FUNDAMENTOS DEL FUTURO

HLB REPORTE DE CIBERSEGURIDAD 2024

www.hlb.global

TOGETHER WE MAKE IT HAPPEN

CONTENIDO

INTRODUCCIÓN 3

DATOS DESTACADOS 4

ENFOCARSE EN LO FUNDAMENTAL 5

DESARROLLAR LA CIBERRESILIENCIA EN TIEMPO REAL 6

GESTIÓN DE RIESGOS DE CIBERSEGURIDAD DE TERCEROS PROVEEDORES 7

CASO PRÁCTICO: DE LA EVALUACIÓN A LA IMPLANTACIÓN 9

EL DOBLE ROL DE LA AI 10

LA IMPORTANCIA DE LA PROTECCIÓN DE SUS DATOS 12

PASAR DE UNA CIBERSEGURIDAD REACTIVA A UNA PROACTIVA 14

FUNDAMENTOS CIBERNÉTICOS DEL FUTURO: EVALÚE SU PREPARACIÓN 16

CÓMO PUEDE AYUDAR HLB 17

METODOLOGÍA DE LA INVESTIGACIÓN 18

AGRADECIMIENTOS 18

INTRODUCCIÓN

En un mundo cada vez más marcado por la transformación digital, comprender el panorama en constante evolución de la ciberseguridad es crucial para los líderes empresariales y los responsables de la toma de decisiones. Las ciberamenazas emergentes exigen medidas más proactivas en las organizaciones para combatir los riesgos antes de que se produzcan incidentes. Tras de una serie de importantes interrupciones a lo largo de 2024, reforzar las defensas de ciberseguridad sigue siendo un imperativo estratégico para las empresas, ya que los profesionales se enfrentan a un número cada vez mayor de ataques sofisticados.

En septiembre de 2024, encuestamos a más de 600 profesionales sénior de TI a través de un cuestionario online sobre las principales amenazas a la ciberseguridad de hoy en día, sus avances en la implementación de ciberestrategias y el doble papel de la IA. La quinta edición del informe de ciberseguridad de HLB ofrece una instantánea del panorama actual de las ciberamenazas y destaca las medidas clave que los líderes han tomado desde 2020 para ser más ciberresistentes.

DATOS DESTACADOS

86%

expresó mayor preocupación por las amenazas relacionadas con la ciberseguridad

64%

De los encuestados consideran la ciberseguridad una prioridad estratégica importante

24%

de las organizaciones llevan a cabo programas de formación continua sobre ciberseguridad

ENFOCARSE EN LO FUNDAMENTAL

En una era en la que las amenazas a la ciberseguridad son cada vez más sofisticadas, no se puede exagerar la importancia de las prácticas fundamentales. Desde 2020, HLB International ha estado midiendo la preparación cibernética de las empresas mundiales. Nuestros últimos datos revelan que muchas organizaciones se enfrentan a la creciente presión de los ciberataques, y que el 39% de ellas ha informado de un aumento en el último año. Sin embargo, a pesar de estas amenazas, algunas organizaciones siguen pasando por alto medidas de seguridad básicas, lo que las hace vulnerables a las infracciones.

In an era of increasingly sophisticated cybersecurity threats, the importance of critical practices cannot be overstated. Since 2020, HLB International has been measuring the cyber readiness of global businesses. Our latest data reveals that many organisations are facing increasing pressure from cyber attacks, with 39% reporting an increase in the last year. Yet despite these threats, some organisations continue to overlook basic security measures, leaving them vulnerable to breaches.

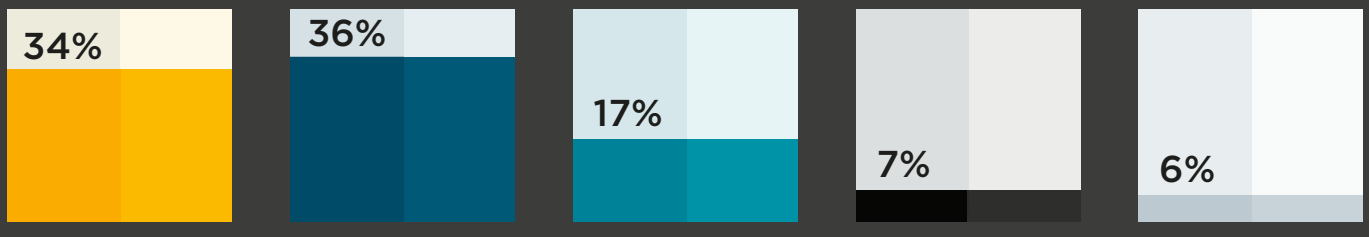
En 2024, el 47% de nuestros encuestados identificaron la explotación del correo electrónico como una que está evolucionando con los rápidos avances de la IA. Los responsables de las empresas deben dar prioridad a la implantación de reglas de cortafuegos sólidas y formar a los empleados para que detecten eficazmente los intentos de suplantación de identidad. A pesar de que el 62 % afirma que la ciberseguridad es una prioridad absoluta, un preocupante 30 % de las empresas solo realiza auditorías de personal anualmente o después de un incidente, lo que ilustra una laguna en las medidas de seguridad proactivas.

«Nuestros datos demuestran una mayor preocupación por las amenazas a la ciberseguridad, y con razón: el 92% ha observado ciberataques en curso, y el 38% afirma que estas amenazas se están intensificando. Sin embargo, resulta alarmante que, aunque la mayoría de las empresas realizan algún tipo de formación en ciberseguridad, para muchas no se hace con la frecuencia suficiente. Es crucial que la formación se convierta en una práctica mensual, sobre todo porque la explotación del correo electrónico sigue siendo uno de los principales riesgos.»

Jim Bourke | Líder de Servicios Tecnológicos y de Asesoramiento, HLB Global

FIG.1: NIVEL ACTUAL DE PREOCUPACIÓN CIBERNÉTICA

¿Cuál es su nivel de preocupación actual en relación con las amenazas a la ciberseguridad de su empresa?



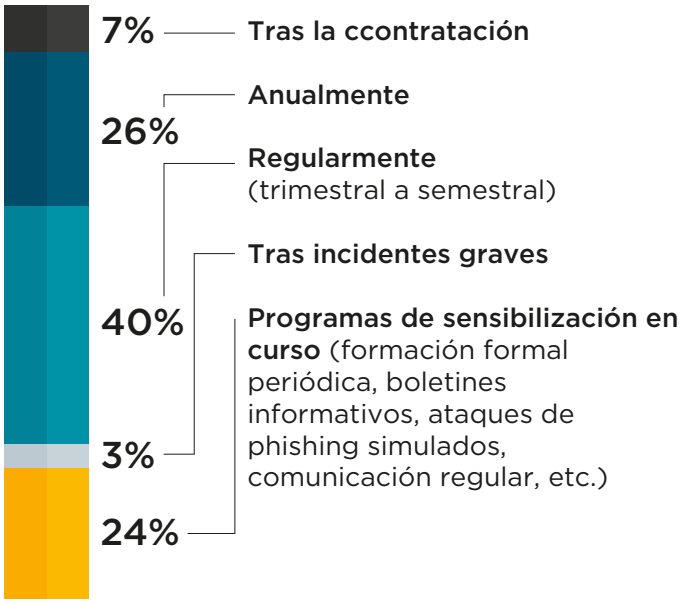
La inversión en programas continuos de concienciación y formación de los empleados es crucial. Las organizaciones pueden reducir significativamente su vulnerabilidad dotando al personal de los conocimientos necesarios para reconocer y responder a posibles amenazas. «Hay que tener en cuenta que los nuevos empleados son más vulnerables a los ataques debido a su falta de concienciación». Afirma Gustavo Solís, director general de HLB México.

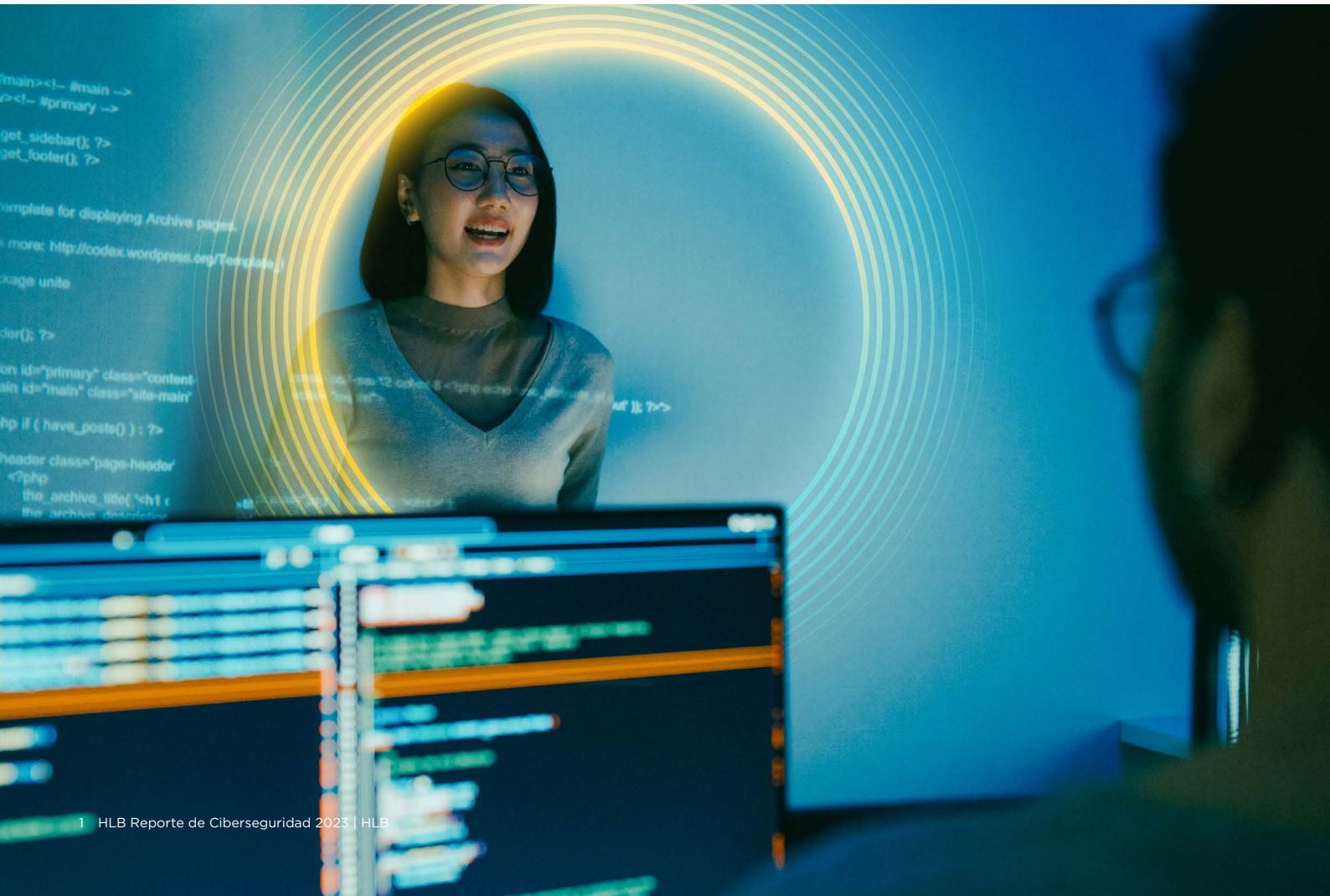
«Algunas de las principales preocupaciones cibernéticas actuales están relacionadas con el factor humano, por ejemplo, la ingeniería social, por lo que la capacitación en ciberseguridad al momento de la contratación junto con programas de concientización continua un imperativo».

Las organizaciones que ejecutan programas de concientización continua aumentaron cuatro puntos porcentuales desde el Informe de Ciberseguridad de HLB del año pasado1 a 24%, lo que indica que el mensaje para que las empresas adopten un enfoque más riguroso de la formación cibernética está surtiendo efecto. Esta tendencia positiva refleja la creciente importancia que los directivos de las empresas conceden a la ciberseguridad; al crear una cultura de concienciación constante, las organizaciones están mejor posicionadas para hacer frente a las ciberamenazas modernas.

FIG.2: NIVEL ACTUAL DE INVERSIÓN EN FORMACIÓN EN CIBERSEGURIDAD

¿Con qué frecuencia invierte su empresa en formación sobre ciberseguridad?





1 HLB Reporte de Ciberseguridad 2023 | HLB

DESARROLLAR LA CIBERRESILIENCIA EN TIEMPO REAL

Las empresas se enfrentan a la realidad de un número creciente de ciberamenazas que pueden tener un efecto importante en las operaciones y la seguridad de los datos. Teniendo en cuenta el aumento del 71% de los ciberataques con credenciales robadas, es evidente la necesidad de que las organizaciones desarrollen y mantengan su ciberresiliencia.

La resistencia cibernética se refiere a la capacidad de una organización capacidad de una organización para prepararse, responder y recuperarse de ciberataques, garantizando una interrupción mínima de las operaciones y salvaguardando la integridad de los datos. Nuestros datos revelan que un impresionante 76% de las organizaciones confían en su capacidad para recuperarse rápidamente de los ciberataques.

«Todavía hay margen de mejora; la mayoría de las empresas conocen los riesgos y se toman en serio la ciberseguridad, pero ciberseguridad, pero podrían hacer más medidas preventivas desde el desde el principio, sin esperar a que impacto de las ciberamenazas se materialice para actuar».

Pablo Kaplan | Socio Director, HLB Argentina

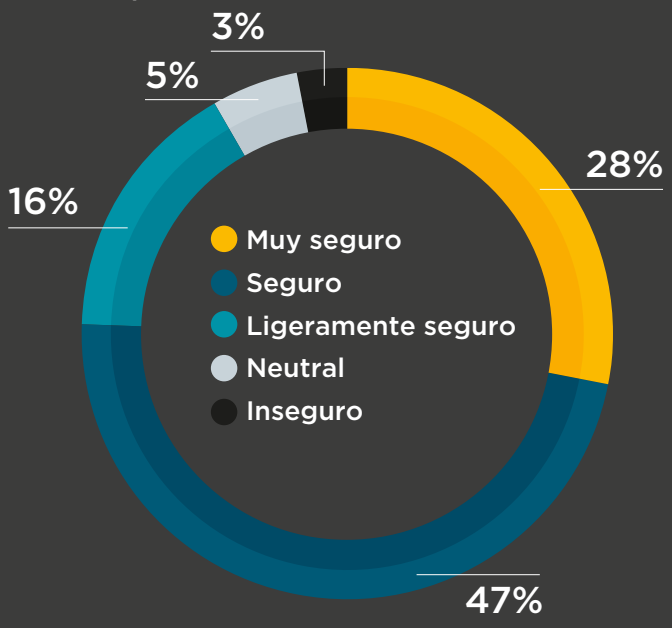
Un componente crucial de la ciberresiliencia es la aplicación de estrategias integrales y proactivas - como el aprendizaje electrónico, los talleres y los simulacros- en lugar de depender de medidas ad hoc. Esto implica una formación periódica en ciberseguridad, que el 40 % de las organizaciones lleva a cabo trimestral o bianualmente, así como el mantenimiento de planes actualizados de respuesta a incidentes, que según nuestra encuesta cuatro de cada cinco empresas ya tienen en marcha.

Las organizaciones también deben adaptarse a la evolución del panorama de las amenazas mediante la integración de tecnologías avanzadas como la IA, garantizando al mismo tiempo la existencia de sólidos controles de seguridad y gobernanza.

El robo y la filtración de datos representan otro 32% de los incidentes3, por lo que es esencial un enfoque polifacético de la ciberseguridad.

FIG.3: CONFIANZA EN LA RECUPERACIÓN TRAS UN CIBERATAQUE

¿Hasta qué punto confía en la capacidad de su empresa para recuperarse rápidamente de un ciberataque?



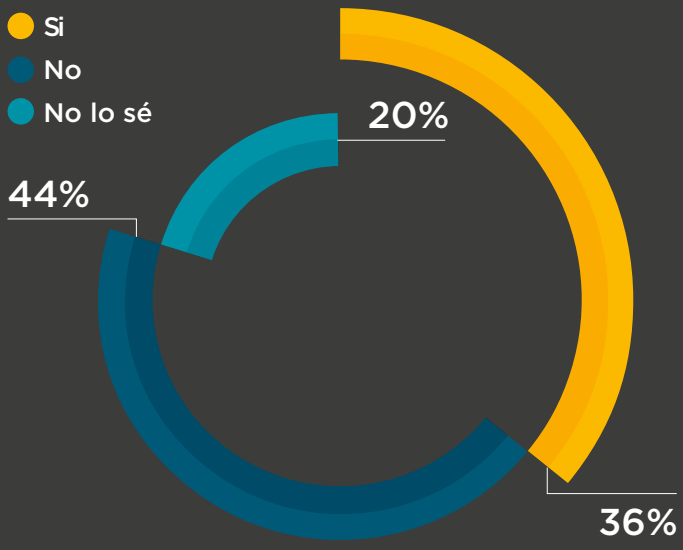
GESTIÓN DE LOS RIESGOS DE CIBERSEGURIDAD DE TERCEROS PROVEEDORES

A medida que se acelera el ritmo de los avances tecnológicos, aumenta la confianza en los proveedores externos como expertos esenciales hiperconcentrados. Sin embargo, pueden plantear importantes riesgos de ciberseguridad y desajustes en la estrategia si los esfuerzos de investigación, selección e incorporación de proveedores no se gestionan correctamente en todo momento.

Nuestra encuesta revela que el 37% de las organizaciones sufrieron una brecha de seguridad a través de un proveedor externo el año pasado, mientras que un preocupante 20% no está seguro del estado de seguridad de sus proveedores, lo que subraya la necesidad crítica de contar con estrategias sólidas de gestión de riesgos de terceros.

FIG.4: PROVEEDORES DE TERCEROS AFECTADOS POR INFRACCIONES EN 2024

¿Alguno de sus proveedores externos se ha visto afectado por una brecha cibernética o un incidente de seguridad en los últimos 12 meses?



Las organizaciones confían cada vez más en pequeños proveedores que pueden carecer de medidas de seguridad sólidas, lo que los convierte en objetivos atractivos para los ciberdelincuentes. Estas preocupaciones son fundadas, dado el coste estimado de 10,5 billones de dólares de los ciberataques en todo el mundo el año pasado.

«Este (el riesgo de los proveedores externos) es un área que a menudo se pasa por alto y se asocia con frecuencia a la explotación del correo electrónico y otros vectores de ataque, lo que provoca impactos potencialmente críticos en las operaciones y la reputación de las empresas», añade Gareth Rees, Ejecutivo Regional de The Missing Link.

Para mitigar estos riesgos, las empresas deben implantar marcos integrales de gestión de proveedores. Los pasos clave incluyen:

1. **Due Diligence:** Antes de contratar a un proveedor, asegúrese de que cumple sus normas de seguridad. Evalúe su postura de seguridad mediante auditorías y evaluaciones.

2. **Obligaciones contracctuales:** Incorpore requisitos de ciberseguridad en los contratos de los proveedores, exigiendo el cumplimiento de las normativas pertinentes, como el GDPR o el NIS2. Esto garantiza la rendición de cuentas y anima a los proveedores a mantener medidas de seguridad adecuadas.

3. **Monitoreo continuo:** Aplique prácticas de supervisión continua para evaluar el estado de la seguridad de los proveedores a lo largo del tiempo. Las herramientas automatizadas pueden ayudar a detectar posibles vulnerabilidades e intervenir a tiempo.

4. **Planes de respuesta a inidentes:** Elabore y actualice periódicamente planes de respuesta a incidentes que tengan en cuenta los riesgos de terceros. Esto permite a las organizaciones responder con rapidez y eficacia en caso de infracción.

4 The 10 Biggest Cyber Security Trends In 2024 Everyone Must Be Ready For Now (forbes.com)

CASO PRÁCTICO:

BRICKWORKS
BUILDING PRODUCTS

DE LA EVALUACIÓN A LA IMPLANTACIÓN CON FÁBRICAS DE LADRILLOS

Brickworks Building Products es uno de los mayores y más diversos fabricantes de materiales de construcción del mundo, con más de 90 años de experiencia. La empresa cuenta con 17 marcas, 45 plantas de fabricación, más de 2.000 productos y 2.500 empleados en todo el mundo.

Consciente de la creciente complejidad de su negocio y del número cada vez mayor de proveedores, socios y clientes, Brickworks comprendió la necesidad de mejorar la seguridad de su correo electrónico y la formación en ciberseguridad. Para conseguirlo, se asociaron con The Missing Link, una empresa conocida por sus innovadoras soluciones de ciberseguridad y actual firma de HLB.

The Missing Link realizó una evaluación exhaustiva de las necesidades actuales y futuras de Brickworks y les puso en contacto con los mejores proveedores. Esta colaboración dio como resultado la implantación con éxito de soluciones avanzadas de seguridad del correo electrónico, aumentando significativamente la protección frente al fraude de correo electrónico y dominios, incluido el compromiso del correo electrónico empresarial. Con estas soluciones, Brickworks puede ahora detectar y detener los ataques de suplantación de identidad por correo electrónico entrante y saliente e ir más allá de DMARC para exponer los riesgos de fraude que plantean sus proveedores.

La formación en ciberseguridad de Brickworks también se reevalúa periódicamente para garantizar su eficacia y pertinencia. Se utilizan simulaciones reales de phishing para formar a los empleados e identificar a los usuarios de riesgo. Gracias a la integración de los datos de las soluciones de seguridad del correo electrónico de Brickworks, se puede identificar al personal más peligroso y ofrecerle una formación especializada y específica.

Este enfoque integral no sólo mejora la postura de Brickworks en materia de ciberseguridad, sino que también ofrece a los comités de gobernanza y a los auditores pruebas tangibles del compromiso de la empresa con la ciberseguridad.

EL DOBLE ROL DE LA AI

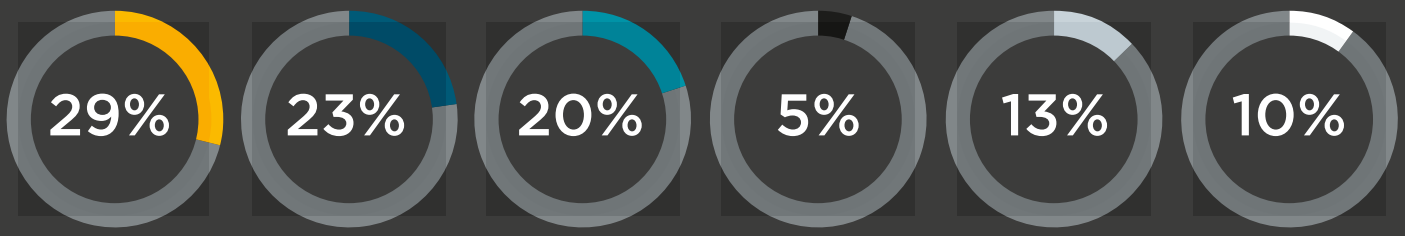
La Inteligencia Artificial (IA) es a la vez un aliado formidable y un adversario impredecible. Tanto para los profesionales de TI como para los expertos en ciberseguridad y los líderes empresariales, comprender el papel de la IA es crucial para garantizar el futuro de sus organizaciones.

No cabe duda de que la IA es una herramienta poderosa para mejorar las medidas de ciberseguridad. Su capacidad para analizar rápidamente grandes conjuntos de datos permite a las organizaciones detectar y responder a las amenazas con una rapidez y precisión sin precedentes. El 29% de las organizaciones encuestadas han implementado controles adicionales de seguridad y gobernanza al aprovechar la IA. Estos controles están diseñados para salvaguardar la integridad de los datos y proteger contra las brechas, reforzando significativamente los marcos de defensa.

Sin embargo, las proezas de la IA son un arma de doble filo. Las mismas capacidades que mejoran la seguridad también pueden ser explotadas por los ciberdelincuentes, dando lugar a ataques impulsados por IA que son más rápidos y sofisticados que los métodos tradicionales. Resulta alarmante que el 28 % de las organizaciones utilicen o tengan previsto utilizar IA sin los controles adecuados, lo que crea vulnerabilidades que pueden explotarse fácilmente.

FIG. 5: CARTOGRAFIAR EL USO ACTUAL Y PREVISTO DE LA AI POR PARTE DE LA ORGANIZACIÓN

¿Su organización aprovecha actualmente, o tiene previsto aprovechar en los próximos 12 meses, tecnologías transformadoras como la IA? En caso afirmativo, ¿ha implantado o va a implantar controles adicionales de seguridad y gobernanza?



29%	23%	20%	5%	13%	10%
Sí, actualmente estamos aprovechando la IA y hemos implantado controles adicionales de seguridad y gobernanza.	Sí, actualmente estamos aprovechando la IA, pero aún no hemos implantado controles adicionales de seguridad y gobernanza.	Tenemos previsto aprovechar la IA en los próximos 12 meses y aplicaremos controles adicionales de seguridad y gobernanza.	Tenemos previsto aprovechar la IA en los próximos 12 meses, pero aún no hemos implantado controles adicionales de seguridad y gobernanza.	No tenemos previsto utilizar la IA en los próximos 12 meses.	No está seguro

Las consecuencias de descuidar la gobernanza de la IA son graves. La posibilidad de que la IA se convierta en un arma se ve agravada por su escalabilidad y sus operaciones autónomas, lo que supone una amenaza significativa para la seguridad de los datos. El 29% ha informado de consecuencias más graves de ciberataques en los últimos 12 meses, lo que subraya la urgencia de una gobernanza integral de la IA.

Para mitigar estos riesgos, las empresas deben priorizar el desarrollo y la implementación de marcos sólidos de gobernanza de la IA, incluido el establecimiento de controles y mecanismos de supervisión para garantizar que la tecnología se utilice de forma ética y segura.

Las empresas deben invertir en auditorías periódicas y evaluaciones de riesgos, identificando posibles vulnerabilidades antes de que puedan ser explotadas por los ciberdelincuentes. Las organizaciones también deben centrarse en integrar la IA con las medidas de ciberseguridad existentes para detectar y prevenir los ataques impulsados por la IA con mayor eficacia.

Al integrar esta cultura de responsabilidad y la gobernanza proactiva, las empresas pueden aprovechar eficazmente el poder de la IA al tiempo que minimizan los riesgos y protegen sus datos y sistemas de ataques sofisticados y de gran impacto.

LA IMPORTANCIA DE LA PROTECCIÓN DE SUS DATOS

Salvaguardar los datos mediante mecanismos duraderos como el cifrado y la clasificación de datos no sólo es aconsejable, sino vital. La creciente sofisticación de las ciberamenazas ha convertido la filtración de datos en un riesgo prevalente, capaz de infligir graves daños a la reputación de las empresas.

El cifrado sigue siendo una herramienta fundamental, que transforma la información sensible en un código indescifrable que sólo pueden descifrar las partes autorizadas, proporcionando así una barrera formidable contra el acceso no autorizado. La clasificación de datos es otro componente crítico, que permite a las organizaciones identificar y clasificar los datos en función de su sensibilidad y valor.

«Con muchas nuevas medidas, marcos y otras legislaciones emergentes de los organismos reguladores de todo el mundo, la necesidad de una clara en materia de protección de protección de datos y ciberseguridad ciberseguridad nunca ha sido mayor».

Mark Butler | Socio Director, HLB Ireland

El cumplimiento normativo acentúa aún más la importancia de la protección de datos. El Reglamento General de Protección de Datos (RGPD), entre otras normativas emergentes como NIS2 y CMMC, ha elevado la responsabilidad de los directores de seguridad de la información (CISO) y los ejecutivos, haciendo cumplir estrictas normas de protección de datos e imponiendo fuertes sanciones por incumplimiento. El informe Perspectivas de la Ciberseguridad 2024 del Foro Económico Mundial (FEM) reitera este hecho, destacando el papel de una normativa eficaz en la mejora de la ciberresiliencia.

FIG.6: CÓMO CUMPLEN LAS ORGANIZACIONES LA NORMATIVA VIGENTE

¿Cómo cumple su organización la normativa vigente en materia de ciberseguridad pertinente para su sector (por ejemplo, GDPR, NIS2, DORA, CMMC)?

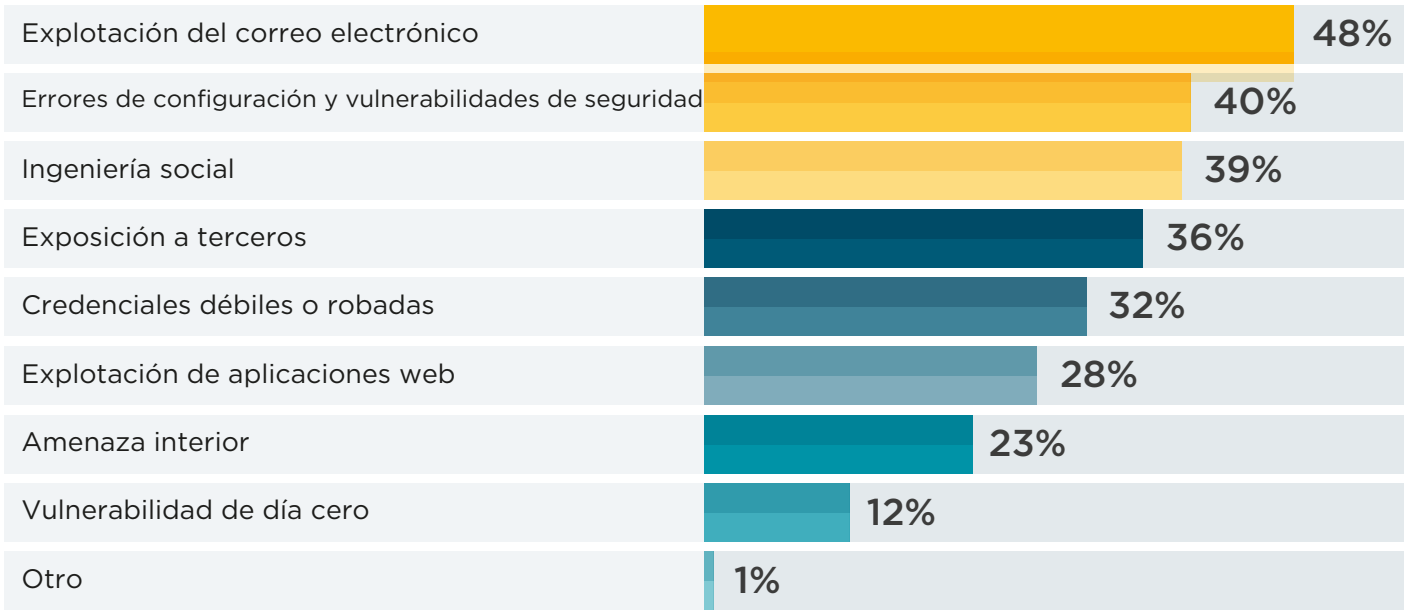
44%	**28%**	**13%**	**4%**
Contamos con un equipo especializado responsable de garantizar el pleno cumplimiento de toda la normativa pertinente.	Hemos implantado herramientas y sistemas automatizados para gestionar y controlar el cumplimiento de la normativa.	Disponemos de medidas básicas, pero estamos trabajando para cumplirlas plenamente.	Actualmente no cumplimos la normativa pertinente en materia de ciberseguridad
5%	**2%**	**0%**	**4%**
Realizamos auditorías y evaluaciones periódicas para garantizar el cumplimiento de la normativa de ciberseguridad.	Recurrimos a consultores externos o a servicios de terceros para mantener el cumplimiento.	Conocemos la normativa, pero aún no hemos aplicado plenamente las medidas de cumplimiento.	No estamos seguros de qué normativa de ciberseguridad es aplicable a nuestra empresa

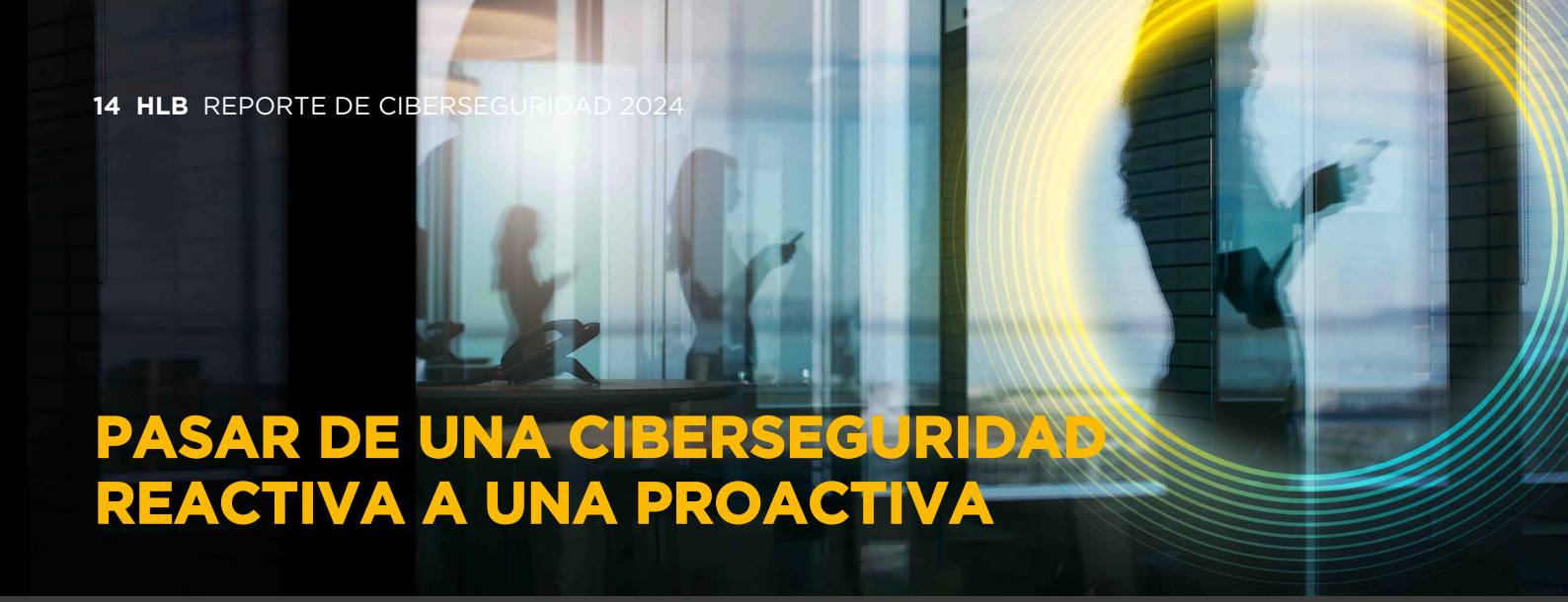
5 Global Cybersecurity Outlook 2024 | World Economic Forum (weforum.org)

Al dar prioridad a la protección de los datos de alto riesgo, las empresas pueden asignar recursos de forma más eficiente y responder con rapidez a las amenazas potenciales. Un impresionante 44% de las organizaciones cuenta ahora con un equipo dedicado, responsable de garantizar el pleno cumplimiento de la normativa pertinente, mientras que otro 28% lleva a cabo auditorías y evaluaciones periódicas.

Continuar por este camino es fundamental para minimizar ciertas ciberamenazas clave, como las desconfiguraciones de seguridad (identificadas por el 40% como uno de los riesgos más prevalentes en 2024) y las credenciales débiles o robadas (identificadas por el 32%).

FIG.7: ¿QUÉ CIBERAMENAZAS CREE QUE SUPONEN UN MAYOR RIESGO PARA SU ORGANIZACIÓN?





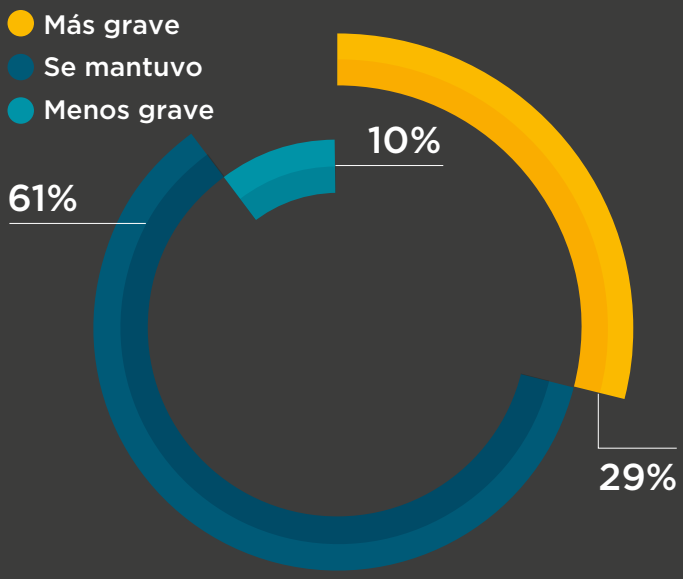
PASAR DE UNA CIBERSEGURIDAD REACTIVA A UNA PROACTIVA

El cambio hacia medidas proactivas de ciberseguridad es esencial. El 97% de las empresas reconoció la necesidad de aumentar sus presupuestos de ciberseguridad en 2024, lo que refleja una conciencia colectiva de las crecientes amenazas digitales.

Mientras que el 39% de las organizaciones informaron de un aumento de los ciberataques en los últimos 12 meses, el 61% declaró que la gravedad de estos ataques se mantuvo igual. Esta relativa estabilidad indica que muchas organizaciones poseen la resistencia básica necesaria para hacer frente a las amenazas inmediatas. Sin embargo, la verdadera seguridad no consiste en sobrevivir a los ataques, sino en anticiparse a ellos y prevenirlos.

FIG.8: CONSECUENCIAS DE LOS CIBERATAQUES EN LOS ÚLTIMOS 12 MESES

¿Las consecuencias de los ciberataques contra su organización han sido más graves, menos graves o se han mantenido igual en los últimos 12 meses?



Un enfoque proactivo implica identificar las vulnerabilidades potenciales antes de que sean explotadas, una práctica que puede reducir significativamente la probabilidad de consecuencias graves.

El 80% de las organizaciones ya dispone de un plan definido de respuesta a incidentes, y otro 12% está diseñando uno. Esta preparación indica una base sólida sobre la que construir estrategias proactivas. Al integrar la gestión de vulnerabilidades basada en el riesgo, los profesionales de TI pueden priorizar las amenazas en función de su impacto potencial, lo que permite asignar los recursos de una forma más específica. asignar los recursos de forma más precisa. Por su parte, la gestión de la superficie de ataque proporciona una visión global de todos los posibles puntos de entrada, lo que permite a las organizaciones reforzar los puntos débiles antes de que sean atacados.

La transición hacia una seguridad proactiva respaldada por nuestros datos, que revelan que El 63% de las organizaciones ya han dado prioridad a la ciberseguridad en sus debates estratégicos. Este compromiso muestra una tendencia más amplia a no limitarse a reaccionar ante los incidentes, sino a anticipar y neutralizar las amenazas antes de que se materialicen..

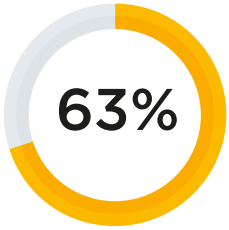
«Aunque muchas empresas dan prioridad a la ciberseguridad dentro de su marco estratégico, y una parte significativa cree poseer los recursos técnicos, humanos y financieros para combatir estos retos, un menor número confía en una rápida recuperación tras un ataque. Esta discrepancia pone de relieve la necesidad de que las organizaciones reevalúen continuamente su preparación, especialmente a medida que los desarrollos de IA se aceleran a nivel mundial.»

Jim Bourke | Líder en tecnología y asesoramiento, HLB Global

Avanzar hacia una seguridad proactiva es una necesidad estratégica. Al adoptar estrategias con visión de futuro, las organizaciones no sólo pueden defenderse contra las amenazas actuales, sino también posicionarse como líderes en resiliencia de ciberseguridad. En última instancia, esta postura proactiva permitirá a las empresas mantenerse a la cabeza de la carrera cibernética, preservando tanto sus datos como su reputación.

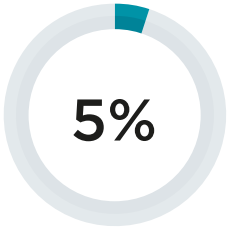
¿HASTA QUÉ PUNTO LA CIBERSEGURIDAD ES UNA PRIORIDAD ORGANIZATIVA?

¿En qué medida es la ciberseguridad una prioridad en la estrategia global de su organización?

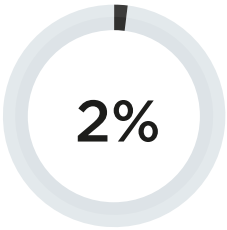


Es una prioridad máxima que se debate periódicamente

Es importante pero se discute de vez en cuando



Sólo se aborda cuando surgen problemas



No es un foco significativo

FUNDAMENTOS CIBERNÉTICOS DEL FUTURO: EVALÚE SU PREPARACIÓN

En una era en la que las amenazas a la ciberseguridad evolucionan a un ritmo sin precedentes, las empresas deben adaptar continuamente sus estrategias para mantenerse a la vanguardia. Comprender, aplicar y preparar para el futuro los fundamentos de la ciberseguridad es crucial para salvaguardar los activos de la organización.

De nuestros datos podemos extraer una serie de recomendaciones:

Ciberseguridad formación en sensibilización
Una formación de concienciación exhaustiva. implica desplegar sesiones de formación periódicas que mantengan a los empleados informados sobre las últimas amenazas y las mejores prácticas. Garantizar el cumplimiento requiere una comunicación coherente en todos los niveles de la organización. Este enfoque no sólo refuerza las defensas, sino que también crea una cultura consciente de la seguridad.

Configuración y seguridad
Ya se realicen internamente por equipos dedicados, o externamente a través de socios especializados, estas evaluaciones ayudan a garantizar que los sistemas sigan siendo sólidos frente a las amenazas emergentes. Estas revisiones deben ser sistemáticas y abarcar todas las infraestructuras críticas, detectando y abordando las posibles vulnerabilidades.

Pruebas de presión para Mejoras proactivas
Realizar pruebas de presión sobre las tecnologías, los procesos y el personal de seguridad es un método estratégico para identificar los puntos débiles antes de que sean explotados. Mediante la simulación de posibles escenarios de ataque, las organizaciones pueden identificar áreas de y mejorar sus defensas en consecuencia. Esta actitud proactiva es vital para mantener la cibernética.

Tercer proveedor Medidas de seguridad
Nuestro plan en cuatro pasos (pgXX) para mitigar los riesgos de terceros ofrece un marco completo para la gestión de proveedores. Garantizar que los proveedores se adhieran a protocolos de seguridad estrictos puede proteger a la organización de las vulnerabilidades introducidas introducidas por socios externos.

Al centrarse en estas áreas fundamentales de la ciberdefensa, las organizaciones pueden seguir siendo resistentes frente a futuras amenazas. Cuando los líderes empresariales comprenden el panorama cibernético y fomentan métodos de evaluación y adaptación continuas, las organizaciones pueden crear un entorno en el que la seguridad esté integrada en todas las facetas de la empresa.

CÓMO PUEDE AYUDAR HLB

La ciberseguridad es un proceso de ciclo de vida, que requiere diligencia e inversión continuas. La formación y la tecnología no son inversiones únicas, ni suficientes para garantizar una resistencia permanente. Los mejores programas de ciberseguridad se centran en conseguir efectos a largo plazo. Los profesionales de ciberseguridad de HLB pueden ayudarle a priorizar los riesgos, evaluar sus sistemas y aplicar los cambios necesarios para proteger su organización. Póngase en contacto con nosotros hoy mismo.

NUESTROS SERVICIOS

CONSULTORÍA SOBRE CIBERRIESGOS

- ANÁLISIS DE LAGUNAS EN EL CUMPLIMIENTO DE LAS NORMAS
- EVALUAIÓN DE RIESGOS
- EVALUACIÓN DE LA MADUREZ DE LA SEGURIDAD
- ESTRATEGIA DE CIBERSEGURIDAD

SOC COMO SERVICIO

- SUPERVISIÓN DE INCIDENTES DE SEGURIDAD
- RESPUESTA A INCIDENTES
- INFORMÁTICA FORENSE
- CAZA DE AMENAZAS

CYBERDRILLS

- EVALUACIÓN DE LA RESPUESTA AL INCIDENTE

CAPACIDADES

- EVALUACIÓN DE CIBERRESILIENCIA
- NACIONAL CIBERRILLOS

EVALUACIONES TÉCNICAS DE SEGURIDAD

- EVALUACIÓN DE LA VULNERABILIDAD
- PRUEBAS DE PENETRACIÓN
- REVISIÓN DEL CÓDIGO FUENTE
- EJERCICIOS DEL EQUIPO ROJO

SEGURIDAD GESTIONADA

- AUDITORÍAS INTERNAS
- INFORMACIÓN SOBRE AMENAZAS
- GESTIÓN Y APOYO TECNOLÓGICOS
- CONCIENCIACIÓN SOBRE SEGURIDAD

METODOLOGÍA DE LA INVESTIGACIÓN

En septiembre de 2024, HLB recopiló más de 600 respuestas de líderes mundiales de TI de diversos sectores. Las respuestas se recogieron a través de una herramienta de encuesta en línea. Además, se han realizado intercambios de correos electrónicos de casos prácticos para recopilar datos de expertos externos en la materia.

Tenga en cuenta que no todas las cifras de este informe suman 100% como resultado del redondeo de porcentajes, la exclusión de respuestas neutras o cuando los encuestados podían elegir más de una respuesta.

AGRADECIMIENTOS

Abu Bakkar
Jim Bourke
Mark Butler
Rita Carolan
Martin Ellis
Toby Henness
Pablo Kaplan
Edward Keck Jr
Yusuf Malik
Gareth Rees
Michael Rooney
Gustavo Solis
Amy Spillard
Nicola Verespejova
Susannah Waters

www.hlb.global

TOGETHER WE MAKE IT HAPPEN

HLB International Limited, registered in England & Wales No. 02181222, registered office: Lynton House 7-12, Tavistock Square, London, WC1H 9LT.