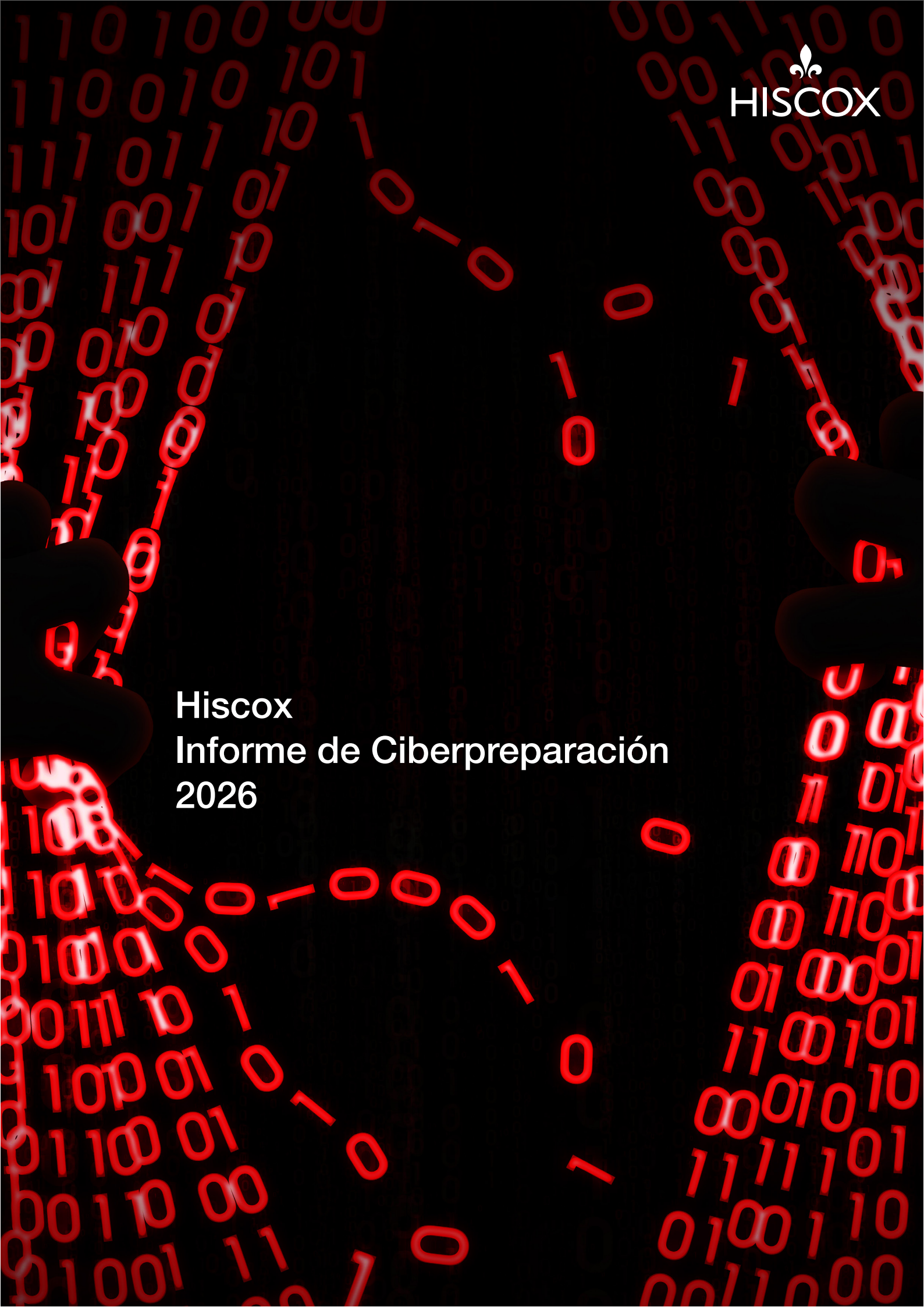


HISCOX

Hiscox
Informe de Ciberpreparación
2026

UNA DÉCADA DE CAMBIOS: DE LA DEFENSA A LA RESILIENCIA

En su décimo año, el Informe de Ciberpreparación de Hiscox evidencia la profunda evolución que ha experimentado el panorama del riesgo cibernético y cómo las empresas están viéndose obligadas a tratarlo como una de las principales áreas de riesgo del negocio.

Durante la última década de nuestra investigación sobre preparación en ciberseguridad, hemos observado un claro cambio en la forma en que las empresas abordan el riesgo cibernético: de reaccionar ante los incidentes a desarrollar una verdadera resiliencia en sus operaciones diarias.

Dicho progreso es visible en el modo en que las organizaciones están comenzando a invertir de una manera más consistente en la formación, tecnología y experiencia especializada; asimismo, se puede apreciar cómo la ciberseguridad está integrándose cada vez más en las estrategias empresariales. Este asunto ha dejado de interpretarse como un desafío operativo independiente para pasar a ser una prioridad a nivel directivo que puede llegar a dar forma a la continuidad, reputación y crecimiento de la empresa. Es razonable afirmar que se ha dado un paso en la buena dirección.

Las responsabilidades también están viéndose afectadas. Se está expandiendo el reconocimiento del riesgo cibernético como un riesgo empresarial y no solo técnico y, en la actualidad, cerca de un tercio de las organizaciones vincula directamente el desempeño y la remuneración de los puestos de responsabilidad con los resultados de la ciberseguridad tras un ciberataque.

Ahora, la resiliencia es una cuestión de preparación, respuesta eficaz y continuar operando frente a la adversidad. Mantener el foco en este asunto es lo que debemos hacer si queremos ser testigos de un progreso significativo.

Eddie Lamb
Director Global de Ciberseguridad
Hiscox

El Informe de Ciberpreparación de Hiscox recorre la experiencia de diversas entidades a lo largo de los Estados Unidos, el Reino Unido y Europa continental (Francia, Alemania, España, Irlanda, Portugal, Italia, Países Bajos y Bélgica).

El estudio ha sido realizado por Wakefield Research del 5 al 17 de junio de 2026 y está basado en las respuestas de más de 6.800 personas responsables de ciberseguridad pertenecientes a entidades con una plantilla inferior a 250 personas empleadas.

DIEZ AÑOS DE PREPARACIÓN CIBERNÉTICA: ¿QUÉ HA CAMBIADO?

Cuando se publicó el primer Informe de Ciberpreparación en 2017, muchas empresas aún preguntaban si la ciberseguridad era principalmente una cuestión de TI. Una década después, esa pregunta ya tiene respuesta.

ANTES VS. AHORA

2017	2026
> Ciberseguridad: un asunto del equipo informático	> Riesgo cibernético: un asunto empresarial
> El foco: las personas hackers y las brechas de seguridad	> El foco: se extiende a la IA, cadenas de suministros, reputación y personas
> La ciberseguridad se centra en: tecnología y prevención	> Resiliencia definida por: preparación, respuesta y recuperación
> 53% de las empresas: cibernovatas	> 97%: activas en la mejora de su resiliencia cibernética
> 40%: tienen seguro cibernético	> 64%: tienen seguro cibernético
> 55%: participación de la dirección ejecutiva en la estrategia cibernética	> 32%: vinculan el desempeño directivo con los resultados de la ciberseguridad
> 57%: habían sufrido al menos un ataque en los últimos 12 meses	> 29%: han sufrido al menos un ataque en los últimos 12 meses

Las cifras son un indicio de la evolución en la actitud y el comportamiento de las empresas en la década pasada. No se pueden comparar las conclusiones, dados los cambios en el enfoque y metodología.

Hace diez años, la pregunta era cómo detener los ciberataques. A día de hoy, la pregunta es cómo avanzar y crecer, a pesar de su existencia.

TRES LECCIONES DE UNA DÉCADA DE INVESTIGACIÓN

La tecnología no es suficiente

En 2017 descubrimos que muchas entidades veían la tecnología como la solución a los ataques. Tras una década, las empresas más preparadas combinan la tecnología con la gobernanza, la formación, el proceso y la responsabilidad.

Ciberseguridad: un asunto de la dirección

Las primeras investigaciones subrayan la importancia de que el consejo de administración se implique. La ciberseguridad se relaciona más al consejo de administración y la estrategia empresarial.

La resiliencia crea una ventaja competitiva

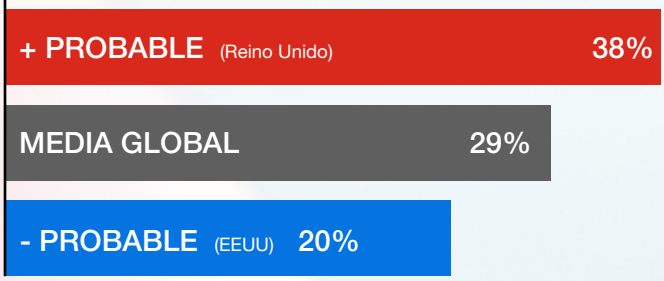
Hay una tendencia creciente a juzgar las entidades, no solo porque sufran un incidente; también por cómo responden, se recuperan y mantienen la confianza de las partes interesadas durante la incidencia.

CIBERATAQUES EN 2026: UN COSTE RUTINARIO PARA LAS EMPRESAS

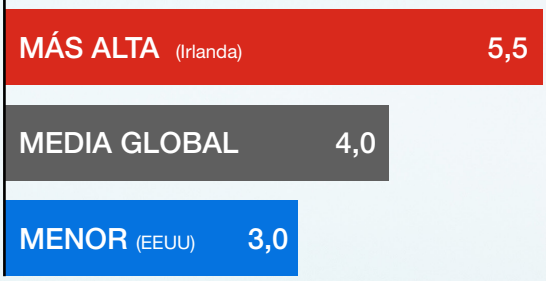
Los ciberataques ya no suponen amenazas ocasionales; ahora son algo habitual para las empresas que operan en la economía digital. Casi **una de cada tres** entidades alrededor del mundo (29%) se han visto afectadas por al menos un ciberataque exitoso en los últimos 12 meses. Se denuncian una media de **cuatro incidencias** durante este intervalo de tiempo.

Las consecuencias son significativas, tanto a nivel financiero como operativo. En la actualidad, los incidentes cibernéticos cuestan a las organizaciones una media de **52.000$** (45.000€) **al año,** además de tener una media aproximada de **32 h** de interrupción operativa.

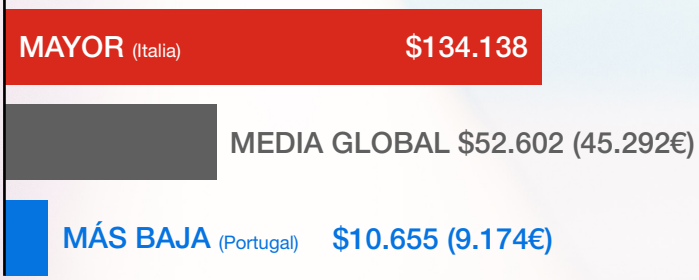
PROBABILIDAD DE SUFRIR UN CIBERATAQUE EXITOSO:



MEDIA – CIBERATAQUES EXITOSOS EN LOS ÚLTIMOS 12 MESES:



MEDIA – COSTE DE UN ATAQUE:



MEDIA – HORAS DE INACTIVIDAD:

DE LA INTERRUPCIÓN OPERATIVA AL IMPACTO EMPRESARIAL

Los efectos de los ciberataques van más allá de la pérdida económica inmediata y presentan claras implicaciones para el rendimiento y el desarrollo de las empresas.

Entre las entidades que han experimentado un ataque:

Un **32%** observa una desaceleración del crecimiento, la expansión y las nuevas iniciativas empresariales.

Un **31%** menciona un aumento del personal y gastos de asesoramiento externo.

Un **30%** declara un impacto negativo en el rendimiento financiero, la valoración de la empresa o la calificación crediticia.

Un **29%** ha perdido oportunidades de negocio o colaboraciones como resultado de un ciberataque.

Las incidencias cibernéticas pueden influir en la toma de decisiones estratégicas, la ralentización del desarrollo y el aumento de la carga sobre los recursos.

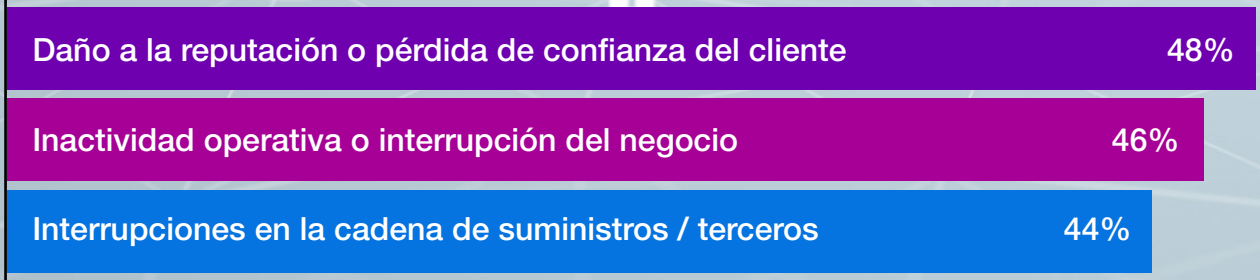
EL IMPACTO MÁS ALLÁ DEL BALANCE GENERAL

El daño a la reputación y la pérdida de confianza del cliente son el mayor riesgo para casi la mitad de las empresas (48%), lo que refleja que la resiliencia de la marca es algo muy importante en un ambiente altamente conectado.

Gran parte de las organizaciones que han sufrido un ciberataque declara haber sufrido **sanciones económicas** (28%) o **publicidad negativa** (26%).

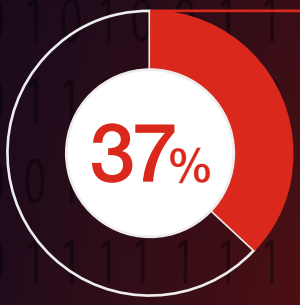
Este cambio de paradigma remarca la manera en que se ha dado el siguiente paso en la percepción que se tiene acerca del riesgo cibernético: de un desafío técnico a una problemática central de la administración empresarial, la cual tiene implicaciones directas para con la competitividad a largo plazo.

LOS TRES RIESGOS QUE ENFRENTAN LAS EMPRESAS EN LA ACTUALIDAD

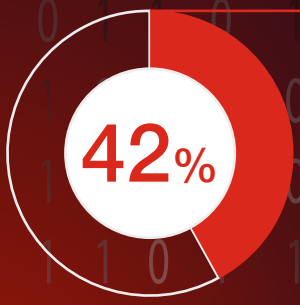


COMPARATIVA INTERNACIONAL

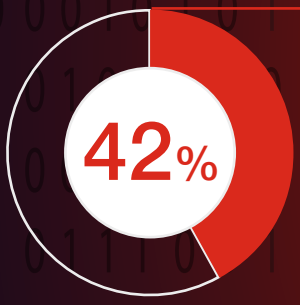
La repercusión de los ciberataques difiere mucho de unos mercados a otros en lo relativo a las pérdidas económicas, la desaceleración del crecimiento o el perjuicio sobre la reputación. Los datos revelan cuáles son los países más afectados.



La empresa alemana presenta la mayor probabilidad de desaceleración del desarrollo, expansión o nuevas propuestas de negocio como resultado de un ciberataque.

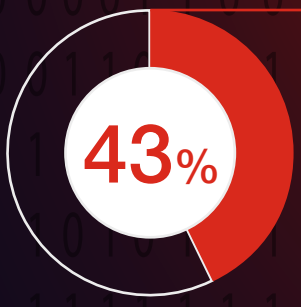


La empresa neerlandesa presenta la mayor probabilidad de experimentar un aumento de los costes de personal o de contratación de expertos externos.

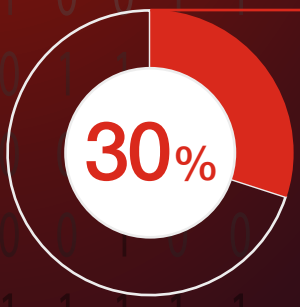


La empresa portuguesa presenta la mayor probabilidad de retraso en la incorporación de la IA u otras nuevas tecnologías.

La empresa italiana presenta la mayor probabilidad de pérdida de oportunidades de negocio o colaboraciones.



La empresa irlandesa presenta la mayor probabilidad de verse afectada por multas sustanciales que conlleven consecuencias en la salud económica de la entidad.



La empresa francesa presenta la mayor probabilidad de verse perjudicada por una mala publicidad que repercuta sobre su imagen y su reputación.

Mientras que la naturaleza del impacto difiere, las incidencias cibernéticas están desmejorando igualmente el crecimiento, la rentabilidad y la reputación en todos los mercados encuestados.

EL RIESGO DE LA IA PASA A PRIMER PLANO

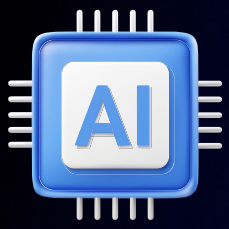
La IA está reconfigurando la amenaza cibernética. A medida que las empresas recurren cada vez más a la IA para aprovechar nuevas oportunidades, también se enfrentan a nuevos riesgos, que van desde modelos manipulados por IAs y datos de entrenamiento comprometidos hasta sistemas sofisticados de fraude cibernético y ataques de ingeniería social.

Las empresas responden con el incremento de la inversión en el talento, la gobernanza y la supervisión, reconociendo que la resiliencia ha de evolucionar a la par que la incorporación.

17% identifica las herramientas y el software de IA como una vía de entrada para los ciberataques.

LAS CONSECUENCIAS CIBERNÉTICAS DE LA IA DURANTE LOS PRÓXIMOS CINCO AÑOS

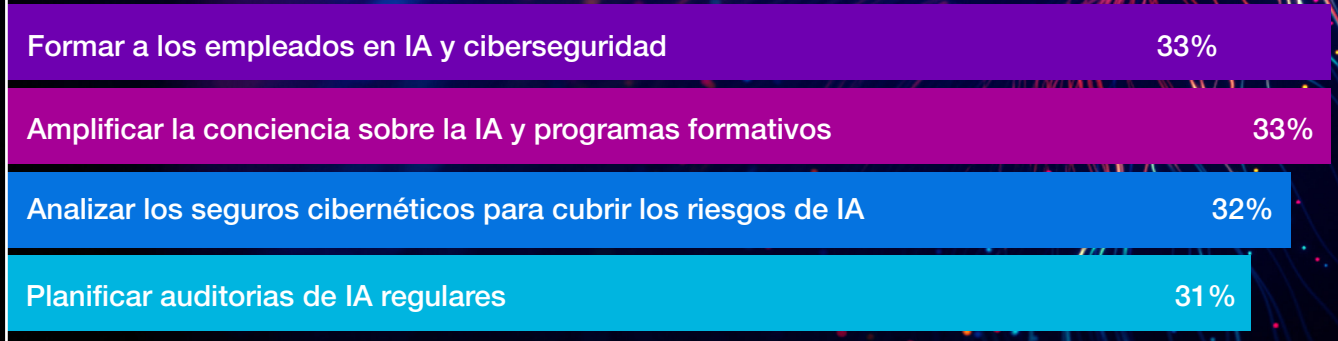
- **48%** Envenenamiento de datos de IA
- **43%** Confianza excesiva en la IA y reducción de la supervisión humana
- **43%** Vulnerabilidades en las herramientas de IA de terceras partes
- **41%** Malware y phishing impulsados por IA



EL MAYOR RIESGO DE LA IA NO ES LA TECNOLOGÍA. ES CÓMO SE USE.

Las empresas no están tan pendientes del futuro de la IA como sí de sus riesgos, incluyendo: datos de entrenamiento corruptos, herramientas vulnerables de terceras partes y reducción de la supervisión humana.

LAS RESPUESTAS DE LAS EMPRESAS



CONSTRUCCIÓN DE LA RESILIENCIA DONDE MÁS IMPORTA: PERSONAS, PROCESOS Y TECNOLOGÍA

Las empresas van más allá de las reparaciones técnicas y refuerzan su resiliencia cibernética mediante un enfoque coordinado que integra capacidades, sistemas y gobernanza. Invierten una media de **51.000$** (44.000€) / año en el desarrollo de su resiliencia cibernética.

PERSONAS

62%: Forma a su personal en ciberseguridad.

ESPECIALISTAS

55%: Contrata a nuevo personal de ciberseguridad.

TECNOLOGÍA

51%: Invierte en nuevos programas.

RESPONSABILIDAD

32%: Vincula el salario e indicadores de rendimiento con los resultados de la ciberseguridad tras un ciberataque.

Inversión en la resiliencia cibernética ($), por país	
España	80.900 $
Italia	73.800 $
Reino Unido	59.700 $
Promedio	51.000 $
EEUU	49.500 $
Alemania	43.600 $
Irlanda	43.600 $
Bélgica	34.600 $
Francia	32.700 $
Países Bajos	26.400 $
Portugal	10.700 $

Salario/desempeño → resultados de la ciberseguridad, por país	
Alemania	41%
Irlanda	36%
Bélgica	35%
Francia	34%
España	33%
Países Bajos	33%
Promedio	32%
Portugal	32%
Italia	32%
EEEUU	26%
Reino Unido	25%

Los países que más invierten no son necesariamente los que presentan los niveles más altos de responsabilidad en los consejos de administración.

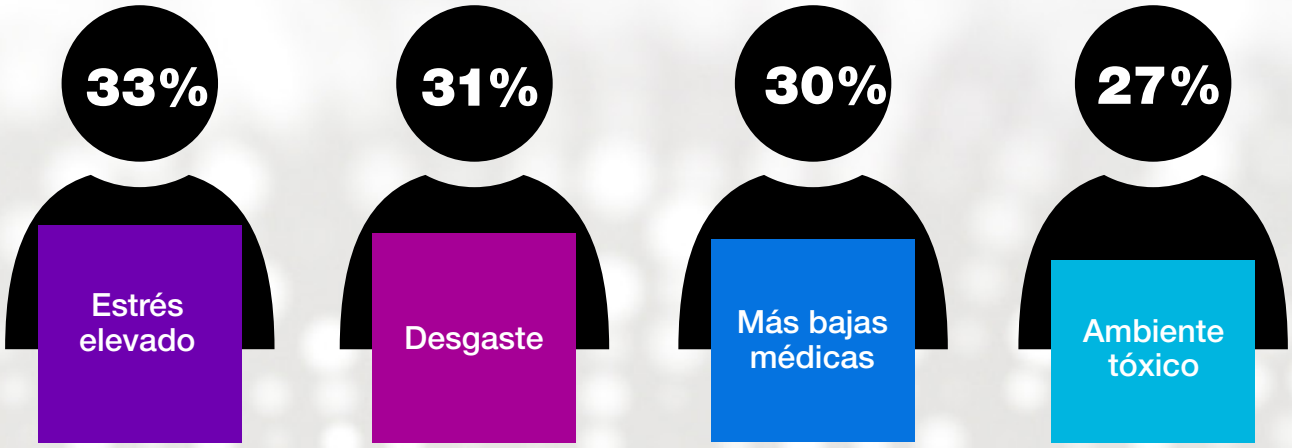
LOS COSTES HUMANOS DE LOS CIBERATAQUES

Las repercusiones de los ciberataques trascienden la tecnología e ingresos. A menudo, las personas empleadas sufren la mayor parte de las consecuencias debido al incremento del estrés, el síndrome de desgaste profesional y la interrupción de su actividad laboral habitual.

A medida que las empresas refuerzan su ciberresiliencia, el bienestar de los empleados, la cultura y el compromiso adquieren cada vez más importancia como indicadores de recuperación.

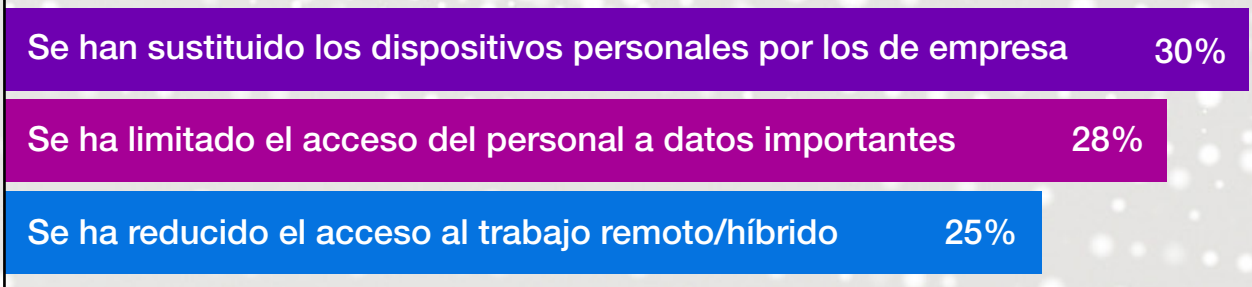
69% **Declara que el personal sufre desgaste / estrés / ambiente tóxico tras un ciberataque.**

IMPACTO SOBRE LAS PERSONAS TRABAJADORAS



LOS CIBERATAQUES RECONFIGURAN CÓMO SE TRABAJA

Entre las entidades que han sufrido un ciberataque:



LA RESILIENCIA ES CUESTIÓN DE PERSONAS

La inversión de las entidades que se recuperan con mayor efectividad no se limita a la tecnología; también potencian la formación, los controles de acceso, la gobernanza y la cultura laboral a fin de brindar apoyo a la plantilla tras la interrupción.

LA RESILIENCIA COMO UNA VENTAJA COMPETITIVA

El panorama cibernético ha cambiado radicalmente tras la última década. Hoy día, el reto que las empresas han de asumir no solo consiste en prevenir ataques, sino en desarrollar la capacidad de responder, recuperarse y seguir operando cuando se produce una interrupción.

Desde nuestra experiencia asegurando riesgos cibernéticos, observamos que las empresas más estables no son las que experimentan menos incidencias, sino las que están preparadas, responden con decisión y aprenden de la interrupción.

CINCO FORMAS DE CONSTRUIR LA RESILIENCIA CIBERNÉTICA

01

Uso de herramientas de confianza

Instalación de programas de seguridad reputados y actualizados en los dispositivos para que se facilite identificar, bloquear y responder a las amenazas.

02

Fortalecimiento de los controles de acceso

Uso de gestores de contraseñas y AM; limitación del acceso a la información sensible solo a quienes lo precisen.

03

Actualización de los sistemas

Actualización de programas y dispositivos para abordar las vulnerabilidades y mantener una protección estable.

04

Copias de seguridad

Creación de copias de seguridad que se prueben con regularidad para restaurar las actividades con rapidez tras una incidencia.

05

Buena administración de los permisos

Revisión y actualización del acceso de usuarios para reducir el riesgo de amenazas y exposición accidental de datos, incluyendo la administración de acceso a sistemas y agentes de IA.

¡Realiza el test! Profundiza en tus debilidades y fortalezas de ciberseguridad con la evaluación de madurez cibernética de Hiscox y compara tu desempeño con el de otras miles de empresas como la tuya.

Hiscox España
C. de Miguel Ángel
11, 4ª planta
28010 Madrid

T +34 915 15 99 00
E info_spain@hiscox.com
www.hiscox.es

0117 09/26