Tendencias en ciberdelincuencia 2024

Lo último en ciberamenazas y en buenas prácticas de seguridad

sosafe

Tabla de contenidos

En 2023, todo cambió. Prepárate para lo que viene a partir de ahora.

2023 ha marcado un punto de inflexión en el contexto global actual. Desde que OpenAI anunció el lanzamiento de ChatGPT-3 en noviembre de 2022 se ha producido una oleada de innovación impulsada por la IA y **un gran cambio en la forma en que interactuamos con la tecnología**. Las repercusiones de este cambio son especialmente evidentes en la seguridad de la información. En este ámbito, la IA se ha convertido en una fuerza muy potente capaz de, por un lado, ayudar a reforzar las defensas de ciberseguridad y, por otro, hacer que los ciberataques sean más sofisticados.

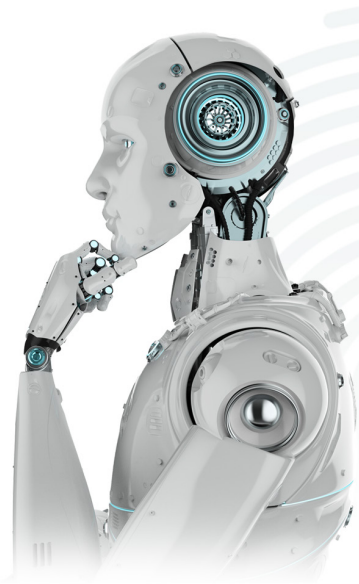
Por tanto, en 2024 tendremos que afrontar una serie de retos que son, en gran medida, resultado de **una tecnología que avanza a una velocidad sin precedentes**: un uso cada vez mayor de la IA en los ciberataques, el arma de doble filo que representan tecnologías emergentes como la 5G y la computación cuántica, y la evolución de la ciberdelincuencia hacia una industria muy profesionalizada. A este complicado panorama se le suman el auge del hacktivismo y los ciberataques en un contexto de crisis políticas mundiales y el aumento de las campañas de desinformación, lo que hace que las amenazas sean más complejas y tengan mayor alcance. Y mientras tanto, los profesionales de la ciberseguridad están cada vez más desbordados frente a esta escalada de amenazas.

En este panorama tan complejo, los hackers utilizarán este año más que nunca el factor humano para llevar a cabo sus ataques, por lo que no nos queda otra opción más que apostar por una cultura de seguridad sólida. Por eso, en este informe analizamos las ocho tendencias de ciberdelincuencia para 2024 y exponemos las mejores prácticas de seguridad para que estés bien preparado para afrontar las diferentes amenazas cibernéticas.

1 El aumento del uso de la IA en los ciberataques: se acerca la tormenta

Según las previsiones, el uso generalizado de la IA ascenderá a más de 300 millones de usuarios en 2024 y a unos 700 millones en 2030.[1] Estas cifras reflejan la magnitud de la revolución que estamos viviendo, pero también son un dato preocupante por sus posibles repercusiones a gran escala y por los riesgos que suponen para la seguridad. Inevitablemente, los **deepfakes** y la **clonación de voz** acaparan toda la atención a la hora de abordar los retos de seguridad que plantea la IA.

Estos dos métodos llevan tiempo siendo habituales entre los cibercriminales, pero con la reciente proliferación de herramientas capaces de producir vídeos deepfake de alta calidad, esta tecnología está más accesible y por lo tanto se utiliza cada vez más, sobre todo en **campañas de desinformación y manipulación social**[2] (más información al respecto en el apartado sobre la tendencia de la «desinformación como servicio»).



1 de cada 4

personas ha sufrido un **ciberataque de clonación de voz** o conoce a alguien que lo ha sufrido.

Fuente: McAfee[3]

La clonación de voz tampoco se queda atrás. Un estudio reciente confirma que una de cada cuatro personas ha sufrido un ciberataque de clonación de voz o conoce a alguien que lo ha sufrido.[3] La policía de Everett (Washington) incluso ha advertido de un aumento de las estafas a particulares en las que se utiliza esta táctica.[4] Los ciberdelincuentes recurren a este tipo de ataques sobre todo para pedir dinero, como sucedió en el caso en el que fingieron el secuestro de una joven para pedir un rescate.[5] Además, ahora también utilizan este método para

1 **Statista (2023).** Artificial Intelligence Worldwide.

2 **Agencia Sinc (2023).** Los "deepfakes" como arma de desinformación y propaganda en tiempos de guerra.

3 **McAfee (2023).** Artificial Imposters—Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam.

4 **Fox 13 Seattle (2023).** Everett Police warn of AI voice-cloning phone scam after case reported in Snohomish County.

5 **La Razón (2023).** Los peligros de GhatGPT: Usan la IA para simular un secuestro.

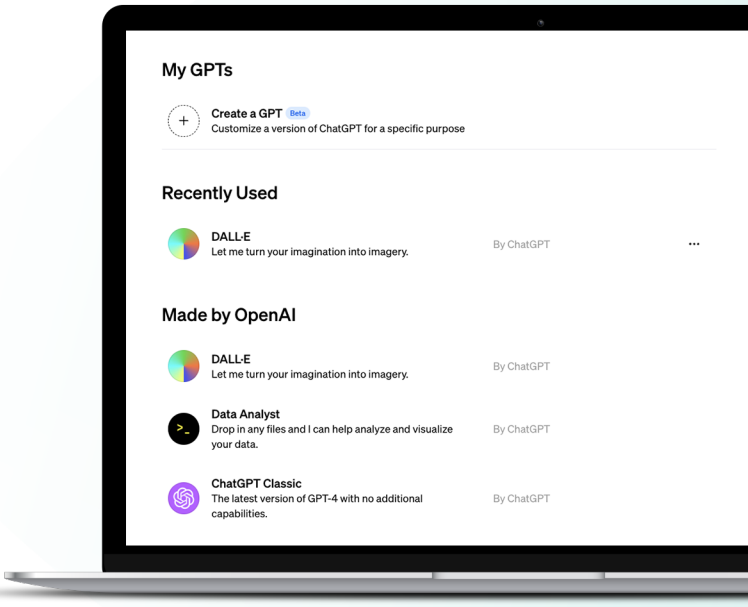
sortear sistemas de autenticación multifactor basados en el reconocimiento de voz. A principios de este año, por ejemplo, una periodista logró acceder a su cuenta bancaria utilizando una grabación de su propia voz clonada.[6] Aunque el experimento de esta periodista no tuvo consecuencias, es un caso que nos muestra el peligroso potencial real de esta tecnología.

Pero este no es, ni mucho menos, el único modo en que los ciberdelincuentes utilizan la IA. Gracias a los avances de la IA generativa en el último año se han incorporado muchas nuevas funciones a las principales herramientas. Algunas de ellas, como la función de ChatGPT que permite leer imágenes, pueden utilizarse con fines maliciosos. De este modo surgen posibilidades como los ataques de **inyección de prompts**, que consisten en hacer que una herramienta siga las instrucciones o prompts que contiene una imagen en lugar de las que escribe el usuario en la herramienta al enviar la imagen.[7] Aunque esto pueda parecer en principio inofensivo, las posibilidades de manipular a los usuarios mediante esta táctica son infinitas.

Se teme, además, que esta función que permite leer imágenes pueda plantear otros problemas, como la posibilidad de **leer códigos CAPTCHA**, una de las barreras de seguridad más conocidas para impedir un uso inadecuado de la tecnología. Hasta hace poco, las restricciones éticas de las propias herramientas impedían que un hacker pudiera utilizarlas para leer códigos CAPTCHA. Sin embargo, se ha demostrado que se pueden descifrar estos códigos utilizando ciertas instrucciones, como una excusa o un pretexto razonable.[8] Esto ha levantado las alarmas de empresas y páginas web de todo el mundo, ya que temen verse **obligados a cambiar a otros métodos de seguridad**.

A medida que la tecnología avanza, **los hackers la van utilizando para construir sus propias herramientas de IA basadas en modelos de lenguaje ya existentes**. Así es cómo aparecieron las primeras alternativas maliciosas a ChatGPT, como FraudGPT y WormGPT.[9] Sin embargo, hasta finales de 2023, para crear este tipo de herramientas (no para usarlas) se necesitaban conocimientos técnicos.

Hace unos meses, OpenAI lanzó una función que permite crear muy fácilmente un GPT, es decir, un chatbot que el usuario puede entrenar para que le ayude con una tarea específica. Todo esto sin tener que programar ni tener conocimientos técnicos, y sin las complicaciones que tienen los programas similares que se encuentran en la dark web. Probablemente, los GPT personalizados serán para muchos un recurso muy útil que les ayude a resolver



6 **Business Insider (2023).** Una persona logra entrar en su cuenta bancaria con una voz generada por IA: así funciona este método que puede ser utilizado por los delincuentes.

7 **Window Central (2023).** GPT-4 Vision: A breakthrough in image deciphering unveils potential for 'prompt injection attacks'.

8 **Digital Trends (2023).** Bing Chat derrota a un CAPTCHA utilizado para detener hackers.

9 **Ciberpro (2023).** FraudGPT: el gemelo malicioso de ChatGPT que los cibercriminales están adquiriendo en la Dark Web.

sus tareas cotidianas, pero también es probable que **en 2024 los ciberdelincuentes los utilicen para crear asistentes personales**[10] especializados en generar textos de smishing muy convincentes, correos de spear phishing o malware polimórfico.[11]

Además de sus potenciales usos maliciosos, los riesgos asociados a la IA también pueden derivarse de sus **limitaciones**. La capacidad de los modelos avanzados de IA para escribir código es un gran avance y una funcionalidad interesante que utilizan hasta el 92 % de los desarrolladores dentro y fuera del trabajo.[12] Sin embargo, los expertos empiezan a dudar de la **fiabilidad del código generado por la IA**, ya que este tipo de herramientas tienden a priorizar la funcionalidad antes que la seguridad.[13] El resultado de esto son todo tipo de fallos de seguridad, como una mayor vulnerabilidad a inyecciones SQL, credenciales «hardcodeadas», o el uso de algoritmos hash de contraseñas no seguros.[14]

Pero posiblemente la limitación más común de la IA es un fenómeno llamado **«alucinación»**, que aplicado a la IA significa que proporciona información falsa o inventada. **Últimamente, los hackers están explotando estas alucinaciones para infiltrar archivos maliciosos**.[15] Cuando el usuario introduce una consulta, la herramienta empieza a «alucinar» y a recomendar nombres de bibliotecas de código inexistentes. El hacker crea a continuación una biblioteca o paquete de código malicioso con uno de esos nombres y lo sube a los repositorios públicos. De este modo, la próxima vez que la herramienta recomiende uno de estos paquetes a un usuario, se descargará la biblioteca de código malicioso que el hacker había subido.

Teniendo en cuenta todas las amenazas asociadas al uso de la IA y la rapidez con que avanza la tecnología, **es necesario identificar y aplicar métodos sólidos para protegernos contra estas amenazas**. Ante la creciente presencia de la IA en todo lo que nos rodea, debemos adoptar un enfoque de ciberseguridad proactivo para mantener la seguridad tanto en el ámbito empresarial como en el privado.

10 **BBC (2023).** ChatGPT tool could be abused by scammers and hackers.

11 **Cyber Security News (2023).** ChatGPT puede usarse para crear malware polimórfico.

12 **GitHub Blog (2023).** Survey reveals AI's impact on the developer experience.

13 **DiarioIT.com (2022).** Los asistentes de IA son más propensos a escribir código inseguro y defectuoso.

14 **MuyComputer (2023).** No acudas a ChatGPT con dudas sobre programación.

15 **Infosecurity (2023).** New ChatGPT Attack Technique Spreads Malicious Packages.

CHECKLIST

Mejores prácticas de seguridad

- **Comprueba el código generado por la IA antes de implementarlo:** aunque hayas especificado en la herramienta que el código que genere deba ser seguro, es recomendable comprobar su fiabilidad con herramientas de revisión automática de código o adoptando un conjunto de medidas de seguridad estandarizadas.

- **Sigue las últimas tendencias en IA y adapta tu estrategia de seguridad en consecuencia:** con el progreso tecnológico, algunas medidas de seguridad pueden dejar de ser fiables, y debes encontrar soluciones alternativas que mantengan un buen nivel de protección para tu empresa. Una buena iniciativa puede ser crear un grupo de trabajo o una unidad de inteligencia dentro de tu organización que se dedique a supervisar y analizar ataques en los que se utilice la IA, así como su impacto en tu estrategia de ciberseguridad.

- **Utiliza las herramientas de IA con responsabilidad:** evita introducir datos personales y confiar exclusivamente en la información que te facilitan. Recuerda que algunas de sus respuestas pueden ser incorrectas o estar desactualizadas, por lo que es conveniente comprobar la veracidad de la información.

- **Aprovecha la IA para reforzar la seguridad de tu empresa:** la incorporación de herramientas de IA puede mejorar notablemente el análisis de grandes conjuntos de datos, lo que permitirá detectar mejor las anomalías e identificar las amenazas en tiempo real con mayor eficacia. La integración de la IA con tu SOAR (sistema de orquestación, automatización y respuesta de seguridad) permite implementar una toma de decisiones automatizada e inteligente y una gestión de incidentes con mayor capacidad de respuesta. Además, el uso de la IA en la automatización sin código permite adaptar rápidamente los flujos de trabajo de seguridad para seguir el ritmo de las amenazas digitales, que no dejan de evolucionar. También es recomendable implantar métodos de autenticación avanzados basados en IA, capaces de aprender y de mejorar continuamente las medidas de seguridad, así como de garantizar el cumplimiento de las políticas y consideraciones éticas mediante una supervisión humana oportuna.

- **Desconfía de los mensajes de voz o vídeo sospechosos:** aunque parezcan auténticos, si contienen peticiones extrañas o afirmaciones sospechosas, es aconsejable ponerse en contacto de otra manera para verificar su autenticidad.

- **Educa a tus empleados sobre los posibles riesgos de seguridad de la IA:** ellos serán tu mejor línea de defensa si saben cómo protegerse a sí mismos y a tu organización de las ciberamenazas. Ofréceles también formación para que aprendan a utilizar la IA generativa de forma responsable, siempre protegiendo los datos sensibles.

2 Más allá de la IA: los ciberdelincuentes están aprovechando todas las nuevas tecnologías

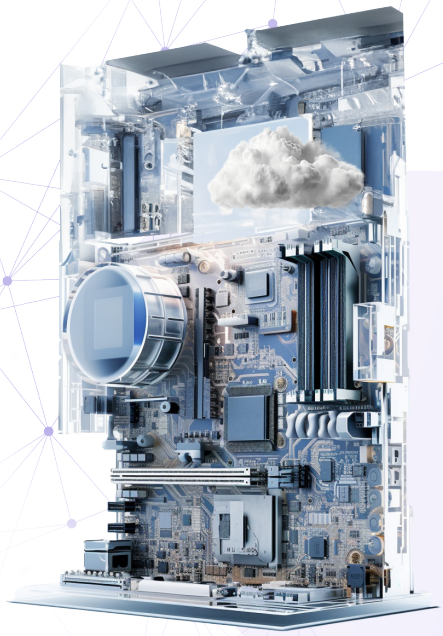
Aunque la IA pueda considerarse la gran innovación de este siglo, los ciberdelincuentes no centran su atención solo en ella, sino que **también** se dedican a explotar otras tecnologías nuevas. El objetivo es ampliar la superficie de ataque y llegar lo más lejos posible. Por eso, cada **tecnología que aparece se convierte tanto en una herramienta como en un nuevo objetivo** de los hackers.

En realidad, esta tendencia no es nueva. Ya vimos patrones similares con otras tecnologías, como **«la nube»**. En los últimos años, las empresas han invertido miles de millones de dólares en cambiar las soluciones de almacenamiento de datos tradicionales por el almacenamiento en la nube. Por supuesto, esta transición no ha pasado desapercibida para los ciberdelincuentes. Según el Informe global de amenazas de CrowdStrike, los ataques dirigidos a sistemas en la nube casi se duplicaron en 2022, y el número de grupos de hackers capaces de lanzar tales ataques se va a triplicar en los próximos años.[1]

Un claro ejemplo de ello fue el ataque de ransomware que se produjo en Sri Lanka a principios de agosto de 2023, en el que los atacantes se infiltraron en el sistema en la nube del gobierno de Sri Lanka después de haber distribuido enlaces maliciosos entre los empleados.[2] El ataque borró cuatro meses de datos almacenados porque el sistema en la nube del gobierno no disponía de copias de seguridad.

Ahora, las tecnologías emergentes como la **computación cuántica** se enfrentan al mismo destino. En este sentido, existe un concepto muy importante para los ciberdelincuentes, que es el de «cosechar ahora, descifrar después» (HNDL, por sus siglas en inglés).[3] Este método consiste en acumular datos cifrados hoy con la esperanza de que los avances en computación cuántica les permitan descifrarlos más adelante. Si esto se produjera, daría lugar a una nueva dimensión de casos de fuga de datos, robos de propiedad intelectual y exposición de secretos de seguridad nacional.

Tras reconocer este problema, el Centro Nacional de Ciberseguridad del Reino Unido redactó en 2020 un informe con consejos para llevar a cabo la transición a algoritmos resistentes a ataques cuánticos



1 **CrowdStrike (2023).** Global Threat Report.

2 **Escudo Digital (2023).** El gobierno de Sri Lanka es víctima de un ataque de ransomware.

3 **Ey (2023).** Por qué las organizaciones deberían prepararse ahora para la ciberseguridad de computación cuántica.

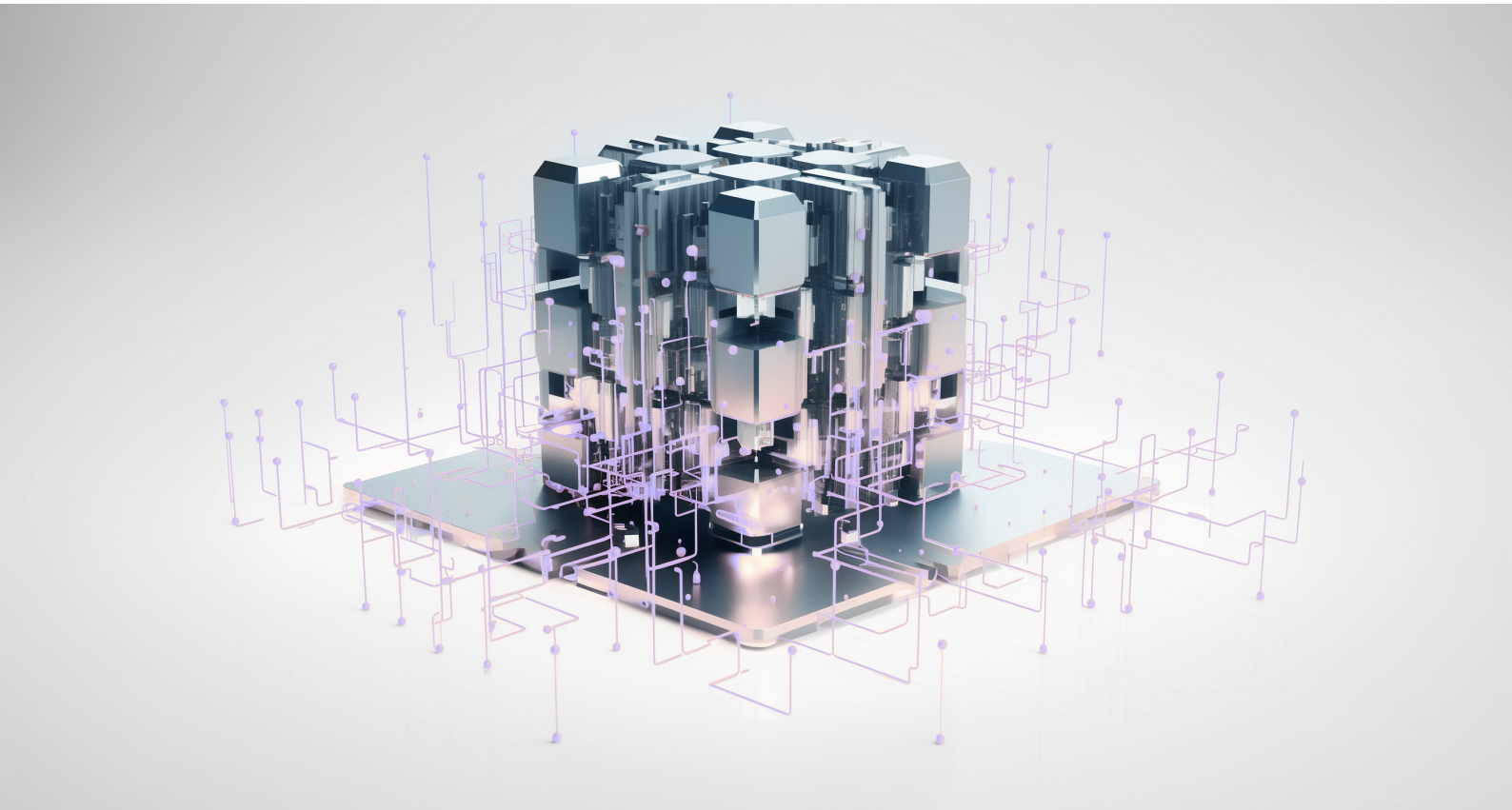
y subrayando la importancia de iniciar pronto este proceso para garantizar la seguridad frente a posibles amenazas de computación cuántica.[4] Sin embargo, la incertidumbre que rodea al calendario de avances de la computación cuántica genera una situación compleja en la que las organizaciones se debaten entre afrontar el coste de adoptar medidas tempranas de prevención y asumir el riesgo de no estar preparadas para un salto inesperado de las capacidades de esta nueva tecnología.

El 5G es otro ejemplo de cómo las nuevas tecnologías pueden convertirse en un arma de doble filo, ya que prometen una conectividad y una velocidad sin precedentes, pero también abren nuevas vías que los ciberdelincuentes pueden explotar. La Agencia de Seguridad de Infraestructuras y Ciberseguridad de EE.UU. (CISA) identifica los siguientes riesgos asociados al 5G: aumento de las vulnerabilidades debido al complejo diseño de la red y a los despliegues locales de 5G; amenazas a la cadena de suministro por hardware y software maliciosos; debilidades heredadas de la infraestructura antigua y componentes de escasa fiabilidad; competencia limitada en el mercado que lleva a depender de soluciones potencialmente inseguras; y una superficie de ataque más extensa que introduce nuevas vulnerabilidades y aumenta el riesgo de fuga de datos.[5]

Todos estos avances subrayan un aspecto crítico: a medida que estas y otras **nuevas tecnologías siguen evolucionando, también lo hacen los métodos y los objetivos de los ciberdelincuentes**. Es una carrera constante en la que cada nuevo adelanto tecnológico encierra una nueva oportunidad de explotación en el mundo de la ciberdelincuencia. Por lo tanto, las estrategias de ciberseguridad deben ser ágiles y adaptables, y han de evolucionar a la misma velocidad que estos avances tecnológicos para hacer frente a las nuevas ciberamenazas.

4 **National Cyber Security Centre (2020).** Preparing for quantum-safe cryptography.

5 **CISA (2023).** 5G Security and Resilience.



CHECKLIST

Mejores prácticas de seguridad

- **Refuerza la seguridad en la nube:** apuesta por sistemas avanzados de copia de seguridad y recuperación de datos, e implementa una rutina de actualizaciones y parches periódicos para garantizar una mejor protección frente a futuras amenazas.
- **Minimiza el riesgo de fuga de datos:** utiliza la microsegmentación para proteger tus datos, así como una rotación rutinaria de las claves de cifrado en función de la clasificación de los datos. Asegúrate también de actualizar el software y las medidas de seguridad de forma continua.
- **Adopta un enfoque de agilidad criptográfica:** prepárate para adaptar rápidamente los algoritmos y métodos criptográficos a las nuevas amenazas.
- **Protege las redes 5G:** analiza y combate las vulnerabilidades en las redes de diseño complejo y en despliegues locales, y protege la seguridad de la cadena de suministro, incluidos los componentes de hardware y software.
- **Reduce las vulnerabilidades de las infraestructuras heredadas:** actualiza o sustituye los sistemas antiguos que puedan tener fallos de seguridad inherentes, y aplica medidas de seguridad al diseño de las nuevas tecnologías.
- **Vigila las amenazas emergentes y adáptate a ellas:** mantente al corriente de las ciberamenazas emergentes, adapta las estrategias en consecuencia e implementa una supervisión continua y un análisis de amenazas en tiempo real.
- **Refuerza los conocimientos de ciberseguridad de tu equipo:** prepara a tu equipo de seguridad y al resto de la plantilla con una formación continua para que sepan reaccionar con rapidez y adaptarse a las nuevas amenazas.

3 La ciberdelincuencia, un negocio cada vez más profesionalizado y rentable

La profesionalización de la ciberdelincuencia sigue avanzando y alcanzará un nivel de madurez más alto en 2024. Uno de los motivos de esta escalada es la propagación del ransomware como servicio (**RaaS**, por sus siglas en inglés). Como ya indicábamos en el informe del pasado año, cualquiera puede abrirse camino en el mundo de la ciberdelincuencia con estas sofisticadas herramientas que, además, añaden un giro radical en cuanto a la complejidad y el impacto de los ataques.

A lo largo de 2023, esta tendencia ha evolucionado hasta duplicarse **el número de víctimas de ataques de ransomware** en comparación con abril de 2022.[1] Este alarmante aumento pone de manifiesto que el ransomware sigue siendo la **amenaza digital más dañina, costosa y predominante para las organizaciones de la región EMEA**.[2]

Este cambio se ve reflejado también en una clara evolución de los ataques de ransomware, que son cada vez más selectivos. Como veremos más adelante, existe una tendencia hacia los **ataques dirigidos contra el sector público y las infraestructuras críticas**, que afectan en particular a la sanidad, la educación y las organizaciones gubernamentales. La razón es que estas instituciones carecen a menudo de recursos de seguridad adecuados, y por lo tanto es más probable que paguen un rescate con tal de mantener el funcionamiento de los servicios esenciales y proteger la información sensible.

Un inquietante ejemplo de esto es lo que ocurrió en Maine en mayo de 2023, cuando un grupo de ransomware aprovechó una vulnerabilidad de MOVEit, un programa de transferencia de archivos que utilizan las administraciones del Estado, para infiltrarse en sus sistemas. Los **atacantes robaron datos de 1,3 millones de personas**, entre los que se incluían nombres, fechas de nacimiento, datos de tarjetas sanitarias, carnés de conducir y otros registros de identificación nacional y fiscal.[3]

Pero estos no han sido los únicos sectores que se han visto afectados. MGM Resorts, una de las principales cadenas de hoteles-casino del mundo, fue atacada por hackers de Scattered Spider, un subgrupo de ALPHV, en septiembre de 2023.[4] Utilizando métodos de ingeniería social, los atacantes encontraron a un empleado a través de LinkedIn y llamaron al servicio de asistencia. **Una conversación de 10 minutos bastó para comprometer a esta empresa multimillonaria**. El ciberataque a los hoteles MGM provocó graves problemas: dejó cajeros automáticos y máquinas de juego fuera de servicio, y bloqueó su página web y los sistemas de reservas. Se estima que la pérdida de beneficios en el tercer trimestre asciende a unos 100 millones, a los que se suman otros 10 millones en gastos de recuperación por asesoramiento tecnológico, honorarios de abogados y otros gastos de consultoría externa.

1 **Black Kite (2023).** Ransomware threat landscape report.

2 **Gulf Business (2023).** Cybersecurity 2023: Threats proliferate but best practice still works.

3 **IT Global (2023).** El Gran Ciberataque de 2023: 62 Millones Afectados, Privacidad en Riesgo.

4 **Europa Press (2023).** Un ataque de ingeniería social obliga a la cadena MGM Resorts a apagar los sistemas informáticos de sus casinos.

> **El promedio de tiempo que se tarda en reanudar las operaciones básicas tras un ataque severo de ransomware es de unos 23 días. Restablecer la plena funcionalidad del sistema completo puede llevar meses.**

Inge van der Beijl
Human resilience enabler and threat communications expert en Northwave, en la Human Firewall Conference 2023

La creciente agresividad de los ciberdelincuentes se manifiesta sobre todo en una intensificación de las tácticas de rescate. **Cada vez es más frecuente la doble extorsión**, es decir, los ciberdelincuentes cifran los datos y al mismo tiempo amenazan con publicarlos. En realidad, este método no es nuevo, pero llama la atención su aumento en los últimos meses.[5] Algunos hackers llegan a emplear una **triple extorsión** agregando otro tipo de ataques, como DDoS, o incluso una **extorsión cuádruple**, presionando además a clientes, proveedores y empleados de la empresa atacada. Este fue el caso del proveedor de hardware Quanta Computer, que se negó a atender las peticiones de rescate del grupo REvil, de modo que los atacantes centraron su atención en Apple, uno de los clientes de Quanta.[6] El grupo no sólo amenazó con divulgar datos confidenciales de productos de Apple sustraídos en el ataque, sino que también trató de aumentar la presión amenazando con revelar esos datos en el lanzamiento del producto de Apple, aprovechando así la atención pública y mediática para maximizar el impacto.

Más allá del ransomware como servicio, la profesionalización de la ciberdelincuencia se sirve de otras tecnologías emergentes como la clonación de voz. Como mencionábamos en el apartado sobre la IA, **la clonación de voz como servicio** (VCaaS, por sus siglas en inglés) se ha convertido en una amenaza inminente que permite incluso a ciberdelincuentes poco experimentados llevar a cabo sofisticados ataques de suplantación de identidad.[7] Con plataformas como ElevenLabs, que permiten a los usuarios crear muestras de voz personalizadas, dar el paso hacia la ciberdelincuencia es cada vez más fácil.

Al tiempo que avanzan la profesionalización y la complejidad de los ciberataques, resulta cada vez más evidente la importancia de preservar la seguridad de la cadena de suministro. Para muchas empresas, la externalización de servicios es una práctica necesaria, pero que también crea nuevas vulnerabilidades, ya que los ciberdelincuentes **pueden infiltrarse en las redes corporativas a través de los sistemas de socios o proveedores**. Un ejemplo de ello es lo que le ocurrió a Airbus en 2023 después de que varios hackers atacaran a uno de sus clientes, Turkish Airlines, lo que provocó una importante pérdida de datos de más de 3000 proveedores.[8] En este contexto, podemos afirmar que somos tan fuertes como nuestro eslabón más débil. Por eso, para mantenerse realmente protegida, una empresa debe cuestionarse también la seguridad de sus proveedores, socios comerciales y clientes.

El pronóstico para el futuro está claro: **la ciberdelincuencia se está convirtiendo en un negocio aún más profesional y rentable**, y no debemos ignorar ni subestimar esta tendencia. Ahora es el momento en que las empresas deben invertir en su seguridad, puesto que los avances de los últimos años no son más que el adelanto de un futuro en el que la ciberdelincuencia desarrollará métodos cada vez más sofisticados para lograr sus objetivos.

5 **IT Digital Security (2023).** De la triple extorsión a la cuádruple: el ransomware sigue avanzando.

6 **ABC (2021).** Apple sufre una filtración de datos de sus dispositivos por culpa de un ataque de 'ransomware'.

7 **La Razón (2023).** ¡Alerta! Esta IA te permite clonar la voz de cualquier persona gratis y hacer que diga lo que quieras.

8 **Escudo Digital (2023).** Airbus sufre un ciberataque y algunos de sus datos son filtrados.

CHECKLIST

Mejores prácticas de seguridad

- **Crea una infraestructura resistente al ransomware:** desarrolla una estrategia de ciberseguridad integral que contemple tanto medidas preventivas como planes de respuesta sólidos. Esto se consigue con sistemas avanzados de detección de amenazas, como detección de anomalías basada en IA, y un modelo de Zero Trust para mejorar la seguridad. Realiza auditorías de seguridad periódicas y desarrolla planes eficaces de recuperación en caso de ataque. Revisa también periódicamente las estrategias de copia de seguridad y asegúrate de contar con un plan de respuesta consolidado para reaccionar de forma rápida y eficaz en caso de fuga de datos.

- **Protégete contra los ataques de ingeniería social y phishing:** conciencia a tus empleados sobre los riesgos de los ataques de ingeniería social, en particular sobre las tácticas utilizadas por los grupos de ransomware. Un entrenamiento continuo basado en micromódulos y simulaciones de phishing les ayudará a conocer los riesgos y a reconocer posibles amenazas. Mediante experiencias de aprendizaje gamificadas y personalizadas, los empleados se sentirán más identificados y aprovecharán mejor los conocimientos adquiridos.

- **Haz frente a las vulnerabilidades de día cero:** desarrolla estrategias para reaccionar rápidamente a ataques de día cero, por ejemplo implantando un sistema de gestión de parches para distribuir actualizaciones de software eficazmente y atajar inmediatamente las vulnerabilidades.

- **Refuerza la seguridad de tu cadena de suministro:** revisa y protege tu cadena de suministro comprobando los protocolos de seguridad de tus socios y proveedores e implementando controles de acceso estrictos y sistemas de vigilancia.

- **Mejora la seguridad e integridad de los datos:** aplica métodos de cifrado avanzados y un enfoque de protección de datos por capas, con estructuras de seguridad centradas en los datos y tecnologías de prevención de pérdida de datos (DLP, por sus siglas en inglés). De este modo reducirás el riesgo de filtraciones y robos de información.

- **Utiliza la inteligencia de amenazas y las métricas:** sírvete de herramientas de inteligencia de amenazas para identificar y analizar las amenazas actuales y futuras. Esto te ayudará a adoptar medidas preventivas y a mejorar la capacidad de reacción en caso de ataque.

ENTREVISTA

Ralf Schneider

Allianz Senior Fellow and Head of Cyber Security and NextGenIT Think Tank

Ralf Schneider cuenta con una impresionante trayectoria profesional en el ámbito de la informática y la ciberseguridad. Tiene más de dos décadas de experiencia y su carrera está marcada por su larga permanencia en Allianz, donde ejerció como CIO del grupo durante trece años. También ha sido miembro del consejo de administración de Allianz Managed Operations & Services, y actualmente es Senior Fellow and Head of Cybersecurity and NextGenIT Think Tank. Se doctoró en Ciencias de la información por la Universidad Ludwig Maximilian de Múnich.

> Los ciberdelincuentes necesitan cada vez menos habilidades y capacidad de organización para lanzar ataques muy eficaces, y eso va a suponer un gran problema.

¿Qué te llevó al mundo de la seguridad de la información?

Empecé en este campo cuando me nombraron CIO del Grupo Allianz, en enero de 2011. Con 3000 oficinas y 63 unidades de negocio en todo el mundo, enseguida me di cuenta de que necesitábamos una infraestructura de comunicaciones que incluyera, entre otras cosas, las videoconferencias. Teníamos que diseñar una infraestructura que permitiera acceder a los recursos informáticos a través de cualquier dispositivo y desde cualquier parte del mundo. Para esto se necesita una infraestructura de red, un centro de datos consolidado que sostenga el funcionamiento de las aplicaciones a escala global y un espacio de trabajo virtualizado — todo ello con la debida protección. No teníamos duda alguna de que la ciberseguridad era un tema fundamental para nosotros.

Cuando salieron a la luz las revelaciones de Snowden en 2013 y hackearon el teléfono móvil de la señora Merkel, vimos que la ciberseguridad era una cuestión cada vez más acuciante. Además de la red de infraestructura, el centro de datos y el espacio de trabajo virtualizado, en 2013 establecimos a escala mundial los elementos Cyber Security Infrastructure, Global Identity and Access Management, Global Privilege Access Management, así como el Allianz Cyber Defense Center.

¿Cómo ves el panorama actual de amenazas y cómo crees que evolucionará en los próximos años?

Desde que comenzó la guerra en Ucrania está claro que nos encontramos en plena guerra cibernética. En el frente de la ciberseguridad intervienen poderes estatales, militares y hackers muy peligrosos. Estos ciberdelincuentes perfeccionan continuamente sus tácticas y se organizan cada vez mejor. A ello se añade la industrialización de los ciberataques, que convierte la ciberdelincuencia en un gran negocio.

También hay un tercer componente: la ciberseguridad tiende a ser cíclica. Los ataques DDoS fueron uno de los principales problemas en 2013, después desaparecieron, y ahora han vuelto a resurgir. También debemos contar con el retorno de los activistas y los kits de hackeo, ahora además con IA. Los delincuentes necesitan cada vez menos habilidades y capacidad de organización para lanzar ataques muy eficaces, y eso va a suponer un gran problema. En lugar de centrarnos en unos pocos grupos, tendremos que combatir cientos, si no miles.

El hecho de que la brecha entre ricos y pobres sea cada vez mayor agrava todavía más la situación. Ya no hace falta ser deportista profesional para ganar mucho dinero; puedes hacerte hacker. Lo bueno es que cada vez sabemos defendernos mejor.

Has mencionado el auge de la IA generativa. ¿Crees que tecnologías como los deepfakes y la clonación de voz se convertirán en un problema masivo?

La clonación de voz y métodos similares están actualmente a la orden del día, pero estas nuevas tecnologías entrañan también otros riesgos. Ya no se trata de encontrar un fallo de seguridad o de identificar a un individuo como punto débil. Ahora se trata de la respuesta, es decir, de desactivar y eludir las herramientas de detección. Precisamente ahí se producirá un gran aumento del uso de la IA.

Ahora mismo no veo grandes peligros porque la IA sigue cometiendo demasiados errores, y hay que saber utilizarla correctamente. Pero todavía estamos al principio del recorrido, y deberíamos prepararnos para el peor de los casos. Por el momento nos beneficia que aún no se haya producido esta gran escalada. Con cada ataque —tanto si tiene éxito como si no— aprendemos y podemos mejorar nuestra línea de defensa. Pero el riesgo no está sólo en la cantidad, sino también en la simultaneidad de los ataques, que se hace posible gracias a la IA. Estos ataques simultáneos a escala podrían plantear un problema grave en el futuro.

¿Cómo crees que podemos seguir el ritmo vertiginoso de estos cambios en el panorama de amenazas?

Debemos tener una higiene cibernética adecuada y prestar atención a las amenazas que van surgiendo. En lo que se refiere a la higiene cibernética, tenemos que empezar desde cero, y esto supone un gran reto. Tampoco creo que vayamos a poder prescindir de una autenticación multifactor. De igual manera que cuando vas a conducir te tienes que abrochar el cinturón, antes de empezar a navegar por Internet, tienes que pasar por la autenticación multifactor. En Allianz implementamos la autenticación multifactor durante la pandemia porque empezó a haber más teletrabajo.

Lo más importante para seguir la rápida evolución de las amenazas es trabajar de forma correcta y exhaustiva desde el principio, y después mantenerse actualizado. Actualmente estamos renovando nuestra plataforma de ciberdefensa y para ello hemos escogido trabajar con una empresa líder en el mercado. Ahora, la gran tarea es integrarlo y empezar a utilizarlo, y ahí es donde estamos invirtiendo. Al final, todo se reduce al factor humano: encontrar a las personas adecuadas y darles la oportunidad de aprender de forma independiente. Si una empresa no se preocupa de concienciar a sus empleados, no llegará muy lejos aunque tenga toda la tecnología del mundo.

Al final, todo se reduce al factor humano: encontrar a las personas adecuadas y darles la oportunidad de aprender de forma independiente. Si una empresa no se preocupa de concienciar a sus empleados, no llegará muy lejos aunque tenga toda la tecnología del mundo.

Otra de las tendencias en ciberdelincuencia es la digitalización, ya que todo está cada vez más interconectado. ¿Qué riesgos de ciberseguridad supone esto?

Tener una página web sin un escudo proxy que proteja de las amenazas es muy arriesgado. Todas las empresas necesitan uno, y eso tiene un precio.

Hoy todo está interconectado a una velocidad vertiginosa. Además, todo funciona con software que puede ejecutar acciones en milisegundos. Controlarlo o supervisarlo es imposible sin automatización, pero tampoco podemos confiar en que la IA lo haga todo por nosotros. Si los que nos atacan usan IA, nosotros también debemos usarla para defendernos. Debemos contar con personas que estén preparadas para evaluar la situación con buen criterio y que dispongan de los conocimientos necesarios para utilizarla. Además, hay que tener en cuenta que los puntos de contacto con los sistemas informáticos no son sólo máquinas, sino personas en la mayoría de las ocasiones. Por eso, es necesario supervisar cada uno de estos puntos de contacto y protegerlos contra los ataques.

La pregunta es: ¿deben las empresas eliminar primero sus vulnerabilidades técnicas y después centrarse en las personas, o al revés? ¿Tienes alguna estrategia holística para incluir el factor humano?

Si te lanzas a todas las batallas a ciegas, vas a perder siempre. Si conoces a tu enemigo, es posible que pierdas la mitad de las veces. Pero si te conoces a ti mismo y a tu enemigo, tienes muchas posibilidades de ganar siempre. La ciberseguridad es un juego de ataque y defensa. En 2013 pusimos en marcha dos controles a escala global. Empezamos por la concienciación y la protección a gran escala contra ataques DDoS y contra ataques a los terminales móviles. Después añadimos las capas de protección, detección, respuesta y recuperación.

Dos mil años de sabiduría nos han enseñado que lo esencial es conocerte a ti mismo —en este caso, tus sistemas informáticos, tu red y tus vulnerabilidades. No puedes defender algo que no conoces. Puesto que son personas quienes manejan los sistemas informáticos, hay que conocer a las personas y tener en cuenta su concienciación en ciberseguridad.

¿Qué opinas de que la formación en ciberseguridad pase de ser un mero requisito para cumplir la normativa a implantarse como un proceso continuo que convierte a las personas en un medio de defensa?

Ante la digitalización que nos rodea, no basta con que nuestros sistemas informáticos sean funcionales, también deben ser seguros y cumplir con las normativas. Pero no todo lo que cumple las normativas es bueno en términos de ciberseguridad. La concienciación es un buen ejemplo. Puedes poner en marcha un programa de concienciación en el que los usuarios cumplimentan la formación en línea únicamente para cumplir con las normativas y que las autoridades reguladoras estén satisfechas. Sin embargo, únicamente con eso no haces que tu empresa sea más segura.

Aquí es donde entra en juego la concienciación de los empleados. Aprendimos pronto que hay que abordar la concienciación con un enfoque divertido y no presionar tanto. También hay que saber elegir el momento adecuado para el aprendizaje. Lo ideal es ofrecer información cuando se acaba de recibir un email de la simulación de phishing o un correo electrónico de phishing real. El siguiente reto es mantener la atención. El botón de aviso de phishing de SoSafe es una herramienta extremadamente útil en este sentido. Cuando los empleados no están seguros de si es un email de phishing real o no, pueden utilizar el botón y este les indica si se trata de un intento de ataque de phishing y por qué. De esta manera, el aprendizaje tiene un éxito muy alto. Además, incorpora el factor diversión y la motivación que supone para los empleados aprender por su cuenta y poder utilizar el botón de aviso de phishing como una especie de asistente. Al aplicar directamente lo que han aprendido, los usuarios obtienen una recompensa inmediata.

> Si los que nos atacan usan IA, nosotros también debemos usarla para defendernos. Debemos contar con personas que estén preparadas para evaluar la situación con buen criterio y que dispongan de los conocimientos necesarios para utilizarla.

Los profesionales informáticos están sometidos a todo tipo de presiones, tanto en lo que respecta a la defensa como a la formación en ciberseguridad. ¿Qué medidas podrían aplicarse para aliviar la carga de estos profesionales?

Tenemos que preguntarnos dónde residen realmente los problemas, realizando simulacros de crisis a todos los niveles, incluso en la cúpula directiva y el consejo de administración. En Allianz llevamos años practicándolo con regularidad. Aquí intervienen varios factores psicológicos. Para empezar, a la gente no le gusta demostrar que es incapaz de hacer algo. En segundo lugar, los beneficios del tiempo que han invertido tienen que estar claros desde un principio y notarse rápidamente. Al fin y al cabo, la formación de concienciación cuesta dinero y recursos.

Uno de los principales retos consiste en mostrar de forma tangible la urgencia de los asuntos de ciberseguridad a los altos directivos de todas las unidades de negocio. Desde la perspectiva de los objetivos empresariales, los sistemas informáticos tienen que ser funcionales y seguros al mismo tiempo. Pero, mientras no ocurra algo muy grave, es difícil saber si las medidas que has implementado han mejorado tu nivel de protección. Demostrar la eficacia y eliminar la desconfianza es muy difícil porque no se puede demostrar que se está más seguro que antes. Hay que probar mediante simulaciones de ataques que eres más rápido, más eficiente y más eficaz a la hora de defenderte.

¿Crees que hay algunos KPI que pueden ayudar a convencer a la cúpula directiva?

En Allianz tenemos ocho indicadores del estado de salud de nuestra ciberseguridad, que calificamos con un sistema de colores: rojo, naranja, amarillo y verde. Estos colores representan de forma visual el éxito de nuestras medidas. Igual que cuando se mide la tensión arterial, el pulso y los niveles de colesterol en el cuerpo humano, nuestros ocho indicadores de salud tienen que estar dentro de unos márgenes determinados.

Dos de estos indicadores han demostrado ser especialmente eficaces. Uno es la tolerancia cero frente a los componentes tóxicos en lo que se refiere a los aspectos técnicos, lo que nos ha llevado a realizar un rastreo de todas nuestras aplicaciones obsoletas y de aquellas que no estaban bien protegidas. También hemos empezado a utilizar más la automatización y a analizar todas las bases de datos y sistemas operativos obsoletos, identificando los componentes tóxicos y renovado sistemáticamente nuestro sistema informático completo. El componente de tolerancia cero se implantó por motivos de seguridad, pero va mucho más allá. El segundo indicador eficaz es nuestra «Awareness Score», una calificación que nos ayuda a saber el nivel de concienciación y que utilizamos para medir las campañas globales en las simulaciones de phishing. Registramos los porcentajes de clics y cuántas personas denuncian un correo electrónico malicioso.

En otra entrevista dijiste que las estructuras jerárquicas de las empresas pueden ser una traba para la ciberseguridad. ¿Puedes explicar a qué te referías?

Los ataques externos realizados con herramientas sólo pueden prevenirse con expertos que dispongan de otras herramientas adecuadas. Los expertos en seguridad son quienes deben decidir qué hay que hacer. La cúpula directiva tiene que estar al corriente de todo y proporcionar los recursos y las iniciativas necesarias en el momento oportuno, pero la ejecución se hace «in situ», por lo que también se requiere autonomía. La dirección establece el marco, pone a disposición los recursos para una ciberdefensa eficaz y coordina a los expertos en seguridad con socios internos y externos.

> Los expertos en seguridad son quienes deben decidir qué hay que hacer. La cúpula directiva tiene que estar al corriente de todo y proporcionar los recursos y las iniciativas necesarias en el momento oportuno.

4 Disidencia digital y ciberataques: las dos caras del hacktivismo y la ciberdelincuencia en un mundo dividido

El panorama de las ciberamenazas esconde mucho más que un conjunto de individuos que buscan su propio beneficio económico o personal. Las crecientes tensiones políticas y sociales son el perfecto caldo de cultivo para otro importante fenómeno que desafía la esfera digital: los **hacktivistas**. Su objetivo es expresar su oposición o su apoyo a causas como conflictos armados o injusticias sociales y para difundir sus ideas **aprovechan vulnerabilidades y fallos de seguridad**. Esta situación no ha hecho más que empeorar en los últimos meses.

Según el último informe de Motorola, el hacktivismo aumentó un 27 % en el tercer trimestre de 2023.[1] Un claro ejemplo de esta tendencia es el grupo de hacktivistas prorrusos DDoSia, conocidos por sus ataques contra entidades occidentales. El crecimiento de este grupo en 2023 fue astronómico: el número de miembros se disparó un 2400 % y alcanzó los 45 000 suscriptores en su canal principal de Telegram.[2]

El conflicto entre Rusia y Ucrania, que ya va por su segundo año, nos muestra que en la era moderna los conflictos se convierten en **guerras híbridas que se libran tanto en el espacio físico como en el digital**. Tanto los hacktivistas como los grupos financiados por Estados utilizan los **ciberataques** como una **poderosa herramienta para la guerra moderna**. Un conocido ejemplo es el ataque del grupo ucraniano Cyber.Anarchy.Squad contra Infotel JSC, un proveedor de telecomunicaciones ruso que ofrece servicios esenciales a los principales bancos e instituciones financieras del país.[3] Este ataque interrumpió el funcionamiento de numerosos sistemas bancarios rusos, que no pudieron procesar pagos en línea durante varias horas.

El reciente conflicto entre Israel y Gaza también pone de relieve la prevalencia de esta amenaza y sus repercusiones. Poco después de estallar el conflicto, el grupo Anonymous Sudan lanzó su primer ciberataque contra los sistemas de alerta de emergencia de Israel, que tenía como objetivo desactivar las notificaciones que avisan a la población civil de ataques con misiles.[4] Casi simultáneamente, KillNet intentó bloquear varias páginas web del gobierno israelí. En el otro bando, el grupo indio de hacktivistas Indian Cyber Force, tomó represalias y paralizó las páginas web de Hamás, Palestine National Bank, Palestine Web Mail Government Services y Palestine Telecommunications Company en apoyo a Israel.[5]

1 **Motorola Solutions (2023).** New Report Outlines Q3 2023 Cyber Threats to Public Safety.

2 **Hfrance (2023).** El proyecto hacktivista pro-ruso DDoSia registra un aumento del 2.400% en el número de miembros.

3 **Ciberseguridad LATAM (2023).** Un grupo de piratas informáticos ucranianos, derribó un proveedor de servicios para bancos rusos.

4 **El Español (2023).** Hackers islamistas buscan el caos en Israel: lanzan una alerta falsa de bomba nuclear a la población.

Pero el hacktivismo no se limita a la guerra y las tensiones políticas; también se extiende a las **protestas sociales**. Por ejemplo, Anonymous Sudan lanzó un ciberataque contra Scandinavian Airlines a principios del año pasado.[6] Este ataque fue en respuesta a la quema pública del Corán ante la embajada turca en Estocolmo protagonizada por un grupo nacionalista de extrema derecha. El incidente causó importantes problemas en el sistema online de la aerolínea y reveló información sensible de los pasajeros, como datos de contacto, detalles de vuelos pasados y futuros, y parte de los números de sus tarjetas de crédito.

Más tarde, también en 2023, el grupo de hackers VulzSec declaró haber comprometido y filtrado datos sensibles de la policía francesa como represalia por unos episodios de violencia policial.[7] El ataque hizo que se relevaran 7092 registros de datos y los perfiles de 30 policías. Este incidente subraya una tendencia al alza: un aumento del 28 % de los ciberataques contra las autoridades del orden público, en gran parte debido al hacktivismo.[8]

Sin embargo, es importante destacar que el objetivo de los hacktivistas no es el beneficio económico, sino la defensa de sus convicciones. Por otro lado, existen ciberdelincuentes que aprovechan cualquier inestabilidad social para sus propios fines. Por ejemplo, siguiendo las mismas tácticas que ya se dieron en el conflicto entre Rusia y Ucrania, se están creando ahora páginas web fraudulentas con supuestos fines benéficos que aprovechan la oleada solidaria ante la crisis de Gaza.[9] Y esto no es todo. A esto le tenemos que añadir los ciberdelincuentes a sueldo de los gobiernos, tal y como se ha comprobado con la campaña «WildCard».[10] En este caso, los hackers atacaron a las instituciones israelíes con el sofisticado malware «SysJoker». Esta complicada situación hace que las organizaciones afectadas lo tengan cada vez más difícil para identificar la autoría de los ataques. Además, de esta manera se crea un panorama de ciberamenazas sumamente complejo en el que intervienen diferentes tipos de hackers con intereses muy distintos.

↗ 28 %

aumento de los ciberataques contra las autoridades del orden público, en gran parte debido al **hacktivismo**.

Fuente: Motorola Solutions[8]

Como las tensiones mundiales siguen escalando sin un final previsible, se prevé que también continúen aumentando los ataques de hacktivistas en 2024. En este contexto, tanto los hacktivistas como los ciberdelincuentes contribuyen de igual forma a la inestabilidad del mundo cibernético. Ambos producen una especie de sinergia antagónica en la que cada parte se aprovecha de las vulnerabilidades que la parte contraria ha generado con sus acciones. Este efecto recíproco genera un entorno cambiante y dinámico de ciberamenazas que es tan complejo como imprevisible.

5 **El Confidencial (2023).** De los cohetes a los ciberataques: el otro conflicto entre Israel y Palestina ya ha estallado.

6 **Escudo Digital (2023).** La aerolínea Scandinavian Airlines es víctima de un ciberataque que deja expuestos datos de clientes.

7 **The Cyber Express (2023).** Cyber Attack on French National Police: VulzSec Hacking Group Claims to Leak Sensitive Data.

8 **Motorola Solutions (2023).** New Report Outlines Q3 2023 Cyber Threats to Public Safety.

9 **Servimedia (2023).** Los ciberdelincuentes usan la guerra entre Israel y Hamás para estafar a través de ONG ficticias.

10 **Público (2023).** Israel, diana de sofisticados ciberataques.

CHECKLIST

Mejores prácticas de seguridad

Crea redes redundantes: utilizar varias rutas de datos te ayudará a mantener la disponibilidad incluso en caso de un ataque DDoS. Esto se consigue con servidores adicionales, centros de datos alternativos o servicios en la nube. Si una ruta se ve comprometida o sobrecargada, el tráfico de datos se podrá desviar a otra ruta y así prevenir interrupciones del servicio.

Realiza periódicamente pruebas de estrés: somete a tu infraestructura a pruebas de estrés para comprobar cómo se comportará si aumenta mucho el tráfico. Los ejercicios de «Red Team» que simulan escenarios de ataques reales pueden ser muy útiles para este tipo de pruebas.

Implementa funciones de limitación de velocidad, limpieza de datos y sobreaprovisionamiento de la capacidad de red: estas estrategias permiten controlar la cantidad de tráfico que acepta un servidor durante un periodo determinado, filtrar tráfico malicioso y mantener mayor capacidad de ancho de banda para hacer frente a picos repentinos de tráfico.

Realiza copias de seguridad periódicas y utiliza almacenamiento externo: guarda periódicamente copias de seguridad de los datos críticos y almacénalos en una ubicación externa o en la nube. De este modo, en caso de producirse un ataque en las instalaciones principales, no se perderán todos los datos. Es aconsejable realizar copias de seguridad inmutables y seguir la regla de backup 3-2-1, que consiste en hacer tres copias completas de los datos. Dos copias se guardan localmente en diferentes dispositivos para facilitar el acceso y la recuperación, y una tercera copia se almacena en una ubicación externa para una mayor seguridad.

Usa la segmentación de red: divide tu red en segmentos para impedir la propagación de malware. Así, si un segmento se ve comprometido, no afectará a toda la red. También es recomendable utilizar la microsegmentación para mejorar la granularidad y la protección de los datos sensibles dentro de los segmentos.

CHECKLIST

Mejores prácticas de seguridad

Restringe los derechos de usuario: implementa una política de derechos de acceso mínimos, concediendo a los usuarios sólo los permisos necesarios para sus funciones. Este enfoque es un elemento clave para conseguir una arquitectura de red Zero Trust que pueda reducir de forma eficaz el riesgo de ciberamenazas internas. Recuerda que también debes revisar y actualizar los permisos con regularidad.

Utiliza un firewall de aplicaciones web (WAF): un WAF sirve para monitorizar el tráfico de las aplicaciones web y de este modo prevenir cambios no autorizados en una página web. El WAF se puede integrar con otras herramientas de seguridad y permite crear un sistema unificado de gestión de amenazas. Dado el caso, puedes decidirte por un WAF avanzado que incorpore machine learning y se adapte automáticamente a las nuevas ciberamenazas.

Implementa métodos de autenticación seguros: aplica una política de contraseñas sólida y añade una capa de protección adicional mediante la autenticación multifactor (MFA), sobre todo en el acceso a sistemas sensibles y al backend de la página web. Siempre que sea posible, utiliza tecnologías de autenticación sin contraseña o con verificación biométrica para mejorar aún más la seguridad.

Usa sistemas de monitorización y alerta: las herramientas de monitorización te permiten controlar el tráfico de la red, el rendimiento del sistema y los registros de acceso. Los sistemas SIEM (gestión de eventos e información de seguridad) y SOAR (orquestación, automatización y respuesta de seguridad) incluyen funciones avanzadas de supervisión, análisis y respuesta automatizadas. Configurando alertas de actividades o cambios inusuales, el equipo de seguridad podrá reaccionar rápidamente ante posibles incidentes de seguridad.

5 Desinformación como servicio: una poderosa herramienta en el arsenal de los ciberdelincuentes

En los años posteriores al escándalo de Cambridge Analytica, las campañas de desinformación han tenido un papel decisivo en la polarización social. La **difusión deliberada de información falsa** es una táctica que cada vez se utiliza más para manipular la opinión pública, dañar reputaciones e influir en el panorama político y empresarial.[1] 2023 marcó un punto de inflexión en estas campañas. Con **el auge de la IA generativa**, producir contenido manipulativo a gran escala es más fácil y barato que nunca, de forma que es **casi imposible distinguir qué es verdad y qué es mentira**.

Un contexto en el que se demuestra claramente el impacto de las campañas de desinformación son las elecciones presidenciales de EE. UU. Durante las elecciones de 2016, la desinformación se propagó de forma masiva por las redes sociales, alimentada por activistas de extrema derecha, intromisiones del exterior y páginas de fake news. También durante las elecciones de 2020 proliferaron las teorías conspirativas y las afirmaciones infundadas de fraude electoral, que llegaron a millones de personas e impulsaron un movimiento antidemocrático.[2] De cara a las elecciones de 2024 aumenta la preocupación por el posible uso los últimos avances en IA para crear **métodos más sofisticados de desinformación**, como deepfakes y campañas de propaganda selectiva.

El **peligro que representan los deepfakes para la democracia** también se vio en las elecciones eslovacas, donde se utilizó un deepfake de audio elaborado con IA para difundir información falsa en las redes sociales.[3] En el audio, que llegó a miles de usuarios, Monika Tódová, una conocida periodista, y Michal Šimečka, líder del partido progresista de Eslovaquia, conversaban sobre posibles formas de amañar las elecciones. A pesar de que los implicados negaron de inmediato haber mantenido esa conversación y de que varias organizaciones verificadoras confirmaron que se trataba de un engaño, la repercusión fue enorme, sobre todo por el momento en que salió a la luz. Al publicarse durante el periodo de silencio de 48 horas antes de las elecciones, los medios de comunicación y los políticos lo tuvieron muy difícil para desmentirlo públicamente.

En este contexto, **la desinformación como servicio (DaaS)** añade un nuevo escalafón en el alcance y la sofisticación de las tácticas de propagación de información falsa. Con este **nuevo modelo de guerra**

1 **Euronews (2022).** La desinformación profundiza la polarización interna en los países según Reporteros Sin Fronteras.

2 **El Mundo (2023).** Donald Trump, acusado de cuatro cargos por intentar alterar las elecciones de 2020.

3 **Wired (2023).** Deepfakes en elecciones de Eslovaquia reafirman que IA es un peligro para la democracia.

de información, cualquiera, tanto si es un particular como una organización, puede comprar y difundir noticias falsas y lanzar campañas de desinformación con una facilidad sin precedentes. Gracias al rápido avance de la IA generativa y a una red de trolls profesionales, bots y sofisticadas herramientas de manipulación online, DaaS se ha convertido en una herramienta al alcance de todos para lanzar campañas de desinformación (igual que el RaaS lo es para los ataques de ransomware).[4] Por supuesto los ciberdelincuentes y hacktivistas no dudarán en beneficiarse de ella.

Esto significa que en **2024 aumentarán las campañas de desinformación, tanto con fines políticos como económicos**, y apuntarán a muy diversos sectores, como la sanidad, las finanzas, la tecnología, la educación y los medios de comunicación. Por un lado, hacktivistas y ciberdelincuentes con financiación estatal seguirán intentando desestabilizar a los gobiernos y a las organizaciones políticas con información falsa para influenciar la opinión pública y ganar adeptos a sus causas. Esto ocurrió, por ejemplo, en 2023 con la difusión de un deepfake que mostraba a hinchas del Atlético de Madrid desplegando una bandera palestina, una imagen falsa que tuvo una gran repercusión en Internet.[5] Este tipo de ataques pueden tener consecuencias económicas mayores, que pueden llegar incluso a **afectar al mercado bursátil**, como sucedió en mayo de 2023 a raíz de una imagen falsa de una explosión cerca del Pentágono. La fotografía fue compartida en las redes sociales y difundida por varios medios de comunicación, entre ellos la agencia de noticias estatal rusa RT, lo cual sembró el miedo y provocó una caída del mercado de valores.[6]

Por otro lado, los ciberdelincuentes que actúan con fines lucrativos tratarán de desestabilizar a organizaciones y empresas de diversas maneras. Contratando DaaS a un precio muy asequible, **emplearán la desinformación en sofisticados ataques de phishing e ingeniería social** para difundir noticias inquietantes y explotar el miedo y la sensación de urgencia de las personas. Pero esto no es todo. Las campañas de desinformación de amplia difusión también pueden **dañar la reputación de las empresas**. En el caso de Wayfair, por ejemplo, conspiradores vinculados al grupo QAnon aprovecharon la confusión de la pandemia para empañar la reputación de esta empresa de comercio online.[7] Utilizando plataformas como Twitter, Instagram y Reddit, difundieron falsas afirmaciones acusando a Wayfair de estar implicada en una red de tráfico infantil. A pesar de los esfuerzos de la empresa por desmentir estas acusaciones, el bulo siguió circulando por Internet, lo que demuestra lo dañina que puede ser la información falsa para la reputación de las empresas.

Los CEO están también en el punto de mira de los ataques con deepfakes, ya que tener una buena imagen pública es una parte importante de su trabajo. Al intervenir con frecuencia en videoconferencias para anunciar resultados empresariales, en juntas de accionistas o en entrevistas televisivas, a los ciberdelincuentes les es fácil recopilar material de audio y vídeo de ellos. Y, como hemos visto en el apartado sobre la IA, este material se puede utilizar para muchos fines.

A medida que proliferan las campañas de desinformación y ponen en jaque al panorama informativo mundial, las empresas son cada vez más conscientes de los riesgos a los que se enfrentan, tales como pérdidas económicas sustanciales y daños a su reputación a largo plazo. Por lo tanto, mientras los ciberdelincuentes sigan perfeccionando y expandiendo cada vez más estas tácticas, las organizaciones tendrán que desarrollar medidas sólidas para proteger su integridad y mantener la confianza de la opinión pública.

4 **Hackernoon (2022).** Desinformación como servicio; El gemelo malvado del marketing de contenidos.

5 **Newtral (2023).** Esta foto de aficionados del Atlético de Madrid desplegando una bandera de Palestina está hecha con inteligencia artificial.

6 **La Razón (2023).** Una imagen de una explosión en el Pentágono creada con inteligencia artificial sacude la Bolsa en EEUU.

7 **BBC (2020).** Wayfair: la falsa teoría conspirativa sobre una empresa de muebles y el tráfico infantil que se volvió viral.

CHECKLIST

Mejores prácticas de seguridad

Evalúa las posibles amenazas: es importante que evalúes periódicamente la susceptibilidad de tu organización a las campañas de desinformación. Un buen método de modelado de amenazas te ayudará a valorar tanto la probabilidad de que tu empresa sea atacada, como las potenciales consecuencias de estas amenazas. También las herramientas de análisis de sentimiento y monitorización de tendencias pueden ser muy útiles para rastrear actitudes y reacciones de la opinión pública, lo que te permitirá anticiparte y elaborar estrategias eficaces para prevenir posibles amenazas de desinformación.

Forma y entrena a tus empleados: dota a tus empleados de los conocimientos necesarios sobre cómo funcionan las campañas de desinformación y sobre su posible impacto en tu organización. Enséñales a contrastar la información, a identificar fuentes en las que puedan confiar y a cuestionar con sentido crítico la veracidad de la información que encuentren online. Implantando una cultura de escepticismo y verificación de la información protegerás a tu empresa de las consecuencias de la información engañosa.

Mejora la comunicación interna: refuerza los canales de comunicación interna para agilizar la respuesta y frenar la propagación de información falsa. Con herramientas de comunicación como Sofie Rapid Awareness, la integración de SoSafe con MS Teams, puedes informar inmediatamente a tus empleados en caso de detectar una campaña de desinformación falsa sobre tu empresa.

Crea un equipo de comunicación de crisis: forma un equipo de respuesta rápida especializado en comunicación de crisis y preparado para contrarrestar rápidamente la desinformación con información objetiva.

CHECKLIST

Mejores prácticas de seguridad

Promueve la vigilancia y la denuncia: fomenta en tus empleados una actitud de alerta y anímalos a notificar cualquier actividad inusual en Internet, como noticias engañosas, deepfakes o contenidos de vídeo o audio manipulados. También es importante que puedan hacerlo sin miedo a ser juzgados, por lo que es recomendable implantar un sistema de denuncia que les permita notificar estos incidentes con facilidad, de forma anónima y sin temor a represalias.

Automatiza la monitorización de las redes sociales: vigila las redes sociales para detectar rastros de ataques DaaS, fake news, imágenes manipuladas y clips de audio falsos. Para esto es imprescindible colaborar estrechamente con los equipos de relaciones públicas y marketing. Existen ya herramientas de monitorización de las redes sociales basadas en inteligencia artificial que detectan y señalan los casos de posible desinformación en tiempo real, lo que permite adoptar medidas inmediatas.

Colabora en inteligencia sobre amenazas: colabora con redes externas de ciberseguridad y asóciate a organizaciones de tu sector, entidades gubernamentales y alianzas mundiales de ciberseguridad para compartir conocimientos sobre tendencias y mejores prácticas en materia de desinformación.

6 2024: un año de desafíos para la seguridad del sector público y las infraestructuras críticas

Aunque el hacktivismo es una de las ciberamenazas a las que se enfrenta el sector público, no es la única. También debe hacer frente a ataques de **ciberdelincuentes apoyados por diferentes Estados y a hackers independientes**, cuyo objetivo es la destrucción de datos, la interrupción de las operaciones, el beneficio económico o el espionaje. Según el informe de IBM sobre el coste de una filtración de datos en 2023, **el coste medio de un ciberataque en el sector público se ha elevado a la escalofriante cifra de 2,60 millones de dólares**.[1]

El hecho de que se haya digitalizado la información sensible que manejan las administraciones públicas, así como los servicios esenciales que prestan, hacen del sector público **un atractivo objetivo para los ciberdelincuentes a la hora de conseguir robar datos confidenciales y provocar interrupciones**. Solo en 2022, el número de **ciberataques** de Estados nación **dirigidos específicamente a infraestructuras críticas aumentó del 20 % al 40 %** en todo el mundo.[2] Este aumento se debe en gran medida a los ataques respaldados por poderes estatales vinculados al conflicto entre Rusia y Ucrania. Puesto que el conflicto de Ucrania y la guerra entre Gaza e Israel siguen todavía activos, cabe esperar que esta tendencia continúe en 2024 y agrave todavía más la situación.

La inmensa cantidad de datos de alto valor que poseen las instituciones públicas es una mina de oro para los ciberdelincuentes. Los últimos incidentes en el sector educativo lo ilustran claramente. El año pasado, **el coste medio de una fuga de datos en el sector de la educación** ascendía a **3,65 millones de dólares**.[3] En un ataque de 2023, el grupo de hackers Vice Society filtró información sensible de la Pates Grammar School de Inglaterra, entre la que se incluían pasaportes escaneados de los alumnos, tablas salariales de la planilla e información sobre contratos.[4] Poco después se registraron más ataques por toda Europa: en universidades de Francia[5] y Alemania[6], los hackers bloquearon varias redes internas e infraestructuras informáticas. Además, en Grecia, un ataque DDoS a la plataforma online de exámenes de secundaria impidió que los institutos pudieran realizar los exámenes con normalidad.[7]

> **La cibernética es un instrumento de poder geopolítico y un nuevo vector de ataque que los Estados utilizan para perseguir sus propios intereses.**

Dra. Katrin Suder
Strategy Expert (digital technologies, business & politics)

1 **IBM (2023).** Coste de la vulneración de datos 2023.
2 **Microsoft (2022).** Informe de protección digital de Microsoft de 2022.
3 **IBM (2023).** Coste de la vulneración de datos 2023.
4 **BBC (2023).** Schools hit by cyber attack and documents leaked.

Las **administraciones públicas de todo el mundo también están sometidas a una enorme presión por este aumento de los ciberataques**. En julio de 2023, un ciberataque dejó fuera de servicio al portal eCitizen de Kenia, una plataforma digital esencial de servicios para la ciudadanía.[8] Esta interrupción bloqueó el acceso online a más de 5000 servicios gubernamentales, dejando a los usuarios sin poder acceder a sus solicitudes de pasaportes, visados de visitantes, permisos de conducir, documentos de identidad e historiales médicos. El ataque también afectó a los servicios de banca móvil y de transporte, lo que demuestra hasta qué punto están interconectados los sistemas modernos y lo vulnerables que esto los hace.

Este incidente pone de manifiesto una realidad innegable: en el complejo panorama geopolítico actual, **todos los niveles de la administración** —municipal, regional, autonómico o nacional— **son vulnerables a las ciberamenazas**. En la mayoría de los casos, estos ataques tienen **consecuencias de gran alcance, ya que no sólo comprometen datos sensibles, sino también la seguridad pública**. Las potenciales consecuencias no son únicamente las interrupciones del servicio, ya que, al afectar también a las infraestructuras críticas, se corre el peligro de provocar crisis financieras e incluso poner vidas en peligro. Además, para paliar las secuelas de estos ataques se necesita mucho tiempo y dinero, lo que pone aún más presión sobre los recursos públicos y fomenta la desconfianza. Esta mayor vulnerabilidad es especialmente evidente en el sector sanitario, donde la integridad y la disponibilidad de los datos son esenciales. El informe

5 **The Record (2023).** Aix-Marseille, France's largest university, hit by cyberattack.

6 **The Record (2023)** Cyberattack on German university takes 'entire IT infrastructure' offline.

7 **AP News (2023).** Extenso ciberataque en Grecia afecta exámenes de secundaria.

8 **BBC (2023).** Kenya cyber-attack: Why is eCitizen down?

Threat Landscape: Health Sector de ENISA revela que **casi la mitad de los ataques de ransomware a instituciones de la sanidad pública acaban con filtraciones o fugas de datos**.[9] Un ejemplo notable ocurrió el pasado mes de marzo en el Hospital Clínic de Barcelona, donde un ataque de ransomware obligó a cancelar 150 operaciones no urgentes y unas 3000 consultas de pacientes en tres centros y en varias clínicas externas.[10]

Los **ataques a las instituciones sanitarias han aumentado en toda Europa durante el último año**. En diciembre de 2023, la red hospitalaria alemana Katholische Hospitalvereinigung Ostwestfalen (KHO) fue víctima de un ransomware que causó interrupciones en tres hospitales.[11] A principios de año, un hospital de Bruselas sufrió un ciberataque que obligó a desviar ambulancias a otros hospitales.[12] En este caso, gracias al plan de emergencia con el que ya contaba, el hospital pudo restablecer los sistemas informáticos solo un día después. Esto demuestra la **importancia de las medidas de prevención y respuesta rápida ante estas situaciones**.

Desafortunadamente, **no siempre se pueden recuperar tan rápido** las instituciones públicas después de un ciberataque. **Los recortes en los presupuestos, la tecnología anticuada y la falta de personal de los equipos lo ponen cada vez más difícil**. La mayoría de estas organizaciones públicas no dispone de los recursos necesarios para aplicar medidas preventivas eficaces. Por ejemplo, según el informe de ENISA, solo el 27 % de las instituciones sanitarias cuenta con un plan de defensa específico contra el ransomware, y el 40 % no dispone de un programa de concienciación sobre seguridad para el personal no informático.[13] Para hacer frente a esto es **esencial implantar medidas preventivas**, como auditorías de seguridad y un modelo Zero Trust, **y establecer una cultura de seguridad mediante una formación de concienciación personalizada** que responda a las necesidades de cada organización. Todas estas medidas son esenciales no sólo para proteger a la propia institución, sino para la seguridad de todos, puesto que se trata de organizaciones de las que depende toda la sociedad.

9 **ENISA (2023).** ENISA Threat Landscape: Health Sector.

10 **La Vanguardia (2023).** El hospital Clínic sufrió un ciberataque exterior "sofisticado" y no puede usar el sistema informático.

11 **Security Affairs (2023).** Lockbit ransomware attack interrupted medical emergencies gang at a German hospital network.

12 **Redacción Médica (2023).** Ciberataque a un hospital de Bruselas una semana después del Clínic.

13 **ENISA (2023).** ENISA Threat Landscape: Health Sector.

CHECKLIST

Mejores prácticas de seguridad

- **Analiza y cuantifica los riesgos:** incorpora el análisis y la gestión de riesgos como parte esencial de las operaciones empresariales. Es importante hacerlo como práctica habitual, pero sobre todo a la hora de implantar nuevas tecnologías o planificar procesos empresariales. Las evaluaciones de riesgos cibernéticos son esenciales para establecer cálculos de riesgo, para garantizar el cumplimiento de las normativas y para mantener la integridad de los datos.

- **Nombra responsables en materia de digitalización:** las instituciones del sector público deberían asignar responsabilidades nombrando cargos que gestionen la transformación digital, como un director de ciberseguridad (CISO). Esta función es fundamental para dirigir las estrategias de seguridad digital.

- **Implementa una arquitectura Zero Trust (ZTA):** el enfoque de este modelo consiste en someter cualquier solicitud de acceso a un proceso de verificación estricto, independientemente de su procedencia. Teniendo en cuenta el creciente número de ciberataques complejos que sufre el sector público, la implantación de una arquitectura Zero Trust adquiere una importancia especial.

- **Aprende de los incidentes y planea con antelación:** aprovecha la experiencia adquirida en incidentes pasados para mejorar el proceso integral de gestión de la seguridad. Elabora un plan de respuesta a incidentes y actualízalo periódicamente. Este plan debe describir los pasos a seguir en caso de un ciberataque para garantizar una respuesta rápida y eficaz que reduzca las consecuencias al mínimo.

- **Realiza auditorías de seguridad periódicas:** lleva a cabo auditorías de seguridad frecuentes y exhaustivas para identificar y abordar las vulnerabilidades del sistema. Este enfoque proactivo te ayudará a descubrir posibles vulnerabilidades antes de que los ciberdelincuentes puedan aprovecharse de ellas.

- **Implanta programas de formación personalizados:** ofrece una formación en ciberseguridad continua y adaptada a las necesidades específicas de tu organización, así como a las funciones de los empleados. Por ejemplo, puedes ofrecer módulos de formación específicos para el sector sanitario que aborden las técnicas de ingeniería social más frecuentes en este sector. Los simulacros de phishing también deben estar adaptados a las peculiaridades de tipo de organización.

ENTREVISTA

John Noble

Non-executive director and chair of the Cyber Security Committee de NHS Digital en Inglaterra

John Noble fue director of Incident Management del Centro Nacional de Ciberseguridad (NCSC) del Reino Unido entre 2016 y 2018. Como tal, dirigió las respuestas a casi 800 incidentes cibernéticos críticos y contribuyó con ello al objetivo de convertir el Reino Unido en el lugar más seguro para el comercio digital. Actualmente es non-executive director de NHS Digital (la división tecnológica del NHS, el Servicio Nacional de Salud del Reino Unido), donde preside el Information Assurance and Cyber Security Committee (comité de garantía de la información y ciberseguridad).

> «El intercambio de información entre gobiernos y la colaboración entre el sector privado y las administraciones públicas nos ayudarán a entender mejor las amenazas digitales.

¿Qué es el Centro Nacional de Ciberseguridad (NCSC), y cuál es su principal objetivo?

El NCSC se creó por iniciativa del entonces primer ministro Gordon Brown y obedece a motivos políticos. El gobierno, consciente de la transición hacia una sociedad digital construida sobre una plataforma insegura como es Internet, vio la necesidad de crear una agencia que ofreciera asesoramiento y apoyo.

¿Por qué se decidió que el NCSC formara parte de la agencia de inteligencia británica GCHQ?

Incorporar el NCSC al Centro Gubernamental de Comunicaciones (el GCHQ) fue una decisión estratégica. Dada su competencia en defensa de redes y como agencia de ciberseguridad establecida, el GCHQ era la organización ideal para acoger al NCSC.

¿Qué papel desempeña el NCSC?

Cuando empezamos nos pusimos a indagar qué podía hacer el gobierno para ayudar y cómo podría contribuir el NCSC a hacer del Reino Unido el lugar más seguro para el comercio digital. Y llegamos a la conclusión de que para ello teníamos que compartir nuestra experiencia con otros gobiernos y crear una alianza entre la administración pública y el sector privado.

¿Por qué es importante que los sectores público y privado colaboren en materia de ciberseguridad?

Tanto las autoridades gubernamentales como el sector privado tienen sus propios puntos fuertes en ciberseguridad, y el NCSC analiza qué medios puede aportar el gobierno para favorecer la colaboración entre ambos. Como resultado se crearon dos iniciativas: la Cyber Information Sharing Partnership (CISP), que permite a las empresas intercambiar información sobre ciberamenazas de forma anónima y en tiempo real, y Cyber 100, una iniciativa que reúne a expertos del sector privado para que compartan sus conocimientos con el NCSC.

Las organizaciones muestran cierto recelo a la hora de compartir sus vulnerabilidades con entidades públicas, porque temen que esta información se utilice en su contra. ¿Cómo podemos transmitir el mensaje de que el gobierno quiere apoyarlas y no perjudicarlas?

Aquí es muy importante la confianza y la sinceridad. Si una agencia de inteligencia detecta una vulnerabilidad en un software y no la revela, los ciberdelincuentes pueden aprovecharse de ella. Una agencia como el NCSC tiene que ganarse la confianza de las empresas para poder recopilar pruebas de estas vulnerabilidades. Esto puede favorecer relaciones muy provechosas e importantes con las empresas.

También creo que ha habido un cambio de enfoque en el gobierno, de manera que ahora prioriza la seguridad de nuestra economía digital y, por tanto, la de las empresas digitales. Tenemos que entender que para proteger nuestra economía digital es necesario compartir la información con los gobiernos.

Ha habido un cambio de enfoque en el gobierno, de manera que ahora prioriza la seguridad de nuestra economía digital y, por tanto, la de las empresas digitales.

¿Qué cambios importantes has observado en el panorama de las ciberamenazas durante las últimas décadas?

El panorama de amenazas, y en particular la ciberdelincuencia, han cambiado mucho en las últimas décadas. Llama la atención el crecimiento explosivo del ransomware, que se ha convertido en un ecosistema muy sofisticado y especializado. Grupos de ciberdelincuentes como Conti funcionan ahora con estructuras y jerarquías similares a las de una empresa, con diferentes departamentos y cargos asignados. Aunque las autoridades logren parar a algunas de estas organizaciones, estas aprenden la lección, cambian y se adaptan.

Se ha extendido una tendencia entre los cibercriminales que consiste en infiltrarse en los sistemas, pero no hacer nada más. ¿Cómo se explica esto?

Cuando detectan vulnerabilidades, los ciberdelincuentes las aprovechan para infiltrarse y dejar un «implante» en muchas empresas distintas que les permita volver y atacarlas más tarde. Esto suele darse en infraestructuras críticas, y por eso es importante parchear rápidamente las vulnerabilidades.

Eliminar vulnerabilidades en el sector público es especialmente difícil, ya que se trata de servicios que están operativos las 24 horas del día. ¿Cómo gestiona el NHS este problema?

El NHS ha aprendido mucho de incidentes como el de WannaCry, el grupo que aprovechó una vulnerabilidad conocida que muchos hospitales no habían solucionado. Este incidente no solo tuvo repercusiones económicas para los hospitales, sino que también afectó a la atención a los pacientes.

Para abordar las vulnerabilidades de los sistemas sanitarios se han implementado dos estrategias clave. La primera consiste en identificar claramente vulnerabilidades críticas que están siendo explotadas activamente y que requieren la aplicación urgente de parches. La segunda es establecer unas normas claras que las organizaciones deban cumplir obligatoriamente.

¿Cómo ha afectado la centralización de los sistemas de salud, como es el caso del NHS británico, a la forma de abordar los retos y vulnerabilidades de la seguridad digital?

La centralización de los sistemas sanitarios tiene efectos tanto positivos como negativos desde el punto de vista de la ciberseguridad. El lado positivo es que en un sistema más centralizado están más claras las normas y pautas a seguir, y esto facilita la comunicación y la implementación de medidas de seguridad en toda la red. Este enfoque centralizado también ha contribuido a mejorar la atención a los pacientes y la reacción ante vulnerabilidades. Sin embargo, también tiene sus inconvenientes. En un sistema centralizado, si una parte del sistema queda comprometida, también puede afectar al resto, es decir, un fallo en un subsistema puede tener consecuencias mayores en el sistema completo.

¿Qué papel tiene la geopolítica en la evolución de las ciberamenazas, y cómo afecta a la interacción entre Estados nación y entidades privadas?

Cuando analizamos una amenaza digital, tenemos que fijarnos en dos cosas: la intención de quien la realiza y su capacidad de llevarla a cabo. Acontecimientos como la invasión de Ucrania han llevado a los países implicados a recurrir a este tipo de ataques para mejorar su situación en la guerra. En cuanto a la capacidad de llevar a cabo estos ataques, estamos viendo cómo los países desarrollan capacidades que se acaban usando en nuestra contra.

¿Y cómo ves el problema del hacktivismo?

El conflicto ruso ha provocado un aumento del hacktivismo en ambos bandos. Hemos visto cómo un ejército digital ucraniano lanzaba ataques contra empresas, grupos mediáticos y otras entidades rusas. Pero también hemos visto cómo grupos prorussos como KillNet, lanzaban ataques DDoS y declaraban abiertamente su intención de atacar a los países que apoyasen a Ucrania.

« El conflicto ruso ha provocado un aumento del hacktivismo en ambos bandos.

¿Existe una zona de intersección donde confluyan la ciberdelincuencia con fines económicos y la ciberdelincuencia por causas políticas?

Normalmente, un Estado decide no emplear métodos cibernéticos por las consecuencias que podría acarrear, como el escándalo que suscitaría. Sin embargo, en un contexto como el de la guerra de Ucrania, a los Estados no les importa lo que puedan pensar los demás ni las posibles consecuencias de sus acciones.

Hasta ahora, estábamos en una situación en la que podíamos actuar en muchos casos de forma muy eficaz contra los grupos de hackers, pero ahora estos grupos colaboran con el Estado. Existe incluso un debate entre políticos rusos de alto rango sobre la posibilidad de legitimar los ciberataques. La idea de que un país pueda legalizar los delitos contra otros es aterradora. Espero que no lleguemos tan lejos.

¿Qué otras estrategias utilizan los países en esta colaboración?

Para los países es importante negar su autoría y así evitar que sus acciones salgan a la luz. Vemos cómo estos Estados nación utilizan muchas de las herramientas que emplean los ciberdelincuentes para poder negar su responsabilidad en los ataques. Por ejemplo, si se descubre un implante de origen comercial en una parte de una infraestructura nacional crítica, es muy difícil saber si detrás de ello está un gobierno o un grupo de cibercriminales. De esta manera, es más fácil para los gobiernos negar que han sido ellos. La disponibilidad de estas herramientas hace que los países utilicen las tácticas de los ciberdelincuentes.

¿Has mencionado otras naciones cuando hemos hablado de Rusia. ¿Qué otros países intervienen en el panorama de amenazas digitales actual?

Si hablamos de los problemas estratégicos más importantes, tenemos que mencionar la creciente influencia de China, las tensiones en el mar de China Meridional y su actitud hacia Taiwán y sus otros vecinos, como Filipinas. China ha mejorado significativamente sus capacidades cibernéticas, lo que se refleja en una mayor sofisticación y la utilización de nuevos ataques de día cero. El país ha reformado sus estructuras de inteligencia para evitar conflictos y ha alcanzado un nivel mucho más profesional. Además, ha ampliado sus áreas de interés. Siempre adopta una visión a largo plazo y va ampliando sus capacidades con el tiempo.

Europa y el Reino Unido, por su parte, coinciden en su visión de la ciberseguridad. Hemos reconocido que tenemos que adoptar una postura más estratégica en lugar de reaccionar a incidentes después de que ocurran.

¿Qué medidas podemos adoptar para mitigar las ciberamenazas, y sobre todo las amenazas persistentes avanzadas (APT)?

El intercambio de información entre gobiernos de todo el mundo y la colaboración entre el sector privado y las administraciones públicas nos ayudarán a entender mejor las amenazas digitales. Compartiendo indicadores de compromiso (IOC) y construyendo una relación de confianza entre ambos sectores podemos superar las reticencias de las empresas y formar un frente unido para detectar y responder de forma eficaz a las ciberamenazas.

¿Te ha gustado la entrevista?

Puedes escuchar **la versión completa** (en inglés) en nuestro podcast Human Firewall. Escucha la conversación entre el Dr. Niklas Hellemann, CEO de SoSafe, y John Noble, en la que aportan más información sobre la importancia de la cooperación internacional en el ámbito de la ciberseguridad.

7 El pretexting y los ataques multicanal van a hacer que los ciberataques sean cada vez más realistas y peligrosos

Cada vez más, los ciberdelincuentes utilizan métodos más avanzados de ingeniería social para conseguir que sus víctimas realicen pagos o revelen datos confidenciales. Esto es lo que ocurre en los casos de **pretexting**: los hackers se hacen pasar por alguien en quien la víctima confía e inventan una historia como cebo para que caiga en la trampa. Según un informe de Verizon de 2023, los **ataques de pretexting representan más del 50 % de todos los incidentes de ingeniería social**, lo que demuestra que los ciberdelincuentes siguen aprovechando las emociones humanas para estafar y manipular.[1]

En los ataques de pretexting más complejos, **los ciberdelincuentes investigan a la víctima por diferentes canales**, como redes sociales, blogs o páginas web, para recabar información detallada sobre ellos que luego utilizan para hacer que la historia que inventen sea más creíble.[2] Así, utilizan referencias al lugar de trabajo, su vida social, mascotas, parejas u otros detalles personales que les permiten crear historias muy convincentes y perfectamente adaptadas a la víctima para ganarse su confianza.

Al mismo tiempo, los canales donde los ciberdelincuentes encuentran estos datos sirven como vectores de ataque. Conforme a nuestro Análisis del riesgo humano de 2023, el phishing por correo electrónico sigue encabezando la lista de las amenazas y afecta al 61 % de las organizaciones.[3] No obstante, el panorama de ciberamenazas sigue en expansión, y el 34 % de los ataques se realizan ahora a través de las redes sociales. Por ejemplo, hay muchas pequeñas empresas que utilizan las redes sociales como principal medio para captar clientes, por lo que están proliferando los casos de chantaje y secuestro de cuentas. Esto es lo que le ocurrió a una pequeña empresa que vendía muesli a través de Instagram.[4] Los hackers contactaron con la propietaria a través de su cuenta de Instagram haciéndose pasar por otra empresa de su confianza. Con el pretexto de participar en una votación para un concurso, le pidieron que hiciera clic en un enlace. Acto seguido, los atacantes secuestraron su cuenta de Instagram y le exigieron un rescate de 10 000 dólares, que ella no tuvo más remedio que pagar para recuperar el control de su negocio. Este es sólo un ejemplo de lo que puede ocurrir. Los ciberdelincuentes también emplean otras tácticas en las redes sociales para atacar a las

1 **Verizon (2023).** Data Breach Investigations Report.

2 **INCIBE (2024).** El ciclo de la Ingeniería Social. ¿Cómo preparan los ciberdelincuentes un ataque de Ingeniería Social?

3 **SoSafe (2023).** Análisis del riesgo humano.

4 **CNBC (2023).** Phishing scams targeting small business on social media including Meta are a 'gold mine' for criminals.

empresas, como apropiarse de las cuentas de sus empleados para sonsacar a otros compañeros información confidencial o para hacer que descarguen archivos adjuntos infectados camuflados como si fueran documentos verdaderos de la empresa.

Las apps de mensajería como WhatsApp y Microsoft Teams también figuran entre los canales favoritos de los hackers para sus ataques, tanto en el ámbito privado como en el profesional. Recientemente, en India, la policía de Calcuta alertó de una serie de ataques por WhatsApp en los que los hackers utilizaban como pretexto el Día Mundial del Yoga para enviar mensajes en los que se ofrecían clases de yoga.[5] Los destinatarios debían hacer clic en un enlace y a continuación compartir una contraseña de un único uso de seis dígitos, que finalmente permitía a los atacantes acceder libremente a la cuenta de WhatsApp de la víctima sin que esta se diera cuenta. Una vez que tenían la cuenta bajo su control, enviaban a todos los contactos de la víctima mensajes en su nombre pidiendo que le enviaran dinero porque se encontraba en una situación de emergencia. En otro ataque a través de la aplicación profesional Microsoft Teams, los atacantes enviaron mensajes a sus víctimas haciéndose pasar por un empleado del departamento de Recursos Humanos y avisando de que su calendario de vacaciones había cambiado.[6] La víctima tenía que descargar un archivo que supuestamente contenía el nuevo plan de vacaciones pero, al hacerlo, en realidad instalaba un malware llamado DarkGate.

Los ciberdelincuentes no dejan de inventar nuevos métodos y siguen perfeccionando sus tácticas para que sus ataques sean todavía más convincentes. Así, ahora también organizan **ataques muy complejos en los que contactan con su víctima a través de múltiples canales**, como SMS, correo electrónico o llamadas telefónicas. En un caso concreto, los atacantes combinaron SMS y phishing por voz para estafar a una mujer: primero enviaron un mensaje solicitando que confirmara haber autorizado una transferencia de 7500 dólares.[7] Al instante, y sabiendo la preocupación que habría provocado en ella el mensaje, el hacker la llamó haciéndose pasar por un agente de investigación de fraudes, y le pidió que cambiara sus credenciales para evitar una supuesta estafa. El atacante consiguió finalmente robar un total de 15 000 dólares procedentes de dos cuentas bancarias de la víctima.

Estos ataques multicanal son todavía más convincentes y eficaces cuando se combinan con la IA. Un ejemplo de esto es lo que le ocurrió a un empleado de la empresa Retool.[8] En primer lugar, los atacantes enviaron un mensaje de texto a la víctima haciéndose pasar por el equipo informático de la empresa para resolver un problema con su nómina. El empleado tenía que acceder con sus credenciales a una landing page, que resultó estar falsificada. Como el empleado tenía activada la autenticación multifactor, los ciberdelincuentes realizaron una llamada con la voz clonada de un miembro del equipo informático y le pidieron la contraseña de un solo uso. Una vez sorteada esta barrera, los atacantes accedieron a las cuentas de 27 clientes y robaron criptomonedas por valor de miles de dólares.

Puesto que los ciberdelincuentes trabajan con medios cada vez más sofisticados y profesionales, **es fundamental extremar la precaución e interiorizar un comportamiento seguro**.

5 **The Times of India (2023).** Police warns netizens about WhatsApp hacking, here's how fraudsters hack accounts.

6 **Digital Trends ES (2023).** ¿Malware en mensajes inocentes en Microsoft Teams?

7 **The Guardian (2023).** Gone in seconds: rising text message scams are draining US bank accounts.

8 **Ciberseguridad Hoy (2023).** Retool culpa de la infracción a la función de sincronización en la nube.

CHECKLIST

Mejores prácticas de seguridad

- **Ofrece formación para verificar los remitentes de mensajes y llamadas:** entrena a tus empleados para que aprendan a verificar de forma autónoma la identidad de los remitentes de los mensajes y de las llamadas. Aunque una llamada parezca auténtica, si se trata de una petición fuera de lo normal o sospechosa, lo mejor es ponerse en contacto directamente con la persona a través de un canal seguro.

- **Controla a los colaboradores externos:** supervisa a todos los colaboradores externos que interactúen con tus sistemas. Si necesitan acceder a información sensible, asegúrate de que cumplan las normas de ciberseguridad de tu organización.

- **Fomenta el aviso de phishing rápido y sin represalias:** promueve una cultura en la que los empleados puedan informar rápidamente de cualquier intento de phishing o actividad inusual sin temer repercusiones. La posibilidad de notificar incidencias con rapidez y sin temor a las consecuencias hace que los equipos de seguridad puedan actuar inmediatamente y evitar así mayores daños en caso de ataque.

- **Actualiza las políticas de seguridad digital:** revisa continuamente las políticas de seguridad digital de tu empresa y actualízalas para protegerte de nuevos métodos de ingeniería social, como el pretexting. Poniendo al día tus políticas conseguirás mantener la solidez y la eficacia de tus defensas.

- **Mejora los planes de respuesta a incidentes:** actualiza periódicamente tus estrategias de respuesta a incidentes para reducir el impacto de los ataques de pretexting u otros métodos avanzados. Establece procedimientos claros para detectar, gestionar y mitigar los ataques con el fin de proteger la continuidad y la seguridad de la empresa. Implementa también ejercicios de tipo tabletop para simular ataques que refuercen la capacidad de reacción en caso de ataque.

- **Forma continuamente a tus empleados:** fomenta el aprendizaje continuo sobre las últimas ciberamenazas, incluidos el pretexting y los ataques multicanal, y afianza los conocimientos teóricos mediante simulaciones prácticas de situaciones reales. Preparar a los empleados para que sepan reconocer y reaccionar a actividades sospechosas es esencial para mantener una plantilla alerta y capaz de identificar y prevenir cualquier actividad fraudulenta.

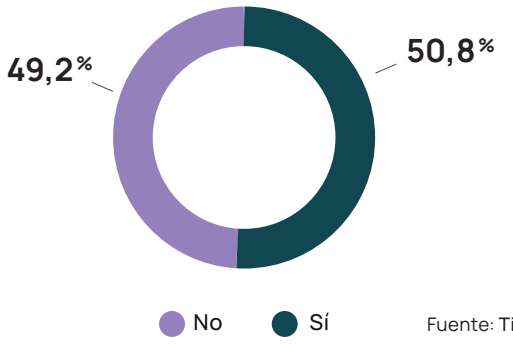
8 El aumento de los casos de burnout va a suponer un reto sin precedentes para los equipos de ciberseguridad

El año pasado ya abordamos el problema del desgaste entre los profesionales de la ciberseguridad. Las tensiones mundiales y la creciente profesionalización de la ciberdelincuencia, reforzada ahora con herramientas de IA, hacen que los ataques sean cada vez más complejos y difíciles de detectar, lo que supone una enorme presión para los equipos de ciberseguridad. La sobrecarga a la que los someten estos incesantes desafíos pone a prueba, más que nunca, su resiliencia y su capacidad para adaptarse a las circunstancias.

Un importante factor que agrava esta presión es la escasez de mano de obra cualificada en el sector. Según el último informe del ISC2, hay 3,9 millones de puestos de trabajo vacantes en el ámbito de la ciberseguridad en todo el mundo, un 12,6 % más que en 2022.[1] Este aumento se concentra sobre todo en Asia-Pacífico (especialmente Japón e India) y América del Norte. También en Europa, la escasez de profesionales de ciberseguridad ha aumentado un 9,7 % con respecto al año pasado. Pero este no es el único problema. Según un estudio de ISACA, el 59 % de las empresas sufren de una falta de personal de ciberseguridad, lo que se traduce en un enorme aumento de la carga de trabajo para los equipos en plantilla y a menudo **lleva a los responsables de seguridad al borde del burnout o incluso a la dimisión**.[2]

Una encuesta realizada a más de mil profesionales de la ciberseguridad de Estados Unidos y Europa lo confirma: el **66 % de los encuestados admite padecer un estrés laboral considerable**, un 51 % está en tratamiento con psicofármacos y el 19 % consume más de tres bebidas alcohólicas al día para afrontar la frustración.[3] Pero las consecuencias van mucho más allá de la carga personal. También provocan **que pasen desapercibidos detalles importantes, reduciendo la capacidad de reacción del equipo frente a las amenazas**, con el consiguiente aumento del riesgo de que se produzca una fuga de datos en la organización. Y este peligro es cada vez mayor, porque los ciberdelincuentes perfeccionan constantemente sus métodos y lanzan ataques cada vez más complejos, como ya hemos visto en los apartados anteriores.

¿Alguna vez te ha recetado un médico medicación para la salud mental?



Fuente: Tines[3]

1 **ISC2 (2023).** How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce.

2 **Europa Press (2023).** Solo el 61% de los equipos de ciberseguridad cuentan con personal suficiente.

3 **Tines (2022).** State of Mental Health in Cybersecurity.

El caso de AccessPress ilustra los enormes problemas a los que se enfrentan los equipos de seguridad.[4] Como proveedor de plugins para WordPress, AccessPress fue objeto de un sofisticado ciberataque en el que los hackers comprometieron 40 temas y 53 plugins utilizados en más de 360 000 páginas web activas. Esto demuestra el gran alcance potencial de los ataques a la cadena de suministro de software. Este incidente, que permitió a los atacantes acceder a una gran cantidad de páginas web, muestra lo eficaces y complejas que son las tácticas a las que nos enfrentamos en el panorama actual de la ciberseguridad, y recalca que no sólo se trata de un problema técnico, sino que está muy relacionado con el elemento humano de la seguridad digital, y sobre todo con la presión que sufren los equipos que velan por ella.

También hay que tener en cuenta que, además de tener que proteger a otros departamentos de la empresa y responder rápidamente a los ataques, el propio equipo de seguridad informática es uno de los departamentos más expuestos a los ciberataques, como vimos en nuestro Análisis del riesgo humano 2023.[5] Uno de los motivos es que los ciberdelincuentes saben que esta situación de estrés les hace más vulnerables, así que explotan su agotamiento como vector de ataque estratégico. Por lo tanto, se dedican a identificar las organizaciones en las que son más evidentes los signos de desbordamiento y desgaste de los equipos, y las atacan.

Teniendo en cuenta todo esto, **es fundamental que las empresas inviertan en sus equipos de ciberseguridad** y en el bienestar de sus empleados. Es importante tener en cuenta estas necesidades a la hora de asignar presupuestos, así como desarrollar planes de desarrollo profesional para fidelizar a los empleados, y de este modo prevenir el burnout, retener el talento y disponer de recursos suficientes para implantar las medidas de seguridad adecuadas. Solo si se adoptan estas medidas, los equipos de seguridad trabajarán de forma eficaz para combatir los ciberataques y mejorar la protección de su empresa.

> **Actualmente, el principal reto del sector de la ciberseguridad es el desgaste de los empleados: hay demasiados datos, demasiados casos y poco tiempo.**

Stéphane Duguin
CEO del CyberPeace Institute

4 **Hackwise (2023).** Ciberdelincuentes implantaron una puerta trasera en docenas de plugins y temas de WordPress.

5 **SoSafe (2023).** Análisis del riesgo humano.

CHECKLIST

Mejores prácticas de seguridad

- **Considera la salud mental y la conciliación de la vida laboral y familiar como prioridades:** desarrolla programas para promover la salud mental y el bienestar de los equipos de seguridad. Los horarios de trabajo flexibles, la oferta de servicios de terapia y descansos regulares pueden contribuir a prevenir el burnout.

- **Implanta herramientas eficaces de detección de ciberamenazas:** utiliza herramientas avanzadas, como sistemas de detección de amenazas basados en IA, y otros instrumentos como el botón de alerta de phishing o PhishFeedback, el asistente de correo electrónico de SoSafe. Estas herramientas ayudan a ahorrar tiempo y a identificar más fácilmente las amenazas.

- **Automatiza el análisis del correo electrónico:** implementa herramientas de automatización para que el Centro de Operaciones de Seguridad (SOC) pueda analizar fácilmente los correos electrónicos notificados. Esto agilizará notablemente el proceso de evaluación de posibles correos peligrosos, y el equipo del SOC podrá concentrarse en cuestiones de seguridad más importantes y que requieren un análisis más detenido.

- **Automatiza las tareas rutinarias:** utiliza la automatización en tareas recurrentes y rutinarias para que los equipos de seguridad puedan centrar su atención en aspectos más relevantes y estratégicos de la ciberseguridad.

- **Fomenta el aprendizaje y la capacitación:** ofrece programas de formación continua y de puesta al día para que tu equipo esté preparado de cara a las últimas ciberamenazas y tecnologías. Fomenta también la colaboración con otros equipos de especialistas y establece un programa de liderazgo en ciberseguridad.

- **Invierte en medidas para retener a los empleados:** pon en marcha planes de desarrollo profesional y programas de promoción para retener el talento y reducir la rotación del personal.

- **Lleva a cabo periódicamente entrevistas de feedback y evaluación:** reúnete personalmente con tus empleados de forma periódica, tanto para darles como para recibir sus comentarios y sugerencias. De este modo entenderás mejor cuáles son sus necesidades y podrás responder a ellas.

En 2024, los ciberataques se centrarán más en el elemento humano

Todas las tendencias de este año llevan a una misma conclusión: **para que nuestras medidas de ciberseguridad sean eficaces debemos centrarnos en las personas**, igual que lo hacen los hackers. Saben que la mejor forma de lograr sus objetivos es jugar con las emociones humanas, por eso, utilizan la ingeniería social como herramienta principal en sus ataques, como hemos mencionado reiteradamente en este informe.

Según el informe Data Breach Investigation Report de Verizon, en 2023 hasta un 74 % de los incidentes estaban relacionados con el elemento humano, e incluso grandes grupos tecnológicos reconocen que el factor humano es una puerta de acceso para explotar la tecnología.[1] Y esto es sólo la punta del iceberg. Según el informe de predicciones para 2024 de Forrester, **este año aumentará todavía más el porcentaje de fugas de datos en las que intervenga el elemento humano**.[2] Con la profesionalización de la ciberdelincuencia y el auge de la IA, los ciberdelincuentes pueden lanzar ahora ataques de ingeniería social realmente convincentes y complejos. Por lo tanto, cada vez es más difícil distinguir los mensajes verdaderos de los malintencionados. Además, puesto que cada vez se utilizan más canales de comunicación diferentes, estas amenazas se propagan más rápido que nunca.

También el Allianz Risk Barometer 2024 prevé que los incidentes de ciberseguridad serán el principal riesgo para las empresas en 2024, y que los responsables de seguridad no podrán pasar por alto el elemento humano en sus estrategias de seguridad.[3] La buena noticia es que existe una poderosa herramienta para evitar este riesgo: **la concienciación y la formación en ciberseguridad**. Sensibilizando a las personas de cara a la seguridad digital y fomentando un comportamiento seguro podemos hacer frente a las ciberamenazas. Debemos tener presente que el objetivo de los ciberataques no son los sistemas, sino las personas. Por lo tanto, también son **las personas las que tienen el poder de detener estos ataques**. Crear una cultura de la seguridad no es solo responsabilidad de la organización, sino de cada una de las personas que la componen. Unidos podemos combatir los desafíos de la nueva ciberdelincuencia y proteger nuestro futuro.

1 **Verizon (2023).** Data Breach Investigations Report.

2 **Forrester (2024).** Predictions 2024: Exploration Generates Progress.

3 **B2B Cyber Security (2023).** Barómetro de Riesgos de Allianz: los ciberataques son el principal riesgo en 2024.

Mejora tu cultura de seguridad sin esfuerzo

Con su plataforma de concienciación, SoSafe permite a las organizaciones reforzar su cultura de seguridad y reducir los riesgos humanos. La plataforma ofrece experiencias de aprendizaje atractivas y simulaciones de ataque personalizadas que ayudan a los empleados a convertirse en defensores activos contra las amenazas en línea, todo ello impulsado por la ciencia del comportamiento para que el aprendizaje sea divertido y eficaz. Las métricas detalladas permiten medir el impacto de los cambios en el comportamiento e indican a las organizaciones dónde se encuentran exactamente sus vulnerabilidades para que puedan responder de forma proactiva a las ciberamenazas. La plataforma SoSafe es fácil de desplegar y ampliar, y fomenta sin esfuerzo hábitos seguros en todos los empleados.

ENSEÑAR — Microaprendizaje interactivo

Una plataforma de aprendizaje basada en la ciencia del comportamiento con la que los empleados disfrutan aprendiendo. Refuerza tus defensas frente a las amenazas digitales y garantiza el cumplimiento de las normativas con experiencias de aprendizaje dinámicas y eficaces a través de diferentes canales para crear fácilmente hábitos seguros a largo plazo.

- Contenidos de aprendizaje gamificados y basados en historias, diseñados para promover la participación y un efecto duradero
- Biblioteca de contenidos guiados de alta calidad y fácilmente ampliable
- Personalización y gestión de contenidos sencilla adaptable a todo tipo de organizaciones

ENTRENAR — Simulaciones de ataque personalizadas

Simulaciones de phishing centradas en el usuario que fomentan hábitos seguros. Entrena a tus empleados para que sean capaces de reconocer los ciberataques con nuestras simulaciones periódicas de spear phishing automatizadas, que afianzan la concienciación de la seguridad en su trabajo diario y reducen de forma eficaz el riesgo y el tiempo de respuesta a las amenazas.

- Simulaciones de ciberataques personalizadas y realistas
- Aprendizaje contextual para reforzar el comportamiento seguro de los empleados
- Fácil notificación de amenazas a través de un solo clic en un botón de aviso de phishing

ACTUAR — Supervisión estratégica de riesgos

Protege tu organización de costosos incidentes utilizando nuestra solución integral de evaluación del riesgo humano. Obtén un análisis completo del nivel de seguridad del elemento humano de tu organización para adelantarte a posibles vulnerabilidades. Supervisa e interpreta el impacto de tus programas de concienciación, analiza los comportamientos y toma decisiones basadas en datos.

- Información contextual detallada, con indicadores clave del rendimiento desde la perspectiva técnica y del comportamiento
- Benchmarking del sector y directrices prácticas
- Creado conforme a los requisitos de la norma ISO/IEC-27001 y con un enfoque de Privacy-by-design

CONECTAR — Sofie Rapid Awareness

Los ciberdelincuentes son más rápidos que nunca, pero tú también puedes serlo. Rapid Awareness te permite contactar rápidamente con tus empleados a través de MS Teams. Implementa el microaprendizaje rápido para combatir las últimas amenazas digitales, refuerza la seguridad de tu equipo con alertas en tiempo real y conviértelo en tu mejor defensa.

- Contacta directamente con tus empleados a través de MS Teams
- Ahorra tiempo y comunícate con fluidez
- Envía alertas de seguridad breves para que los empleados las procesen fácilmente
- Controla y supervisa el número de empleados que leen las alertas

Human Firewall Conference

HuFiCon es un encuentro europeo sobre ciberseguridad diseñado para ayudar a los profesionales de la seguridad a transformar sus equipos en **ciberhéroes**. Ven y participa en charlas de expertos y talleres prácticos, y forma parte de una comunidad decidida a poner el factor humano en el centro de la ciberseguridad.

¿Estás decidido a liderar el futuro de la ciberseguridad?

¿Donde? Polígono Halle Tor 2, Colonia (Alemania)

¿Cuando? 14 y 15 de noviembre de 2024

Participa en HuFiCon24

Contacto

Si tienes alguna pregunta sobre este informe, contacta con:

Laura Hartmann
Head of Corporate Communications
press@sosafe-awareness.com

sosafe

SoSafe GmbH
Lichtstrasse 25a
50825 Colonia, Alemania

info@sosafe.de
www.sosafe-awareness.com/es
+49 221 65083800