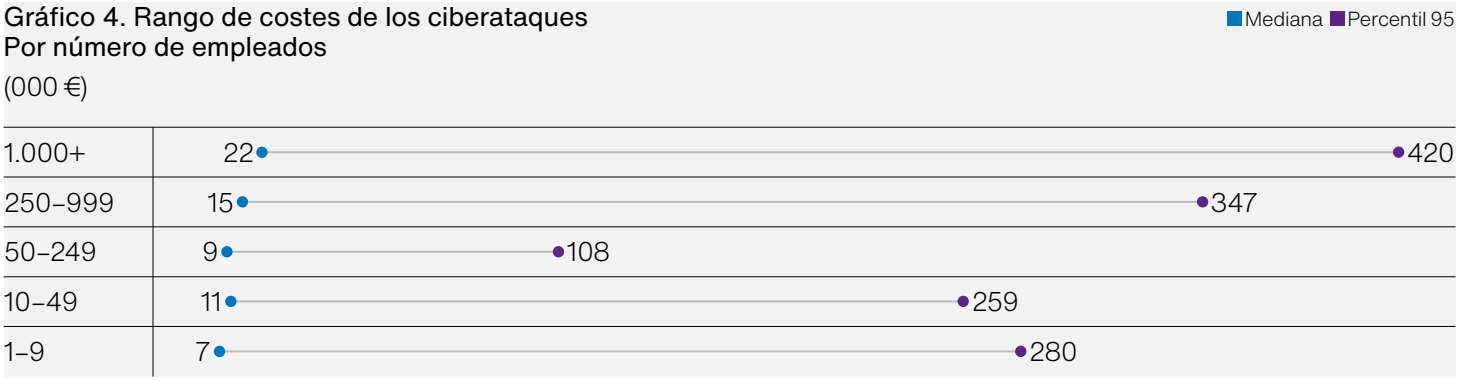
Pero hay grandes variaciones por sectores. Mientras las empresas de servicios profesionales, de construcción y de servicios financieros se mostraron propensas especialmente a citar el servidor corporativo como punto más habitual de entrada, las empresas que tratan con el público, especialmente las de venta al por menor/mayor y las de energía, mostraron más probabilidad de haber sufrido una brecha a través del sitio web de la empresa. Los dispositivos móviles propiedad de la empresa, que mencionan algo más de una cuarta parte de las empresas atacadas (el 26%), parecen ser áreas de especial vulnerabilidad para los sectores más móviles, como el de transporte y logística y el de ocio y turismo (mencionados por el 32% y el 30%, respectivamente).

Las pequeñas empresas de entre 10 y 49 empleados parecen susceptibles especialmente a la vulnerabilidad de los servidores o al peligro de las credenciales (que menciona el 41% frente al 37% de media), pero es sorprendente que las empresas grandes también aparezcan en gran medida en cada área. Los datos sugieren que la inversión en un sitio web sofisticado puede ser contraproducente: las empresas más grandes de nuestro grupo de estudio tienen muchas más probabilidades de haber sufrido un ataque a través del sitio web (como un ataque DDoS).

Las empresas expertas parecen haber experimentado las mismas vulnerabilidades que el resto. Sorprendentemente, el 44% de los expertos mencionó su servidor corporativo como primer punto de entrada para los hackers, en comparación con el 37% del grupo de estudio en su conjunto. El sitio web de la empresa también lo menciona el 36% de los expertos.

Las empresas alemanas tienen que trabajar en casi todos estos ámbitos. Por ejemplo, el 44% y el 41% afirmaron que el servidor propiedad de la empresa o el servidor en la nube (ya sea por vulnerabilidad directa del servidor o por compromiso de las credenciales) proporcionaron el primer punto de entrada para los hackers. Las empresas estadounidenses parece también que han sido vulnerables especialmente en la mayoría de estas áreas.

Gráfico 4. Rango de costes de los ciberataques
Por número de empleados
(000 €)



Costes financieros
La amplia variedad de resultados hace que la ciberamenaza contenga peligros añadidos. Es fácil pasar por alto toda la importancia que tienen los datos relativos a los costes de los ciberataques. Si se observan solamente las cifras medias o los promedios, puede parecer que es contenible el impacto financiero. Pero detrás de esas cifras hay una serie de efectos y consecuencias que deberían provocar un escalofrío a cualquier CEO.

Lo más llamativo del gráfico (ver Gráfico 4.) es la gran variedad e imprevisibilidad de los resultados de los incidentes en cada grupo de tamaño de nuestro estudio. El gráfico muestra tanto el coste medio como el coste del percentil 95 de la suma de todos los ciberataques experimentados en los últimos 12 meses.

Aunque puede que parezca que los costes medios son asumibles, conviene recordar lo que representa el valor promedio. Es el punto medio. Mientras que la mitad de los afectados habrá soportado costes de ciberataques hasta esa cifra, la otra mitad habrá sufrido vulneraciones más costosas. Lo que muestra el gráfico es que esos costes pueden ser dos, tres o incluso cuatro órdenes de magnitud superiores.

Las pequeñas empresas se resienten
Las pymes fueron las que sufrieron las mayores pérdidas en relación con el tamaño de la empresa. Para las microempresas con menos de 10 empleados, el coste medio de todos los ataques de este año superó ligeramente los 8.273 €. Sin embargo, en el percentil 95 y superior había empresas que sufrieron pérdidas de 280.000 €. Algunos se encontraron con resultados aún peores. Una empresa alemana de servicios empresariales experimentó vulneraciones que supusieron un coste por empleado equivalente a 430.909 €.

En el extremo opuesto, la mitad de las grandes empresas lograron contener los costes de los ciberataques en menos de 21.818 €. Pero, en el percentil 95 experimentaron pérdidas de casi 40 veces ese nivel. No puede subestimarse este impacto. Una de cada seis empresas víctimas de ciberataques este año (el 17%) afirmó que el impacto era lo suficientemente grave como para "amenazar sustancialmente la solvencia/viabilidad de la empresa".

Las empresas alemanas vuelven a destacar por la gravedad de los ataques. Suponen más de un tercio del impacto financiero total, 43,5 millones de Euros, la mitad de los cuales corresponden a dos sectores, el minorista/mayorista y el farmacéutico/sanitario. Las empresas alemanas encabezaron también el ranking por coste medio de todos los ciberataques (21.545 €) y por mayor ataque individual (4,6 millones de Euros). En el extremo opuesto, las empresas irlandesas soportaron unos costes medios de solo 7.545 €.

Los datos sobre los costes proceden de las 1.709 empresas que hicieron un seguimiento del coste de los ciberataques. Resulta alentador que vayan aumentando las cifras que miden el impacto. Un número creciente de empresas afirman que ahora pueden “medir claramente el impacto empresarial de los incidentes de seguridad que afectan a su negocio”: el 62%, frente al 60% del año pasado y el 57% del año anterior.

Afortunadamente, los hackers no se salen siempre con la suya. El 9% de las encuestadas (y el 11% de las expertas) afirmaron que consiguieron repeler o remediar todos los ataques que se lanzaron contra ellas antes de que causaran daños. Las empresas británicas son las que mejor lo hacen (el 13%) y las estadounidenses las que peor (solo el 6%). Pero, debe tenerse en cuenta que la defensa o reparación con éxito siguen suponiendo un coste importante. En general, el coste medio fue solo ligeramente inferior al de un ataque solucionado con éxito. Nada es gratis.

La reputación de la marca está en juego
El efecto de una vulneración grave va mucho más allá de los costes financieros inmediatos. Casi una cuarta parte de las empresas víctimas de ataques (el 23%) citó la publicidad negativa y su impacto sobre la marca de la empresa y su reputación. Esto supone un fuerte aumento respecto al 14% que afirmó lo mismo el año pasado. No es de extrañar que las grandes empresas, muchas de las cuales tienen marcas reconocidas mundialmente, fueran las más propensas a declarar un impacto sobre su reputación.

€6,6m

Importe total abonado por 241 empresas que pagaron rescate.

Las empresas de atención al público encabezan la lista de las afectadas (el 28% de las empresas de ocio y turismo y el 25% de las de alimentación y bebidas). El 23% de los encuestados mencionó también el aumento de los costes asociados a la notificación a los clientes. Puede ser relevante que una de las tareas principales que se han propuesto las ciberexpertas este año sea "mejorar la seguridad de los servicios y aplicaciones de cara al cliente".

Más de una de cada diez empresas afectadas (el 11%) pagó "una sanción importante que tuvo un impacto significativo en la salud financiera de la empresa". En EE.UU., la cifra fue del 18%, lo que indica que las regulaciones estrictas de los principales estados que contemplan sanciones por vulneraciones de la privacidad, como la Ley de Privacidad del Consumidor de California (CCPA), están teniendo un impacto. El número de empresas que dicen haber perdido clientes pasó del 11% al 19%. Casi el mismo número (el 18%) afirma tener más dificultades para captar nuevos clientes, frente al 15% del año anterior.

Ransomware: poco más de la mitad paga

Alrededor de una sexta parte de las empresas (el 16%) que informaron de ciberataques tuvieron que hacer frente a una extorsión. Las empresas belgas y alemanas son las que tienen más probabilidades de sufrir ataques (el 19%), y las holandesas las que menos (el 13%).

Algo más de la mitad de los afectados (el 58%) pagaron un rescate, ya sea para recuperar los datos o para evitar la publicación de información sensible. El territorio más fructífero para los especialistas en ransomware fue Estados Unidos, donde el 71% de los afectados pagaron (la proporción en Irlanda fue mayor, del 75%, pero en una muestra de solo 20 empresas, lo que no es significativo a efectos estadísticos). Las empresas españolas son las menos propensas a pagar: solo el 44% de ellas lo hizo.

Las 241 empresas que pagaron un rescate transfirieron un total de 6,6 millones de Euros. La cantidad media que se pagó en concepto de rescate fue de 10.818 € y el mayor pago lo hizo una entidad alemana (86.273 €). Una empresa francesa se situó solo unos pocos dólares por

Gráfico 5. Métodos frecuentes de ataques de ransomware
(%)

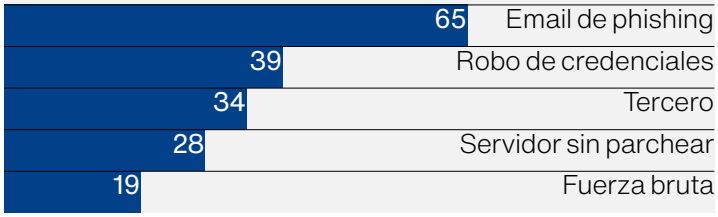
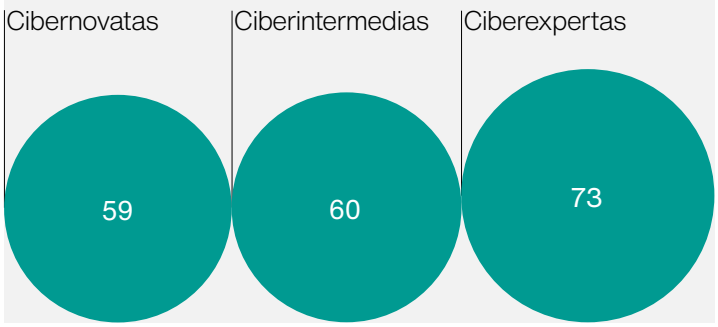


Gráfico 6. Vuelta a la normalidad en una semana
(%)



La visión de Hiscox

No hay duda de que el ransomware es el mayor quebradero de cabeza a la hora de hacer negocios online. Empresas de todos los tamaños suelen ser víctimas de bandas de ransomware. Sin embargo, como muestra nuestra investigación, los expertos obtienen mejores resultados cuando ocurren ataques. Tuvieron menos ataques de ransomware, menos fueron víctimas de correos electrónicos de phishing y, cuando fueron atacados, se recuperaron más rápidamente. En Hiscox nos tomamos el ransomware increíblemente en serio. Nuestros formularios de propuesta están destinados específicamente a promover una buena protección contra el ransomware, alentando así a nuestros clientes a mejorar y mantener su ciberresiliencia.

detrás. Una cuarta parte de las empresas que pagaron un rescate eran empresas del sector de telecomunicaciones, medios y tecnología (TMT).

El importe del rescate pagado fue únicamente una parte de la historia. Por primera vez pedimos a los encuestados que evaluaran los costes de recuperación, tanto del mayor ataque de ransomware, como de todos los ataques de ransomware de los últimos 12 meses. Los resultados fueron bastante impactantes: por lo general, el coste de la recuperación estuvo a punto de duplicar el impacto financiero, representando el 45% de los costes totales (el coste del rescate y de la recuperación combinados).

Más del 60% de las empresas que pagaron rescates se concentraron en tres países: Estados Unidos (el 21%), Alemania (el 21%) y Francia (el 19%). Alemania compartió el primer puesto con Bélgica en cuanto al número de empresas que informaron de uno o más ataques de ransomware (el 19%).

Las pequeñas empresas son víctimas del phishing

Los correos electrónicos de suplantación de identidad fueron la principal vía de entrada para los ciberdelincuentes. Casi dos tercios (el 65%) de las víctimas de ransomware mencionaron este método de entrada, aún más en los Países Bajos y Alemania (el 76% y el 74%, respectivamente). Las pequeñas empresas fueron víctimas del phishing con más frecuencia que el resto. Alrededor del 74% de las empresas con menos de 10 empleados que fueron víctimas de extorsión mencionaron este punto de entrada. Esta cifra contrasta con el 65% únicamente de las empresas más grandes de nuestro estudio. El robo de credenciales y los proveedores externos (o proveedores de servicios gestionados) fueron las dos siguientes vías que se citaron (mencionadas por el 39% y el 34% de las víctimas) (ver Fig. 5.).

Las empresas estadounidenses parecen haber sido vulnerables especialmente a la entrada a través de un proveedor tercero/Proveedor de Servicios Gestionados (MSP), un servidor sin parches o el robo de credenciales.

Una vez encontrado un objetivo lucrativo, los hackers suelen volver a por más. Algo menos de 200 empresas pagaron a los extorsionistas más de una vez. Unas 76 empresas pagaron entre tres y cinco veces, mientras que 14 pagaron cinco veces o más. Una de cada cuatro empresas (27%) pagó tres veces o más para recuperar datos y una de cada cinco (22%) pagó tres veces o más para evitar la publicación de datos confidenciales.

¿Qué tal les fue a las ciberexpertas?

En general, muy bien. Es menos probable que tengan que hacer frente a exigencias de rescates (el 13% de ellas, frente al 16% de las cibernovatas y el 17% de los ciberintermedias) o que sean víctimas de correos electrónicos de phishing (el 56% de ellas, frente al 65% de media en todas las empresas objetivo).

Es menos probable también que hayan pagado un rescate, lo que sugiere que tienen a menudo la experiencia para desviar un ataque de ransomware o remediarlo después. Algo más de la mitad de las ciberexpertas (el 54%) pagaron, frente a dos tercios (el 68%) de las cibernovatas. También es probable que las ciberexpertas se recuperen más rápidamente (ver Fig. 6.).

Sin embargo, teniendo en cuenta todos los ciberataques, las expertas sufrieron un coste tan grande como el que sufrieron las novatas y las intermedias juntas, a pesar de constituir solamente el 20% de nuestro grupo de estudio. Este es, sin embargo, el efecto de las grandes empresas. Algo más de la mitad de los ciberexpertas son empresas y constituyen los mayores objetivos, sufriendo los mayores ataques.

Sin embargo, las ciberexpertas no estuvieron siempre atentas: fueron más propensas a dejar entrar a los intrusos a través de un servidor sin parches (mencionado por el 38% de las expertas frente al 28% de la media) o mediante ataques de fuerza bruta contra las credenciales del servidor, en los que los ciberdelincuentes repasan simplemente secuencias de números o contraseñas populares (el 25% frente al 19% de media).

Modelo de ciberpreparación

Las empresas son fuertes en el área tecnológica, pero más débiles en cuanto a empleados.

A medida que evolucionan los riesgos ciber, también debe hacerlo la forma en la que medimos la preparación y la resiliencia. Por primera vez desde el inicio de este informe, hemos revaluado lo que significa que una empresa sea experta en ciberseguridad. Nuestro nuevo modelo es una evaluación de madurez de no solo de la preparación, sino también de la resiliencia de una empresa en la gestión de intentos y de ciberataques.

Nuestro modelo de ciberpreparación tiene dos dimensiones. Cuantifica las capacidades de las empresas en seis áreas operacionales dentro de la ciberseguridad (denominadas "ámbitos") y las alinea con preguntas concebidas para evaluar la importancia de las personas, los procesos y la tecnología ("funciones") en cada esfera. Combina las dos puntuaciones para proporcionar una imagen compuesta de la cibermadurez (ver Gráfico 7.).

Como parte del proceso, el modelo destaca esferas específicas de fortaleza o debilidad. Muchas de ellas son coherentes sorprendentemente en todos los países y sectores, lo que pone de manifiesto las lecciones que muchas empresas deben tener en cuenta.

Solo una de cada cinco empresas (el 20%) se califica como ciberexperta (aunque supone un ligero avance con respecto al modelo utilizado en años anteriores). La mitad de las empresas se sitúan en la franja media de intermedias. Las cibernovatas constituyen el 30% restante.

Estados Unidos lidera el camino

Las empresas estadounidenses son las que salen mejor paradas, con la mayor proporción de ciberexpertas (el 25%) y la menor de cibernovatas (el 27%), aunque van a la zaga de sus homólogas alemanas y francesas en cuanto a puntuación media global. Resulta interesante que el buen comportamiento de las empresas estadounidenses se refleje en el menor coste medio de los ataques. Las empresas españolas están algo alejadas, ya que sólo el 9% de las empresas aparecen como ciberexpertas y el 35% como cibernovatas. Ocupan el último lugar de la tabla en todos los grupos de tamaño de empresa.

El Reino Unido es una especie de enigma. Aunque es el segundo país, después de Estados Unidos, en cuanto a la proporción de ciberexpertas (el 23%), sus microempresas (de 1 a 9 empleados) son las peores de los ocho países, con un 62% de cibernovatas. Las empresas más pequeñas de España e Irlanda alcanzaron también un baja calificación, con un 58%.

Por sectores, el de TMT es el que tiene la mayor proporción de ciberexpertas (el 25%), superando al sector de los servicios financieros y al sector industrial, que lideraron el año pasado (ver Fig. 8.). Puede que no sea una coincidencia que los tres primeros sectores (TMT junto con la energía y los servicios financieros) sean también los tres más atacados. En el otro extremo de la escala, los servicios profesionales, el ocio y turismo y los servicios a empresas tienen las proporciones más altas de cibernovatas (el 41%, el 41% y el 39%, respectivamente).

No es de extrañar que el número de ciberexpertas sea claramente mayor en las empresas más grandes, aunque hay poca diferencia en las puntuaciones de preparación entre las empresas grandes (250-999 empleados) y las empresas de más de 1.000 trabajadores. La mayor proporción de ciberexpertas se encuentra entre los negocios a escala empresarial y las grandes empresas estadounidenses (el 36% y el 35%, respectivamente). Las empresas británicas son las siguientes (el 33%). A nivel mundial, más de la mitad (53%) de las empresas con menos de diez empleados obtienen la calificación de cibernovatas, al igual que un tercio de las que se encuentran en el grupo de empleados de 10 a 49.

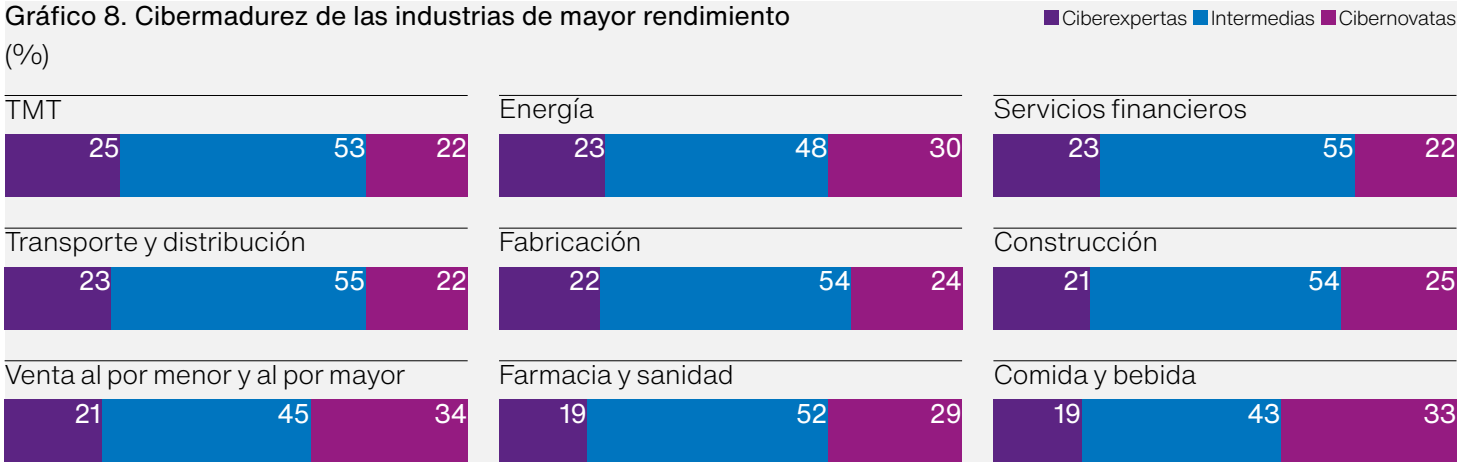
Gráfico 7. Cómo funciona el modelo de evaluación de madurez

Nuestro modelo evalúa la madurez de la empresa transversalmente a través de seis áreas operacionales (dominios) utilizando el marco de medición COBIT® y la arquitectura de seguridad SABSA®. Los seis dominios (véase la tabla debajo) constituyen todos los elementos necesarios para instalar, dirigir, gestionar y gobernar un sistema de seguridad eficaz. Cada dominio se mide contra cada uno de estos tres ámbitos: personas, procesos y tecnología. Las empresas se puntúan sobre una escala de cinco puntos. Cualquier puntuación superior a cuatro califica a la empresa como "ciberexperta". A partir de 2,5 se les considera "ciberintermedias". Por debajo de 2,5, se clasifican como "cibernovatas".

	Personas	Procesos	Tecnología	Promedio total
Gestión de la resiliencia empresarial	3.12	3.13	3.10	3.12
Gestión de contraseñas y criptografía	2.93	2.90	2.94	2.93
Gestión de identidades y accesos	3.05	2.95	2.94	2.97
Gestión de eventos e información de seguridad	2.93	3.10	2.99	2.99
Gestión de amenazas y vulnerabilidades	3.00	3.12	3.28	3.13
Gestión de la confianza	3.07	3.05	3.09	3.07
Promedio total	3.02	3.04	3.06	3.03

Gráfico 8. Cibermadurez de las industrias de mayor rendimiento

(%)



64%

El 64% de los encuestados dicen estar "muy seguros" sobre su ciberpreparación.

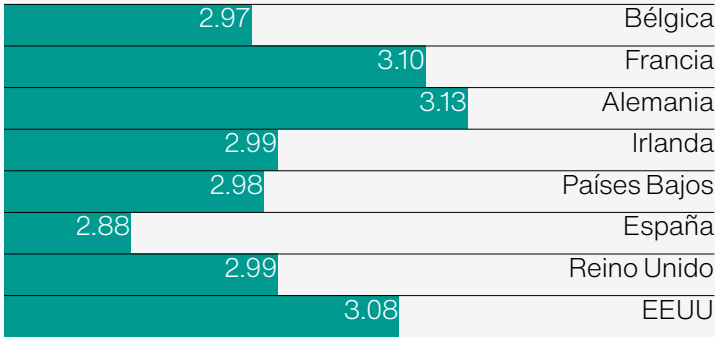
Lo que nos dice el modelo
Utilizando las puntuaciones globales de ciberpreparación, el modelo pone de manifiesto una brecha dramática entre las ciberexpertas y el resto, con una media del 4,38 para las expertas y solo del 1,69 para las novatas (ver Gráfico 10.). A la hora de analizar los puntos fuertes y débiles de las empresas, el desglose entre dominios y funciones es instructivo.

Dominios
Hay dos dominios que destacan como puntos fuertes relativos: la gestión de las amenazas y la vulnerabilidad, y la gestión de la resiliencia empresarial (donde las empresas obtuvieron una media del 3,13 y 3,12, respectivamente). Las empresas alemanas obtuvieron las mejores puntuaciones, seguidas de cerca por las francesas y las estadounidenses. Las empresas españolas obtuvieron la puntuación más baja, al igual que en todos los dominios. Las puntuaciones aumentan de acuerdo con el tamaño de la empresa y se estabilizan una vez que se alcanza la marca de 250 empleados.

En el conjunto de los seis dominios, hay tres sectores que destacan. El sector de TMT obtuvo la mejor puntuación, como cabía esperar, pero el sector de servicios financieros y el sector del transporte/ distribución quedaron muy cerca. Los servicios profesionales fueron los que obtuvieron las peores puntuaciones.

Numerosas empresas quedaron rezagadas por las bajas puntuaciones en criptografía y gestión de contraseñas (ocio y turismo, servicios empresariales y servicios profesionales, en particular) y, en menor medida, en gestión de identidades y accesos. Esto es preocupante. La criptografía es la base de todo sistema informático moderno y es fundamental para cualquier otro control. Cabe destacar que el informe muestra una fuerte correlación entre la incidencia de los peligros del correo electrónico empresarial y las bajas puntuaciones obtenidas en la configuración y gestión de los controles criptográficos.

Fig. 9. Puntuaciones compuestas de preparación



Funciones
En cuanto a las funciones, el modelo puntúa las operaciones de ciberseguridad de las empresas en tres ámbitos: personas, procesos y tecnología. En general, las puntuaciones más bajas se dan en el primer ámbito, lo que indica que muchas empresas tienen trabajo que hacer para contratar y formar a personas cualificadas debidamente y con experiencia.

Como podría esperarse, los niveles de experiencia suelen aumentar en función del tamaño de la empresa. Las empresas más pequeñas, con menos de 10 empleados, están muy alejadas, pero muchas carecen de la capacidad de emplear a un especialista en este ámbito.

Una vez más, las empresas alemanas y francesas son las que marcan la pauta, y las estadounidenses no se quedan atrás. Las empresas españolas cierran la lista, con una puntuación baja especialmente en tecnología. Al igual que con los dominios anteriores, el sector TMT ocupa el primer lugar, aunque tanto los servicios financieros como el transporte / distribución obtienen una puntuación más alta en el proceso (ver Gráfico 9.).

Resulta interesante, en un año en el que ha aumentado el número de ciberataques, que una mayor proporción de encuestados afirme estar “muy seguro de su preparación en materia de ciberseguridad”: el 64%, frente al 62% del año anterior y el 57% del año precedente. Sigue existiendo un gran abismo entre las ciberexpertas, que en un 84% expresan confianza en su preparación, y las cibernovatas (solo un 43%).

La visión de Hiscox

No es sorprendente que algunas medidas de ciberseguridad más establecidas obtengan puntuaciones más altas. Por ejemplo, copias de seguridad y recuperación ante desastres en "Gestión de la resiliencia empresarial" y medidas como firewalls y antivirus en "Gestión de amenazas y vulnerabilidades". Las puntuaciones también destacan una debilidad general en "Criptografía y gestión de claves", donde incluso los expertos tienden a tener un desempeño deficiente. Este es un problema común. Entre las áreas más complicadas de dominar, la criptografía sufre una notoria escasez de habilidades.

Gráfico 10. Puntuaciones compuestas de preparación

Cibernovatas	Personas	Procesos	Tecnología	Promedio total
Gestión de la resiliencia empresarial	1.83	1.86	1.75	1.81
Gestión de contraseñas y criptografía	1.58	1.54	1.52	1.55
Gestión de identidades y accesos	1.80	1.71	1.63	1.69
Gestión de eventos e información de seguridad	1.57	1.90	1.61	1.65
Gestión de amenazas y vulnerabilidades	1.65	1.85	2.24	1.91
Gestión de la confianza	1.76	1.71	1.72	1.73
Promedio total	1.70	1.76	1.74	1.72

Ciberexpertas	Personas	Procesos	Tecnología	Promedio total
Gestión de la resiliencia empresarial	4.44	4.43	4.43	4.43
Gestión de contraseñas y criptografía	4.29	4.25	4.34	4.29
Gestión de identidades y accesos	4.37	4.29	4.38	4.34
Gestión de eventos e información de seguridad	4.32	4.34	4.38	4.35
Gestión de amenazas y vulnerabilidades	4.34	4.36	4.29	4.33
Gestión de la confianza	4.37	4.37	4.46	4.41
Promedio total	4.35	4.34	4.38	4.36

Lo que nos pueden enseñar las ciberexpertas

Gestionar el riesgo

Es imposible garantizar una seguridad total. Pero tener la capacidad de responder rápida y eficazmente, y de recurrir a la experiencia externa cuando las cosas se ponen feas, garantiza la resiliencia. Esto es lo que hacen las ciberexpertas. Casi la mitad (el 47%) afirma tener una póliza de ciberseguridad independiente, frente al 45% del año pasado. Pero el abismo entre ellas y el resto se ha ampliado. Entre las cibernovatas, solamente el 11% dice ahora lo mismo (frente al 18% del año pasado).

Nombrar a un responsable

Muchas empresas son demasiado pequeñas para poder justificar la existencia de un especialista en ciberseguridad, pero eso no es motivo para dejar de asignar a alguien la responsabilidad de esta materia o de designar a un proveedor de servicios externo para que realice el trabajo. Casi la mitad (el 48%) de las empresas con menos de 10 empleados y el 45% de las cibernovatas afirmaron no tener una función definida para la ciberseguridad.

Hacer frente a las principales vulnerabilidades

Siete de cada diez ciberexpertas consideran que el paso al teletrabajo aumenta su vulnerabilidad a los ataques. Solo el 40% de las cibernovatas está de acuerdo con ellas. La prioridad número uno de las ciberexpertas para este próximo año es hacer frente a las "amenazas y vulnerabilidades existentes". Así lo mencionan casi tres cuartas partes de ellas (el 74%). El doble de ciberexpertas que de cibernovatas tienen la intención de reforzar la seguridad de los servicios y aplicaciones orientados al cliente. Nos están diciendo algo.

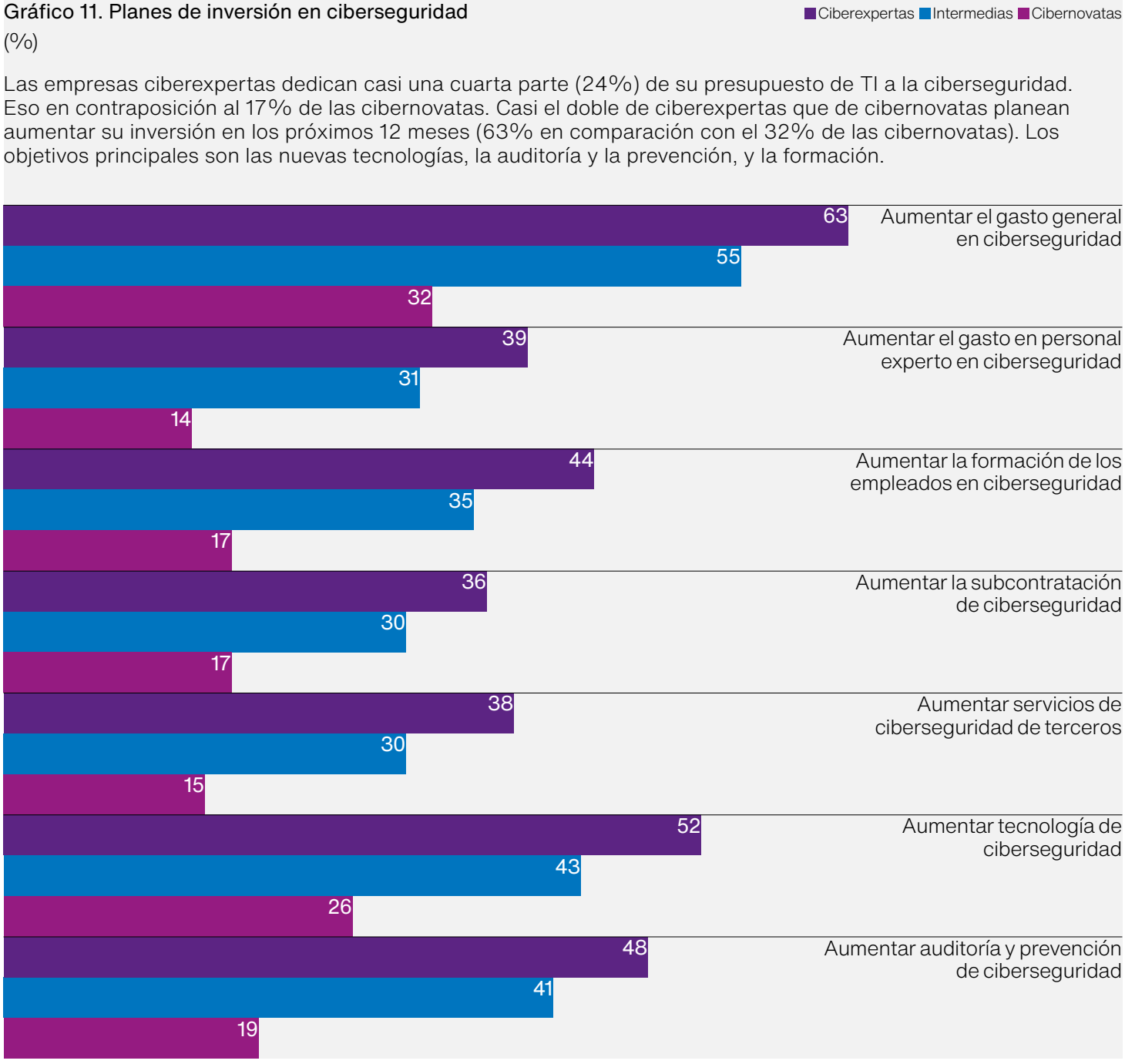
Copias de seguridad, preferiblemente fuera de las instalaciones

Las ciberexpertas mostraron una mayor tendencia a repeler todos los ataques antes de que causen daños. Una de cada siete (el 14%) afirmó que los ataques DDoS/ ransomware no habían tenido ningún impacto financiero. Una de las razones esgrimidas es la mayor probabilidad de estar en condiciones de recuperar sus datos. Casi dos quintas partes (el 39%) lo hicieron tres o más veces el año pasado. Es crucial hacer lo básico, por ejemplo, una copia de seguridad de todos los datos, preferiblemente fuera de las instalaciones.

Gráfico 11. Planes de inversión en ciberseguridad

(%)

Las empresas ciberexpertas dedican casi una cuarta parte (24%) de su presupuesto de TI a la ciberseguridad. Eso en contraposición al 17% de las cibernovatas. Casi el doble de ciberexpertas que de cibernovatas planean aumentar su inversión en los próximos 12 meses (63% en comparación con el 32% de las cibernovatas). Los objetivos principales son las nuevas tecnologías, la auditoría y la prevención, y la formación.



Construir la resiliencia

El gasto en ciberseguridad representa ahora una parte mucho mayor del gasto global en TI, ya que las empresas intensifican sus medidas de prevención.

Las empresas han reorientado radicalmente sus presupuestos de TI en el último año. Aunque el gasto medio en TI ha cambiado poco en general, la proporción que se dedica a la ciberseguridad ha aumentado un destacable 63%. La empresa media dedica ahora más de una quinta parte (el 21%) de su presupuesto de TI a la ciberseguridad, frente a algo menos del 13% el año anterior. Esto supone un gran cambio de actitud.

Dada la proporción importante de pequeñas empresas, el aumento global del gasto en ciberseguridad en nuestro grupo de estudio es un 25% más modesto, de 10.400 a 13.000 millones de Euros, o un 23% después de ajustar el aumento del número de encuestados de 4.313 a 4.412.

Las empresas alemanas fueron las que más gastaron por término medio en ciberseguridad, con 5,0 millones de Euros, lo que supone un aumento del 155% con respecto al año anterior, tal vez como reconocimiento de su vulnerabilidad manifiesta, que se expone en otra parte de este informe. Las empresas belgas fueron las que menos gastaron (1,6 millones de Euros).

En los distintos sectores, las empresas energéticas fueron las que más dinero destinaron (12,2 millones de Euros de media en ciberseguridad). Les siguieron las compañías de servicios financieros (5,1 millones de Euros de media), y las empresas del sector industrial (4,9 millones de Euros). Las empresas de viajes fueron las que menos gastaron (646.364 €), pero eso puede reflejar el hecho de que muchas entraron en hibernación con el inicio de la pandemia.

El crecimiento más rápido ha ocurrido en los extremos opuestos del espectro empresarial, el más pequeño y el más grande (ver Fig. 13.). Las empresas de entre 10 y 49 empleados también han aumentado el gasto más de diez veces, hasta los 359.091 €. En el extremo opuesto, las grandes empresas dedican ahora una media de 11,8 millones de Euros, frente a los 3,8 millones de Euros de hace dos años. Sin embargo, en términos de gasto por empleado siguen estando muy por detrás del resto, lo que sugiere que las empresas más grandes tienen capacidad todavía para aumentar el gasto.

Gráfico 12. El gasto medio por empresa en ciberseguridad o en dos años

(m€)

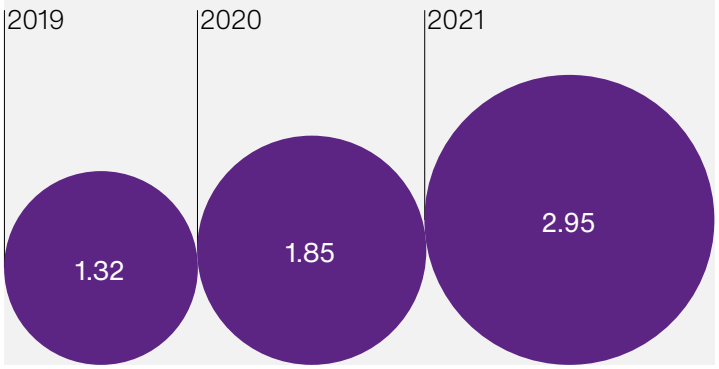


Gráfico 13. Gasto en ciberseguridad Por número de empleados

(€)

	2021	2020
1–9	112.455	12.090
10–49	359.159	72.202
50–249	289.399	255.884
250–999	1,751.905	784.380
1.000+	11,876.082	7,299.115

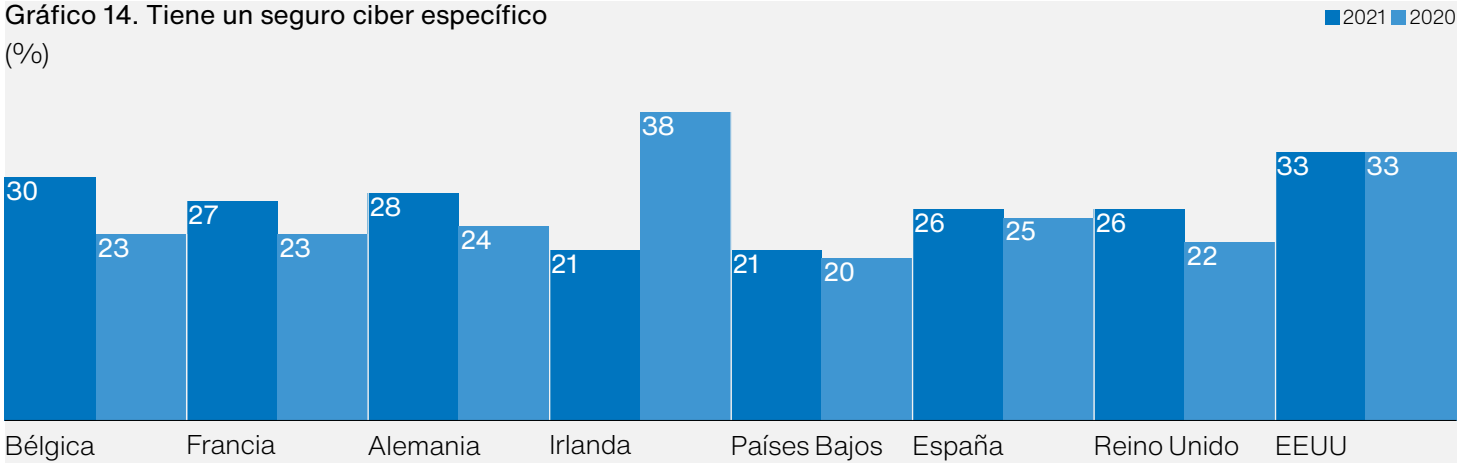
El aumento del gasto parece que va a continuar, aunque a un ritmo algo menos desmedido. A nivel de cada empresa, el incremento del presupuesto previsto para el año que viene es del 51% de media. Esto contrasta con el 72% del año anterior, que resultó ser bastante preciso.

La visión de Hiscox

En 2020, las empresas se vieron obligadas a trabajar de forma remota de un día para otro, pasar del contacto físico al online e interactuar con los clientes en un canal completamente diferente. Un beneficio del cambio repentino al mundo online fue reconocer la importancia de desarrollar la ciberresiliencia y, por lo tanto, un aumento en el gasto en ciberseguridad. Sin embargo, los ataques, los impactos y el enfoque en la seguridad cibernética difieren según la industria, por lo que algunos estarán mejor preparados para gestionar cambios drásticos en el futuro.

Gráfico 14. Tiene un seguro ciber específico

(%)



¿Dónde se gasta el dinero?

Dos de cada cinco empresas (40%) indican que planean aumentar el gasto en tecnología de ciberseguridad entre un 5% y un 10%, mientras que el 36% dice lo mismo con respecto a la auditoría y prevención de la ciberseguridad. Por todo ello, disminuye el número de empresas que mencionan un mayor gasto en personal y formación (del 35% al 27% en personal y del 40% al 32% en formación). Esto parece desafortunado dada la debilidad relativa del segmento "personas" de nuestro modelo de ciberpreparación.

También se observa que en este año son menos las empresas que toman medidas decisivas tras un ataque. Entre las que han un sufrido un ataque, la proporción de las que dicen que evalúan la seguridad y/o la privacidad regularmente ha bajado del 32% al 19%, mientras que el número de las que introducen requisitos adicionales de ciberseguridad/auditoría ha bajado del 26% al 20%. En consonancia con los resultados anteriores, solo el 16% menciona el gasto adicional en la formación de los empleados y el cambio cultural, frente al 25% del año pasado.

Un panorama mixto para los seguros ciber

La contratación del seguro ciber está aumentando, tanto a través de pólizas específicas (el 27% tiene ahora una, frente al 26%) como de otros seguros con coberturas ciber (el 34% frente al 32% del año pasado). El número de empresas que tiene previsto adquirir una póliza específica ha crecido marginalmente, del 11% al 12%, mientras que la proporción que tiene previsto agregar cobertura de seguro ciber a una póliza existente se mantuvo estática, en un 7%. El número de las que dicen que no tienen cobertura y que no tienen previsto adquirirla ha descendido (el 18% frente al 21% del año anterior).

La compra de una póliza específica es más alta entre las empresas de 250 o más empleados (el 36% para las empresas de 250 a 999 empleados y el 38% para las empresas de más de 1000 empleados). Llegar a las empresas más pequeñas sigue siendo un reto: casi la mitad de las que tienen menos de 10 empleados (el 44%) dicen que no tienen intención de contratar un seguro. Lo que antecede es preocupante, teniendo en cuenta la evidencia de este estudio de que las empresas más pequeñas son vulnerables a los ataques de phishing y al robo de credenciales, y el potencial de pérdidas enormes que van más allá de la media.

Las empresas estadounidenses siguen siendo líderes en este ámbito (ver Gráfico 14.). Un tercio (el 33%) cuenta con una cobertura independiente; las empresas belgas ocupan el segundo lugar en la tabla, con un 30%. Las empresas irlandesas, españolas y alemanas son las más propensas a decir que están cubiertas como parte de otra póliza (el 43%, el 37% y el 36% respectivamente).

46%

Aumento medio en el porcentaje de personal que trabaja en remoto debido a Covid-19.

Destacan dos sectores: servicios financieros y TMT. Entre los primeros, el 39% tiene una póliza ciber independiente, mientras que el 37% tiene cobertura como parte de otra póliza. En TMT, las cifras equivalentes son el 34% y el 37%. Las empresas del sector industrial son las que más recurren a otra póliza (el 42%).

Abismo en la percepción del impacto del Covid-19

A pesar del aumento de casos de phishing relacionados con el coronavirus y la explosión del trabajo desde casa, puede sorprender que la comprensión de la amenaza añadida que supone la pandemia sea desigual. Menos de la mitad de los encuestados (el 47%) afirma que su organización "ha sido más vulnerable a los ciberataques desde el comienzo de la pandemia", aunque la cifra se eleva a cerca del 59% entre las empresas con 250 o más empleados. Existe un abismo claro de percepción entre las empresas más pequeñas, de las que menos de un tercio (el 31%) reconoce su mayor vulnerabilidad.

En general, los niveles de trabajo a distancia han aumentado considerablemente. La empresa media de nuestro grupo de estudio ha aumentado el porcentaje de su plantilla que teletrabaja del 14% al 60%. Pero el cambio se concentra en una minoría de empresas. Dos de cada cinco (el 41%) afirman haber aumentado el número de empleados que en remoto, mientras que el 29% ha incrementado el uso de tecnologías basadas en la nube y el 32% emplea más tecnologías de colaboración. En cada caso, el porcentaje aumenta en función del tamaño de la empresa.

Hay más preocupación por la cuestión específica del teletrabajo. Casi tres de cada cinco empresas (el 58%) están de acuerdo en que "debido a que trabajan desde casa más empleados, mi organización es más vulnerable a los ciberataques". Una vez más, la percepción está más extendida entre las empresas más grandes (rozando el 69% en las empresas de 250 empleados o más).

Las empresas más grandes son también más propensas a haber actuado para limitar su vulnerabilidad creciente: más de dos tercios de las empresas y de las que tienen más de 250 empleados dicen haber reforzado sus ciberdefensas (el 68% y el 67%, respectivamente).

Gráfico 15. Mayor ciberseguridad debido a Covid-19

Número de empleados

(%)

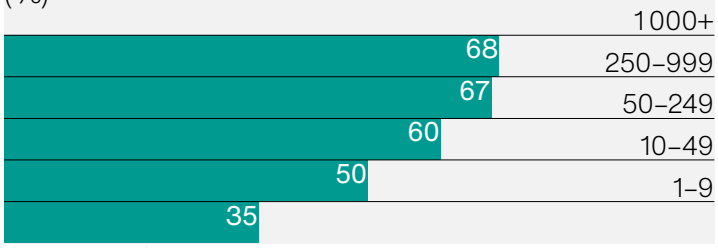


Gráfico 16. Cambios debido a Covid-19

(%)

Mayor número de personal que trabaja en remoto	41
Contratación pausada	33
Mayor uso de tecnologías de colaboración	32
Costes operativos reducidos	31
Mayor uso de tecnologías basadas en la nube	29
Pagos en línea ampliados	27
Planes de transformación digital acelerados	27
Canales de comercio electrónico existentes ampliados	20
Volumen reducido de cambios de TI	18
Nuevos canales de comercio electrónico añadidos	18
Número consolidado o reducido de proveedores	15

En el caso de las empresas más pequeñas, de hasta nueve empleados, la cifra equivalente es solo del 35%. Las cifras indican que hay todavía una franja amplia de empresas, y no solo las más pequeñas, que no han asumido aún la vulnerabilidad añadida que supone el teletrabajo.

El quinto estudio anual internacional Hiscox Cyber Readiness Report se ha llevado a cabo en colaboración con la empresa de investigación de mercados Forrester. El informe proporciona no solo un panorama actualizado de la ciberpreparación de las organizaciones, sino que ofrece también un plan de buenas prácticas en la lucha contra una amenaza en constante evolución. La investigación se basa en una encuesta realizada a ejecutivos, jefes de departamento, directores de TI y otros profesionales clave escogidos de una muestra representativa de 6.042 organizaciones de ocho países por tamaño y sector, por ser las personas que están en primera línea de la batalla empresarial contra la ciberdelincuencia. Los encuestados realizaron la encuesta online entre el 5 de noviembre de 2020 y el 8 de enero de 2021.

Nivel (%)	
Fundador/Ejecutivo de nivel C	50
Vicepresidente	13
Director	22
Gerente	16

Sector (%)	
Servicios empresariales	8
Energía	4
Construcción	8
Servicios financieros	8
Comida y bebida	4
Gobierno y organizaciones sin ánimo de lucro	5
Fabricación	8
Farmacia y sanidad	8
Servicios profesionales	8
Inmobiliario	4
Venta al por menor y al por mayor	9
TMT	16
Transporte y distribución	5
Ocio y turismo	4

Número de empleados (%)	
1.000+	25
250–999	15
50–249	15
10–49	16
1–9	29

Departamento (%)	
Dirección ejecutiva	14
Comercio electrónico	2
Finanzas	9
Asesoramiento general	2
Recursos humanos	6
TI y tecnología	21
Marketing y comunicación	3
Operaciones	11
Propietario	21
Compras	2
Gestión de productos	3
Gestión de riesgos	3
Ventas	5

Hiscox España

c/ Miguel Ángel, 11 4º planta
28010 Madrid

+34 915 15 9900
info_spain@hiscox.com
hiscox.es/hiscox-cyber-readiness-report-2021

21486 04/21