sosafe

Análisis del **riesgo humano** 2023

Opiniones y estrategias de expertos para protegerse mejor de los ciberataques en Europa

« Debemos acercar la ciberseguridad a las personas, hacer que la sensibilización esté presente en todos los ámbitos de nuestras vidas y tomar iniciativas en torno a la fusión de la ciberseguridad y los negocios.

Dr. Niklas Hellemann
CEO de SoSafe

Editorial

Suena evidente, pero ahora es más cierto que nunca: el panorama actual de las ciberamenazas está extremadamente tenso y avanza a una velocidad vertiginosa.

Lo que hemos presenciado en los últimos años, y en 2022 en particular, solo puede describirse como una evolución acelerada. La tensión mundial, los conflictos geopolíticos y las constantes interrupciones de la actividad empresarial han creado un mundo volátil, lo que aumenta drásticamente la superficie de ataque de los ciberdelincuentes y los lleva a profesionalizar aún más sus modelos de negocio. Al mismo tiempo, avances tecnológicos como las herramientas de IA generativa han democratizado el «arte de la ciberdelincuencia». El resultado es que hoy en día nos hallamos frente a innumerables hackers potenciales que disponen de las herramientas necesarias no solo para maximizar el alcance de sus ataques, sino también su porcentaje de éxito.

Desde SoSafe llevamos años advirtiendo de que los ciberdelincuentes podrían utilizar tácticas sofisticadas basadas en la IA, como los deepfakes, para perpetrar ataques a gran escala. Recientemente se ha facilitado el acceso a herramientas muy potentes de IA generativa, poniendo la ciberdelincuencia al alcance de cualquiera. En un estudio interno realizado este año, comprobamos que los correos de phishing pueden crearse un 40 % más rápido con la ayuda de ChatGPT. Esta es solo una de las maneras en que los delincuentes utilizarán la IA para ampliar su negocio.

Estos avances nos demuestran que la seguridad de la información no es un ámbito en el que debamos dormirnos en los laureles. Por definición, la ciberseguridad debe evolucionar y adaptarse constantemente, y también forma parte de ella adoptar nuevas tecnologías para mantenernos mejor protegidos frente a las nuevas tácticas de ataque. Pero si de algo podemos estar seguros es de que los atacantes seguirán intentando encontrar la manera de sortear incluso las barreras tecnológicas más sofisticadas; y a menudo lo conseguirán. Son plenamente conscientes de que su máxima garantía de éxito es jugar con las emociones de las personas, y así lo han demostrado recientes brechas de seguridad como las de Uber o Reddit. La ingeniería social es una eterna mina de oro. La buena noticia es que es un riesgo que podemos minimizar de forma muy eficaz con los métodos adecuados.

Por este motivo, quizá no sea de extrañar que la sensibilización encabece la lista de prioridades en materia de seguridad entre las organizaciones encuestadas para este informe. Uno de los principales factores que influyen en si pueden invertir suficientes recursos en su cultura de seguridad es el grado de concienciación del equipo directivo sobre los ciber riesgos. En cierto modo, eso es lo que nos proponemos hacer con nuestro Análisis del riesgo humano, ya que estamos convencidos de que nuestros datos pueden aportar nuevas perspectivas. En él, compartimos información de primera mano sobre las tácticas de los ciberdelincuentes y el papel que desempeña el factor humano en ese contexto, pero también ofrecemos recursos para entablar conversaciones, especialmente sobre la seguridad de la información y la sensibilización.

Un análisis en profundidad de los datos de nuestra plataforma, una exhaustiva encuesta a profesionales europeos de la seguridad y entrevistas con expertos de nivel ejecutivo de diversos sectores lo confirman: debemos acercar la ciberseguridad a las personas, hacer que la sensibilización esté presente en todos los ámbitos de nuestras vidas y tomar iniciativas en torno a la fusión de la ciberseguridad y los negocios. Es la única forma de salir de la ruina multimillonaria que supone la ciberdelincuencia actualmente. Debemos evolucionar tan rápido como evoluciona el panorama de las amenazas.

Dr. Niklas Hellemann
CEO de SoSafe

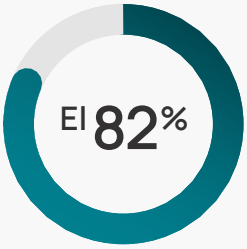
Tabla de contenidos

Resumen ejecutivo

El panorama digital europeo está tenso:

1 de cada 2

organizaciones ha sido víctima de un ciberataque en los últimos 3 años.



de las organizaciones tampoco espera que la situación vaya a mejorar en el próximo año.

> Vivimos en la era de la digitalización. Casi todo está interconectado y se puede hackear.

Dra. Katrin Suder
Experta en estrategia (tecnologías digitales, empresas y política)

Las 3 tácticas más usadas por los ciberdelincuentes:

1. Malware
2. Phishing
3. Ransomware

Los 3 departamentos más afectados:

1. Informática
2. Finanzas
3. Seguridad

Y la ciberdelincuencia está en auge:

3 de cada 4

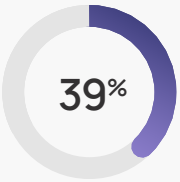
profesionales de la ciberseguridad afirman que el riesgo de su organización ha aumentado debido a las **crisis geopolíticas**, la **IA** y el **teletrabajo**.

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

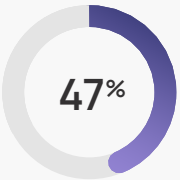
Stéphane Duguin
CEO del CyberPeace Institute

8 de cada 10

afirman que la seguridad de su organización **depende cada vez más de la seguridad de sus socios y proveedores.**



Más de un tercio de las empresas que sufrieron un ataque de ransomware pagaron el rescate.



Casi la mitad de las empresas pequeñas se vieron obligadas a pagar.

El potencial oculto de las nuevas tecnologías en la ciberdelincuencia:

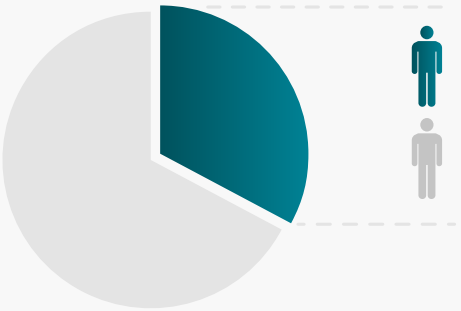
> Los ciberdelincuentes disponen desde hace tiempo de tecnología muy avanzada, como la clonación de voz. Sin embargo, no hemos visto ataques de ingeniería social sofisticados en casos reales a gran escala. Una explicación puede ser que lo sencillo sigue funcionando, pero es muy probable que esto cambie con las filtraciones de potentes modelos de lenguaje y el desarrollo exponencial de la IA generativa en todos los ámbitos.

Dr. Niklas Hellemann
CEO de SoSafe

El 80 % de los expertos en ciberseguridad considera que la ingeniería social y el phishing suponen un riesgo importante para su organización:

1 de cada 3

usuarios clica en contenido malicioso en correos electrónicos de phishing, y, de estos ...



1 de cada 2

procede a introducir información personal.

En un panorama de ciberamenazas actual cada vez más tenso, las técnicas de ingeniería social que se aprovechan de la presión o la autoridad para generar

emociones negativas

son las más eficaces.

> Cada vez recibimos más correos de phishing, y cada nueva oleada es más intensa que la anterior.

Sascha Czech
Director de seguridad informática del
Hospital Universitario de Münster

> Cuando trabajan desde casa, al ser un entorno más relajado, muchos usuarios no se concentran igual. Intercalan muchas tareas personales en su flujo de trabajo, lo que se traduce en falta de atención.

Dr. Stefan Lüders
Director de seguridad informática del CERN

Los nativos digitales son un

↗ 65 %

más propensos a pulsar en correos de phishing que los usuarios de más edad.

Perspectivas de futuro: ¿están las empresas preparadas?

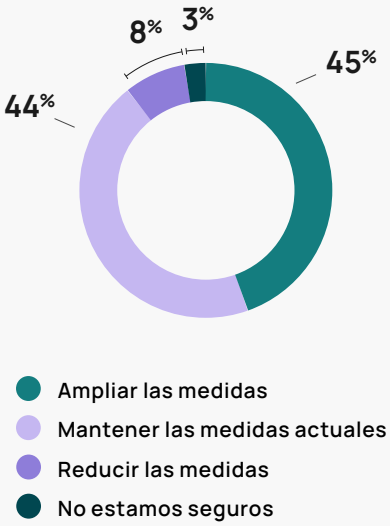
> A menudo escuchamos: “Si no está roto, no lo arregles”; pero cuando se produce un ataque, las consecuencias pueden ser muy graves.

Thomas Tschersich
Director de seguridad informática de Telekom Alemania

Top 3 prioridades de los departamentos de informática y de seguridad

1. Aumentar la concienciación de los empleados en materia de seguridad
2. Mejorar la gestión de identidades y accesos
3. Garantizar la seguridad del trabajo híbrido

9 de cada 10 organizaciones tienen previsto mantener o reforzar sus medidas de sensibilización el año que viene.



> Todo lo que podamos abarcar a través de la concienciación de los empleados nos hace más resilientes como empresa. Ahorramos tiempo, dinero y estrés, y evitamos más riesgos.

Thomas Schumacher
Director general de Accenture Security

Según los profesionales de la ciberseguridad, los factores que más influyen en una mayor concienciación entre los empleados son los siguientes:

1. Medidas de sensibilización a través de apps de comunicación
2. Formación personalizada
3. Customización de los programas de concienciación

Metodología y fuentes de los datos

Encuesta a profesionales de la ciberseguridad

Para llevar a cabo esta encuesta a gran escala sobre el estado de la ciberseguridad en las organizaciones, trabajamos con Censuswide, una consultora internacional de estudios de mercado con sede en Londres. En febrero de 2023 se entrevistó a más de 1000 profesionales de la seguridad de 6 países europeos (Reino Unido, Alemania, Austria, Suiza, Francia y Países Bajos). Estos profesionales representan organizaciones de entre 10 y más de 5000 empleados pertenecientes a todos los sectores.

Datos de la plataforma de SoSafe

Para el análisis de las distintas técnicas de ingeniería social, se examinaron de forma anónima 8,4 millones de correos electrónicos de simulaciones de phishing llevadas a cabo en 3000 organizaciones que usan la plataforma SoSafe Awareness, lo que proporcionó información exclusiva sobre los niveles del riesgo humano y el porcentaje de éxito de las diferentes tácticas de ataque en las organizaciones.

Phish Test

En este estudio sobre la concienciación general sobre el phishing, se enviaron más de 9000 correos de simulación de phishing a usuarios que se habían registrado en 2022. Los participantes recibieron tres simulaciones de ataque a lo largo de una semana, todos ellos considerados de complejidad moderada. Los usuarios debían identificar estos mensajes. Si clicaban en ellos, se les redirigía a recursos de concienciación relacionados con el contenido del mensaje.

La ciberdelincuencia es el riesgo nº1 para las empresas: ¿qué tiene que ver con ella el comportamiento humano?

Riesgo empresarial nº1

Los incidentes de ciberseguridad representan el mayor riesgo para las empresas

Fuente: Barómetro de Riesgos de Allianz 2023 [1]

4,35 M de dólares

Coste medio de una vulneración de datos

Fuente: Coste de la vulneración de datos 2022 de IBM 2022 [2]

Si hay algo en lo que están de acuerdo los expertos en seguridad es que la ciberdelincuencia es un riesgo importante para las empresas de todo el mundo. Desde hace varios años, informes del sector como el Barómetro de Riesgos de Allianz y el Coste de la vulneración de datos de IBM han demostrado que descuidar las precauciones de seguridad puede tener efectos devastadores para las empresas, tanto en términos de pérdidas financieras como de deterioro de su reputación.

Numerosos factores, desde la geopolítica y la inteligencia artificial hasta la escasez de personal en informática y ciberseguridad, parecen empeorar aún más la situación. Y, a medida que los ciberdelincuentes perfeccionan sus estratagemas y las adaptan a estos cambios tecnológicos y sociales, muchas organizaciones tienen dificultades para seguir el ritmo y dar con las herramientas adecuadas para protegerse con eficacia.

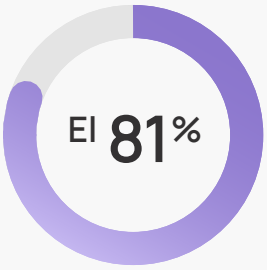
1 de cada **2**

empresas ha sufrido un ciberataque en los últimos 3 años, y el 64 % estima que el riesgo de sufrir otro es elevado.

El panorama para los próximos meses y años no parece precisamente halagüeño. Los expertos en ciberseguridad encuestados para este informe lo tienen claro: el 82 % no espera que la situación mejore en los próximos meses.

El denominador común

A pesar de la complejidad del panorama digital actual, todos los ciberataques tienen un hilo conductor: el factor humano. Por fuertes que sean las medidas técnicas de protección, las personas siguen sucumbiendo a ingeniosas tácticas de la ingeniería social. Para ponerlo en perspectiva: el phishing (uno de los métodos de ingeniería social por excelencia) es la segunda táctica de ciberataque de mayor éxito. Solo el malware y el ransomware suponen un riesgo comparable, según los profesionales de la ciberseguridad encuestados. Curiosamente, estos dos tipos de ataque también suelen tener su origen en algún tipo de interacción humana, como cuando un empleado revela sus credenciales sin saberlo.



de los profesionales de la seguridad afirman que el **phishing y la manipulación emocional de los empleados** suponen un riesgo importante para su organización.

Esto demuestra que las técnicas de ingeniería social siguen siendo la estrategia favorita de los ciberdelincuentes, que no dejan de innovar en este sentido, puesto que se trata de herramientas sencillas y rentables para infiltrarse en los sistemas de las empresas. La buena noticia es que las organizaciones pueden tomar medidas para reforzar eficazmente su componente humano como parte de su estrategia global de seguridad de la información.

Las personas como primera y última línea de defensa

Cuando las empresas transforman la narrativa y aprovechan el comportamiento humano y la psicología del mismo modo que lo están haciendo os ciberdelincuentes, pueden convertir a sus empleados en verdaderos guardianes de su seguridad y del acceso a sus sistemas.

1 **Allianz (2023).** Barómetro de Riesgos de Allianz.

2 **IBM (2022).** Coste de la vulneración de datos 2022. Una carrera de millones de dólares para detectar y reaccionar.

Todo lo que podamos abarcar a través de la concienciación de los empleados nos hace más resilientes como empresa. Ahorramos tiempo, dinero y estrés, y evitamos más riesgos.

Thomas Schumacher
Director general de Accenture Security

El incidente de Reddit[3] lo ilustra muy bien: a principios de 2023, la empresa sufrió una filtración de datos causada por un ataque de phishing muy sofisticado que expuso documentos internos y código fuente. Sin embargo, lo que ocurrió fue un claro ejemplo del impacto positivo de concienciar a los empleados y de crear una cultura sólida de seguridad en las empresas: la persona que hizo clic en el correo electrónico de phishing se percató inmediatamente del ataque y lo comunicó al equipo de seguridad interno, que logró restringir el acceso al ciberdelincuente. De no haberlo hecho, la historia podría haber acabado de forma muy distinta.

La mejor forma de contrarrestar los ataques de los ciberdelincuentes es vencerlos con sus propias armas: comprender nuestras pautas de comportamiento y centrarnos en ellas para poder responder de manera proactiva. En este informe analizaremos más de cerca el estado de la ciberseguridad y la concienciación de los empleados prestando especial atención a Europa. También exploraremos cómo las organizaciones pueden sacar partido de la ciencia del comportamiento para protegerse ante un panorama de amenazas digitales cada vez más complejo. Aunque los datos hablan por sí mismos, daremos la palabra también a expertos de diferentes sectores, que nos darán su opinión sobre las prioridades para los profesionales de la seguridad actualmente.

3 **WeLiveSecurity (2023).** Reddit sufre el robo de código fuente tras acceso a sus sistemas.

« Vivimos en la era de la digitalización. Casi todo está interconectado y se puede hackear.

Dra. Katrin Suder
Experta en estrategia (tecnologías digitales, empresas y política)

La Dra. Katrin Suder es una de las expertas en estrategia más reconocidas en el ámbito de las tecnologías digitales, los negocios y la política. Asesora a numerosas empresas, incluyendo multinacionales alemanas y estadounidenses. Además, es especialista en física y neuroinformática, doctorada en inteligencia artificial y tiene años de experiencia en el mundo empresarial y político. Hasta 2021 dirigió el consejo digital alemán (Digitalrat) bajo el gobierno federal de Angela Merkel. De 2014 a 2018 fue secretaria de Estado en el Ministerio Defensa alemán. Trabajó en la consultora global McKinsey durante 14 años, recientemente como directora, y es miembro de varios consejos de supervisión alemanes e internacionales, incluyendo el de Cloudflare.

En nuestra Human Firewall Conference, afirmaste que lo único que te quita el sueño son los ciberataques. ¿A qué se debe?

La cibernética es una peligrosa herramienta militar, pero también un arma muy eficaz y rentable para los delincuentes, ya que les permite realizar sus ataques sin ser detectados. Encontrar al culpable no es imposible, pero requiere mucho tiempo. También es increíblemente rentable si lo comparamos, por ejemplo, con un avión de combate. Además, conlleva un bajo riesgo personal, ya que nadie tiene que arriesgar la vida, aunque esto no quita que los ciberataques puedan ser potencialmente devastadores. Cuando estaba en el Ministerio Federal de Defensa alemán, la cuestión de la seguridad empezó a referirse cada vez más a la seguridad en el ciberespacio, y por ello añadimos esta nueva dimensión a nuestra estrategia de defensa. Actualmente, los incidentes de ciberseguridad son uno de los mayores riesgos que veo cuando trabajo con empresas, que sufren constantemente ataques informáticos. La cuestión no es si te atacarán, sino cuándo, y con qué rapidez reaccionas y cómo gestionas la situación.

La situación geopolítica está cada vez más inestable y fragmentada. ¿Qué efecto está teniendo esto en los peligros ya presentes en el ciberespacio?

La cibernética es un instrumento geopolítico de poder y un nuevo vector de ataque que los gobiernos utilizan para perseguir sus propios fines. Nuestro nuevo orden mundial ha provocado un continuo descenso de las fuerzas reguladoras, mientras que los intereses nacionales, como el espionaje o los intentos de agresión, cobran mayor importancia.

Los gobiernos están invirtiendo en tecnología armamentística al apostar por la cibernética, lo que les permite provocar efectos devastadores haciendo una inversión mínima. No se trata solo de datos y dinero; a veces entran en juego incluso vidas humanas.

En las circunstancias actuales, ¿responde el repunte de los ciberataques a motivaciones exclusivamente (geo)políticas?

No, no tiene motivaciones exclusivamente geopolíticas. Muchos ciberataques son perpetrados por agentes paraestatales que se comportan como soldados no vinculados a un país específico. No están sujetos a ninguna ley, no se puede responsabilizar de estos ciberataques a ningún país en concreto y no se puede alegar que hayan incumplido algún tipo de convenio – eso es lo que hace que la situación sea tan sumamente complicada. En nuestro nuevo orden mundial, en el que los fuertes intereses nacionales desempeñan un papel fundamental, estas estructuras pueden seguir creciendo. Los hackers paraestatales se aprovechan de los cambios geopolíticos para obtener beneficios, por ejemplo, apoyando intereses políticos o vendiendo datos robados por cantidades astronómicas. La geopolítica alimenta la ciberdelincuencia en tanto que las crisis geopolíticas van seguidas de un aumento de los ciberataques no solo por motivaciones políticas, sino también delictivas.

¿Qué otros avances están repercutiendo en nuestra ciberseguridad?

Vivimos en la era de la digitalización. Casi todo está interconectado y se puede hackear. La digitalización también ha conferido más importancia a la tecnología, lo que abre nuevas puertas para los atacantes.

¿Cómo afecta esto a nuestras infraestructuras críticas? Las centrales eléctricas no solían estar conectadas a Internet, ¿sigue siendo eso cierto si consideramos la distribución descentralizada de la energía?

Por supuesto, siempre habrá zonas aisladas que no dependan de Internet, como por ejemplo las que tienen las fuerzas armadas de algunos países. Pero las infraestructuras críticas están cada vez más interconectadas, cosa que me preocupa. La cantidad de personas que son atacadas y manipuladas directamente crece a un ritmo alarmante, y estas personas podrían, a su vez, tener acceso a redes aisladas. Existen leyes y ordenanzas sobre infraestructuras críticas que pretenden regular este ámbito, pero si contemplamos la red de suministro descentralizada, como por ejemplo a los pequeños proveedores municipales, les resulta más difícil protegerse. No cuentan ni con los recursos financieros ni con el personal necesario para implantar los sistemas informáticos adecuados.

¿Podemos siquiera mantener un control sobre todos estos avances del mundo de la ciberseguridad?

A menudo se dice que en el ciberespacio todo es nuevo, que no lo habíamos visto antes, pero no es verdad. Los principios básicos, como la protección y la seguridad, son los mismos; proteger tus cuentas con buenas contraseñas, por ejemplo, debería ser tan fácil como lavarse las manos, etc. Creo que es importante que no actuemos como si todo en el espacio digital fuera nuevo, imprevisible e incontrolable. Es falso y nos hace sentir impotentes.

« En los últimos 10 años, las empresas han invertido más en tecnología que en las personas. Ahora comienzan a darse cuenta de que la tecnología no lo es todo y de que la ingeniería social, especialmente el phishing, es un verdadero problema.

Dra. Katrin Suder
Experta en estrategia (tecnologías digitales, empresas y política)

Hablemos de defensa. Estás en la junta asesora de Cloudfare. ¿Se habla hoy de ciberseguridad en los consejos de administración?

Por supuesto. Varía de un sector a otro, porque cuanto menos digitalizado está un sector, menos relevante es la ciberseguridad, pero en general, según mi experiencia, los ciberataques se consideran uno de los principales riesgos. Sin embargo, no todas las juntas cuentan con un miembro versado en este tema. También es una cuestión generacional, porque estas juntas suelen estar dirigidas por personas con más experiencia vital y, a menudo, menos experiencia en digitalización y cuestiones cibernéticas. Además, la cibernética es una batalla incansable y feroz que va a un ritmo vertiginoso, y en la que siempre hay que aprender y mantenerse al día. Por eso es tan importante desarrollar nuevos modelos, como poner a personas más jóvenes con conocimientos específicos en puestos en la junta asesora, aunque no hayan dirigido nunca una empresa, o invertir más en formación para los empleados. La pregunta que todos debemos hacernos es: ¿cuál es el nivel de concienciación sobre ciberseguridad de nuestra empresa y cómo lo mantenemos actualizado? Muchas empresas, sobre todo medianas, se enfrentan hoy a este reto.

¿Hacen las empresas lo suficiente para protegerse, sobre todo en lo que respecta al factor humano?

Las empresas nunca podrán invertir suficiente en concienciación en materia de ciberseguridad. Hace pocos años que muchas de ellas tomaron conciencia de la cuestión del factor humano, por lo que aún van a tardar un tiempo en desarrollar prácticas recomendadas y en encontrar la manera de seguir el ritmo de semejante carrera desenfrenada. En los últimos 10 años, las empresas han invertido más en tecnología que en las personas. Ahora comienzan a darse cuenta de que la tecnología no lo es todo y de que la ingeniería social, especialmente el phishing, es un verdadero problema.

«Tecnología vs humanos»: un debate habitual en la seguridad de la información es qué debe priorizarse y cómo. ¿Qué opinas al respecto?

Es un debate sin sentido. No estamos pidiendo a las empresas decidir entre invertir en su infraestructura o en sus empleados. Por supuesto que las empresas pueden tratar de subsanar sus puntos débiles con la tecnología y optimizar sus estrategias de defensa utilizando software, y deben hacerlo, pero es crucial que inviertan también en las personas.

Has mencionado que existe una batalla incansable y feroz en la seguridad de la información. ¿Las empresas ven la ciberseguridad como una medida de formación puntual o han acabado por entender que hay que invertir continuamente en este ámbito?

El phishing afecta a las empresas, y la mayoría de ellas se han dado cuenta de que para resolver este problema es fundamental actuar con diligencia y constancia. Sin embargo, mantenerse en primera línea de batalla no es tan fácil y muchas de ellas siguen empleando medidas tradicionales: presentaciones interminables de PowerPoint, vídeos «divertidos» o seminarios presenciales que pretenden formar a los empleados en este tema. Pero si tenemos en cuenta la cantidad de información que debemos impartir a nuestros empleados (aparte de la ciberseguridad, hay temas como el cumplimiento normativo, la protección de datos o los criterios ESG), tenemos que incorporar conceptos como la gamificación y otros métodos eficaces utilizados en la formación de adultos. En este sentido, muchas empresas están todavía en la retaguardia.

¿Qué preguntas se hacen las juntas consultivas para evaluar la ciberseguridad humana y técnica en la empresa?

WEn las juntas asesoras aún no estamos totalmente preparados y dotados de personal en este sentido. Las preguntas y los debates se suelen

centran en el control y los procesos y creo que deberíamos implicarnos aún más y plantear preguntas como: «¿Cuál es el potencial de peligro de nuestro modelo de negocio?» ¿Qué datos almacenamos y dónde lo hacemos? ¿Cuánto podría perjudicar un ciberataque a nuestro modelo de negocio en la situación actual? ¿Cuáles son nuestros vectores de ataque geopolíticos? ¿Qué medidas de contingencia tenemos?» Al principio parece complicado, pero no lo es. En producción, por ejemplo, también se debaten cuestiones específicas como los costes de una interrupción o los porcentajes de error.

¿De qué manera pueden las empresas convertir la ciberseguridad en un requisito interno?

La ciberseguridad es un tema clásico de la gestión de riesgos. Las empresas la integran en sus procesos de gestión de riesgos o bien la convierten en una cuestión complementaria y establecen su propia evaluación de ciber riesgos. He visto antes las dos opciones, y ambas pueden funcionar.

¿Podría considerarse la ciberseguridad un tipo de impuesto digital? ¿Tenemos que aceptar que la creciente digitalización conlleva un aumento de los costes?

Naturalmente, tenemos que poner precio a esta nueva dimensión de la seguridad. El problema es que han subido las primas de los seguros de asistencia sanitaria (COVID), política industrial, seguridad física, energía y ciberseguridad. En consecuencia, las empresas tienen más gastos, y los márgenes EBIT también están bajo presión debido a la evolución geopolítica. En términos generales, esto significa que estamos perdiendo riqueza porque los márgenes EBIT que no se obtienen no pueden destinarse a inversiones, empleados, etc. Desde una perspectiva geopolítica, no veo por qué habrían de disminuir estas primas. El estado tampoco puede suplirlo ni regularlo todo, y lo estamos viendo en tiempo real. Por eso creo que, en este debate, la analogía con los impuestos puede inducir a error.

¿Qué papel debe desempeñar el estado en lo que respecta a la ciberseguridad?

Una de las funciones más importantes del estado es invertir en formación actualizada, y eso no se está haciendo lo suficiente en el ámbito de la informática. Todo el mundo debería aprender en la escuela al menos las nociones básicas de ciberseguridad y cómo trabajar con datos. Además de la educación, necesitamos unas autoridades (digitales) competentes que funcionen, así como más apoyo y puntos de contacto, que no abundan en el mundo cibernético.

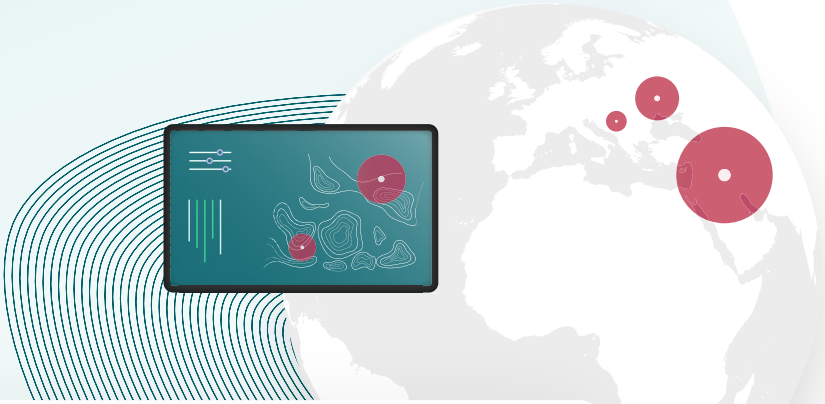
¿Cómo resolver la escasez de personal en el sector de la informática?

Si queremos mejorar la seguridad, tenemos que pensar más allá de la automatización en el ámbito de la informática. Ya no hablamos de despidos y de mejorar la eficiencia mediante la automatización, sino de si podemos seguir garantizando la ciberseguridad. La escasez general de personal es real, y las consecuencias son palpables para muchos, aunque se hace sentir aún más en las disciplinas CTIM (ciencia, tecnología, informática y matemáticas). Al mismo tiempo, la demanda sigue creciendo. Esta situación exige nuevas soluciones, como la escalabilidad mediante la automatización, y tenemos que seguir aumentando nuestra capacidad siempre que podamos, ya sea con ChatGPT u otra tecnología.

Has mencionado a ChatGPT: ¿cómo influye la IA en la ciberseguridad?

La IA generativa me preocupa menos desde el punto de vista laboral que desde la perspectiva de la educación y la democracia. Nos está dando un nuevo cometido educativo: si cada vez tenemos más IA generativa, tenemos que empezar a plantearnos cómo podemos categorizar la innovación o el contenido. ¿Cómo evaluamos los textos? ¿Cómo investigamos? El resultado de estas herramientas procede de una máquina, y los destinatarios del resultado carecen de una fuente humana que sirva de referencia para evaluarlos. Los usuarios deben aprender a evaluar las respuestas que les dan las herramientas de IA.

Un campo de batalla mundial: cómo la geopolítica está definiendo el panorama de la ciberdelincuencia



> Vivimos en la era de la digitalización. Casi todo está interconectado y se puede hackear.

Dra. Katrin Suder
Experta en estrategia (tecnologías digitales, empresas y política)

Esta cita de la doctora Suder recalca una verdad trascendental sobre nuestro mundo moderno: el vertiginoso avance de la tecnología y la creciente interconexión de nuestros dispositivos y sistemas digitales han generado oportunidades sin precedentes para la comunicación, el comercio y la innovación, pero también están poniendo a prueba nuestra resiliencia en el ámbito de la ciberseguridad.

La interrelación de la digitalización y la geopolítica ha creado una industria de la ciberdelincuencia compleja en la que cibercriminales financiados por gobiernos, organizaciones delictivas y hackers independientes explotan las vulnerabilidades de la infraestructura digital por motivos políticos y económicos. Es en medio de este panorama donde la ciberseguridad se ha convertido en un asunto preocupante para gobiernos, empresas y particulares.

Ciberataques gubernamentales: el futuro incierto de las potencias mundiales

Paradójicamente, tras una rápida digitalización y décadas de progresiva globalización, el mundo experimenta ahora una tendencia geopolítica muy peculiar: la **desglobalización**. Aunque los primeros indicios ya eran visibles en 2008, este proceso se ha acelerado recientemente debido a la competencia estratégica entre Estados Unidos y China.[1] La tensión y la rivalidad entre estas dos superpotencias mundiales se ha extendido al ámbito de la ciberseguridad: ambas se han acusado mutuamente de participar en ciberataques financiados por el gobierno contrario, así como de robos de propiedad intelectual y espionaje. El año pasado, sin ir más lejos, varios sitios web oficiales de Taiwán experimentaron ataques DDoS que coincidieron con la visita de la congresista estadounidense Nancy Pelosi, lo que levantó sospechas sobre una supuesta implicación de China en los ataques.[2]

Otro ejemplo es el actual conflicto entre Israel e Irán, dos países que a lo largo de los años han llevado a cabo operaciones cibernéticas encubiertas el uno contra el otro. Tras el infame gusano Stuxnet, que tenía como objetivo el programa nuclear iraní, se han producido otros muchos ciberataques, como un intento de filtración de datos en la infraestructura de agua y alcantarillado de Israel en abril de 2020, un ciberataque contra el puerto de Shahid Rajaee en mayo de 2020[3], ciberataques contra los sistemas de transporte del país en julio de 2021 y un ataque a una página web de citas LGBTQ israelí en el que se filtró información personal de los usuarios en octubre de 2021.[4] A medida que se intensifican este tipo de ciberataques, también en el contexto de la guerra de Rusia contra Ucrania, aumenta la preocupación de que **sus objetivos hayan pasado de estar principalmente relacionados con la defensa a interrumpir infraestructuras críticas y la vida civil.**

1 **El País (2019).** La guerra comercial entre EE UU y China acelera la desglobalización.

2 **Huffington Post (2022).** Hackean las pantallas de lugares públicos de Taiwán con insultos a Nancy Pelosi.

3 **Iniseg (2020).** Ciberguerra entre Irán e Israel.

4 **Clarín (2021).** Israel e Irán amplían su guerra cibernética y ahora atacan objetivos civiles.

« El número de intentos de ciberataques ha aumentado en un 8000 % desde febrero de 2022.

Sascha Czech
Director de seguridad informática del Hospital Universitario Uniklinikum Münster

Sascha Czech es el director de seguridad informática del Hospital Universitario de Münster (UKM) y, como tal, es responsable de la seguridad corporativa del centro. El UKM fue el primer hospital de Alemania en establecer un Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) gestionado por su propio personal especializado. En 2022, la organización Certification Information Security (CIS) lo nombró director de seguridad de la información (CISO) del año por toda su labor en el proceso.

Has ocupado diversos puestos de responsabilidad en materia de ciberseguridad en el sector sanitario. En tu experiencia, ¿cuáles han sido los mayores retos a los que te has tenido que enfrentar?

El panorama de las amenazas digitales se está volviendo más peligroso, y lleva siendo así desde hace algún tiempo. No es solo que cada vez haya más métodos de ataque nuevos, sino que también hay un repunte del típico «ruido de fondo» constante. En mi opinión, la combinación de la ciberseguridad y la seguridad del perímetro físico es el mayor reto al que el sector sanitario se enfrenta actualmente.

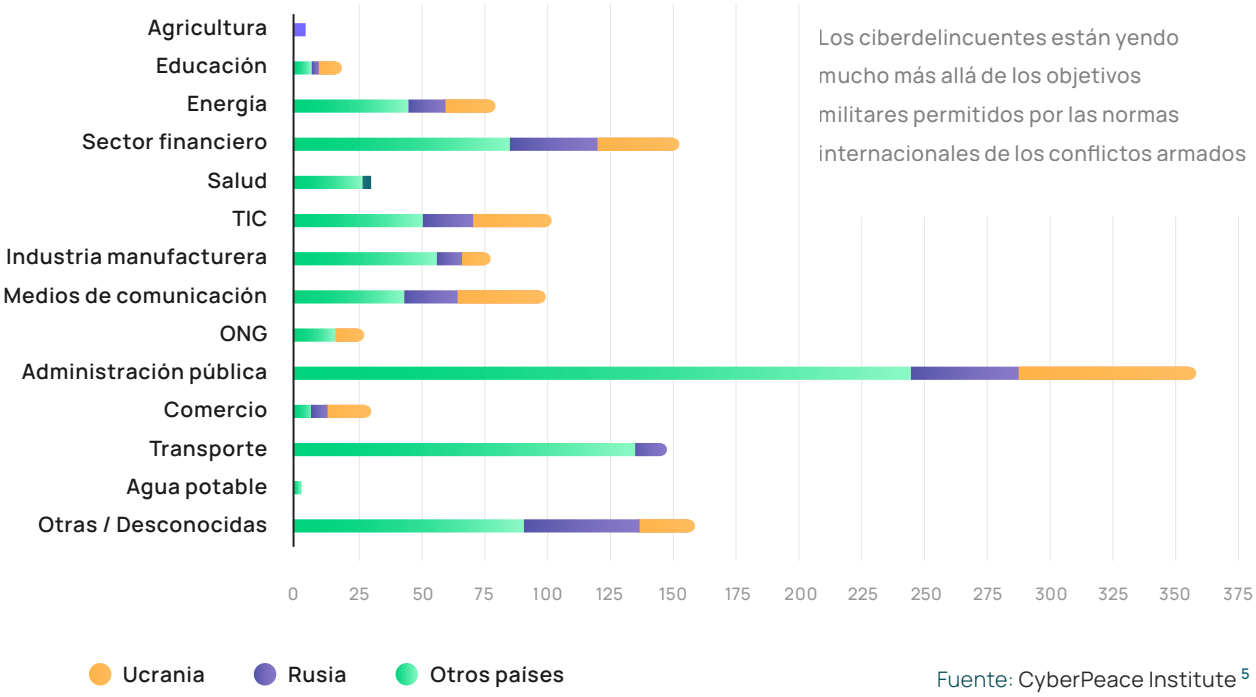
¿Cuáles crees que son las principales causas?

Para empezar, indudablemente, a la tensa situación política. En el Hospital Universitario de Münster, desde febrero del año pasado hemos observado un **aumento aproximado del 8000 %** del «ruido de fondo» con respecto al año anterior. Los correos electrónicos maliciosos, ya sean de phishing o ransomware, también son cada vez más frecuentes. Las oleadas de ataques también se están volviendo mucho más intensas.

¿Has notado un cambio de actitud generalizado hacia la seguridad de la información?

Creo que el tema está mucho más presente después de haber acaparado la atención de los medios de comunicación, pero hay que encontrar la manera de que la gente sea consciente de su propia responsabilidad y esté dispuesta a seguir aprendiendo. En el momento en que los empleados dejen de pensar que la ciberseguridad es aburrida o demasiado compleja y se den cuenta de que es la clave del éxito, la empresa habrá ganado la batalla. Al principio agrupamos la ciberseguridad con otras cuestiones de seguridad general, como la protección contra incendios. También nos aseguramos de que los empleados experimenten una simulación de ciberataque para que vean lo rápida y fácilmente que puede producirse, y cuáles podrían ser las consecuencias. Con esto queremos conseguir cambiar su forma de entender la ciberseguridad: las personas no son solo otra línea de defensa, son la más valiosa.

Número de ciberataques por sector según su ubicación en el contexto del conflicto armado entre Rusia y Ucrania.



Fuente: CyberPeace Institute [5]

Los retos para las empresas

> Sería casi ingenuo suponer que los delincuentes no saben desde hace tiempo que los ataques en el ciberespacio pueden ser muy lucrativos.

Dr. Stefan Lüders
Director de seguridad informática del CERN

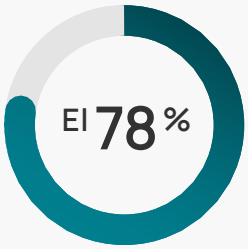
El hecho de que **las crisis geopolíticas y la ciberseguridad estén inextricablemente unidas** no solo afecta a los gobiernos y a las infraestructuras críticas, sino también a las empresas de todo el mundo. En los últimos años, hemos visto muchas veces cómo las empresas han sido objeto de ciberataques relacionados con tensiones geopolíticas.

Por ejemplo, los gobiernos de Estados Unidos y Reino Unido culparon a Corea del Norte del ataque causado por WannaCry, que afectó a más de 300 000 ordenadores en 150 países, incluidos hospitales, empresas y bancos, y causó daños por valor de miles de millones de dólares.[6]

5 **Cyberpeace Institute (2023).** Impact & Harm. How do cyberattacks and operations impact civilians?

6 **Europa Press (2017).** Reino Unido se suma a EEUU y culpa a Corea del Norte del virus ‚WannaCry'.

En 2021 también se acusó al gobierno chino de estar detrás del ataque a Microsoft Exchange, que golpeó al menos a 30 000 organizaciones en todo el mundo.[7] Estos ataques muestran las graves repercusiones y riesgos de seguridad que pueden suponer los conflictos mundiales para las empresas de todo el mundo.



de los profesionales de la seguridad afirma que la situación geopolítica ha aumentado el riesgo de ciberseguridad de su organización

Las tensiones geopolíticas distan mucho de ser los únicos acontecimientos mundiales que los ciberdelincuentes intentan explotar para sus propios fines. Horas después del colapso del Silicon Valley Bank en marzo de este año, los ciberdelincuentes empezaron a registrar dominios sospechosos, a crear páginas de phishing y a preparar estafas por correo electrónico corporativo comprometido (Business Email Compromise).[8] A medida que crece la inestabilidad mundial, los ciberdelincuentes seguirán adaptando sus estrategias de ataque y dando prioridad a las industrias y regiones más vulnerables en ese momento.

Las crisis geopolíticas como armas cibernéticas: así atacan los hackers a los ciudadanos

> Los civiles se ven implicados en grandes ciberataques a causa de una crisis o un conflicto concreto. Esto es muy preocupante porque significa externalizar abiertamente los ciberataques, lo que difumina los límites entre quién es civil, quién es militar y quién es el objetivo.
>
> **Stéphane Duguin**
> CEO del CyberPeace Institute

En tiempos de tensiones geopolíticas, las personas tienden a **tener las emociones a flor de piel y a polarizar sus opiniones**, lo que las vuelve más vulnerables a los ataques de ingeniería social. Los ciberdelincuentes son conscientes de ello y se aprovechan de estas tensiones difundiendo información errónea, manipulando la opinión pública o incluso instigando a la violencia. También emplean ataques de phishing a través de múltiples canales para infundir una sensación de urgencia y miedo en la gente, lo que puede llevarlos a tomar decisiones precipitadas y mal informadas.

7 **El Mundo (2021).** EEUU, la UE y la OTAN acusan a China del hackeo global a Microsoft.

8 **Ciberseguridad TIC (2023).** La quiebra de Silicon Valley Bank genera una oleada de estafas.

La guerra de Rusia contra Ucrania provocó un fuerte aumento de ciberataques coordinados como parte de la ofensiva, lo que afectó a organizaciones y particulares tanto de estos países como de todo el mundo. Incluso ahora, un año después del conflicto, se han descubierto cientos de sitios web falsos gestionados por estafadores que engañaban a las personas que querían hacer donaciones para Ucrania.[9]

Teniendo en cuenta el gran impacto que tiene la geopolítica en el panorama de la ciberseguridad, ahora depende de nosotros mantenernos informados y adoptar las medidas de seguridad necesarias para afrontar la compleja industria de la ciberdelincuencia, que se encuentra en constante evolución.

> **La guerra se libra de forma híbrida, y muchas personas han recurrido a la ciberdelincuencia para apoyar a un bando u otro. Cuando termine el conflicto, habrá un alto porcentaje de "desempleo" entre estos atacantes, y estos "ciberdesempleados" buscarán un nuevo reto.**

Tobias Ludwichowski
Director de seguridad informática de Signal Iduna

9 **WeLiveSecurity (2022).** Cibercriminales aprovechan situación en Ucrania para promover estafas.

Ingeniería social: la eterna mina de oro

Las 3 tácticas más usadas por los ciberdelincuentes:

1. Malware
2. Phishing
3. Ransomware

> Seguimos viendo casi siempre los mismos puntos de entrada en los ciberataques: la infiltración mediante malware o el robo de información sensible, por ejemplo, a través de phishing.

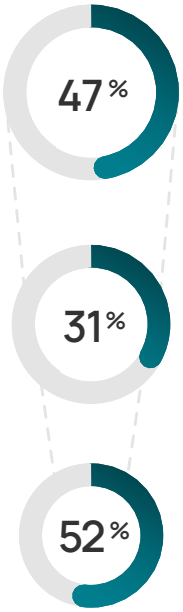
Dr. Stefan Lüders
Director de seguridad informática del CERN

A pesar de que el panorama geopolítico actual convulso y las crisis mundiales estén ampliando la superficie de ataque de los ciberdelincuentes y los avances tecnológicos les estén ayudando a escalar sus modelos de negocio, las tácticas de ataque más sofisticadas están ganando terreno muy lentamente (más información en la próxima sección). Parece que los ciberdelincuentes siguen apostando por lo que mejor saben hacer: la ingeniería social, a menudo en forma de phishing.

Y es que esta es la segunda técnica de ciberataque más utilizada en nuestra encuesta, junto con el malware y el ransomware, que también suelen comenzar con phishing u otros tipos de manipulación psicológica. De hecho, más **del 61 % de los profesionales de la ciberseguridad afirman que sus empresas han recibido correos electrónicos maliciosos**, y esta tendencia no parece sino acelerarse.

> Cada vez recibimos más correos de phishing, y cada nueva oleada es más intensa que la anterior.
>
> **Sascha Czech**
> Director de seguridad informática del Hospital Universitario de Münster

Los ciberdelincuentes siguen recurriendo al phishing tan a menudo por varias razones. Los datos de nuestra plataforma muestran que este tipo de ataque sigue siendo muy eficaz para obtener información confidencial o para acceder a los sistemas de una empresa, como demuestra el hecho de que uno de cada tres usuarios haga clic en contenido malicioso en correos electrónicos de phishing.



Porcentaje de apertura

Casi 1 de cada 2 usuarios abre correos electrónicos de phishing...

+ 2 desde 2022

Porcentaje de clics

un tercio de ellos hace clic en contenido malicioso...

+ 1 desde 2022

Porcentaje de interacción

y la mitad de ese tercio interactúa además con ese contenido.

- 6 desde 2022

Aunque los usuarios se hayan vuelto algo más cautos a la hora de interactuar con contenido malicioso en comparación con 2022 (del 58 % al 52 %), los porcentajes actuales siguen siendo alarmantes. Seguimos viendo que cuando se hace clic en un correo, la mitad de las personas interactúa con él, por ejemplo, introduciendo datos en pantallas de inicio de sesión falsas. **Es probable que los nuevos avances tecnológicos, como la IA generativa, hagan aumentar aún más estos indicadores clave de rendimiento (KPI)**, lo que permitirá a los ciberdelincuentes mejorar el contenido de los correos de phishing y escalar su producción (más información en la próxima sección).

Pero ¿por qué es tan eficaz la ingeniería social como táctica de ataque? Para lograr sus objetivos, los ciberdelincuentes recurren a diversos vectores que adaptan continuamente a las tendencias actuales para incrementar el impacto de sus ataques. Un análisis más detallado de estos vectores muestra por qué manipular las emociones humanas es la clave de sus estrategias: da muy buenos resultados, independientemente de las precauciones técnicas que hayan implantado las empresas.

Ajustes técnicos para potenciar los efectos de la manipulación

Un enfoque fácilmente escalable que utilizan los ciberdelincuentes para aumentar la eficacia de sus ataques de phishing consiste en introducir modificaciones técnicas en el formato de los mensajes de correo electrónico, ya sea incluir un archivo adjunto, un enlace, la referencia a una máscara de entrada a o imitando un hilo de conversación. Todos estos vectores siguen funcionando muy bien, aunque los porcentajes de éxito de los correos de phishing que han sido adaptados desde un punto de vista técnico están bajando en comparación con años anteriores. Cabe destacar que **los usuarios parecen haberse vuelto más precavidos con los archivos adjuntos**, lo que se traduce en un descenso del porcentaje de clics del 8 % con respecto a 2022.

Porcentajes de clic según el tipo de ataque (comparado con 2022)

Archivos adjuntos	Enlaces
32% -8	25% -1
Máscaras de entrada	**Hilos de conversación**
27% -2	34% -5

Del mismo modo, uno de los componentes básicos en el arsenal de los ciberdelincuentes son las técnicas de manipulación de direcciones de correo. Mientras que hacer simples cambios en el dominio de destino solo consigue que haga clic una de cada cinco o seis personas, **la ciberocupación de subdominios y la suplantación de direcciones de correo electrónico son más eficaces a la hora de engañar a los usuarios**, con un porcentaje de clics del 27 % y del 29 %, respectivamente.

Esta evolución demuestra que los usuarios son cada vez más conscientes de los métodos de manipulación técnica. Dado que los métodos de ataque más tradicionales, como adjuntar un archivo malicioso, están empezando a perder protagonismo y los porcentajes de clics están cayendo, los atacantes pronto comenzarán a dejar de lado la manipulación técnica en masa y pasarán a utilizar técnicas más sofisticadas.

Porcentaje de clic según el método de ataque

Ocupación de dominios con erratas

17%

Suplantación de direcciones de correo

29%

Ocupación de subdominios

26%

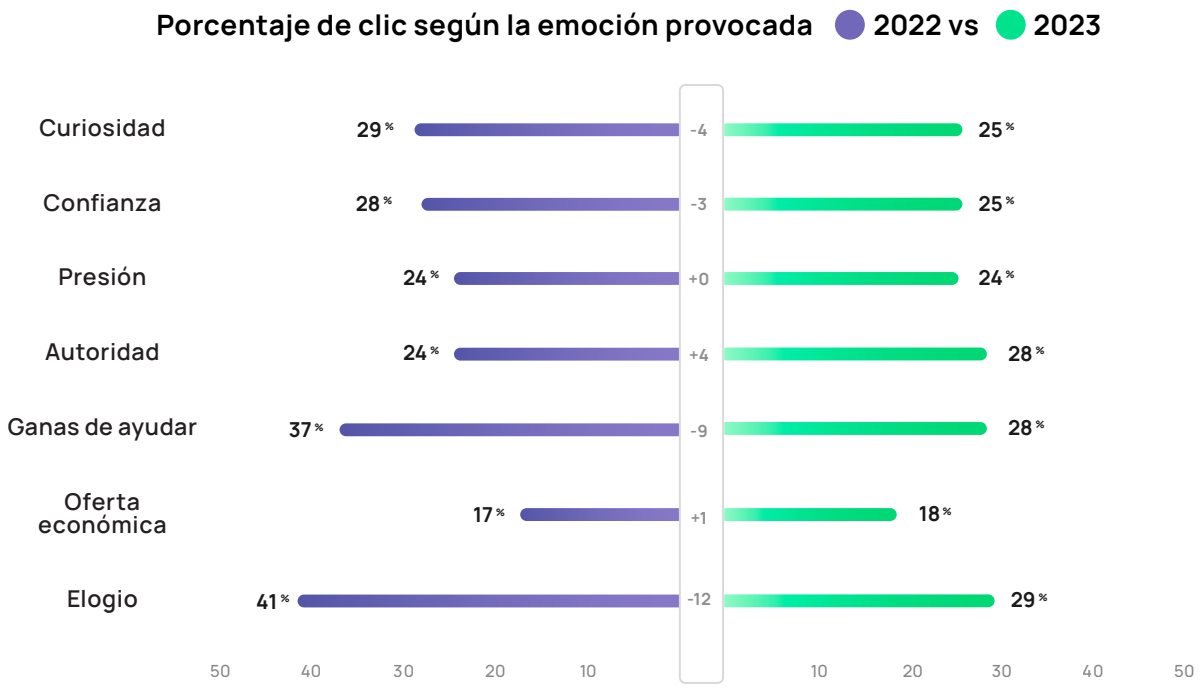
Ocupación de dominios

20%

El aspecto psicológico: el engaño emocional

En última instancia, para los ciberdelincuentes, el poder de la ingeniería social reside en su versatilidad. Como ilustra claramente un análisis más detallado de los vectores psicológicos en las campañas de phishing, esta táctica utiliza nuevos acontecimientos sociales o políticos para manipular las emociones humanas. El grado de convicción del contenido de un correo de phishing y su capacidad para tocar la fibra sensible en términos de persuasión emocional tienen un papel decisivo en el número de personas que acaban haciendo clic.

En comparación con 2022, se aprecia un cambio en cuanto a qué emociones son las más prometedoras para los ciberdelincuentes. Si bien provocar emociones positivas mediante el elogio y la buena voluntad suele generar un mayor porcentaje de clics, ha aumentado ligeramente el éxito de las tácticas que generan **emociones negativas**, como imponer autoridad, presionar y hacer peticiones económicas. Esto hace pensar que los usuarios se han vuelto más susceptibles a este tipo de manipulación y explotación emocional. Una posible explicación de esta tendencia es que en el último año la sociedad ha sido testigo de un gran número de crisis y conflictos, y los ciudadanos están preocupados e inquietos, lo que facilita que los delincuentes provoquen reacciones negativas.



Por otra parte, los asuntos de phishing más frecuentes muestran que las campañas con más éxito entre los empleados se aprovechan de las emociones negativas: cuatro de los cinco más populares juegan con un elemento de presión.

Top 5 asuntos de phishing en 2022

1. Coche averiado (presión/curiosidad)
2. Invitación a Teams (curiosidad)
3. Error en la nómina (presión/curiosidad)
4. Tu contraseña de la oficina caduca hoy (presión)
5. Te has perdido esta conversación de Teams (presión/curiosidad)

El papel decisivo de una formación en ciberseguridad actualizada para prevenir el phishing

La buena noticia es que la sensibilización de los empleados ante estas y otras tácticas de ingeniería social puede aumentarse de manera constante mediante una formación en ciberseguridad actualizada. Como muestran los datos de la plataforma SoSafe Awareness, **una combinación de aprendizaje virtual gamificado, simulaciones de phishing y herramientas de aviso de phishing contextuales puede aumentar los porcentajes de aviso de phishing hasta en un 80 %**, lo que contribuye significativamente a la protección de las organizaciones frente a los ciberataques y a la rapidez con que pueden reaccionar ante las amenazas. Para ello, es crucial adoptar un enfoque centrado en las personas y que utilice métodos basados en la ciencia del comportamiento. Algunos enfoques como el Modelo de Seguridad Conductual (o Behavioral Security Model), que combina el contexto, el conocimiento, la motivación y el comportamiento pueden servir de guía para los profesionales de la ciberseguridad (véase también el Análisis del riesgo humano 2022).

« Existe la idea errónea de que el ciberespacio no está regulado, y no es verdad. Hay muchas leyes sobre ciberseguridad, pero no se aplican correctamente.

Stéphane Duguin
CEO del CyberPeace Institute

Stéphane Duguin es el CEO del CyberPeace Institute. Lleva veinte años analizando el uso fraudulento de la tecnología como arma contra las comunidades más vulnerables. Es experto en transformación digital y convergencia de tecnologías disruptivas. Es miembro del consejo de administración de la Iniciativa Datasphere y forma parte del comité asesor del Global Forum on Cybercrime Expertise (GFCE). Antes de liderar el CyberPeace Institute, Stéphane Duguin ocupó un alto cargo en Europol, donde llevó a cabo importantes operaciones contra el cibercrimen y el terrorismo digital.

El enfoque del CyberPeace Institute se centra en el ser humano. Según tu experiencia, ¿qué consecuencias tienen los ciberataques en las personas?

Nunca debemos olvidar que, en la mayoría de los casos, los ciberataques tratan de jugar con la psicología de la víctima, lo que significa que existe un factor de manipulación. Por ejemplo, el ransomware es uno de los pocos ciberdelitos que hace que la víctima sea cómplice. Cuando sufrimos un ataque de ransomware, debemos tomar decisiones complicadas que tienen un impacto psicológico, como pagar el rescate o denunciar el ataque. La segunda parte es la culpa que se genera en la víctima. Las ONG sufren muchos ataques en los que los atacantes se hacen pasar por el CEO de la empresa, conocidos como fraude del CEO. Cuando eso ocurre, la persona que ha sido engañada se ve sometida, en muchos casos, al escrutinio de la organización.

Pero hay otra consecuencia que es más sistémica: las consecuencias del ataque para aquellos que se benefician de las acciones de la organización. Esto es algo que vemos en el sistema sanitario, por ejemplo. Un estudio de Vanderbilt muestra que el impacto de un ciberataque en un hospital sigue notándose después de varios meses, o incluso un año después. Vanderbilt describe cómo pacientes en estado crítico recibieron una atención sanitaria de menor calidad que la que se les hubiera dado antes del ataque, lo que incrementó las probabilidades de que sus afecciones tuvieran consecuencias fatales.

Tampoco podemos subestimar los efectos psicológicos a largo plazo en las víctimas. Un ejemplo que ilustra esto muy bien es el ataque de ransomware a la clínica finlandesa Vastaamo. Tras la negativa del centro a pagar el rescate, los ciberdelincuentes extorsionaron a todos y cada uno de los pacientes de la clínica, amenazando con revelar su información psicológica privada. Ante esta situación, el país tuvo que crear una unidad especial de apoyo para atender a más de 25 000 víctimas.

Si analizamos el panorama actual de las amenazas, ¿cómo ha cambiado en el último año?

Básicamente, se ha disparado el modelo de negocio de la ciberdelincuencia como servicio. Hemos asistido a un aumento muy rápido de los grupos delictivos que utilizan tecnologías innovadoras. Los ciberdelincuentes colaboran muy bien entre ellos y están ahora aprovechando las nuevas tecnologías como vectores de ataque. Lo estamos viendo con ChatGPT, pero ya lo vimos hace tiempo con la llegada de los deepfakes.

El segundo aspecto que no ha mejorado es la forma en que los gobiernos protegen a la gente de las amenazas digitales, lo que implica garantizar que las leyes, las normas y los reglamentos se apliquen bien en el ciberespacio. Existe la idea errónea de que el ciberespacio no está regulado, y no es verdad. Hay muchas leyes sobre ciberseguridad, pero no se aplican correctamente. Los organismos encargados de hacer que se cumpla la ley no tienen suficientes recursos para dar una respuesta sistémica. Otra forma en que los gobiernos no contribuyen a mejorar el panorama digital es mediante los ataques de cibervigilancia. Cuando los países siguen usando sus recursos para llevar a cabo este tipo de ataques, están invirtiendo en «ciberinseguridad» a nivel global, ya que para que esa cibervigilancia funcione, tienen que existir vulnerabilidades en el ciberespacio.

El tercer aspecto es algo que vemos desde hace tiempo, pero que, por desgracia, está en auge ahora más que nunca en el contexto del conflicto de Ucrania: la involucración de los civiles en los ciberataques. Esto significa que la población civil participa en grandes ciberataques a raíz de una crisis o un conflicto concreto. Por ejemplo, hemos presenciado cómo algunos grupos delictivos rusos lanzaban ciberataques a todo aquel que estuviera en contra de los intereses de Rusia y cómo hackers voluntarios se unían al ejército informático ucraniano. Esto es muy preocupante porque implica externalizar abiertamente los ciberataques, lo que difumina los límites entre quién es civil, quién es militar y quién es el objetivo.

Con la aparición de nuevas herramientas como ChatGPT, el campo de la inteligencia artificial está experimentando un auge considerable. ¿Cómo crees que afectará esto al panorama de la ciberseguridad?

Ya en 2017, todo lo que presenciamos en relación con la tecnología deepfake fue una gran innovación de la IA. Ha pasado bastante tiempo, y ahora los grupos delictivos pueden generar contenido muy convincente y auténtico para manipular a la gente, por ejemplo, una voz o una cara conocida, o un correo electrónico bien redactado. Otro aspecto de la tecnología de IA es su uso para evaluar mejor nuestro ecosistema social a fin de crear ataques o vectores de ataque de ingeniería social muy inteligentes.

También hay otra estrategia en auge entre los grupos delictivos: los ataques generados o asistidos por IA que permiten automatizar mejor el ataque y descubrir más fácilmente la infraestructura. Desde el punto de vista defensivo, esto significa que debemos implantar herramientas de IA para protegernos mejor.

« Actualmente, el problema con esto es que el principal reto del sector de la ciberseguridad esel desgaste de los empleados: hay demasiados datos, demasiados casos y poco tiempo.

Has mencionado las ventajas de utilizar la IA en nuestra estrategia de defensa de ciberseguridad. ¿Qué retos anticipas en este sentido?

El gran riesgo que corremos es que la IA generará muchos datos que los humanos tendrán que analizar. Actualmente, el problema con esto es que el principal reto del sector de la ciberseguridad es el desgaste de los empleados: hay demasiados datos, demasiados casos y poco tiempo. Desgraciadamente, la IA no hará sino agravar este problema porque multiplicará la cantidad de datos, lo cual resulta bastante preocupante

Vectores demográficos que aumentan el éxito de la ingeniería social

Más allá de lo que los ciberdelincuentes decidan al desplegar sus artimañas, existen otras variables demográficas que parecen influir en sus porcentajes de éxito. Sorprendentemente, la edad siempre ha sido un factor decisivo en la frecuencia con la que la gente hace clic en el contenido malicioso de los correos de phishing: **los nativos digitales son un 65 % más propensos a clicar que los usuarios de más edad**. Una posible explicación de esta disparidad es que los usuarios de más edad, dada su experiencia acumulada y su comportamiento más prudente en Internet, podrían estar mejor preparados para reconocer y evitar posibles amenazas. En cambio, los nativos digitales (en este análisis, personas de entre 18 y 40 años) se fían más fácilmente de la comunicación digital al haber crecido con ella, y tienden a no cuestionar la legitimidad de aquello a lo que se enfrentan tan a fondo como sus homólogos de más edad (personas de entre 41 y 60 años).

Los usuarios más jóvenes (18 – 40 años) son un

↗ 65%

más propensos a clicar en correos de phishing que los usuarios de más edad (41 – 60).

Desde el principio, debemos considerar la probabilidad de un ciberataque en nuestra cultura y en nuestras tareas profesionales diarias.

Thomas Schumacher
Director general de Accenture Security

Sectores en el punto de mira

En lo que respecta al éxito de la ingeniería social y el phishing, también se observan variaciones entre los distintos sectores. Las industrias que se han visto muy afectadas por los últimos acontecimientos sociales, como los sectores de la logística, la energía y el turismo, registran los porcentajes más elevados de clic en mensajes de phishing. Por otra parte, entre los sectores con los porcentajes de clic más bajos se encuentran aquellos con una elevada proporción de trabajadores de primera línea, por ejemplo, la agricultura, la construcción, y los productos químicos y las materias primas.

Sector	Porcentaje de clics
Transporte y logística	38%
Energía y medio ambiente	35%
Turismo y gastronomía	35%
Farmacéutico y sanitario	33%
Comercio electrónico	32%
Educación	31%
Servicios y artesanía	29%
Finanzas, seguros y servicios inmobiliarios	28%
Tecnología y telecomunicaciones	27%
Metalurgia y electrónica	26%
Medios de comunicación y marketing	25%
Consumo y FMCG	25%
Comercio	24%
Sociedad	24%
Administración y defensa	24%
Internet	23%
Ocio	23%
Agricultura	20%
Construcción	20%
Economía y política	20%
Productos químicos y materias primas	16%

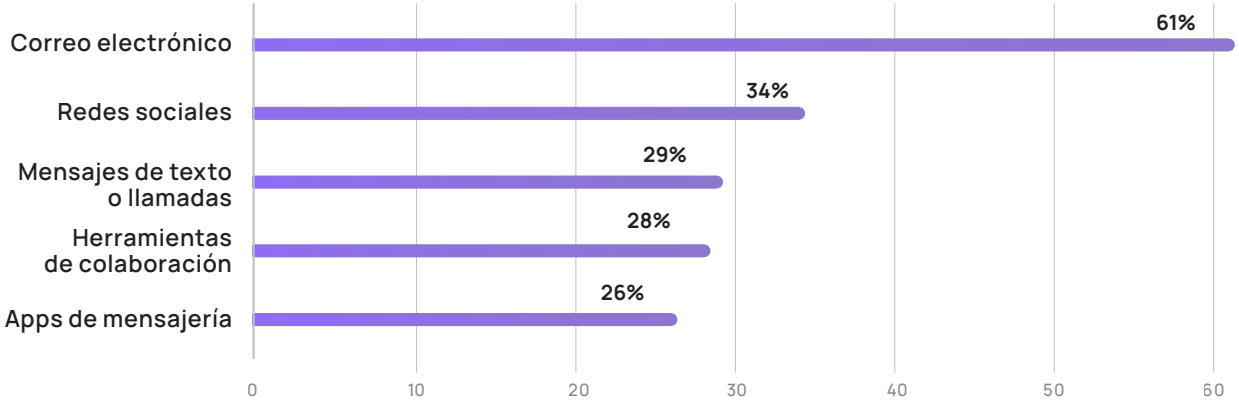
El futuro del phishing: del correo electrónico a las herramientas de colaboración y las redes sociales. ¿Qué será lo próximo?

La innovación es la mejor amiga de los ciberdelincuentes, que no solo han encontrado vectores técnicos, psicológicos o demográficos para mejorar sus ataques, sino también nuevas herramientas para perpetrarlos. Aunque los ataques por correo electrónico siguen siendo los más populares, hay otros canales que no dejan de ganar adeptos.

Poco a poco, el correo electrónico está dejando de ser el único canal de comunicación en las empresas, y lo más probable es que en los próximos años se diversifiquen otras herramientas de colaboración y comunicación, lo que supone un avance muy provechoso para los delincuentes.

De hecho, **los primeros ataques multicanal ya han provocado enormes daños**, como en el caso de Uber.[1] Los atacantes se hicieron pasar por el departamento de informática de la empresa a través de un mensaje de WhatsApp y lograron que un empleado aceptara una notificación de autenticación multifactor. En consecuencia, la empresa se vio obligada a desconectar gran parte de sus sistemas para restringir el acceso de los ciberdelincuentes a información confidencial.

Canales más usados en ciberataques a empresas en 2022



> **Cuando empezamos a trabajar con nuevos tipos de tecnología, debemos tener en cuenta los riesgos desde el principio. De lo contrario, todo terminará en un desastre.**
>
> **Thomas Tschersich**
> Director de seguridad informática de Telekom Alemania

Hoy en día, las empresas no están lo bastante protegidas frente a las estrategias de ingeniería social, que no harán sino mejorar a medida que los progresos tecnológicos se aceleran por momentos, como la IA generativa está poniendo de manifiesto. Por eso muchas organizaciones han empezado a invertir más recursos en su cultura de seguridad y ahora centran sus estrategias en las personas.

1 **WeLiveSecurity (2022).** Uber sufrió ciberataque y lograron acceso a sus sistemas.

« Una estrategia global debe incluir tres pilares: tecnología, personas y procesos.

Thomas Schumacher
Director general de Accenture Security

Thomas Schumacher es el director general de Accenture Security en Austria, Suiza y Alemania. También es miembro del ASG Leadership Team y del global Accenture Security Leadership Team. Schumacher lleva más de 20 años asesorando a grandes empresas alemanas en temas de seguridad informática e infraestructuras informáticas seguras. Es experto en proyectos de transformación complejos en diversas industrias, especialmente en el contexto de la digitalización, la integración posterior a fusiones y adquisiciones y el aumento de la eficiencia informática.

En tu opinión, ¿cuál es el aspecto más importante que deben tener en cuenta las empresas en relación con su estrategia de seguridad?

Desde mi punto de vista, el tema de la ciberseguridad y la resiliencia cibernética, como lo llamamos en Accenture, empieza en el plano estratégico. Una estrategia global debe incluir tres pilares: tecnología, personas y procesos. Las empresas deben ser capaces de responder a preguntas como «¿de qué se compone nuestro ADN?», «¿qué necesitamos para que nuestra empresa siga funcionando, pase lo que pase?» y «¿qué queremos proteger en primer lugar?». Una vez realizado este ejercicio, podemos empezar a pensar en cuál es la mejor manera de proceder. Muchas empresas siguen enfocando este proceso bastante al azar, pero esto acaba saliendo a la luz, como muy tarde, cuando se produce un ataque.

Mencionas el factor humano como uno de los aspectos de las estrategias de seguridad. ¿Qué función cumplen específicamente los empleados?

Siempre puedes decir que los empleados clicarán en algo tarde o temprano, y probablemente sea cierto, porque no podemos protegernos de todo, pero la cuestión es con qué rapidez caerán todas las barreras protectoras. Por eso hay que sincronizar las tres dimensiones: la tecnología, las personas y los procesos. Creo que no es recomendable confiar únicamente en la tecnología, porque los costes aumentan de forma desproporcionada. Todo lo que podamos abarcar a través de la concienciación y la formación de los empleados, con el apoyo de la tecnología adecuada, nos hace más resilientes como empresa. Esto se debe a que el componente humano protege a las organizaciones de todo tipo de tácticas de ataque, no solo de las diseñadas para un uso específico. Ahorramos tiempo, dinero, estrés, y evitamos más riesgos.

¿Cuál es el mayor reto en relación con el factor humano?

Creo que el mayor desafío es nuestra cultura del error. Si alguien hace clic en un correo de phishing, no queremos que piense: «Prefiero callarme y no decírselo a nadie.» Lo que realmente importa en esos casos es actuar con rapidez, avisar inmediatamente del incidente, ser conscientes de lo que está ocurriendo y de cómo manejar la situación.

¿Crees que es un factor condicionado por la cultura general de la empresa?

Hasta cierto punto, se puede comparar con la educación infantil. Yo mismo tengo un hermano mayor, y aprendí bastante pronto a negar las cosas cuando la situación se pone fea. Pero esta actitud no es muy inteligente a largo plazo, porque lo más probable es que el problema nos explote más adelante. Por eso es sumamente importante que se cree una cultura de aviso de incidentes, y decir que está bien (e incluso es bueno) que alguien notifique rápidamente un incidente que ha provocado. Esta actitud aún no es común ni está muy extendida, especialmente entre las pymes , sobre todo cuando entran en juego pérdidas económicas.

¿Cómo se puede influir positivamente en esta cultura?

Creo que lo primero que hay que subrayar de nuevo es que no podemos evitar los ciberataques ni los errores humanos. Desde el principio, debemos considerar la probabilidad de un incidente de seguridad en nuestra cultura y en nuestras tareas profesionales diarias. Además, deberíamos agilizar los canales de aviso o incluso hacerlos anónimos para que, en última instancia, las consecuencias no recaigan sobre los usuarios. Esto es más fácil en las grandes empresas, porque la conexión entre la pérdida económica y la inversión que hay que hacer es menor que en el caso de un particular.

Si hablamos de la concienciación sobre ciberseguridad, ¿crees que se está produciendo una transición de la formación y las políticas obligatorias hacia la formación continua?

Sigo viendo que muchas empresas se guían por los requisitos de cumplimiento de normativas, pero, por supuesto, cada vez son más las empresas que entienden la necesidad de formar a sus empleados. Sobre todo, en el caso de los empleados que teletrabajan, contar con conocimientos básicos de ciberseguridad aporta un gran valor añadido. Otra cosa que vemos es que algunas empresas piensan que tienen que crear sus propias soluciones de formación, cuando en realidad hoy en día hay muchas herramientas en el mercado que cubren específicamente sus necesidades.

¿Las grandes y medianas empresas enfocan de forma diferente la concienciación en materia de seguridad?

A mi modo de ver, un problema de fondo de las grandes empresas es que creen tener las cosas bajo control. Sin embargo, de nuevo, creo que esto ocurre porque el tema de la resiliencia cibernética es, de por sí, muy complejo. Quizá haya que ver más allá. Ahora mismo estamos en un momento en el que debemos protegernos de ciberataques, amenazas físicas, catástrofes naturales y una pandemia. Son demasiados riesgos de los que protegerse, y encontrar una respuesta a todos ellos es mucho más difícil que protegernos «solo» de los ciberataques. Sin embargo, la complejidad también añade otra dimensión a la ciberseguridad: debemos preparar a los empleados para situaciones completamente nuevas, como que de repente ya no puedan trabajar en las sucursales de su empresa. Tenemos que acercar la resiliencia cibernética a la resiliencia empresarial.

« Es sumamente importante que se cree una cultura de aviso de incidentes, y decir que está bien (e incluso es bueno) que alguien notifique rápidamente un incidente que ha provocado.

¿Crees que esta situación está haciendo que la formación continua de concienciación sea más necesaria?

La tecnología está evolucionando mucho, pero los ataques también. Por tanto, también debemos adaptar en cierta medida nuestros hábitos cotidianos. Es un patrón de comportamiento clásico: soy consciente de que los tiempos han cambiado, posiblemente también debido a los avances técnicos, pero yo sigo como hace 20 años. Por eso creo que debemos dejar de decirle a la gente lo que tiene que hacer y asegurarnos de que las conductas seguras se conviertan en habilidades personales. Y el motivo de hacer esto no está únicamente relacionado con el trabajo; si hoy me compro un coche y tiene la tecnología de arranque sin llave «keyless go», también tendré que aceptar que todo está interconectado y adaptar mi comportamiento en consecuencia. Así pues, debemos seguir reforzando esta idea de seguridad también en nuestra vida privada e incorporarla de forma más permanente a nuestro día a día para que todo el mundo sea capaz de cuestionar su propio comportamiento en cualquier momento.

La innovación tecnológica de la que hablas existe desde hace mucho tiempo, pero los hackers están siguiendo la ley del mínimo esfuerzo. ¿Estás de acuerdo?

Sí, los ataques a menudo son bastante simples y, sin embargo, tienen éxito, pero también vemos ataques devastadores perpetrados por atacantes que tienen tantos recursos económicos que convierten cualquier plan en realidad. Estoy bastante seguro de que el primer ordenador cuántico lo tendrá algún ciberdelincuente que lo utilice para vulnerar procedimientos criptográficos. Tenemos que ser conscientes de que algunos hackers disponen de enormes recursos, y debemos prepararnos adecuadamente.

Todo esto suena bastante intimidatorio. ¿Deberíamos también quitarle el miedo a la gente?

El miedo siempre es un mal maestro. La cuestión es más bien: ¿qué se puede hacer?, ¿cómo podemos ayudar? No es imposible; solo hay que tener unas reglas básicas de juego.

¿Cómo han evolucionado los presupuestos de ciberseguridad? ¿Se están adaptando a esta evolución?

De nuevo, tenemos que distinguir entre grandes empresas y pequeñas y medianas empresas, y depende también del sector. Las autoridades llevan desde 2014 presionando al sector financiero, es decir, bancos y aseguradoras, para que adopten iniciativas de seguridad. Han superado la fase en la que provocar miedo hace que inviertan más en ciberseguridad. Este tipo de empresas controlan y limitan mucho sus inversiones porque han aprendido a lidiar con el problema. Lo que aún no sabemos es si estos sectores están invirtiendo adecuadamente. Yo creo que no, porque se siguen centrando demasiado en comprar ciertas herramientas, y siguen creyendo que implementándolas se pueden eliminar por completo los riesgos.

Muchas empresas medianas pensaban que la resiliencia cibernética no les afectaba, pero con los ataques se han dado cuenta de que no es así. El gran peligro en este sentido es que las medidas se introduzcan al azar y se quieran resolver los problemas solo con tecnología. A menudo, estas empresas ni siquiera tienen departamentos internos de informática. Así pues, necesitamos una nueva generación de empresas que puedan evaluar los riesgos cibernéticos además de los riesgos de mercado.

Te gustaría decir algo a otros responsables de seguridad?

En primer lugar, la resiliencia cibernética es un problema social que hay que resolver. Eso significa que todos debemos trabajar juntos para encontrar una solución; cuanto más unidos trabajemos, más éxito tendremos.

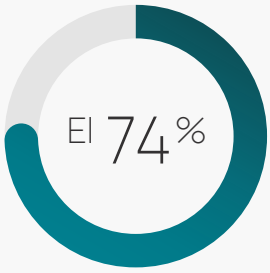
En segundo lugar, no vamos a ganar ninguna medalla por gestionar los riesgos mejor que nadie. Se trata de «sobrevivir». Quizá resulte un poco apocalíptico, pero es bastante apropiado para la situación. El peligro está ahí, y tenemos que comunicarlo con más firmeza, pero sin asustar a nadie.

La IA y la ciberdelincuencia: el impacto fulminante de la innovación tecnológica

La proliferación de innovaciones de IA está exacerbando el panorama de amenazas cibernéticas, ya que los hackers explotan estas nuevas tecnologías para crear nuevos tipos de ataques. Los deepfakes, la clonación de voz y el phishing generado con IA han irrumpido en el panorama de las amenazas digitales como armas muy potentes. Además, las herramientas de IA están democratizando la ciberdelincuencia al simplificar el proceso de elaboración de correos electrónicos y software malicioso. De forma paralela, el uso generalizado de ChatGPT plantea dudas acerca de la privacidad de los datos y del potencial uso indebido de información sensible de los usuarios.

Por otro lado, el uso de herramientas de IA podría intensificar la manipulación social y contribuir al aumento de las tensiones globales si se usan para fines poco éticos, como la desinformación y la propaganda. Los sistemas de autenticación biométrica, que considerábamos seguros, están también en el punto de mira de los hackers, ya que la IA puede ayudar a eludirlos con cierta facilidad. A medida que los ámbitos digital y geopolítico colisionan, las implicaciones de la IA en la guerra cibernética requieren un enfoque más proactivo hacia la ciberseguridad y una reevaluación de las estrategias de defensa actuales.

ChatGPT-4 ha traducido estos párrafos



de los profesionales de la ciberseguridad afirman que la inteligencia artificial empeorará los ciberataques

Deepfakes y clonación de voz: cuando la IA alimenta la ingeniería social

La tecnología del deepfake no se ha inventado ahora en 2023, pero está en boca de todos continuamente, y con razón: los hackers la están usando para la **manipulación masiva y para avivar las tensiones mundiales**. El vídeo deepfake de Zelenski que circuló en 2022 en el que anunciaba la rendición de Ucrania es uno de tantos ejemplos.[1]

La tecnología del deepfake no se utiliza solo con fines políticos; también se ha visto en ataques sofisticados que combinan vishing y clonación de voz para robar datos y dinero tanto a particulares como a empresas. Hace poco, en Arizona, una madre llegó a creer que su hija de 15 años había sido secuestrada al escuchar por teléfono sus desesperados gritos de auxilio. Afortunadamente la madre acabó sabiendo que su hija estaba a salvo y que su voz había sido replicada con inteligencia artificial. Sin embargo, lo más significativo del caso es que la madre aseguró que nunca dudó de la autenticidad de la voz de su hija.[2] En otro caso, unos ciberdelincuentes se hicieron pasar por el CEO de una empresa con un deepfake de audio y convencieron a un empleado para que transfiriera 35 millones de dólares a un grupo de estafadores.[3] Esta tecnología **se está volviendo incluso más sofisticada** con herramientas como VALL-E de Microsoft, que puede replicar cualquier voz con solo escuchar tres segundos de una grabación.[4]

A medida que las organizaciones de todo el mundo van adoptando progresivamente la autenticación biométrica como una alternativa potencialmente más segura que las contraseñas y los PIN, crece la preocupación por el uso de la clonación de voz y de los vídeos deepfakes, pues podrían sortear estos nuevos métodos de autenticación. Tanto es así, que en algunas regiones de Estados Unidos se ha prohibido el software de reconocimiento facial para uso gubernamental.[5] A medida que la tecnología del deepfake evolucione y se conozcan nuevos usos, **tanto el sector público como el privado** tendrán que colaborar para concienciar sobre las posibilidades y limitaciones que ofrece esta tecnología.

Explotando la IA generativa: ChatGPT como atacante

Con la llegada de nuevas herramientas de IA, los ciberdelincuentes están aprendiendo cómo exprimir su potencial para perfeccionar y ampliar aún más sus tácticas de ataque más eficaces, especialmente la ingeniería social. Aunque las herramientas de IA generativa como ChatGPT prohíben explícitamente los usos fraudulentos,

1 **El Confidencial (2022).** El primer 'deep fake' usado en un conflicto armado muestra a Zelenski rindiéndose.

2 **La Opinión (2023).** Utilizan voz recreada por inteligencia artificial para fingir el secuestro de una niña y pedir rescate.

3 **La Vanguardia (2021).** Roban 35 millones de dólares clonando la voz de un director con inteligencia artificial.

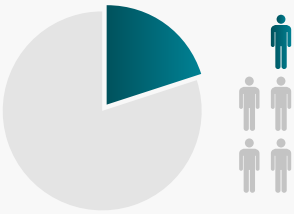
4 **MuyComputerPRO (2023).** VALL-E, la IA de Microsoft capaz de imitar voces.

5 **El País (2019).** San Francisco, primera ciudad en prohibir la tecnología de reconocimiento facial en EE UU.

los hackers han encontrado muchas formas de eludir las restricciones.

Los correos de phishing generados por ChatGPT y otras herramientas de IA generativa están bien diseñados y redactados, por lo que resultan **menos sospechosos** que los intentos tradicionales de phishing masivo. Esto significa que **cada vez es más difícil detectarlos, tanto para los filtros de spam como para las personas**.

Un estudio reciente del equipo de ingeniería social de SoSafe muestra que, con herramientas de IA generativa, los hackers pueden redactar correos de phishing al menos un 40 % más rápido. Y lo que es más significativo: los datos, tomados de la plataforma SoSafe Awareness que evaluó de forma anónima unas 1500 simulaciones de phishing en marzo de 2023, revelaron que el 78 % de los usuarios abrieron los correos de phishing generados por IA. De este porcentaje, uno de cada cinco hizo clic en contenidos maliciosos, como enlaces o archivos adjuntos.[6] Y esto es solo el principio: en la prueba se utilizaron correos de phishing no personalizados escritos por ChatGPT-3.5. Sin embargo, casi a diario aparecen nuevas herramientas de IA basadas en modelos de lenguaje mejorados, y el paso de ChatGPT-3 a ChatGPT-4 ya ha marcado un antes y un después en el ámbito de la personalización de correos de phishing.



1 de cada 5

personas hace clic en correos de phishing generados por IA

Sin embargo, el phishing es solo una de las muchas tácticas que los hackers han conseguido perfeccionar mediante la IA. Con esta tecnología, cualquier persona con unos conocimientos informáticos mínimos puede generar código malicioso «polimórfico» capaz de sortear los mecanismos de seguridad tradicionales.[7] Estas herramientas se convierten, pues, en armas muy poderosas al alcance de cualquiera, democratizando así la ciberdelincuencia.

Los mecanismos que impiden que ChatGPT genere código malicioso solo funcionan si el modelo entiende lo que está haciendo. Si las instrucciones se dividen en pasos individuales, es sencillo eludir estas medidas de seguridad.

EUROPOL [8]

6 **SoSafe (2023).** One in five people click on AI-generated phishing emails, SoSafe data reveals.

7 **IT Digital Security (2023).** ChatGPT podría utilizarse para crear malware polimórfico altamente complejo.

8 **EUROPOL (2023).** ChatGPT The impact of Large Language Models on Law Enforcement.

9 **elEconomista.es (2023).** OpenAI reconoce un fallo en ChatGPT que filtró los datos y métodos de pago de los usuarios.

10 **El País (2023).** Italia bloquea el uso de ChatGPT por incumplir la normativa de protección de datos.

11 **World Economic Forum (2023).** Por qué el diseño de la inteligencia artificial debe priorizar la privacidad de los datos.

12 **Xataka (2023).** OpenAI ha usado millones de textos para entrenar a ChatGPT. El problema es que muchos de ellos tienen copyright.

ChatGPT: ¿es seguro usarlo?

Las herramientas de IA requieren una cantidad ingente de datos para funcionar de forma efectiva. Inevitablemente, esto suscita preocupación entre usuarios y organizaciones, que dudan de la privacidad y seguridad de los datos que introducen en la herramienta.

¿Cuáles son los riesgos?

Almacenar cantidades masivas de datos en grandes servidores no está exento de riesgos. A principios de este año, un error relativamente sencillo en ChatGPT permitió a muchos usuarios leer los chats de otros, o incluso sus números de teléfono y correos electrónicos.[9] Este incidente no ha hecho sino agravar los problemas existentes en torno al almacenamiento y uso de datos confidenciales por parte de OpenAI. Tanto es así, que Italia prohibió temporalmente ChatGPT, alegando una falta de justificación legal para recopilar datos sensibles de usuarios para el entrenamiento de su algoritmo y poniendo de manifiesto problemas de incumplimiento del RGPD.[10]

Otros ataques, que utilizan métodos como la ingeniería inversa para extraer datos confidenciales de los usuarios a partir del chat, podrían suponer graves consecuencias y dar lugar a filtraciones masivas de datos.[11] Además, los expertos advierten de que estas herramientas se podrían piratear para alterar sus resultados con fines de desinformación o manipulación social, especialmente en el contexto de las crisis mundiales que estamos viviendo.

El contenido que genera ChatGPT también puede entrar en conflicto con las leyes de propiedad intelectual y de derechos de autor. Aunque las condiciones de uso de OpenAI atribuyen al usuario la autoría de los resultados y aseguran que el contenido que genera la herramienta es original (aunque no necesariamente único), las respuestas que proporciona pueden proceder de contenido que esté sujeto a derechos de autor de terceros.[12]

¿Qué podemos hacer?

Aunque se trate de una tecnología reciente, organizaciones como la Unión Europea ya están aprobando nuevas leyes y regulando los aspectos legales de la utilización de herramientas de IA. Ahora bien, los usuarios también pueden protegerse siguiendo algunas recomendaciones:

- **No introduzcas nunca información sensible, ni personal ni profesional.** Se podrían recopilar estos datos para posteriores análisis o mejoras de la herramienta o quedar expuestos en caso de filtración de datos.
- **Comprueba siempre la veracidad de los resultados.** La IA no es perfecta y puede hacer suposiciones falsas o haber aprendido de fuentes engañosasn.
- **Pide asesoramiento jurídico antes de utilizar el producto con fines comerciales.** Es conveniente asegurarse de no estar infringiendo ninguna ley ni derecho intelectual.

El potencial oculto de las nuevas tecnologías en la ciberdelincuencia

No cabe duda de que la tecnología avanza a un ritmo vertiginoso y, con ella, las posibles aplicaciones de la IA al mundo de la ciberdelincuencia. Sin embargo, si bien ya se han visto algunos casos de ataques sofisticados, **los hackers aún no han aprovechado todo el potencial de estas herramientas en ataques a gran escala**. Mientras los métodos convencionales como el phishing masivo o el spear phishing sigan siendo capaces de abrir una brecha en las líneas de defensa humana y de infiltrarse en los sistemas, es poco probable que los ciberdelincuentes dediquen el tiempo y los recursos que se necesitan para orquestar ataques aún más sofisticados. No obstante, a medida que las herramientas de IA siguen mejorando e incrementando el alcance y el éxito de los ciberataques más comunes, la ciberdelincuencia se democratiza y la amenaza de los ciberataques crece más que nunca, tanto para las organizaciones como para los usuarios.

> Los ciberdelincuentes disponen desde hace tiempo de tecnologías muy avanzadas, como la clonación de voz. Sin embargo, no hemos visto ataques de ingeniería social sofisticados en casos reales a gran escala. Uno de los motivos posibles es que lo sencillo sigue funcionando. Ahora bien, es muy probable que esto cambie con las filtraciones de potentes modelos de lenguaje y el desarrollo exponencial de la IA generativa en todos los ámbitos.
>
> **Dr. Niklas Hellemann**
> CEO de SoSafe

Fortalecer la línea de defensa humana contra los ciberataques con IA

La IA se utiliza desde hace tiempo en ciberseguridad para ayudar a los profesionales en infinidad de tareas, como la predicción y detección de ataques y la respuesta automatizada a incidentes de seguridad. Sin embargo, los avances recientes en herramientas de IA generativa han permitido a los atacantes utilizar la misma tecnología con fines poco éticos, transformando el panorama de los ciberataques y **democratizando la ciberdelincuencia**. A medida que surgen posibles nuevos usos fraudulentos de la IA, las fuerzas de seguridad, las instituciones internacionales y las empresas de herramientas de IA doblan sus esfuerzos para evitar que los hackers utilicen esta tecnología como vector de ataque.

Pero hecha la ley, hecha la trampa, y los hackers no paran de idear nuevas formas de atacar a sus víctimas. Si queremos evitar graves consecuencias, los equipos de ciberseguridad deberán adoptar nuevas estrategias para adaptarse a un panorama de amenazas digitales que está en constante cambio, y en el que ahora entra en juego la IA. A medida que se hace cada vez más difícil detectar las amenazas mediante controles de seguridad técnicos, se hace imprescindible una cultura de seguridad sólida que fomente la concienciación y refuerce el componente humano.

> Aunque la tecnología siempre esté avanzando y aliviándonos la carga de trabajo en lo que a seguridad se refiere, el riesgo humano sigue presente y, por lo tanto, debemos asegurarnos de que nuestro cortafuegos humano esté bien configurado.
>
> **Stefanie Boem**
> Responsable de protección de datos de Sport-Thieme

Una nueva era de amenazas digitales: la profesionalización de la ciberdelincuencia

El auge de las herramientas de IA generativa no solo ha democratizado la ciberdelincuencia, sino que también ha **impulsado su creciente profesionalización**. Además, los ciberdelincuentes se han sumado a las tendencias de la ciberdelincuencia como servicio (CaaS) para profesionalizar aún más sus modelos de negocio. La conjunción de estos factores ha creado un caldo de cultivo fértil para que colaboren, innoven y lancen ataques contra organizaciones vulnerables.

Concretamente, el **ransomware** se ha convertido en un componente clave en el ámbito de la CaaS. Desde su aparición a finales de la década de los 80, **ha seguido siendo uno de los principales métodos de ciberataque**, provocando el miedo tanto de empresas como de particulares.

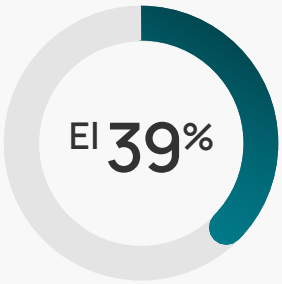
Nuestra encuesta también lo corrobora: el ransomware sigue siendo uno de los tipos de ciberataque más comunes, ya que 1 de cada 3 empresas que sufrieron un ciberataque en los últimos 3 años fue víctima de este tipo de malware. Es más, entre las víctimas de ransomware, un alarmante porcentaje, el 39 %, admitió haber pagado el rescate exigido. Además, casi la mitad de las empresas pequeñas se vieron obligadas a pagar.

Sin embargo, es en los últimos años cuando el ransomware ha experimentado su mayor transformación: la eclosión del ransomware como servicio (RaaS) en la última década y su continuo crecimiento ilustran cómo los ciberdelincuentes están adaptando y diversificando sus estrategias de negocio para potenciar aún más sus actividades delictivas.

> **El ransomware es uno de los pocos ciberdelitos que precisa que la víctima sea cómplice. Al sufrir un ataque de ransomware, la víctima debe tomar decisiones complicadas que tienen un impacto psicológico, como pagar el rescate o denunciar el ataque.**
>
> **Stéphane Duguin**
> CEO del CyberPeace Institute

El **31%**

de las empresas que sufrieron un ciberataque en los últimos 3 años fueron víctimas de ransomware



de ellas admitió haber pagado el rescate

El ransomware como servicio es una pandemia que se expande a empresas de todo el mundo

Hoy en día, **no es necesario tener grandes habilidades de piratería o unos conocimientos informáticos avanzados** para perpetrar ataques de ransomware. Tal y como demostraron las filtraciones de Conti[1],basta con navegar por la dark web y realizar un pago en criptomonedas para acceder a plataformas de ransomware como servicio (RaaS) con modelos de suscripción y atención al cliente personalizada. Un reciente estudio de IBM indica que un ataque de ransomware fructífero cuesta a las empresas, de media, la friolera de 4,54 millones de dólares (sin incluir el rescate)[2], lo que indica que sus efectos económicos siguen causando estragos en las empresas. Además, la facilidad de acceso a estas plataformas de RaaS ha aumentado de manera exponencial el número de posibles ciberdelincuentes.

4,54 M de dólares

Coste medio por ataque de ransomware en una empresa (sin incluir el rescate)

Fuente: IBM [2]

La conocida operación RaaS de REvil lo ilustra perfectamente. Esta banda de hackers sacudió el mundo empresarial en 2021 con un ataque masivo a la cadena de suministro del proveedor de software Kaseya, afectando a miles de organizaciones de todo el mundo. El incidente se saldó con una petición de rescate inaudita de 70 millones de dólares, la mayor hasta la fecha.[3] Aunque Kaseya optó por no pagar, otras de las grandes organizaciones que fueron víctimas de RaaS, como la aseguradora CNA Financial y el productor cárnico brasileño JBS, fueron noticia por pagar algunos de los rescates más elevados de la historia, por valor de 40 y 11 millones de dólares, respectivamente.[4]

1 **WeLiveSecurity (2021).** Ransomware Conti: principales características y cómo operan sus afiliados.

2 **IBM (2022).** Coste de la vulneración de datos 2022. Una carrera de millones de dólares para detectar y reaccionar.

3 **IT Digital Security (2021).** Los autores del ataque a Kaseya piden rescates que alcanzan los 5 millones de dólares.

4 **Ciberseguridad (2021).** Los 15 ciberataques más importantes en 2021.

Los 10 rescates más altos pagados por las empresas

Organización	Rescate	Tipo de ransomware	Origen
CNA Financial	40 000 000 $	Phoenix	Rusia
JBS	11 000 000 $	REvil/Sodinokibi	Rusia
CWT	4 500 000 $	Ragnar Locker	N/D
Brenntag	4 400 000 $	DarkSide	Europa del Este
Colonial Pipeline	4 400 000 $	DarkSide	Europa del Este
Travelex	2 300 000 $	REvil/Sodinokibi	Rusia
UCSF	1 140 895 $	Netwalker Ransomware	N/D
BRB Bank	957 245 $	LockBit	Europa del Este
Condado de Jackson, Georgia	400 000 $	Sam Sam	Irán
Universidad de Maastricht	218 000 $	Ransomware Ciop	Rusia

Fuente: Immunefi [5]

El grupo de RaaS HIVE también acaparó titulares el año pasado por sus ciberataques a gran escala. Además de atacar a grandes multinacionales del sector informático y petrolero, HIVE puso en peligro los datos y sistemas informáticos de organizaciones sanitarias y públicas. Desde junio de 2021, los ataques de HIVE han afectado a más de 1500 empresas en 80 países, lo que ha supuesto a sus víctimas un desembolso de casi 100 millones de euros en rescates.[6]

Un nuevo protagonista, el ransomware Sugar, fue detectado por primera vez por el equipo de seguridad de Walmart en noviembre de 2021 y está pensado para atacar dispositivos individuales y pequeñas empresas en lugar de grandes redes corporativas.[7] Al cambiar su enfoque y pasar a pedir rescates más bajos, estos ciberdelincuentes pueden atacar a una variedad más amplia de víctimas y a la vez pasar más desapercibidos ante las fuerzas de seguridad. Esto demuestra cómo son capaces de forjar alianzas, aunar recursos y aprender unos de otros con el objetivo de diseñar ataques más coordinados y eficaces.

Crear alianzas en una red global compleja

El ataque a Kaseya muestra el gran poder del ransomware como servicio, pero también nos hace ver cómo la profesionalización de la ciberdelincuencia ha provocado un **aumento espectacular de la escala, el impacto y la complejidad de los ataques a la cadena de suministro**, lo que deja a las

5 **Immunefi (2023).** Top Crypto Ransomware Payments Report.

6 **CSO ComputerWorld (2023).** El FBI desmantela al grupo de 'ransomware' Hive.

7 **La Razón (2022).** Sugar, el 'ransomware' dirigido a particulares y pequeñas empresas que pide rescates de baja cuantía.

empresas expuestas en un panorama digital interconectado. En el ataque, los ciberdelincuentes tenían como objetivo el software VSA de la empresa, una herramienta de control remoto utilizada para supervisar y proveer servicios informáticos de los clientes.[8] Al infiltrarse en este software, los atacantes lograron vulnerar simultáneamente los sistemas de miles de empresas que utilizaban los servicios de Kaseya, lo que nos recuerda de nuevo hasta qué punto **nuestra seguridad depende de la seguridad de los demás**.

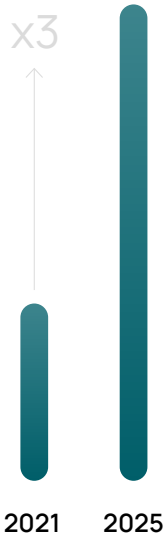
8 de cada 10

profesionales de la ciberseguridad afirman que la seguridad de su organización **depende cada vez más de la de sus socios**.

En los ataques a la cadena de suministro, los ciberdelincuentes tienden a explotar los eslabones más débiles, a menudo proveedores o prestadores de servicios más pequeños y menos seguros, para atacar a su objetivo principal. Un claro ejemplo de este modus operandi ocurrió a principios de este año, cuando Nissan Norteamérica anunció que uno de sus proveedores de desarrollo de software había sufrido una filtración de datos que expuso los nombres y las fechas de nacimiento de miles de clientes de Nissan.[9]

Un reciente ataque contra la app 3CX Desktop también muestra el enorme alcance que pueden tener los ataques contra las cadenas de suministro digitales. 3CX es el desarrollador de un sistema telefónico basado en software utilizado por más de 600 000 organizaciones en todo el mundo, entre ellas BMW y Pepsi.[10] Siguiendo el ejemplo de SolarWinds, los atacantes infectaron los archivos instaladores de 3CXDesktopApp con troyanos para distribuir entre las redes de sus clientes un tipo de malware que les permitió recopilar información de sus sistemas y robar datos de los principales navegadores.

No hay indicios de que esta tendencia vaya a remitir pronto. De hecho, Gartner prevé que para 2025, el 45 % de las organizaciones de todo el mundo habrá sufrido ataques a la cadena de suministro digital, lo que supone triplicar la cifra de 2021.[11]



El 45 %

de las organizaciones habrá sufrido ataques a sus cadenas de suministro digitales de aquí a 2025

Fuente: Gartner [11]

Ahora que las organizaciones dependen cada vez más de servicios y software de terceros para seguir el ritmo de un panorama digital que está en constante evolución, es vital que refuercen sus estrategias de seguridad para protegerse ante los complejos obstáculos que presentan las cadenas de suministro digitales de hoy en día.

8 **IT Digital Security (2021).** Un ataque contra el proveedor de TI Kaseya afecta a más de mil empresas.

9 **Escudo Digital (2023).** Nissan Norteamérica sufre un problema de seguridad y expone los datos de 18.000 clientes.

10 **MuyComputerPRO (2023).** Un nuevo malware ataca a la cadena de suministro de 3CX Desktop App.

11 **Gartner (2022).** Las 7 principales tendencias en ciberseguridad para 2022.

Cuando empezamos a trabajar con nuevos tipos de tecnología, debemos tener en cuenta los riesgos desde el principio. De lo contrario, todo terminará en un desastre.

Thomas Tschersich
Director de seguridad informática de Telekom Alemania y CEO de Telekom Security

Thomas Tschersich es director de seguridad informática de Telekom Alemania y CEO de Telekom Security. Se encarga de la ciberseguridad y de otras tareas de seguridad operacional en Telekom. Es licenciado en ingeniería eléctrica y presidente de la junta directiva de la iniciativa alemana de seguridad en Internet Deutschland sicher im Netz. Además de las numerosas funciones de asesoramiento que desempeña, es miembro del Consejo alemán de ciberseguridad y del Consejo asesor de UP KRITIS.

¿Crees que las empresas interpretan bien la ciberseguridad y configuran adecuadamente sus estrategias?

La seguridad tiene mucho que ver con la actitud. Muchos equipos de ciberseguridad prohíben por completo o complican innecesariamente las cosas, pero creo que hay que encontrar un punto medio entre la seguridad y la comodidad, porque si no se tiene en cuenta la importancia de esta última, los usuarios encontrarán una manera de sortear las medidas de seguridad.

¿Puedes poner algún ejemplo?

Lo podemos ver en todo tipo de ámbitos. Si obligas a los usuarios a cambiar todo el tiempo su contraseña, esta será cada vez más débil. Y aunque se les obligue a establecer una autenticación multifactor para sus cuentas, no tardarán en aparecer problemas como la «fatiga de MFA», en la que los ciberdelincuentes bombardean al usuario con notificaciones de autenticación hasta que este se cansa y finalmente confirma. Si se prohíben los dispositivos USB, la gente podría enviar archivos confidenciales a su cuenta personal de correo electrónico para copiarlos desde allí. Esto nos lleva a preguntarnos si es mejor guardar el archivo en una memoria USB protegida y supervisada o en una cuenta personal.

Estoy firmemente convencido de que las medidas de seguridad deben ser transparentes y comprensibles. Si la gente entiende por qué se aplican determinadas medidas y procesos, la motivación para acatarlos es mucho mayor. Si no lo entienden, les resultará más molesto y tratarán de encontrar la manera de eludirlos.

Muchas empresas tratan desde hace tiempo las políticas de seguridad como una lista de tareas. ¿Crees que debemos seguir usándolas hoy en día?

Cuando empecé a trabajar en Telekom, también me encargaba de las políticas. Ahora bromeo con que yo me dedicaba a escribir políticas y 200 000 compañeros a ignorarlas. Por supuesto, hay que poner por escrito ciertas cosas para cumplir con ciertas normativas, pero nunca he conseguido nada solo con políticas y nunca he oído que ningún hacker se haya amedrentado por la política de seguridad de una empresa.

Creo que limitarse al ámbito legal es uno de los mayores errores que podemos cometer en materia de seguridad. Cumplir la certificación ISO-27001, por ejemplo, no nos hace seguros, solo demuestra que somos capaces de serlo. No podemos escudarnos en estas normativas y certificaciones.

¿En qué debemos basarnos entonces?

La practicidad es más importante para mí, incluyendo medidas como la gestión de parches, que me permite subsanar rápidamente cualquier vulnerabilidad. Tenemos pocas políticas y las utilizamos para describir nuestros requisitos generales de seguridad, lo cual nos ahorra tiempo que podemos invertir en aplicar las medidas. Determinamos nuestras necesidades de seguridad en nuestro proceso de evaluación de la privacidad y la seguridad, y adoptamos inmediatamente las medidas técnicas y organizativas apropiadas. Este enfoque es mucho más eficaz y corta de raíz los problemas de seguridad.

¿Qué consejos darías a las organizaciones para que diseñen una buena estrategia de seguridad?

Muchas empresas no tienen una estrategia de seguridad porque temen lo compleja que pueda resultar. Soy un firme defensor de encontrar soluciones sencillas y rápidas, por lo que mostramos a esas empresas que en la elaboración de una estrategia de seguridad intervienen muchos pequeños pasos. Empecemos actualizando el software de la empresa para partir de una buena base. A continuación, invirtamos en medidas técnicas de defensa para protegernos mejor, como antivirus y detección y respuesta de endpoints. Luego viene la concienciación de los empleados, que, en realidad, es algo que debería no terminar nunca.

¿Cómo pueden las empresas mejorar la concienciación de sus empleados en materia de ciberseguridad?

La concienciación sobre ciberseguridad antes era sinónimo de formación en línea. Para mí, eso significa pasar de pantalla en pantalla rápidamente y responder a unas pocas preguntas. Este tipo de formación daba una imagen negativa de lo que significa la ciberseguridad, y más que enriquecedor, era molesto para los empleados.

¿Cómo podemos hacer que sea más eficaz?

La concienciación en materia de seguridad debe ser amena y ofrecer a los empleados un beneficio secundario al aplicarla también a su vida personal. De esta manera, verán la ciberseguridad como una ayuda, y adaptarán su comportamiento en consecuencia. Es especialmente importante que el aprendizaje sea directo y contextualizado para aprovechar el momento en que la atención más alta y el aprendizaje es más efectivo. Por ejemplo, cuando hacemos simulaciones de ataques de phishing, estas no sirven de nada si los usuarios no reciben información de los resultados hasta varias semanas después. Necesitan esa información en el momento óptimo para el aprendizaje, que es a medida que se desarrolla la simulación.

« Los ataques se han vuelto tremendamente sofisticados, y eso es peligroso.

Estamos presenciando la aparición de nuevos métodos de ataque y tendencias en el ámbito de la ciberseguridad. ¿Qué opinas de esto?

Siempre he sido reacio a usar la palabra «tendencia». Antes, el término de moda era «blockchain», y antes de eso, «la nube». No deberíamos dejarnos llevar siempre por estas modas. Creo que el mayor problema es que no nos estamos ocupando de lo básico.

Hay muchos temas que afectan a la ciberseguridad: el robo de identidad (mediante phishing o ataques de fraude del CEO), los ataques de denegación de servicio distribuidos y el ransomware. Estos son los principales vectores de los que tenemos que hablar actualmente. Además, no mantener el software actualizado suele ser una de las causas fundamentales. Luego está la concienciación. Haces clic en un archivo por curiosidad o porque quieres ayudar a alguien, y abres la caja de Pandora. Los ataques se han vuelto tremendamente sofisticados, y eso es peligroso. Antes, al detectar una errata o un texto generado por una máquina, sabíamos inmediatamente que no se trataba de un correo genuino. Hace ya tiempo que esto quedó atrás y que los correos de phishing no son reconocibles a primera vista.

La inteligencia artificial, en concreto el Machine Learning, se utiliza desde hace tiempo como medida de defensa. Ahora estamos viendo cómo la IA generativa facilita nuevos tipos de ataques, entre otros los de clonación de voz. ¿Has visto este tipo de ataques en el mundo real?

Hemos visto cómo se han manipulado voces en ataques de fraude del CEO. El mayor reto reside en que todos estamos acostumbrados a las videoconferencias, y esta nueva tecnología permite que participantes ficticios se cuelen en estas llamadas. Por eso, en el futuro tendremos que adoptar una perspectiva diferente de las «identidades digitales». Necesitamos una «identidad para todo», por así decirlo, para servicios, máquinas, etc.

¿Estás observando un cambio en la forma de ver la seguridad en el nivel ejecutivo?

Un cambio de percepción, sí, pero no necesariamente un cambio de comportamiento. Aunque la seguridad siga siendo uno de los principales temas de debate en cualquier reunión con clientes, sigo escuchando: «Si no está roto, no lo arregles». Sin embargo, cuando se produce un ataque, las consecuencias pueden ser muy graves.

Al final, la prevención es siempre la mejor opción. ¿Es esto aún más cierto para las empresas que ya hayan sufrido algún ataque en el pasado?

Por desgracia, el hecho de haber sido víctima de un ciberataque suele tener únicamente efectos a corto plazo. Después de un ataque, los departamentos suelen analizarlo y elaborar un plan de acción, pero una vez que el plan se concreta y se presupuesta en varios millones de euros, el ataque queda demasiado lejos y ya no se recuerdan las consecuencias. Esto hace que se acabe decidiendo no invertir esa cantidad de dinero en ciberseguridad. Esta situación es muy frecuente en las pequeñas empresas. En las más grandes, la concienciación es distinta, pero estas cuentan con equipos enteros dedicados a eso.

A menudo se ve la ciberseguridad como un conjunto de costes indirectos que no afectan a la productividad. No obstante, si hay un fallo de seguridad, los costes indirectos se pueden transformar rápidamente en directos. Los daños a largo plazo pueden ser inmensos.

¿Qué tecnologías recomendarías a otros directores de seguridad informática?

La nube ha cambiado el mundo de forma radical. Antes, la ciberseguridad estaba garantizada por la integridad de la red, pero esto ya no es así. Por otro lado, Amazon y Microsoft ofrecen cortafuegos. Esto significa que debemos centrarnos en la gestión de identidades, el cifrado y la gestión de derechos. La tendencia de trabajar desde cualquier lugar también confiere más importancia al endpoint. Siempre debemos poder comprobar el grado de fiabilidad de un dispositivo en un momento dado, lo que requiere una combinación de soluciones de detección y respuesta (EDR) y acceso condicional. Por último, pero no por ello menos importante, la infraestructura debe parchearse y supervisarse con regularidad. Las medidas de concienciación permiten a las empresas tachar estas medidas técnicas de su lista, de modo que puedan centrarse en problemas específicos y formar a los empleados con la periodicidad adecuada y de un modo más relevante para ellos.

> « A menudo escuchamos: “Si no está roto, no lo arregles”; pero cuando se produce un ataque, las consecuencias pueden ser muy graves.

Thomas Tschersich
Director de seguridad informática de Telekom Alemania

Desgaste y escasez de personal: el mayor temor de los equipos de seguridad ante el panorama digital actual

En un momento en el que los ciberdelincuentes profesionalizan sus modelos de negocio e innovan constantemente, no es de extrañar que la excesiva carga de trabajo y el desgaste —o burnout— lleven a muchos profesionales de la seguridad a dejar sus puestos. Un estudio de la Asociación de Auditoría y Control de Sistemas de Información (ISACA) reveló que, en 2022, **al 60 % de las organizaciones les costaba retener a sus profesionales de ciberseguridad**. El estudio apuntaba a un alto nivel de estrés en el trabajo como una de las principales razones para irse de la empresa [1]. Esta situación se ve agravada por la escasez de 3,5 millones de trabajadores que sufre actualmente el sector de la ciberseguridad [2].

3,5 millones

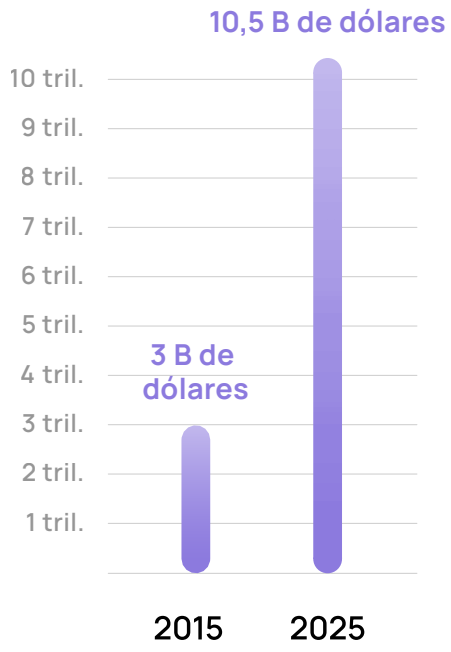
de puestos sin cubrir en el sector de la ciberseguridad

Fuente: Chartered Institute of Information Security (Instituto Colegiado de Seguridad de la Información) [2]

1 **ISACA (2022).** State of cybersecurity 2022: cyber workforce challenges.

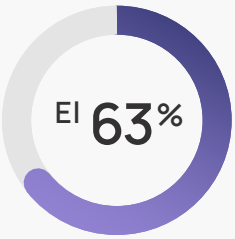
2 **Chartered Institute of Information Security (2022).** The security profession 2021/2022.

En consecuencia, al resto de profesionales de la ciberseguridad les resulta cada vez más difícil seguir el ritmo de la vertiginosa evolución de la ciberdelincuencia, un sector mundial cuyos costes se prevé que alcancen los 10,5 billones de dólares anuales en 2025, frente a los 3 billones de 2015 [3].



Fuente: Cybersecurity Ventures [3]

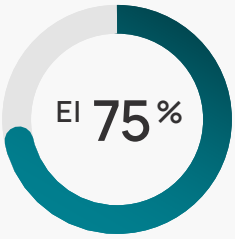
En los capítulos anteriores ya hemos visto cómo los ciberdelincuentes desarrollan constantemente nuevas estrategias y explotan las últimas tecnologías, lo que pone aún más a prueba los limitados recursos de unos equipos de seguridad ya sobrecargados de trabajo. Esto crea un círculo vicioso en el que la falta de personal contribuye al desgaste, lo que a su vez recrudece la ardua batalla que el sector está librando contra las amenazas del panorama digital actual.



de los expertos en ciberseguridad afirma sentirse estresados por el aumento de las amenazas digitales

Los modelos de trabajo híbridos ponen a prueba a los equipos de seguridad

Aunque algunos empleados están ahora volviendo al trabajo presencial tras dos años de teletrabajo, el modelo de trabajo híbrido sigue en alza, y cada vez son más las organizaciones que adoptan este enfoque de trabajo, más flexible que los tradicionales. Sin embargo, la comodidad y rentabilidad del modelo de trabajo híbrido van acompañadas de un elevado riesgo de amenazas digitales.



de los expertos en seguridad creen que el teletrabajo/trabajo híbrido aumenta el riesgo de ciberataques

3 **Security Magazine (2023).** One of the biggest threats of a cybersecurity team? Employee burnout.

Algunos de los factores clave que contribuyen a este riesgo tan elevado son:

- **Vulnerabilidades en las redes domésticas.**

  Las redes wifi domésticas suelen ser menos seguras que las profesionales y facilitan el acceso a datos sensibles a los ciberdelincuentes. Algunos de los motivos son una encriptación menos segura, el uso de las configuraciones por defecto y la falta de actualizaciones periódicas.

- **Conexión a redes públicas no seguras.**

  Los empleados que trabajan en remoto son más propensos a trabajar mientras se desplazan. Por ejemplo, pueden atender sus últimas llamadas del día en un tren usando la red pública, lo que aumenta considerablemente los riesgos cibernéticos.

- **Sobrecarga cognitiva.**

  Las interacciones virtuales sobrecargan nuestra mente, reducen la concentración y aumentan la eficacia de las estafas de phishing. Los ciberdelincuentes aprovechan esta circunstancia para atacar cuando los trabajadores bajan la guardia, por ejemplo, al final de la jornada laboral [4].

- **Mayor uso de herramientas de colaboración.**

  El teletrabajo a menudo implica una mayor dependencia de herramientas como Microsoft Teams, lo que ofrece nuevos canales que los ciberdelincuentes pueden explotar.

- **Formación insuficiente del personal.**

  El rápido cambio a modelos de trabajo híbridos ha hecho que algunos empleados hayan cambiado a esta modalidad sin disponer de la suficiente formación en ciberseguridad.

> Cuando trabajan desde casa, al ser un entorno más relajado, muchos usuarios no se concentran igual. Intercalan muchas tareas personales en su flujo de trabajo, lo que se traduce en una falta de atención.
>
> **Dr. Stefan Lüders**
> Director de seguridad informática del CERN

El resultado: el burnout como nuevo vector de ataque favorito

La combinación de estrés, falta de personal y aumento de la superficie de ataque debido a los nuevos modelos de trabajo crea un entorno propicio para los ciberdelincuentes, que **se aprovechan de que los expertos en ciberseguridad están agotados** y son más propensos a pasar por alto detalles y a tener dificultades para resolver los problemas con eficacia [5].

> 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 **VentureBeat (2022).** Why hybrid work is leading to cybersecurity mistakes.

5 **Security Magazine (2023).** One of the biggest threats of a cybersecurity team? Employee burnout.

Según nuestra encuesta, además de tener que garantizar la protección de otros departamentos de la empresa y atajar rápidamente los ataques dirigidos contra ella, los equipos de seguridad son también uno de los departamentos con mayor riesgo de sufrir un ciberataque.

Los 3 departamentos con mayor riesgo de sufrir un ciberataque

1. Informática
2. Finanzas
3. Seguridad

Conscientes de las vulnerabilidades que surgen cuando los equipos de seguridad padecen estrés, los ciberdelincuentes usan el burnout como un nuevo vector de ataque y tienden a **dirigir sus esfuerzos específicamente hacia organizaciones con equipos que parecen más susceptibles** desde fuera.

Esto pone de relieve la necesidad de que las empresas inviertan (también económicamente) en la retención de empleados, en los recursos adecuados y en formación continua para capacitar a sus profesionales de seguridad y fomentar una cultura de seguridad resiliente, capaz de sortear con eficacia un panorama digital muy complejo.

« Es importante que las estrategias de cibernética y de seguridad de la información se observen siempre desde tres perspectivas: las personas, la tecnología y los procesos.

Tobias Ludwichowski
Director de seguridad
informática de Signal Iduna

Tobias Ludwichowski tiene formación en ingeniería industrial y ha desempeñado una gran variedad de roles en el grupo de compañías aseguradoras SIGNAL IDUNA desde 2015, entre otros: puestos de supervisión en gestión de riesgos y gestión de sistemas informáticos, jefe de la Oficina de Seguridad Informática desde 2022, y director de seguridad informática del grupo SIGNAL IDUNA.

¿Ha cambiado la percepción de la seguridad informática a lo largo de los años, sobre todo a nivel del equipo directivo y de la junta consultiva?

La normativa relativa a la seguridad informática para las aseguradoras está evolucionando rápidamente, y cada vez se aprueban más leyes y normativas. La Autoridad Federal Alemana de Supervisión Financiera lleva ya algunos años adoptando una actitud activa al respecto. En general, se está ejerciendo mucha presión sobre la cúpula directiva en lo que respecta a este tema, a lo que se suma un panorama de amenazas cada vez más complejo. Por este motivo, la concienciación en materia de ciberseguridad del equipo directivo ha aumentado drásticamente en los últimos años. Afortunadamente, ahora se pueden destinar más recursos a esto.

Abordemos ahora el tema de los seguros en el ámbito cibernético. Como representante del sector, ¿qué tendencias de mercado observas en este campo?

Observamos una tendencia a orientar los seguros de riesgos cibernéticos hacia pocos proveedores que estén dispuestos a ampliar su cobertura de riesgos cibernéticos. Esto se debe a que para una empresa es difícil calibrar y comprender el riesgo cibernético cuando, además, nos enfrentamos a un mercado de amenazas digitales muy dinámico. Es sumamente complicado determinar objetivamente lo bien cubierta que está una empresa en este sentido, tanto ahora como en el futuro. Una póliza también tiene que ser atractiva para el cliente. Por ejemplo, a las empresas medianas no les sirve de mucho que la cobertura se limite a 200 000 euros. También hay que asegurarse de que las

empresas sigan combatiendo el riesgo de forma activa, aunque tengan cobertura de ciberseguridad, y que no se duerman en los laureles. Todo esto hace que en estos momentos el tema de los seguros de riesgos cibernéticos sea complicado.

¿Cómo podemos hacer que la ciberseguridad sea menos opaca y se convierta en un proyecto común en el que, idealmente, todo el mundo quiera participar activamente?

Hay que adoptar un enfoque doble. El primero es la comunicación y formación continuas para hacer visibles los posibles efectos de los incidentes de seguridad. Por ejemplo, ayuda informar activamente a los empleados de la situación de amenaza y de determinados comportamientos. Esto también les puede servir fuera del trabajo, por ejemplo, informándoles sobre cómo proteger sus cuentas personales, haciendo así el tema de la ciberseguridad menos abstracto y más tangible.

En segundo lugar, debemos integrar las prácticas de ciberseguridad en los procesos empresariales hasta el punto de que los empleados ni siquiera se den cuenta de que están contribuyendo a mejorar la seguridad. Hay que configurar los procesos para que los empleados los cumplan automáticamente, lo que a la larga supone menos trabajo para ellos. Enviarles pautas y esperar que las lean, entiendan y plasmen en un comportamiento correcto no es efectivo.

> Si no se ponen en marcha los procesos adecuados y si los empleados no son capaces de reconocer los riesgos, las herramientas técnicas, por buenas que sean, no servirán para nada.

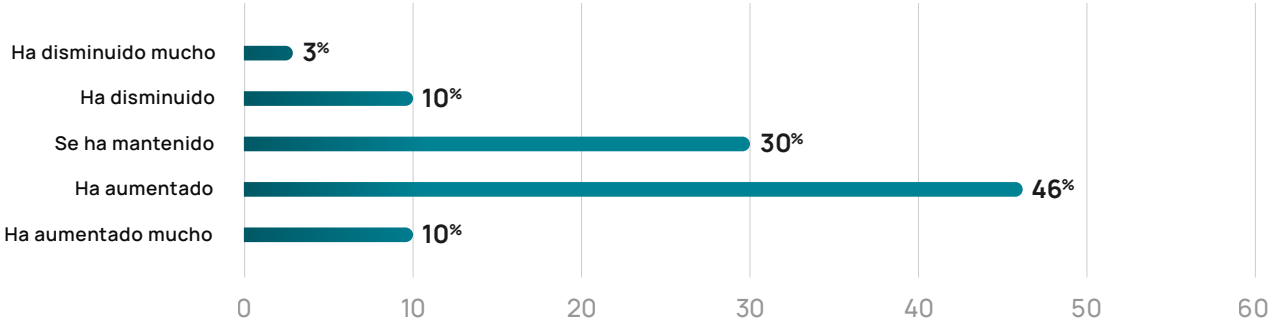
Tobias Ludwichowski
Director de seguridad informática de Signal Iduna

La ciberseguridad, una de las prioridades de la junta directiva: ¿por qué se ha ganado un sitio en la mesa ejecutiva?

En respuesta a todos estos retos, las organizaciones están empezando a priorizar la gestión de la seguridad. De hecho, **el 56 % de los expertos en seguridad de nuestra encuesta afirmaron que su equipo directivo concede más importancia a la ciberseguridad** que el año anterior.

Este cambio de mentalidad en el que se pasa a considerar la seguridad como un componente esencial de la estrategia empresarial, la gestión de riesgos y el éxito del negocio a largo plazo (en lugar de una mera cuestión informática), **está provocando cambios significativos en las estructuras de las empresas**. Al integrar la ciberseguridad en el nivel ejecutivo, las empresas pueden alinear mejor sus estrategias de seguridad con los objetivos empresariales, asignar los recursos necesarios, facilitar el cambio y establecer unas líneas de responsabilidad claras. Nuestra encuesta también pone de manifiesto los beneficios de que la ciberseguridad cobre cada vez más importancia en la junta directiva:

¿En qué medida ha aumentado o disminuido el interés del equipo directivo de tu empresa por la ciberseguridad durante el último año?



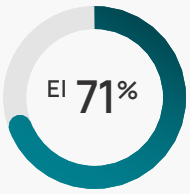
Las organizaciones cuya junta directiva es consciente de los riesgos cibernéticos son un

↗ 67 %

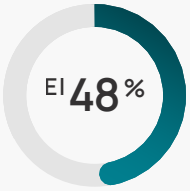
más propensas a tener recursos suficientes para cubrir sus necesidades de seguridad que aquellas en las que la junta desconoce los riesgos

Por su parte, Gartner prevé que, para 2026, **los contratos de trabajo de los altos cargos ejecutivos tendrán requisitos de rendimiento en materia de riesgos de ciberseguridad en al menos un 50 % de los casos** [1]. Sin duda, esta evolución influirá en la rapidez y calidad de las decisiones que se toman en materia de seguridad, ya que cada vez más las tomarán personas ajenas al departamento de informática. En consecuencia, las responsabilidades pasarán a otros directivos de la empresa. Teniendo en cuenta esto, países como Estados Unidos están empezando a aplicar normas de ciberseguridad que afectan a los miembros de las juntas directivas. En marzo de 2022, la Comisión de Bolsa y Valores (SEC) propuso una norma según la cual las empresas que cotizan en bolsa deben hacer público si su equipo ejecutivo cuenta con miembros expertos en ciberseguridad, ya que los inversores pueden considerarlo importante a la hora de tomar decisiones sobre inversiones y de votar a los directivos [2].

Nivel de concienciación en materia de seguridad percibido en la empresa en función de la sensibilización de la junta directiva



de los expertos afirman que el nivel de concienciación general en su organización es alto cuando el equipo directivo está concienciado



afirma que la concienciación general es alta cuando el equipo directivo desconoce los riesgos

Este interés del equipo directivo por la ciberseguridad está repercutiendo considerablemente en la resiliencia cibernética de las organizaciones, así como en el componente humano. Según nuestra encuesta, el nivel de concienciación a la ciberseguridad percibido en una empresa depende en gran medida de la sensibilización de sus altos cargos: el 71 % de los expertos encuestados que creen que su equipo directivo es plenamente consciente de los riesgos cibernéticos considera que la sensibilización a la seguridad en su organización es mucho mayor que la de aquellos que creen que su equipo directivo no está concienciado (48 %).

1 **Gartner (2022).** Gartner Says the Cybersecurity Leader's Role Needs to Be Reframed.

2 **World Compliance Association (2022).** La SEC está a punto de forzar a los CISO a las salas de juntas de Estados Unidos.

Sobrevivir en la jungla de amenazas digitales: el papel de la junta directiva

> **La cibernética es una batalla incansable y feroz que va a un ritmo vertiginoso, y en la que siempre hay que aprender y mantenerse al día. Por eso es tan importante desarrollar nuevos modelos, como poner a personas más jóvenes con conocimientos específicos en puestos del consejo asesor, aunque no hayan dirigido nunca una empresa, o invertir más en formación para los empleados.**
>
> **Dra. Katrin Suder**
> Experta en estrategia
> (tecnologías digitales, empresas y política)

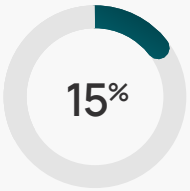
Seguir el ritmo de un panorama de ciberataques en constante evolución es similar a correr una carrera que no solo no tiene fin, sino que aumenta constantemente de velocidad. Aunque el equipo directivo está empezando a priorizar la ciberseguridad, no todos sus miembros tienen una amplia experiencia en digitalización y cuestiones cibernéticas. De hecho, la mayoría están más acostumbrados a confiar en sus años de experiencia para afrontar las situaciones. Por eso es fundamental tener una mentalidad abierta tanto para **educar y formar continuamente a los cargos directivos**, como para **crear nuevas estructuras en las juntas directivas**, a las que se deben añadir perfiles más especializados, aunque eso implique aceptar personas con menos años de experiencia en el mundo de los negocios. Otra posible solución es invitar periódicamente al equipo de seguridad a las reuniones del equipo directivo para entablar debates abiertos y honestos sobre el nivel de seguridad de la empresa y sobre cómo repercute este en el riesgo general de la empresa. La adaptabilidad y la colaboración para identificar las áreas de alto riesgo y para establecer objetivos relacionados con la seguridad que reduzcan el riesgo general pueden mejorar significativamente la resiliencia cibernética.

Aumentan los presupuestos de ciberseguridad, pero sigue sin ser suficiente

En los últimos años, ha habido una tendencia al alza en la inversión en ciberseguridad de las organizaciones. Gartner prevé que **el gasto mundial en seguridad y gestión de riesgos aumente más de un 11 % en 2023**, hasta alcanzar los 188 000 millones de dólares, frente a los 158 000 millones de 2021 [3]. Este avance es especialmente positivo ahora que los equipos directivos están empezando a priorizar la ciberseguridad e incluso a incluirla en el orden del día de los ejecutivos. De hecho, según nuestra encuesta, solo el 15 % de las empresas que no disponen de suficientes recursos de seguridad pueden priorizar su cultura de seguridad, frente al 94 % de las que cuentan con recursos suficientes.

Sin embargo, una ciberseguridad eficaz requiere un enfoque que vaya más allá de la inversión en tecnología y herramientas. Alinear los esfuerzos de seguridad con los objetivos empresariales y priorizar la ciberseguridad en el equipo directivo también son iniciativas muy eficaces, pero todo ello debe formar parte de una estrategia más amplia.

De las empresas que carecen de suficientes recursos de seguridad, solo el



prioriza su cultura de seguridad

mientras que

de las empresas con suficientes recursos lo hace

Teniendo en cuenta que la frecuencia de los ciberataques aumenta a un ritmo mayor que el incremento de los presupuestos de seguridad, y que además los ciberdelincuentes son conscientes de lo fructífero que puede llegar a ser explotar el componente humano (más del 82 % de las filtraciones de datos están relacionadas con el factor humano [4], es ahora más importante que nunca contar con **medidas eficaces de concienciación sobre ciberseguridad** que fomenten de forma eficaz comportamientos seguros entre los empleados.

3 **Gartner (2022).** Gartner Identifies Three Factors Influencing Growth in Security Spending.

4 **Verizon (2022).** 2022 Data Breach Investigations Report.

> Solemos decir que los costes informáticos son demasiado elevados, pero en realidad estamos haciendo una inversión que permite que el negocio crezca, que mejore la calidad del servicio y que se ahorren costes en cada departamento de la empresa gracias a la automatización.

Jens Becker
Director de sistemas de información (CIO) y de digitalización (CDO) del Grupo Zurich Alemania

Jens Becker ha sido el director de sistemas de información y de digitalización del Grupo Zurich Alemania desde enero de 2021. En este puesto se encarga de impulsar la iniciativa "Evolución Acelerada" del servicio informático de Zurich. Antes de Zurich, Becker trabajó como consultor informático en la multinacional KPMG y ocupó varios puestos de liderazgo en el departamento de informática de AXA durante más de 12 años. Fue responsable de varios proyectos de digitalización, introdujo el modelo DevOps cuando lidereaba el departamento de operaciones de TI e inició la migración a la nube de AXA, entre otros proyectos.

En tu opinión, ¿qué debemos hacer para que el equipo directivo se implique más en la concienciación en materia de seguridad?

La mayor parte del cuerpo directivo comprende que la seguridad es una prioridad o debe serlo. La cuestión es si esa toma de conciencia se pondrá en práctica, si conducirá a una concienciación sostenible en materia de seguridad o si, en algunas situaciones, seguirán optando por no bloquear el ordenador ni cifrar los datos.

Creo que para aumentar la concienciación general de la sociedad en materia de seguridad y hacer que la gente comprenda la situación real, la necesidad de mejorar la resiliencia cibernética y la forma correcta de gestionar los datos sensibles, no debemos centrarnos solo en el ámbito empresarial, sino también en otros niveles. De hecho, debería ser una asignatura obligatoria para todos desde que somos pequeños. Los alumnos deben comprender que les pueden robar sus contraseñas y su identidad. Debemos sensibilizarlos, aunque sin asustarlos, para que aprendan a afrontar los ataques correctamente.

A nivel de empresa o corporación, las expectativas son, lógicamente, aún mayores. Los empleados deben tratar los datos de sus clientes con cuidado y ser especialmente conscientes de la responsabilidad que tienen. Esto es algo que también

debatimos a nivel de la junta directiva, donde además recalcamos que cada departamento es responsable de abordar temas como los conceptos de autorización, la gestión de la continuidad de las actividades de la empresa y el tratamiento individual de los datos.

En un evento reciente, dijiste que las empresas no deberían ahorrar en informática, sino gracias a la informática. ¿Podrías explicar esto?

Por supuesto. Solemos decir que los costes informáticos son demasiado elevados, pero en realidad estamos haciendo una inversión que permite que el negocio crezca, que mejore la calidad del servicio y que se ahorren costes en cada departamento de la empresa gracias a la automatización.

Debemos automatizar las actividades sencillas y repetitivas para que nuestro equipo de atención al cliente pueda centrarse en tareas más complicadas. Los chatbots son una solución rentable para atender llamadas, validar solicitudes de clientes y clasificar sus peticiones. De este modo, el empleado que antes se encargaba de estas tareas puede centrarse en resolver las incidencias. La automatización también ayuda a ajustar los tiempos de respuesta a las expectativas de los clientes. Antes esperábamos dos semanas a que nos contestaran a una carta, pero ahora esperamos que nos respondan a un correo electrónico en dos días. Una atención rápida aumenta la satisfacción del cliente y reduce los costes de procesamiento.

Ya que hablamos de digitalización, también deberíamos centrarnos en digitalizar todo lo que producimos, por ejemplo, las cartas. En este aspecto nuestra industria tiene mucho trabajo por hacer. Si invertimos en digitalización, nuestros esfuerzos se verán recompensadas con una reducción de los costes de envío y de papel y con una reducción de las emisiones de CO2.

Entonces, ¿es mejor invertir hoy para minimizar los riesgos?

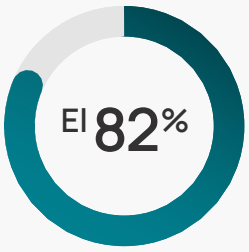
Sin duda. Es mejor instalar un cortafuegos hoy que tener que apagar el fuego mañana y pagar los gastos de reparación. Ahora bien, hay que encontrar el equilibrio adecuado. Según algunas directrices oficiales, las empresas deberían invertir el 7 % de su presupuesto de informática en ciberseguridad. Sin embargo, podrías invertir todo el presupuesto en ciberseguridad y aun así no estar completamente seguro. Por eso es necesario adoptar un enfoque apropiado, que se centre en los riesgos principales. Los estándares NIST e ISO, entre otros, sirven para orientar, pero también son útiles como indicador de un cierto nivel de seguridad de cara a tus socios. En definitiva, es importante seguir invirtiendo en seguridad y no dormirse nunca en los laureles.

En general, ¿crees que las empresas invierten suficiente en seguridad o que este tema sigue viéndose como un asunto pendiente con el que ya es lidiará en algún momento?

Sí y no. En cuanto a la primera pregunta, creo que se está invirtiendo mucho, pero nunca es suficiente. Por eso Zurich sigue el llamado «enfoque de clasificación forzada», que consiste en crear una matriz de riesgos en la que introducimos nuestros riesgos de seguridad y los tratamos poco a poco según esa matriz. Respecto a la segunda pregunta, llevamos varios años haciéndolo y no bajaremos la guardia en el futuro.

Perspectivas de futuro: por qué debemos integrar la ciberseguridad en nuestra vida cotidiana

En los capítulos anteriores hemos visto cómo la ciberdelincuencia ha evolucionado hasta alcanzar una gran magnitud y también profesionalizarse. Los ciberdelincuentes no pierden el tiempo: se aprovechan de cualquier vulnerabilidad empleando técnicas innovadoras y sofisticadas. Este panorama en constante evolución supone un gran reto para empresas, gobiernos y particulares, que luchan constantemente por salvaguardar sus recursos en un mundo cada vez más interconectado. Lo más preocupante es que **el futuro próximo tampoco parece muy halagüeño**: según nuestra encuesta, 8 de cada 10 profesionales de la seguridad prevén que el panorama de amenazas no mejorará en los próximos 12 meses.



de los expertos en seguridad prevén que el panorama de las amenazas no mejorará en el próximo año.

Un análisis más profundo de los datos demostró también que la ingeniería social sigue siendo un elemento clave en los ciberataques, independientemente de que las empresas ya dispongan de numerosas medidas de seguridad técnicas. Además, dado que los ataques a través del correo electrónico continúan siendo tremendamente populares entre los ciberdelincuentes y que otros canales, como las redes sociales y las herramientas de colaboración, están ganando fuerza poco a poco, las organizaciones están empezando a ser conscientes del valor de una cultura de seguridad robusta que coloque el foco de su estrategia en el factor humano.

Recibimos constantemente miles de correos de spam inofensivos. El problema es que, a pesar de tener numerosos controles de seguridad, también llegan a nuestra bandeja de entrada correos de phishing peligrosos. Los empleados deben aprender a no caer en estas trampas; por eso es tan importante para nosotros la formación en ciberseguridad.

Frank Heymann
Senior team manager del departamento de informática de Buhlmann

Por tanto, disponer de una formación en ciberseguridad que sea eficaz se convierte en un factor clave para que las empresas afronten los peligros que las amenazan y para que sus empleados sean capaces de protegerla de manera proactiva, tanto de correos electrónicos maliciosos, como de ataques a través de otros canales de comunicación nuevos.

En los últimos 10 años, las empresas han invertido más en tecnología que en las personas. Ahora comienzan a darse cuenta de que la tecnología no lo es todo y de que la ingeniería social, especialmente el phishing, es un verdadero problema. Muchas de esas empresas van por el buen camino, pero aún les queda bastante por hacer.

Dra. Katrin Suder
Experta en estrategia
(tecnologías digitales, empresas y política)

Nuestra mejor baza es la formación en ciberseguridad

Las personas tenemos más facilidad para comprender los comportamientos de otros seres humanos. Si confías únicamente en la tecnología y das por hecho que lo detectará todo, estás cometiendo un grave error.

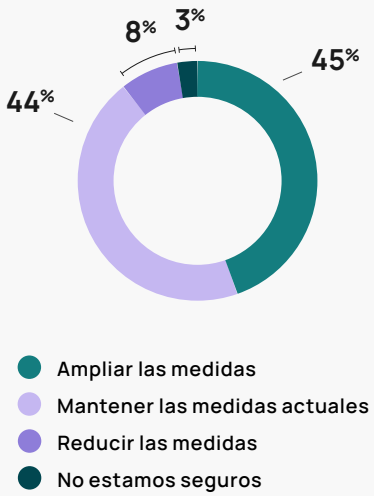
Tobias Ludwichowski
Director de seguridad informática de Signal Iduna

La buena noticia es que muchos departamentos de informática y seguridad ya han tomado conciencia de la necesidad de abordar el factor humano en sus organizaciones. Nuestra encuesta pone de manifiesto que la máxima prioridad de los expertos en seguridad es mejorar la concienciación de los empleados en materia de seguridad, seguida de la gestión de identidades y accesos, y de la protección del trabajo híbrido y de los procesos existentes. Además, 9 de cada 10 expertos también respondieron que su empresa mantendrá o aumentará sus medidas de concienciación en ciberseguridad.

Prioridades de los departamentos de informática y de seguridad

1. Aumentar la concienciación de los empleados en materia de seguridad
2. Mejorar la gestión de identidades y accesos
3. Garantizar la seguridad del trabajo híbrido
4. Proteger los procesos existentes

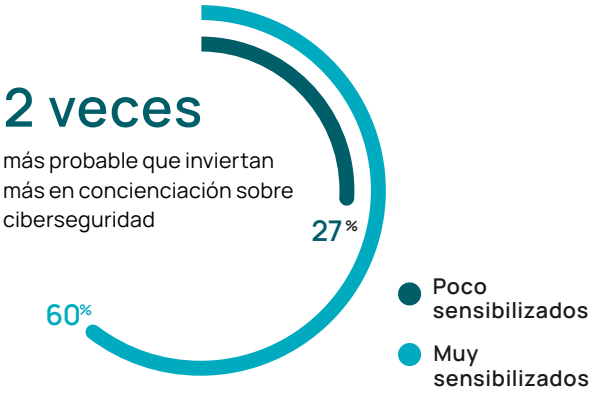
¿Qué planes tiene la empresa respecto a la ampliación o reducción de medidas de concienciación en materia de seguridad en 2023?



Y esto requiere el apoyo de la junta directiva

En el capítulo anterior ya hemos hablado de lo importante que es que se reconozcan y se debatan las cuestiones de seguridad en el nivel ejecutivo, un aspecto que corroboran los datos de nuestra encuesta: existe una relación directa entre la sensibilización del equipo directivo en materia de seguridad y la prioridad que se le concede a invertir en concienciación sobre seguridad.

Consecuencias de un alto nivel de concienciación por parte del equipo directivo



La encuesta revela, además, que **el 94 % de las empresas que destinan recursos suficientes a la ciberseguridad consideran que crear una cultura de seguridad es una prioridad** dentro de su organización. En cambio, solo el 15 % de las que no cuentan con recursos suficientes lo prioriza. Esta diferencia pone de manifiesto aún más el impacto tan significativo que tienen la disponibilidad de recursos y la concienciación del equipo directivo en el compromiso de una organización con la ciberseguridad.

Por eso es crucial que los equipos de seguridad e informática se comuniquen continuamente con la junta directiva y que respalden sus peticiones de presupuesto para medidas de seguridad con métricas que muestren el éxito de dichas medidas e indicadores clave de rendimiento (KPI). Y es que para asegurarse de que la ciberseguridad siga siendo una prioridad en los próximos años, estos profesionales tendrán que explicar cómo cambia el comportamiento de los empleados con el tiempo y cómo esto repercute en la seguridad de la empresa, en lugar de centrarse solo en métricas como el porcentaje de clics. Un ejemplo de cómo medir el impacto de las medidas de seguridad en una empresa es demostrar cómo aumenta el porcentaje de incidentes detectados por los empleados después de instalar un botón de aviso de phishing.

La ciencia del comportamiento: presente y futuro de la concienciación en ciberseguridad

Aunque la concienciación en ciberseguridad no sea una novedad en el mundo empresarial, está experimentando ahora un cambio radical que tiene como objetivo responder eficazmente a todos los retos del panorama digital actual. Los **modelos de formación tradicionales**, centrados principalmente en el cumplimiento de las normativas y otras obligaciones legales, **no bastan** para ganarse la atención y la implicación de los empleados ni ofrecen un nivel de formación suficiente para combatir el panorama de amenazas actual. Los datos de nuestra encuesta reflejan estas limitaciones:

Las 3 razones principales por las que a los usuarios les cuesta la formación en ciberseguridad:

1. **La cantidad de tiempo que requiere**
2. **La información es demasiado genérica**
3. **La formación es demasiado repetitiva**

Esto demuestra claramente que las organizaciones necesitan cultivar una cultura de seguridad sólida que vaya más allá del mero cumplimiento de las

normativas y que fomente activamente comportamientos seguros entre los empleados, todo ello adaptándose también a sus modelos de trabajo y a sus apretadas agendas. Para lograrlo, **los programas de concienciación sobre seguridad deben centrarse completamente en el factor humano e incorporar métodos basados en la ciencia del comportamiento**, como el microaprendizaje, la gamificación y los recordatorios automatizados para que los empleados puedan tomar decisiones informadas no solo en sus actividades laborales diarias, sino también en su vida personal.

Al poner la ciberseguridad al alcance de todos e integrarla en nuestra vida cotidiana, las organizaciones fomentarán la concienciación en todos los ámbitos y lograrán una verdadera sinergia entre la ciberseguridad y el funcionamiento de la empresa. Esta estrategia proactiva es crucial para luchar contra la implacable y multimillonaria industria de la ciberdelincuencia a la que nos enfrentamos hoy en día. Para no quedarnos atrás, debemos adaptarnos y evolucionar constantemente, al mismo ritmo que el panorama de las amenazas.

Impulsando un cambio de comportamiento sostenible

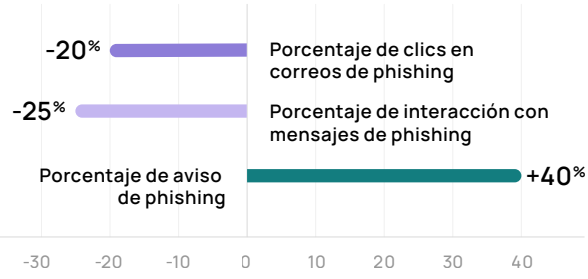
Hay diversos enfoques y métodos que ayudan a las organizaciones a sacar el máximo partido de sus iniciativas de concienciación y a adaptarlas al contexto individual de cada empleado y a sus necesidades. Por ejemplo, la **repetición espaciada** a través de diferentes canales permite a los usuarios repetir lo que han aprendido a un ritmo que fomenta resultados duraderos. Otro ejemplo de este tipo de enfoque es el **nudging** o recordatorios automatizados por correo electrónico que fomentan las interacciones con los usuarios y los mantienen informados. El **microaprendizaje** también es un método eficaz para reforzar el aprendizaje y mejorar la retención. En la plataforma SoSafe Awareness podrás encontrar contenidos fáciles de seguir y que se sirven de historias con personajes para mejorar la participación del usuario.

Este enfoque de formación en ciberseguridad basado en la ciencia del comportamiento se traduce en un porcentaje más elevado de finalización de los módulos que, a su vez, reduce el porcentaje de clics y de interacción con correos electrónicos de phishing. Además, gracias a este método, aumenta el porcentaje de aviso de incidentes por parte de los empleados. Como muestran los datos de nuestra plataforma, SoSafe otorga a las organizaciones las herramientas necesarias para protegerse de manera proactiva contra las amenazas digitales del panorama actual.

organisaties een aanzienlijke stap in de richting van het beveiligen van hun activa en het proactief afweren van aanvallen.

Uso del producto

Resultados de usuarios con un alto porcentaje de finalización de módulos



Clicar o no clicar, esa es la cuestión

Otro factor que contribuye a la eficacia de la formación en ciberseguridad es el hecho de que esté contextualizada. Un ejemplo del éxito de este tipo de concienciación son **las simulaciones de phishing**, que ponen a prueba los conocimientos que los usuarios han adquirido en su formación. Se trata de un aprendizaje implícito y basado en incidentes concretos que promueve los comportamientos seguros mediante simulaciones realistas de amenazas que ocurren en situaciones cotidianas. Muchos expertos coinciden en que combinar simulaciones y experiencias de aprendizaje contextual ayuda a reducir eficazmente los riesgos:

> En un mundo en el que nos bombardean con información y no tenemos tiempo para aprender, es fundamental proporcionar a los empleados unidades de aprendizaje cortas y pertinentes en ese momento. Debemos presentárselas justo después de cometer un error, cuando la motivación para aprender es muy alta. Por ejemplo, se les puede enseñar una página con consejos de seguridad después de que hagan clic en un correo de simulación de phishing. Cualquier empleado tiene tiempo para hacer una formación de cinco minutos, por muy ajetreada que sea su jornada laboral.
>
> **Martin Schmidt**
> Director global de asesoramiento digital de Freudenberg Home and Cleaning Solutions

> Es especialmente importante que los usuarios reciban información de cómo lo están haciendo en ese momento. Necesitan recibir esa información en el momento óptimo para el aprendizaje, que es a medida que se desarrolla la simulación.
>
> **Thomas Tschersich**
> Director de seguridad informática de Telekom Alemania

> Tras interactuar con una simulación de phishing y entender bien por qué han cometido un error, la mayoría de los usuarios terminan la experiencia más informados y mejor equipados para combatir los riesgos.
>
> **Dr. Stefan Lüders**
> Director de seguridad informática del CERN

Incorporar **componentes y herramientas contextuales** a la infraestructura existente puede permitir a los empleados participar activamente en la lucha contra los ciberataques. Por ejemplo, los empleados que tienen acceso al **botón de aviso de phishing** de SoSafe muestran un porcentaje de interacción con correos de phishing un 30 % menor que los que no disponen del botón. Por lo tanto, esta funcionalidad reduce las posibilidades de éxito de los ataques, además de ofrecer otras ventajas:

Impacto del botón de aviso de phishing

↗ 38%
Porcentaje de adopción de la formación

↗ 25%
Porcentaje de finalización de los módulos

La llamada a la innovación: funcionalidades que solicitan las empresas

En nuestra encuesta a profesionales de la seguridad en Europa, preguntamos qué otras funcionalidades podrían tener un gran impacto en su formación de ciberseguridad. Esto es lo que dijeron:

Esto demuestra que los profesionales de la seguridad están comprendiendo la necesidad de acercar la seguridad a las personas. La **concienciación multicanal**, por ejemplo, es una forma interesante de hacerlo que ofrece un enfoque más conversacional. Las medidas de concienciación rápida que emiten alertas sobre nuevas tácticas de ataque a través de diferentes herramientas de comunicación como Microsoft Teams son un método para integrar la seguridad en la rutina laboral diaria. El **aprendizaje personalizado**, que tiene en cuenta las diferentes funciones y responsabilidades de cada empleado para adaptar la experiencia de aprendizaje a sus necesidades, también es una de las estrategias más efectivas de un programa de concienciación, lo que subraya una vez más la necesidad de que la formación en ciberseguridad se adapte al contexto y circunstancias de cada usuario.

Por último, otra importante iniciativa para catapultar el éxito de la concienciación es la **personalización de los programas formativos,** incluyendo opciones como adaptar la plataforma a la imagen de marca de la empresa o integrar en la misma plataforma el contenido y las políticas de seguridad de la empresa. En resumen, la formación en ciberseguridad no debe concebirse como una fórmula universal, sino más bien como un plan que se ha de diseñar de forma única y meticulosa para ajustarse a las necesidades específicas de cada organización y cada usuario.

Funcionalidades que podrían hacer que la formación en ciberseguridad tuviera un mayor impacto, según expertos en ciberseguridad:

1. Concienciación a través de apps de comunicación
2. Aprendizaje personalizado
3. Customización de los programas

Medidas recomendadas

La raíz del problema: las medidas de seguridad tienen que evolucionar al mismo ritmo que los comportamientos humanos

1 La seguridad debe estar por encima de todo

Si algo nos está demostrando el panorama digital actual es que la ciberseguridad es algo que nos afecta a todos. Nadie puede negar ya que la digitalización y el progreso tecnológico nos han expuesto a todo tipo de amenazas en línea. Para protegernos eficazmente de unos ataques cada vez más avanzados, debemos incorporar las recomendaciones de ciberseguridad a nuestra vida cotidiana. Al mismo tiempo, las organizaciones deben llevar las cuestiones de seguridad a la junta directiva y trabajar juntos para compatibilizar las actividades de la empresa con una estrategia de ciberseguridad. Y es que, al fin y al cabo, las medidas de seguridad solo tendrán un verdadero impacto si se les da suficiente prioridad en el contexto general de la organización. Si las empresas consiguen comprender que la ciberdelincuencia no afecta únicamente a las personas como individuos, sino también al éxito de los negocios, no será necesario seguir luchando por conseguir los recursos necesarios.

2 Cambiar el comportamiento es la clave del éxito a largo plazo

Una manera clara y tangible de comunicar los logros en materia de seguridad y concienciación a las partes interesadas de la organización son las métricas referentes al comportamiento de los empleados. Antes, las empresas se basaban solo en métricas como el porcentaje de clics en mensajes de phishing o el porcentaje de finalización de los módulos de formación. Aunque estas métricas constituyen un primer paso para demostrar el nivel de concienciación de los empleados, es fundamental mostrar cómo la formación en ciberseguridad es capaz de cambiar el statu quo para conseguir convencer a los responsables de una organización de la importancia de la concienciación. En el ámbito de la sensibilización, dos ejemplos de métricas de comportamiento importantes son el porcentaje de aviso de phishing y la puntuación de riesgo. Como muestran los datos de nuestra encuesta, aunque 1 de cada 2 organizaciones sigue confiando en las métricas tradicionales, **las métricas de comportamiento ya se utilizan en un tercio de las empresas** y cada vez cobran más importancia. En un momento en que los ciberdelincuentes recurren cada vez más a la ingeniería social, las métricas de comportamiento y las puntuaciones de riesgo humano se convertirán pronto en las únicas pruebas fiables de cuán protegidas están las empresas frente a las complejas amenazas del panorama actual.

3 Adaptarse, adaptarse y adaptarse

La ciberseguridad es uno de los ámbitos que probablemente haya evolucionado más en los últimos años y décadas. Y la razón está muy clara: los avances tecnológicos han hecho imposible estancarse. Pero las cosas se están acelerando aún más, y esto obliga a las organizaciones a ser aún más rápidas a la hora de adaptar sus estrategias al nuevo contexto actual, caracterizado sobre todo por la progresiva profesionalización de los modelos de negocio de los ciberdelincuentes y una rápida evolución en la complejidad de las amenazas digitales. Los equipos de seguridad deben dejar atrás la concepción de que la formación tiene como único objetivo el cumplimiento de normativas y acercarse más a una visión integral de la ciberseguridad como parte de la estrategia de negocio global. Pero no solo eso, también deben velar por adaptar las medidas de seguridad a las personas, sus experiencias, su contexto y sus riesgos individuales. Esta adaptación constante puede suponer un reto en una situación en la que los recursos de seguridad son escasos y los equipos sufren un alto desgaste, pero es un reto que se puede superar si se elige a los socios adecuados.

4 Convertir a las personas en el eje central de nuestra estrategia

A fin de cuentas, en medio de las desalentadoras circunstancias a las que nos enfrentamos hoy en día, es esencial volver a centrarnos en el factor humano de la seguridad. Son las personas quienes son atacadas, son las personas quienes sufren las consecuencias de los ataques y son las personas quienes, en última instancia, pueden prevenir los ataques. Crear una cultura de la seguridad sólida en las organizaciones – y una mentalidad de seguridad sólida en nuestra vida privada – es algo que nos ayudará muchísimo a todos a evitar los efectos devastadores que podría tener en el futuro la ciberdelincuencia profesionalizada. La mejor forma de protegernos es alinear las estrategias de seguridad con las necesidades de las personas y poner en práctica las aplicaciones de la ciencia del comportamiento a este campo. Porque si de algo podemos estar seguros es de que los delincuentes seguirán innovando. Debemos permanecer alerta, adaptarnos a la realidad actual y tomar la iniciativa para preparar a nuestros empleados para todos los retos que nos aguardan.

Construye una línea de defensa humana sólida

La plataforma de concienciación de SoSafe permite a las organizaciones reforzar su cultura de seguridad y mitigar el riesgo humano. Además, ofrece una experiencia de aprendizaje estimulante y participativa, así como simulaciones de ataque personalizadas que enseñan a los empleados a protegerse activamente contra las amenazas en línea. Nuestros métodos están basados en la ciencia del comportamiento para que el aprendizaje sea ameno a la vez que efectivo. La plataforma ofrece también un análisis detallado de los resultados que permite medir el impacto de las medidas de concienciación en términos de cambios en el comportamiento de los empleados, detectando así las vulnerabilidades que es necesario combatir para asegurar una respuesta proactiva ante las amenazas. La plataforma de SoSafe es fácil de implementar y escalar, y fomenta comportamientos seguros entre los empleados sin que tengan que hacer grandes esfuerzos.

ENSEÑAR

Microaprendizaje estimulante

Una plataforma de aprendizaje basada en la ciencia del comportamiento con la que los empleados disfrutan aprendiendo. Mejora tu resiliencia frente a las amenazas digitales y cumple con las normativas gracias a una formación dinámica y eficaz que utiliza diversos canales para promover, sin grandes esfuerzos, comportamientos seguros duraderos en tus empleados.

- Aprendizaje con contenido gamificado y basado en historias diseñado para promover la participación y la continuación del aprendizaje.
- Biblioteca de módulos de navegación intuitiva y con posibilidad de implementación de contenido propio
- Opciones de customización y de gestión de contenido sencillas y que se adaptan a cada empresa

ENTRENAR

Simulaciones de ataque personalizadas

Simulaciones de phishing personalizadas para cada usuario que fomentan comportamientos seguros. Enseña a tus empleados a detectar un ciberataque a través de simulaciones de spear phishing periódicas y automatizadas. Adoptarán, además, comportamientos seguros que perdurarán en el tiempo y que aplicarán en su día a día profesional. Esta es la manera más efectiva de minimizar riesgos y reducir el tiempo de respuesta a una amenaza en una situación en que cada minuto cuenta.

- Simulaciones de ciberataques personalizadas y realistas
- Explicaciones pedagógicas contextuales que refuerzan el comportamiento seguro de los empleados
- Botón de aviso de phishing para informar de posibles amenazas con tan solo un clic.

ACTUAR

Supervisión de riesgos estratégica

Protege a tu organización de costosos incidentes con nuestra solución integral de evaluación del riesgo humano. Obtén una perspectiva global del nivel de seguridad del componente humano en tu empresa para que puedas anticiparte a posibles vulnerabilidades. Supervisa y comprende el impacto de tus programas de concienciación, analiza el comportamiento de tus empleados y toma decisiones informadas respaldadas por datos.

- Información contextual que incluye indicadores de rendimiento tanto técnicos como de comportamiento
- Benchmarking y consejos prácticos
- Desarrollado para responder a las exigencias de la normativa ISO/IEC-27001 y para priorizar la privacidad.

Agradecimientos

Gracias a todas las personas que han contribuido a la elaboración de este informe, y en especial a todos los entrevistados por compartir su tiempo y sus conocimientos con nosotros.

Jens Becker
Director de sistemas de información (CIO) y de digitalización (CDO) del Grupo Zurich Alemania

Stefanie Boem
Responsable de protección de datos de Sport-Thieme

Sascha Czech
Director de seguridad informática del Hospital Universitario de Münster

Stéphane Duguin
CEO del CyberPeace Institute

Frank Heymann
Senior team manager del departamento de informática de Buhlmann

Tobias Ludwichowski
Director de seguridad informática de Signal Iduna

Dr. Stefan Lüders
Director de seguridad informática del CERN

Martin Schmidt
Director global de asesoramiento digital de Freudenberg Home and Cleaning Solutions

Thomas Schumacher
Director general de Accenture Security

Dra. Katrin Suder
Experta en estrategia (tecnologías digitales, empresas y política)

Thomas Tschersich
Director de seguridad informática de Telekom Alemania y CEO de Telekom Security

Contacto

Para obtener más información sobre este informe y sus datos, por favor contacta con:

Laura Hartmann
Responsable de comunicación
press@sosafe-awareness.com

Exención de responsabilidad:

Se ha hecho todo lo posible para garantizar que el contenido de este documento sea correcto. Sin embargo, no asumimos ninguna responsabilidad por la exactitud, integridad y actualidad del contenido. En particular, SoSafe no asume responsabilidad alguna por los daños o consecuencias derivados del uso directo o indirecto de este documento.

(ISC)² | CPE SUBMITTER

Obtén créditos CPE de (ISC)² con este informe:

SoSafe ofrece a los miembros de (ISC)² la oportunidad de obtener créditos de formación profesional continua (CPE). Las certificaciones de ciberseguridad de (ISC)² están reconocidas en todo el mundo como el más alto nivel de excelencia en ciberseguridad.

Escanea el código QR para saber cómo obtener tus puntos CPE después de leer este informe.

sosafe

SoSafe GmbH
Lichtstraße 25a
50825 Colonia
Alemania

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