HISCOX

INFORME DE CIBERPREPARACIÓN 2025

Las pymes toman medidas contra las amenazas actuales y futuras a la ciberseguridad

Índice

El informe de Ciberpreparación de Hiscox se basa en una investigación realizada por Wakefield Research sobre 5750 empresas, en la que se entrevistó a las personas responsables de la estrategia de ciberseguridad de sus empresas. Esto abarca al propietario, director o socio de aquellas empresas con menos de 50 empleados y al CIO, CISO o director/vicepresidente de seguridad o IT de aquellas empresas con entre 50 y 249 empleados.

La investigación se llevó a cabo entre el 29 de julio y el 8 de agosto de 2025, mediante una invitación por correo electrónico y una encuesta online. Los encuestados se pueden desglosar por zonas geográficas de la siguiente manera: 1000 encuestados en Estados Unidos, Reino Unido, Francia, Alemania y España, respectivamente; 500 encuestados en Irlanda y 250 en Portugal.

Como datos de investigación, esto supone una muestra representativa de empresas aseguradas y no aseguradas que pueden haber presentado o no una reclamación al seguro tras un incidente. No tiene por qué reflejar nuestra propia experiencia en materia de reclamaciones ni la del sector asegurador en general.

Introducción

Eddie Lamb
Director Global de Cyber
Hiscox

El auge del comercio digital ha generado enormes oportunidades para las pequeñas empresas, lo que les ha permitido innovar, llegar a nuevos mercados y jugar un papel cada vez más importante en la economía mundial. Es posible que el avance más importante de los últimos tiempos sea la inteligencia artificial (IA), que ha permitido a las pymes usar herramientas y recursos que antes estaban fuera de su alcance.

Pero estas oportunidades también entrañan retos. A medida que las empresas adoptan nuevas tecnologías, también deben desenvolverse en un entorno en el que las ciberamenazas en constante evolución pueden poner en peligro su éxito de nuevas maneras. Esta novena edición del Informe de Ciberpreparación de Hiscox está diseñada para ayudar a las pequeñas y medianas empresas (pymes) a desentrañar mejor los riesgos a los que se enfrentan en nuestro mundo en rápida evolución e impulsado por la tecnología, así como las medidas que pueden adoptar para minimizar su exposición a dichos riesgos. Como persona que ha creado y desarrollado su propia pequeña empresa, es algo que me apasiona en particular.

Conversamos con 5750 empresas de Reino Unido, Estados Unidos, Francia, Alemania, España, Irlanda y Portugal para comprender el impacto que los ciberataques tienen en sus negocios y las amenazas más comunes a las que se enfrentan. Más de la mitad afirmó haber sufrido un ciberataque en los últimos 12 meses y un tercio de ellas afirmó haber recibido una multa regulatoria como resultado de una violación de datos tan grave que estaba a la altura de afectar a la salud financiera de su empresa.

Esto subraya la necesidad de que las pymes tomen todas las medidas necesarias para proteger los datos de los clientes, de acuerdo con los requisitos normativos, como el Reglamento General de Protección de Datos (RGPD) de Europa o las leyes de protección al consumidor que aplica la Comisión Federal de Comercio (FTC) en EE. UU.

Los ataques con ransomware siguen representando una amenaza muy persistente para muchas empresas. Las pymes con las que hablamos nos contaron sus propias experiencias con ataques de ransomware y algunas pagaron varias veces para intentar proteger sus datos confidenciales, aunque pagar el rescate no garantiza la recuperación de dichos datos. Tres de cada cinco pymes que pagaron un rescate afirmaron haber recuperado una parte o la totalidad de sus datos, pero, a pesar de pagar el rescate, a casi un tercio se les exigió más dinero.

Nuestro informe también analiza el impacto de la IA en las pequeñas empresas, a las que puede beneficiar o perjudicar. Si bien la IA ofrece oportunidades y nuevas formas de detectar y responder a las amenazas, también introduce nuevas vulnerabilidades, lo que crea puntos de entrada ciegos y expone brechas en la seguridad de los datos que los hackers pueden aprovechar de manera muy similar a como lo hacían con los ciberataques hace diez o quince años. Con la creciente integración de la IA en las actividades empresariales cotidianas, nuestros equipos de especialistas en Hiscox se centran en definir sus riesgos, establecer una cobertura para ella y proporcionar los conocimientos y la formación necesarios en torno a ella para apoyar a los propietarios de pequeñas empresas de todo el mundo.

Sin embargo, aunque el panorama cibernético pueda estar construido sobre arenas movedizas, la respuesta de las pymes es proactiva y pragmática. La inmensa mayoría de las pymes (94 %) prevé aumentar sus inversiones en ciberseguridad y protección de datos durante los próximos 12 meses. Esto incluye la contratación de ciberespecialistas, la actualización de los programas de formación, la realización de comprobaciones periódicas de vulnerabilidad y la reevaluación de los riesgos en sus cadenas de suministro.

En Hiscox, nos complace colaborar con estas empresas para ofrecerles seguros, conocimientos, experiencia y apoyo. Nuestros más de 20 años de experiencia en seguros de privacidad y ciber y nuestro trabajo con más de 80 000 clientes de seguros ciber en todo el mundo, nos permiten ayudar cada día a las empresas a recuperarse de incidentes, reforzar sus defensas y desarrollar una resiliencia a largo plazo.

En lo que respecta a la ciberseguridad y la resiliencia empresarial, no podemos permitirnos el lujo de dormirnos en los laureles y dar por concluido nuestro trabajo. Por el contrario, debemos mantener nuestra determinación colectiva de combatir la ciberdelincuencia y priorizar un compromiso continuo con la gestión de los riesgos ciber.

Esperamos que este informe inspire a más empresas a valorar su propio nivel de ciberpreparación mediante nuestro modelo de madurez cibernética, fomente el debate y contribuya a la elaboración de estrategias cibernéticas aún más fundamentadas.

Resumen ejecutivo

El 83%
declaró una mejora en la ciberresiliencia.

Nadie ha dicho nunca que mantener la seguridad de las pymes (pequeñas y medianas empresas) sea una tarea sencilla. Este fundamental grupo impulsa el 50 % de la economía mundial, y quienes las dirigen se enfrentan a un amplio abanico de retos, en muchos casos, compaginando responsabilidades en todos los ámbitos, desde las operaciones, las ventas, el marketing, la marca, la tecnología y los recursos humanos, entre otros.

Una de sus tareas más complicadas es la de evaluar los riesgos, lo que les exige comprender la constante evolución de las amenazas a las que se enfrentan las empresas. La complejidad de estas amenazas sigue en aumento a medida que los avances tecnológicos, como los agentes de inteligencia artificial, transforman el mundo que nos rodea.

En esta novena edición del Informe anual sobre ciberpreparación de Hiscox, analizamos el impacto de estos riesgos digitales en rápida evolución, lo que implican y cómo las pequeñas empresas pueden tomar medidas para atenuar su exposición.

Casi todas las pymes (94 %) prevén aumentar sus inversiones en ciberseguridad y protección de datos en los siguientes 12 meses, actualizar la formación ciber de los empleados (70 %) y contratar personal adicional para aumentar la ciberresiliencia (60 %).

El informe de este año revela la determinación de las pymes de no solo invertir en software y formación, sino también de mantenerse al día con evaluaciones de riesgos y comprobaciones de vulnerabilidad frecuentes, además de contratar pólizas de ciberseguro para cuando las cosas se compliquen.

Gracias a este enfoque proactivo, las empresas están mostrando una mayor confianza, mientras que el 83 % afirma haber mejorado la ciberresiliencia de su empresa en los últimos 12 meses.

La complejidad de los riesgos digitales sigue aumentando. Las empresas se enfrentan al reto de gestionar las secuelas de los ataques de ransomware, entre los que encontramos los cambios normativos, como una nueva ley en Australia que obliga a las empresas a revelar las cantidades pagadas en concepto de rescate. Se trata de una norma que también podría adoptarse en otros países, pues una amplia mayoría (71 %) de las empresas considera que estas revelaciones deberían ser obligatorias.

A pesar de este apoyo, las opiniones divergen sobre si estos requisitos deberían aplicarse a las empresas privadas. La mayoría (53 %) cree que las empresas privadas no deberían estar obligadas a revelar de forma abierta su situación financiera en lo que respecta a los pagos de rescates por ransomware.

Aunque nunca ha sido tan difícil hacer negocios debido a las amenazas online (el 60 % considera que la ingeniería social basada en IA, el malware de IA y los ataques de phishing serán las principales amenazas que surgirán en los próximos cinco años), está claro que los expertos en ciberseguridad y los directivos trabajan sin descanso para proteger a sus organizaciones, empleados y clientes.

En los últimos 12 meses, el 59 % de las pymes han sufrido un ciberataque, pero en lugar de quedarse de brazos cruzados, están invirtiendo, formando a su personal y actualizando sus sistemas para adaptarse a un panorama en constante desarrollo.

Resultados principales

El 59 %
de los encuestados sufrió un ciberataque en los últimos 12 meses.

El 33 %
recibió multas significativas tras sufrir un ciberincidente.

El 94 %
está aumentando la inversión en ciberseguridad y protección de datos.

El 60 %
está contratando personal adicional para aumentar su ciberresiliencia.

El 88 %
realiza evaluaciones trimestrales sobre riesgos de proveedores y socios.

El 91 %
realiza comprobaciones de cibervulnerabilidad cada tres meses.

El 27 %
experimentó un ataque de ransomware en los últimos 12 meses

El 71 %
apoya la declaración obligatoria de los pagos de ransomware.

Estado de los ataques

El 60%
pagó un rescate y logró la recuperación total o parcial de los datos.

Las entidades que han sufrido un ciberataque en el último año no solo han tenido que hacer frente a un incidente, sino que es probable que hayan sido atacadas en múltiples ocasiones. Casi tres de cada cinco (59 %) empresas han sufrido al menos un ciberataque en los últimos 12 meses.

Entre las empresas que sufrieron un ataque, las más grandes o las que tienen mayores ingresos fueron más propensas a sufrir un mayor número de incidentes. Por ejemplo, las empresas con ingresos anuales de 10 millones de dólares o más y aquellas con ingresos de entre 1 y 10 millones de dólares que sufrieron un ataque en el último año tuvieron más ataques de media (unos seis) que aquellas con ingresos inferiores a 1 millón de dólares (unos cuatro).

Del mismo modo, entre las empresas que sufrieron un ataque, las que tenían entre 50 y 249 empleados registraron una media de siete ataques en el último año, frente a las empresas que tienen entre 11 y 49 empleados (una media de unos cinco ataques) y las que tenían entre uno y diez empleados (una media de cuatro ataques).

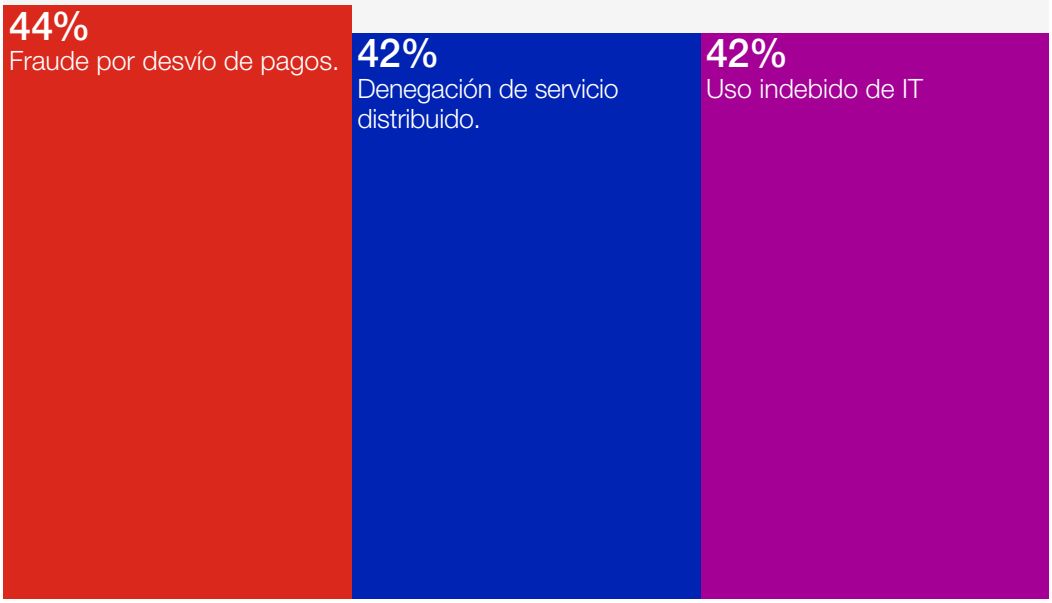
Entre las empresas que notificaron incidentes, el número medio de ataques osciló entre unos tres en sectores como el químico, inmobiliario y de los medios de comunicación, frente a unos ocho en el sector sin ánimo de lucro. Un ciberataque exitoso puede causar daños inmediatos y considerables, como la interrupción de las operaciones, el aumento de los costes y la exposición de datos confidenciales.

Las empresas están viendo cómo los atacantes se aprovechan de las vulnerabilidades de su propio hardware y de los socios con los que trabajan. Los dispositivos de Internet of Things (IoT) propiedad de las empresas fueron el punto de entrada más común para los ciberataques durante el último año (33 %), seguidos por las vulnerabilidades en las cadenas de suministro, como los sitios web de los proveedores (28 %) y los servidores corporativos en la nube (27 %). Las herramientas y el software de inteligencia artificial fueron el primer punto de entrada para el 15 % de las empresas.

A ninguna empresa le gusta tener que pagar a los delincuentes por secuestrar sus datos, pero cuando se trata de ataques de ransomware, es normal que las empresas hagan todo lo posible por recuperar aquello que podrían perder, lo que significa pagar el rescate cuando se les exige. De aquellas que pagaron un rescate, el 60 % recuperó parte o la totalidad de sus datos. Dos de cada cinco (41 %) recibieron una clave de recuperación, pero, aún así, tuvieron que reconstruir sus sistemas.

Pagar un rescate no siempre significa resolver el problema. Por el contrario, los atacantes exigieron más dinero al 31 % de los que pagaron. El 27 % de los que pagaron un rescate sufrieron un ataque adicional, aunque no necesariamente por parte de la misma entidad.

Estado de los ataques
Resultados de los ataques sufridos por las empresas en los últimos 12 meses.



Estado de los ataques
continuación

El 71%
de las empresas cuenta con algún tipo de ciberseguro.

Las secuelas de un ciberataque pueden ser graves y duraderas y, en ocasiones pueden poner en peligro la subsistencia de una empresa. Un 33 % de las empresas afectadas incurrieron en multas importantes como para perjudicar su salud financiera, mientras que muchas también informaron de un descenso en los indicadores de rendimiento empresarial (30 %), un aumento de los costes de notificación a los clientes (29 %) y una mayor dificultad para atraer nuevos clientes (29 %).

El panorama es complejo para quienes tienen que afrontar una multa. Las empresas que operan en el extranjero pueden estar sujetas tanto a sanciones en su país de origen, como en el país o región donde operan. Una violación de datos puede dar lugar a multas por no proteger la privacidad de los clientes en mercados como California, Canadá o la UE, donde las sanciones reglamentarias pueden suponer millones para las empresas.

El seguro es una herramienta que utilizan las empresas para mitigar los efectos de estos ataques. La mayoría de las empresas encuestadas (71 %) cuentan con una póliza de seguro o cobertura ciber como parte de otra póliza.

Las empresas con diez o menos empleados son menos propensas (65 %) a tener un seguro ciber que aquellas con entre 11 y 49 empleados (79 %) o aquellas con entre 50 y 249 empleados (82 %).

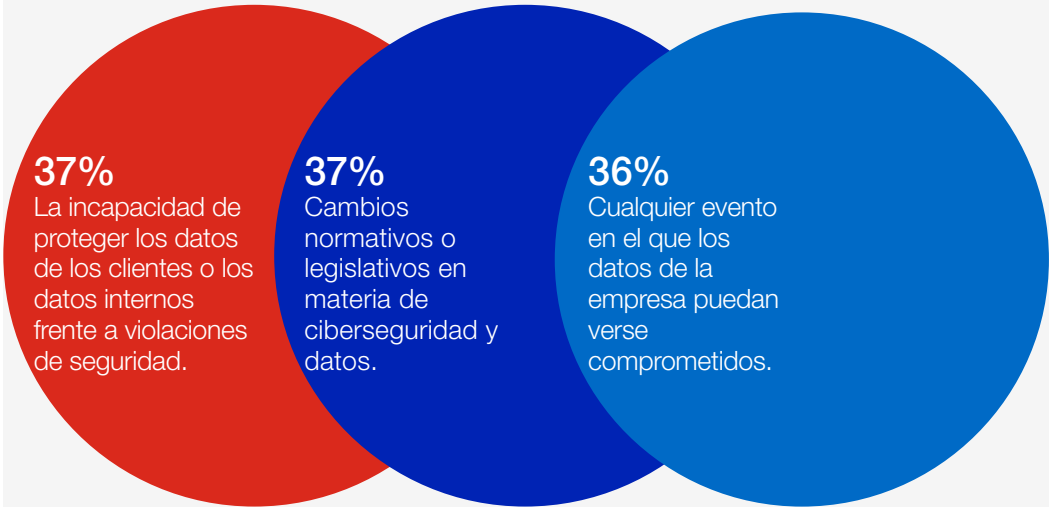
El impacto de los ciberataques en el personal de la empresa es considerable. Los incidentes cibernéticos causan un alto nivel de estrés a los empleados (39 %) y pueden provocar agotamiento (32 %) o un aumento de las bajas por enfermedad (31 %).

Si bien la experiencia puede generar un mayor sentido de compañerismo (38 %) y lealtad hacia la empresa (43 %), esto solo pone aún más de relieve la necesidad de que las empresas apoyen a sus empleados durante y después de un ataque.

El informe de este año revela cómo la inteligencia artificial está transformando realmente el panorama de las ciberamenazas. Pero, más allá de eso, destaca el doble papel de esta tecnología: por un lado, aunque está emergiendo como un activo estratégico para reforzar la ciberresiliencia de las empresas, también se ha convertido en una herramienta para los ciberdelincuentes, un hecho que aumenta la sofisticación y la complejidad de los ciberataques.

Ana Silva
Directora de PSC
Hiscox Iberia

Principales riesgos ciber
Los tres mayores riesgos para las empresas.



Nunca se debe subestimar el impacto humano de un ciberataque. Los empleados se enfrentan a un enorme estrés, un factor que puede provocar un aumento del absentismo o incluso un gran desgaste. Apoyar al personal tras las consecuencias no solo es lo correcto, sino que ayuda a la empresa a recuperarse y a desarrollar una mayor resiliencia para el futuro.

Mike Maletsky
Vicepresidente y líder de prácticas
Tecnología y ciberseguridad
Hiscox USA

Medidas

El 79%
invierte en ciberseguridad adicional para los empleados que teletrabajan.

Casi todas las empresas están destinando recursos a la prevención de ataques y el 94 % prevé aumentar la inversión en ciberseguridad y protección de datos durante el próximo año. Portugal (45 %) y España (40 %) encabezan la lista de países en los que se espera un aumento considerable de la inversión.

Más de la mitad (54 %) de las empresas del sector automovilístico a nivel mundial tienen previsto aumentar en gran medida su inversión en ciberseguridad y protección de datos. A continuación se sitúan el sector público (49 %), las telecomunicaciones (47 %) y el químico (45 %).

El cumplimiento normativo también juega un papel destacado, ya que el 81 % de las empresas se están adaptando de manera activa para cumplir con los crecientes requisitos normativos en cuanto a ciberseguridad. Las empresas que sufrieron un ciberataque durante el último año fueron más propensas (87 %) a informar de que se estaban adaptando a las normativas que aquellas que no sufrieron ningún ataque (72 %).

El teletrabajo representa otro reto de seguridad para las empresas y el 79 % ha invertido en formación adicional en ciberseguridad para las personas que teletrabajan con el fin de ayudar a prevenir ataques.

Las comprobaciones de seguridad periódicas son otra forma que tienen las empresas para mitigar las amenazas cibernéticas. El 91 % realiza, al menos una vez cada tres meses, comprobaciones de vulnerabilidad cibernética, como simulaciones o pruebas de penetración.

Las empresas están investigando más allá de sus propios sistemas y personal cuando consideran dónde pueden originarse las amenazas. Con ese propósito, el 88 % de las empresas realizan evaluaciones de riesgos al menos una vez al trimestre para determinar los riesgos de ciberseguridad de sus proveedores y socios.

La experiencia impulsa la acción
Las empresas que han sufrido ataques en los últimos 12 meses son más propensas a invertir en formación que aquellas que no lo han sido.

El 87 %
invirtió en formación y sufrió un ciberataque.

El 68 %
invirtió en formación, pero no sufrió ningún ciberataque.

Ciberresiliencia

Las empresas creen que, a pesar de las continuas amenazas y sus consecuencias, están avanzando: la gran mayoría (83 %) ha mejorado su ciberresiliencia en los últimos 12 meses. Estas mejoras se han logrado gracias a una combinación de factores, entre los que encontramos el aumento de la plantilla dedicada a puestos de seguridad, la inversión en software y el aumento de la formación en ciberseguridad para los empleados.

A pesar de la confianza en la mayor resiliencia de su empresa, los responsables de ciberseguridad no pierden de vista su responsabilidad: son plenamente conscientes de las nuevas amenazas, muchas de ellas impulsadas por la inteligencia artificial, que exigirán aún más vigilancia y trabajo duro.

Nuestro modelo de madurez ciber es una herramienta gratuita que ayuda a las empresas a comprender sus fortalezas y debilidades en materia de ciberseguridad.

El riesgo ciber tiene que ver tanto con las personas como con la tecnología. Trabajamos en la ciberprotección con miles de microempresas y nanoempresas y, una y otra vez, el factor de riesgo más importante es el factor humano. Cuando se crea una empresa, a menudo, hay que compaginar diferentes funciones, por lo que es fundamental contar con apoyo ante los distintos riesgos ciber a los que se enfrenta la empresa, como el compromiso del correo electrónico empresarial, el fraude por desvío de pagos y la ingeniería social. Por eso, en Hiscox, trabajamos con nuestros clientes en su formación y las simulaciones de phishing para reforzar su resistencia frente a los estafadores y los actores maliciosos cotidianos y liberarlos para que puedan centrarse en lo que mejor saben hacer.

Diva Aoun
Directora de Cyber
Hiscox Europe

Mejora de la ciberresiliencia
Las empresas se están protegiendo contra futuras amenazas.

La IA es una herramienta revolucionaria para empresas de todo perfil y tamaño, pero aumenta la vulnerabilidad de las empresas frente a los riesgos ciber si no cuentan con la experiencia o la protección adecuadas. Nuestros productos de seguro de responsabilidad civil profesional y ciber aseguran la protección contra reclamaciones derivadas del uso de la IA, incluidas las situaciones en las que un hackeo afecta a la IA.

Nicolas Kaddeche
Director de Suscripción
Técnica y Ventas Directas
Hiscox France

La IA y amenazas futuras

El 49 %
cree que se necesita un liderazgo más decisivo durante un ataque.

El rápido auge de los servicios integrados de IA generativa abre nuevas vías para combatir las amenazas, incluso cuando los delincuentes utilizan esta tecnología para crear nuevos ataques.

Casi dos tercios (65 %) de los responsables de la seguridad de sus pymes consideran que la IA es más un activo que una vulnerabilidad para su negocio. Portugal es el país más propenso a considerar la IA como un apoyo para la seguridad, con un 86 %, mientras que Estados Unidos y Reino Unido son menos propensos a pensar de este modo, con un 58 % y un 59 %, respectivamente.

Las tres principales amenazas emergentes impulsadas por la IA en los siguientes cinco años serán los ataques de ingeniería social (60 %), el malware y los ataques de phishing basados en IA (60 %) y el control de los datos de la empresa por parte de la IA (60 %).

Para el 22 % de las empresas, las infraestructuras (a través de un ataque físico o por proxy a los servicios públicos) y los empleados (a través de ingeniería social o phishing) son los puntos de entrada más probables para las infracciones o los ataques de ransomware. El software y los sistemas (20 %) y los socios externos (20 %) también están considerados como puntos de entrada habituales.

Las empresas pueden hacer frente a las ciberamenazas de manera más eficaz si los empleados son más conscientes de cuáles pueden ser esas amenazas y qué hacer en caso de un ataque.

Casi todos los que han sufrido un ataque (96 %) creen que una mayor concienciación o entendimiento de los ciberataques y los procedimientos es clave para mejorar los tiempos de respuesta en caso de futuras violaciones de seguridad.

La clave para reducir el daño es mejorar el tiempo de evaluación de un ataque ocurrido o que está ocurriendo y responder como es debido. Muchos de los que han sufrido un ataque creen que estar más al tanto de las posibles amenazas antes de que pasen ayudaría a mejorar los tiempos de respuesta (57 %).

Comprender mejor qué hay que buscar mientras se produce el ataque (56 %) es otra vía para acelerar la respuesta. En cuanto a qué hacer a continuación, casi la mitad (49 %) sugiere que sería útil comprender mejor a quién hay que informar del ataque. Del mismo modo, para el 49 %, los tiempos de respuesta podrían mejorar si los responsables fueran más resolutivos a la hora de responder frente a un ataque.

Planificación ante la amenaza de la IA
Las organizaciones están tomando medidas para protegerse contra las amenazas en constante evolución y tienen previsto hacer lo siguiente durante los próximos tres años.

El 37 %
se asegura de que las pólizas de seguro incluyan riesgos relacionados con IA.

El 36 %
forma a sus empleados sobre el conocimiento de las amenazas de la IA.

El 36 %
realiza auditorías periódicas sobre el uso de la IA.

El 33 %
contrata a empleados con conocimientos sobre IA.

El 33 %
contrata consultores de seguridad en IA.

Declaraciones obligatorias

El 71 %
está de acuerdo con el concepto de revelar los costes del pago de rescates.

A principios de este año, en Australia entró en vigor una ley pionera en su ámbito que obliga a todas las empresas a comunicar a las autoridades gubernamentales el coste de cualquier pago de rescate realizado como parte de un ataque de ransomware en un plazo de 72 horas.

Aunque la mayoría (71 %) se mostró partidaria de revelar los costes del pago de rescates, las ventajas y desventajas de esta medida siguen siendo objeto de debate.

Los propietarios, CIO, CISO y directores/vicepresidentes de IT mostraron un alto grado de conformidad (entre el 71 % y el 77 %), pero podemos apreciar que los directores/vicepresidentes de seguridad eran mucho menos partidarios de la nueva medida (50 %).

Las empresas que no sufrieron ningún ciberataque en el último año se mostraron más propensas (85 %) a estar de acuerdo con que las declaraciones sean obligatorias frente a aquellas que sí sufrieron un ataque (61 %).

El 54 % de las empresas afirma que las declaraciones obligatorias pueden ayudar a los clientes y a las partes interesadas a evaluar su salud financiera, mientras que el 52 % cree que ayuda a las autoridades a combatir el ransomware. La mayoría de las empresas de Portugal (52 %) y España (52 %) también lo consideran una forma de acabar con el estigma de pagar para proteger los datos.

Sin embargo, las preocupaciones siguen latentes: el 49 % advierte que las declaraciones obligatorias podrían alentar a los atacantes, en tanto que el 53 % afirma que las empresas privadas no deberían tener la obligación de divulgar sus finanzas de forma pública.

Aunque parece que los rescates seguirán pagándose, con resultados variables, el debate sobre la declaración de los pagos (en concreto, en el caso de las empresas privadas) es probable que se recrudezca, sobre todo si nuevas leyes o normativas obligan a abordar la cuestión.

> *La introducción de la obligación de declarar se encontrará, de forma inevitable y con cierta resistencia, pero la necesidad de desmantelar el modelo de negocio de la ciberdelincuencia es algo que todo el mundo reconoce. A medida que el Reino Unido avanza con bravas medidas para combatir el ransomware y reforzar la seguridad nacional, sigue siendo necesario que las pequeñas empresas se hagan cargo de su ciberseguridad y sigan invirtiendo en su equipo y sus defensas.*
>
> **Alana Muir**
> Directora de Cyber
> Hiscox UK

El debate sobre declarar
Razones por las que se debería exigir o no a las empresas que revelen los pagos de rescates que han realizado en ataques de ransomware.

A favor de declarar

El 54 %
afirma que la divulgación de información ofrece a los clientes y a las partes interesadas una imagen más clara de la salud financiera de una empresa.

El 52 %
considera que una mayor transparencia podría ayudar a las autoridades a responder frente a otros incidentes relacionados con ransomware.

En contra de declarar

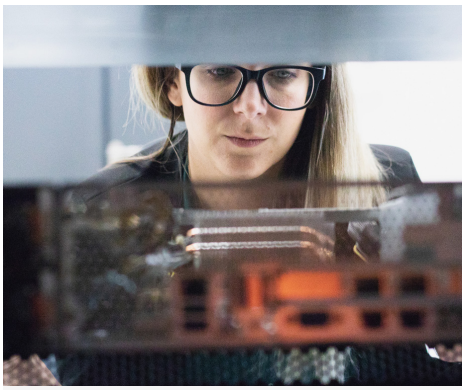
El 53 %
considera que las empresas privadas no deberían estar obligadas a revelar información financiera.

El 49 %
alerta de que declarar podría incentivar a los delincuentes a participar en ataques de ransomware.

Comparaciones entre países

Vulnerabilidad ciber
Irlanda (42 %) tuvo el índice más bajo de ciberataques en los últimos 12 meses. Alemania (67 %) y el Reino Unido (65 %) fueron los países con mayor probabilidad de sufrir al menos un ataque.

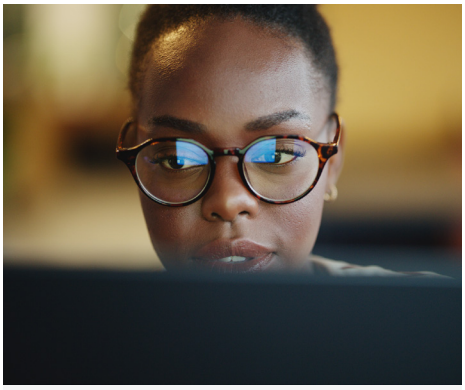
Recuperación de datos
Entre los que pagaron un rescate, Estados Unidos (74 %) tuvo el índice más alto de recuperación de datos tras un ataque de ransomware, mientras que Irlanda (53 %*) se situó en el extremo opuesto de la escala.



Regulación
Portugal (86 %) e Irlanda (85 %) se muestran más seguros en la capacidad de sus empresas para adaptarse a los nuevos requisitos normativos en ciberseguridad frente a EE. UU. (76 %).

IA
Portugal (86 %) es mucho más partidario de considerar la IA como un activo de seguridad que como una vulnerabilidad. Estados Unidos (58 %) y el Reino Unido (59 %) se muestran menos partidarios de esta opinión.

Declaración obligatoria
Estados Unidos (80 %) es el país que más apoya la declaración obligatoria del pago de rescates por ransomware. El apoyo es menor en Alemania (65 %), Portugal (65 %) y España (62 %).



Seguro
La cobertura de los seguros ciber, ya sea como póliza independiente o como parte de otra póliza, varía según el país. Francia posee la tasa de contratación más baja: un 61 %.

*Tamaño de línea base reducida; los resultados son direccionales.

Consejos de ciberseguridad para las pymes

Instalar un paquete de seguridad de software con buena reputación.	Es posible que una de las formas más eficaces de atenuar las ciberamenazas más recientes sea instalar un software de seguridad en todos los dispositivos. Estos programas combinan múltiples herramientas y funciones que pueden ayudar a identificar y bloquear automáticamente actividades sospechosas y tomar medidas proactivas para eliminar la causa de la amenaza. La última generación de software de seguridad funciona con inteligencia artificial y, a menudo, combina funciones cruciales como antivirus, firewall de red, administradores de contraseñas y copias de seguridad de datos para ofrecer un conjunto integral de controles complementarios que protegen contra amenazas como el ransomware.
Utilizar un gestor de contraseñas y una autenticación sólida.	Las contraseñas débiles o reutilizadas son el objetivo principal de los hackers que buscan acceder sin autorización a los sistemas empresariales. Un buen gestor de contraseñas puede ayudar a crear contraseñas complejas y almacenarlas de forma segura. Muchos gestores ahora también pueden supervisar las violaciones de contraseñas y notificar la necesidad de realizar cambios. Cuando se combinan con el uso de la biometría y la autenticación multifactorial (MFA), proporcionan capas de seguridad mejoradas para sus identidades digitales. Los gestores de contraseñas no solo ayudan a reducir los riesgos cibernéticos, sino que también son más cómodos para los usuarios y mejoran la experiencia digital conjunta.
Mantener los sistemas y software actualizados.	Los sistemas operativos y aplicaciones obsoletos suelen contener vulnerabilidades que los atacantes pueden aprovechar. Es recomendable establecer una rutina para instalar actualizaciones en todos los dispositivos y plataformas de la empresa. También conviene habilitar las actualizaciones automáticas para aplicar parches de seguridad de forma rápida y segura, siempre desde el proveedor verificado. Las actualizaciones regulares fortalecen la seguridad y garantizan que dispositivos y software funcionen al máximo rendimiento con las últimas funciones.
Realizar copias de seguridad de los datos de la empresa de forma segura y comprobar los procesos con regularidad.	Aun con sólidas defensas, siempre existe el riesgo de pérdida de datos o ataques de ransomware. Las copias de seguridad frecuentes y seguras, almacenadas fuera de línea o en la nube, garantizan que las empresas puedan recuperarse con agilidad si ocurre lo peor. Hoy en día, las copias de seguridad de datos a menudo se pueden automatizar mediante el uso de software para garantizar que se capturen y almacenen de forma segura, pero siempre vale la pena probarlas de vez en cuando para confirmar que los datos se pueden restaurar y minimizar el costoso tiempo de inactividad.
Ser selectivo con respecto a quién puede acceder a los datos.	No todos los empleados necesitan acceder a todos los datos de la empresa. Se puede reducir el riesgo de amenazas internas y fugas accidentales de datos con la restricción de permisos para que las personas solo tengan acceso a la información y los sistemas necesarios para sus funciones específicas. Se debe revisar y actualizar estos permisos con frecuencia, sobre todo, después de cambios de funciones o bajas de personal para mantener su posición de seguridad. Si se utiliza IA, también es importante gestionar los permisos de acceso asociados a los agentes y aplicaciones de IA. Si no se configuran bien, pueden poner de manifiesto debilidades involuntarias en los controles de acceso a los datos y dar lugar a la divulgación accidental de datos.

Hiscox
22 Bishopsgate
Londres EC2N 4BQ
Reino Unido

+44 (0)20 7448 6000
enquiries@hiscox.com
hiscoxgroup.com