proofpoint

Europa y Oriente Medio

INFORME

State of the Phish 2024

Acciones peligrosas, amenazas reales y resiliencia de los usuarios en la era de ciberseguridad centrada en las personas

proofpoint.com/es

INTRODUCCIÓN

Los titulares suelen centrarse en las ingeniosas estrategias de ingeniería social y las vulnerabilidades de día cero utilizadas por los ciberdelincuentes. Sin embargo, la realidad es que no siempre tienen que esforzarse tanto. Según los resultados de la encuesta realizada para el informe State of the Phish 2024, el 71 % de los empleados reconoció haber realizado acciones peligrosas, como compartir contraseñas y hacer clic en enlaces desconocidos, o proporcionar credenciales a una fuente no segura. El 96 % de ellos lo hicieron siendo plenamente conscientes del riesgo. Las personas son un componente esencial de toda estrategia de defensa eficaz, pero también pueden ser el más vulnerable. Pueden cometer errores, caer en la trampa de las estafas o simplemente ignorar las buenas prácticas de seguridad.

El informe mundial de este año se basa en una encuesta entre 7 500 usuarios y 1 050 profesionales de la seguridad de 15 países, incluidos 8 de Europa y Oriente Medio. Asimismo incluye datos obtenidos de nuestros productos e investigaciones sobre amenazas, así como de las conclusiones de los 183 millones de mensajes de ataques de phishing simulados enviados por nuestros clientes durante un período de 12 meses, y más de 24 millones de mensajes de correo electrónico denunciados por los usuarios de nuestros clientes durante el mismo período. Por segundo año consecutivo, hemos recopilado tres resúmenes regionales que destacan matices y variaciones locales.

La mayoría de los usuarios de Europa y Oriente Medio no saben si la seguridad es su responsabilidad o de otros. Y esta falta de claridad puede tener consecuencias desastrosas. Nuestros datos muestran correlaciones sorprendentes entre actitudes y resultados en toda la región.

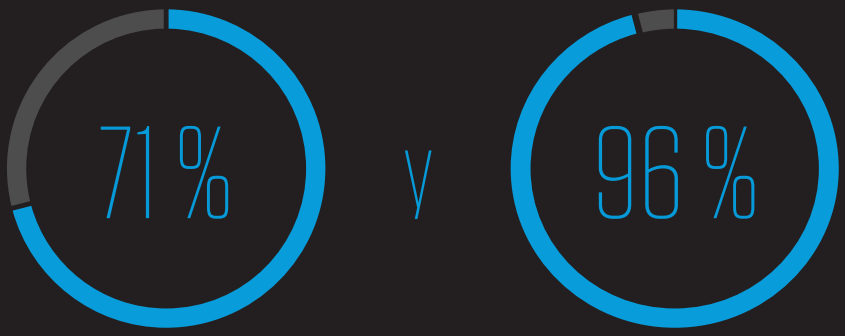
Cada día, los usuarios de la región eligen entre seguridad y comodidad. Este resumen regional muestra que la mayoría de las veces se decantan por la comodidad. En las páginas siguientes, examinamos más de cerca las actitudes de los profesionales de la seguridad y de los usuarios, así como algunas tendencias clave en materia de amenazas. Finalizaremos con algunas sugerencias que deberían ayudar a los usuarios a cambiar su comportamiento y empezar a dar prioridad a la seguridad.

ÍNDICE

Conclusiones principales: A nivel mundial

Más de 1 millón

ataques que se lanzan utilizando la infraestructura de elusión de MFA EvilProxy al mes. Sin embargo, el 89 % de los profesionales de la seguridad todavía creen que la autenticación multifactor ofrece una protección integral frente a la usurpación de cuentas.

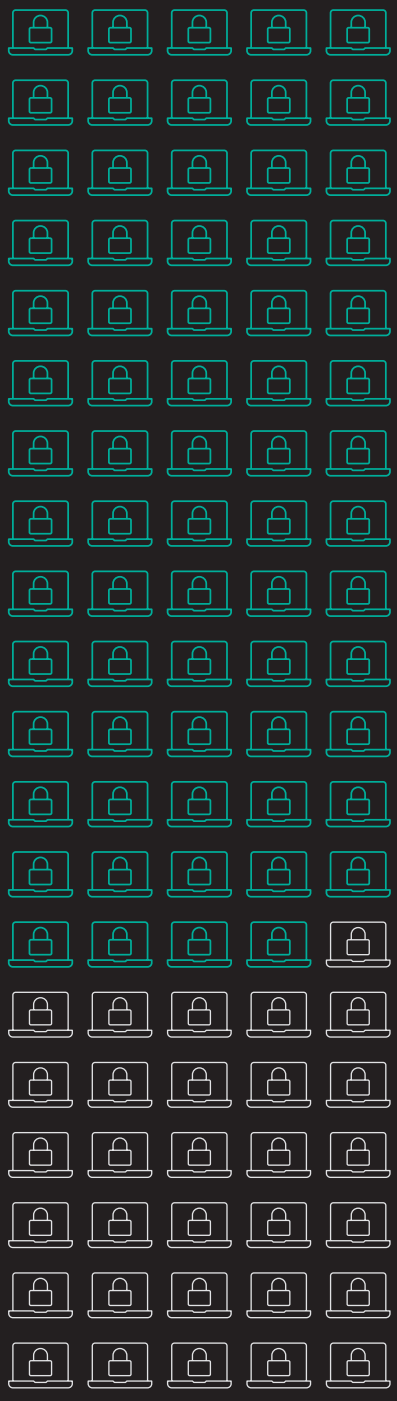


de los usuarios realizaron alguna acción peligrosa

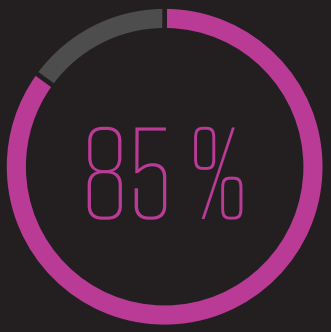
de ellos eran conscientes del riesgo.

66 millones

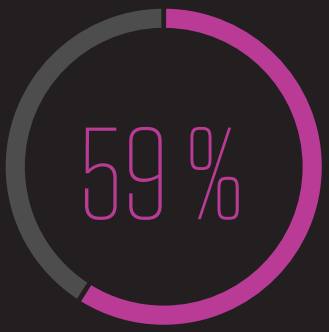
de ataques BEC detectados por Proofpoint de media al mes.



69 % de las organizaciones resultaron infectadas por ransomware.



profesionales de la seguridad afirmaron que la mayoría de los empleados saben que la seguridad es su responsabilidad, pero



de los usuarios no lo sabían o afirmaban no tener ninguna responsabilidad al respecto.

10 millones

de mensajes TOAD que se envían cada mes.

Microsoft sigue siendo la marca más usurpada, con

68 millones

de mensajes maliciosos asociados a la marca o a sus productos.

58 % de los usuarios que han llevado a cabo acciones peligrosas han adoptado un comportamiento que les habría hecho vulnerables a las tácticas habituales de ingeniería social.

Datos destacados de Europa y Oriente Medio

Para el informe State of the Phish de este año hemos entrevistado a 7500 usuarios y 1050 profesionales de la seguridad en 15 países. Este resumen se centra en los siguientes países:

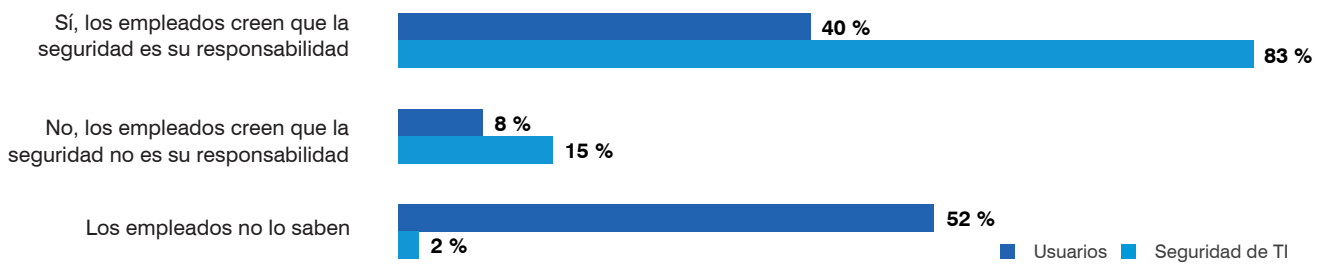
- Francia
- Alemania
- Italia
- Países Bajos
- España
- Suecia
- Reino Unido
- Emiratos Árabes Unidos

Son muchas las variaciones entre regiones y entre los ocho países que abarca este resumen, dada la diversidad de sus lenguas, culturas y niveles de madurez digital. La región es geográfica, cultural y económicamente diversa. Sin embargo, hay un ámbito en el que existe cierta uniformidad. Más usuarios de la región admitieron haber realizado una acción peligrosa que la media mundial (76 % frente a 71 %). Sin embargo, el porcentaje de personas que afirmaron saber que existían riesgos fue del 95 %, solo un punto por debajo de la media mundial.

A escala nacional, el 86 % de los encuestados de Emiratos Árabes Unidos admitió haber llevado a cabo una acción peligrosa, el porcentaje más alto de todos los países encuestados. Las organizaciones emiratíes también registraron el mayor número de ataques de phishing selectivo, lo que pone de manifiesto la estrecha relación entre la concienciación de los usuarios y los niveles de seguridad. Sin embargo, Emiratos Árabes Unidos registró el mayor número de usuarios que consideran que la seguridad es su responsabilidad (62 % frente a una media mundial del 41 %).

Los usuarios suecos son los menos propensos a afirmar que la seguridad es responsabilidad suya. Esto concuerda con el número superior a la media de usuarios que realizan acciones peligrosas (82 %) en Suecia.

Responsabilidad en materia de seguridad (Europa y Oriente Medio)

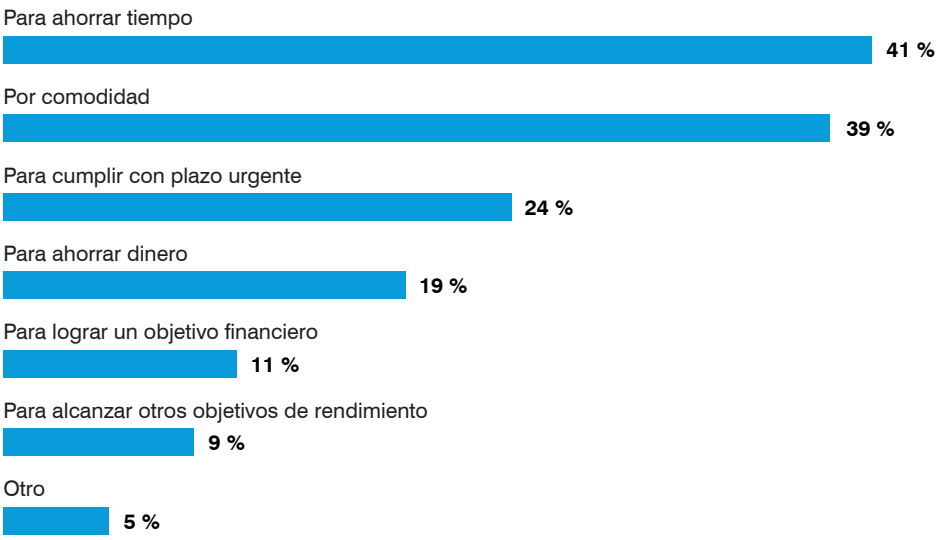


Los profesionales de la seguridad de la región mencionaron la reutilización de contraseñas como el comportamiento más arriesgado. Por desgracia, compartir y reutilizar contraseñas es el segundo comportamiento más común entre los usuarios. Sin embargo, hay buenas noticias para los equipos de seguridad: acceder a sitios web inapropiados es la única otra acción en su "top 5" que también figura entre los comportamientos más adoptados por los usuarios.

Clasificación	Comportamientos de riesgo (clasificados por los profesionales de la seguridad)	Comportamientos de riesgo (clasificados por los usuarios)
1	Reutilizar o compartir contraseñas	Utilizar un dispositivo profesional para actividades personales
2	Hacer clic o descargar un adjunto procedente de un desconocido	Reutilizar o compartir contraseñas
3	Subir datos sensibles a nubes de terceros no aprobadas	Conectarse a un lugar público sin utilizar una VPN
4	Proporcionar credenciales a una fuente no fiable	Responder a un mensaje (de correo electrónico o SMS) de un desconocido
5	Acceder a un sitio web inapropiado	Acceder a un sitio web inapropiado

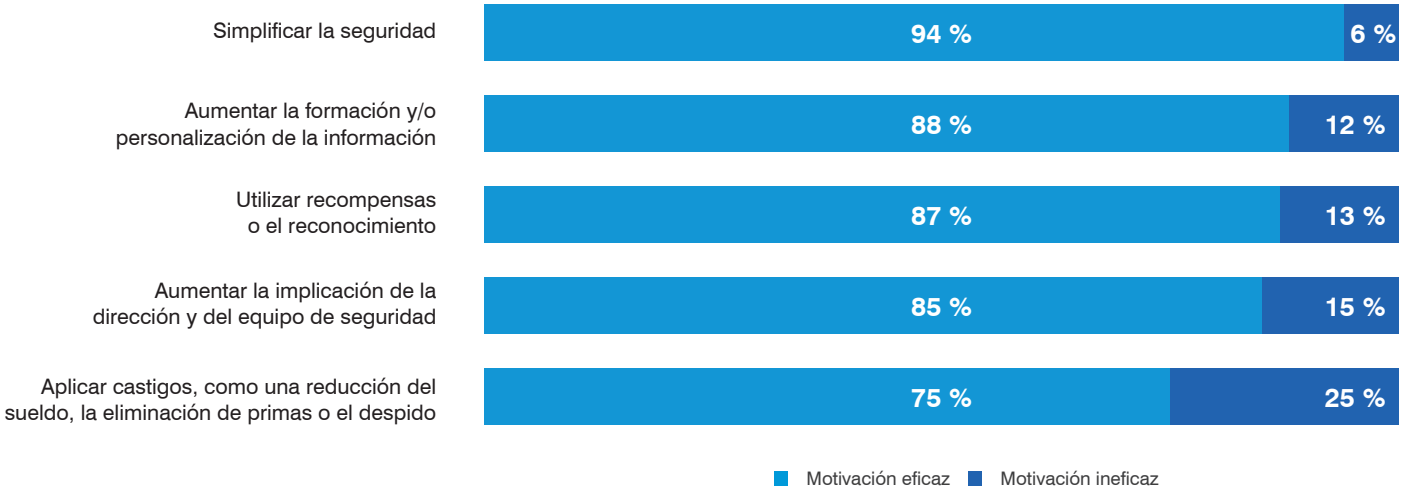
Pero, ¿qué lleva a los usuarios a realizar acciones peligrosas? El ahorro de tiempo fue la respuesta más frecuente, seguida de cerca por la comodidad. En el Reino Unido, la comodidad ocupa el primer lugar y el ahorro de tiempo el segundo.

¿Qué lleva a los usuarios a realizar acciones peligrosas?



Los usuarios de Europa y Oriente Medio explican claramente por qué llevan a cabo acciones peligrosas. Pero, ¿cómo se les podría animar a dar prioridad a la seguridad? Al igual que a escala mundial, la mayoría mencionó la simplificación de la seguridad como la motivación más eficaz y las sanciones como la menos eficaz.

Estrategias para motivar a los usuarios a hacer de la seguridad una prioridad



78 %
de las organizaciones alemanas sufrieron ataques TOAD, pero solo

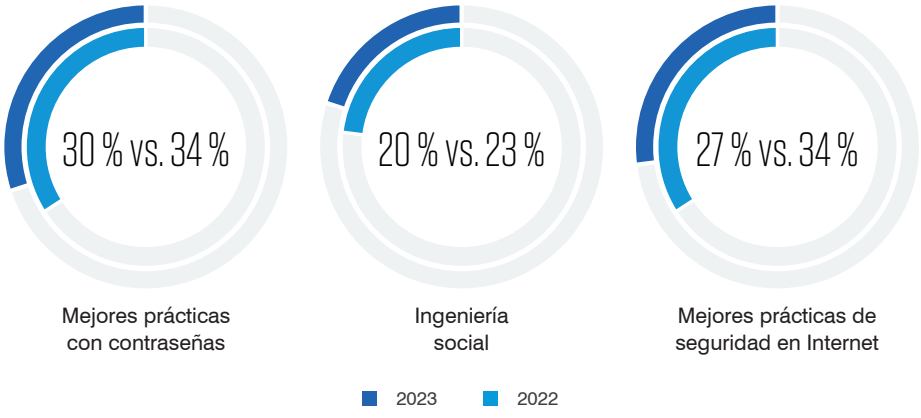
21 %
ofrecen formación sobre la táctica.

Oportunidades de mejora

El 95 % de las organizaciones de la región utilizan inteligencia sobre amenazas para informar sobre sus programas de formación y de concienciación en materia de seguridad. Sin embargo, existen importantes lagunas. Mientras que la mayoría de las organizaciones sufrieron ataques por teléfono o TOAD, menos de un tercio ofrecieron formación sobre esta táctica. En Alemania, el 78 % de las organizaciones sufrieron ataques TOAD, pero solo el 21 % los utilizó como tema de formación en seguridad: una de las mayores disparidades entre los ataques diarios y los temas de formación.

En general, en toda la región se dedica más tiempo a la formación en materia de seguridad. España ha registrado el mayor aumento, con un incremento del 120 % en el número de empresas que dedican tres horas o más al año a este tipo de formación.

Sin embargo, el porcentaje de empresas que ofrecen estos temas de formación esenciales parece estar disminuyendo:



Se trata de temas de seguridad fundamentales. Si menos usuarios saben cómo configurar contraseñas seguras, evitar los señuelos habituales y navegar por Internet de forma segura, los ciberdelincuentes no tardarán en aprovecharse.

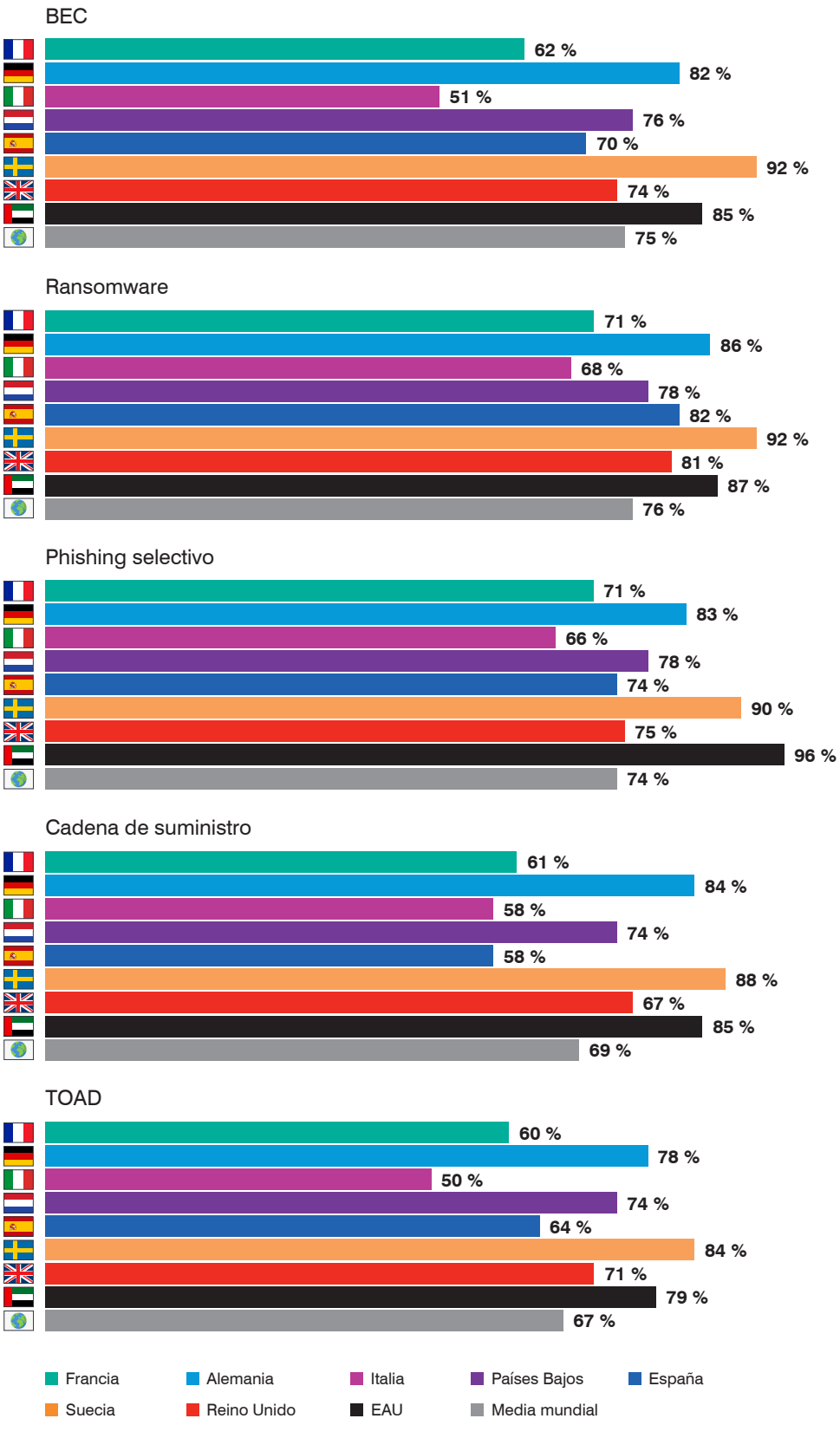
Panorama de amenazas en Europa y Oriente Medio

El año pasado, el panorama regional de las amenazas siguió en gran medida las tendencias mundiales. Las estafas Business Email Compromise (BEC) han disminuido en todo el mundo, pero se ha producido un aumento de los ataques en países de habla no inglesa. Esto podría estar relacionado con el auge de herramientas de IA generativa como ChatGPT, que pueden utilizarse para redactar señuelos de correo electrónico convincentes. Se han observado tendencias similares en otros países no anglófonos del mundo. En general, el 75 % de las organizaciones fueron víctimas de al menos un ataque de phishing, frente al 88 % de 2022.

La región se vio afectada por un número ligeramente superior de ataques TOAD: un 70 % frente a la media mundial del 67 %. El 84 % de las empresas suecas han sufrido un ataque TOAD, el porcentaje más alto de la región.

Al igual que a escala mundial, las empresas de Europa y Oriente Medio informaron de un aumento de las consecuencias negativas de los ataques con éxito. Las sanciones económicas aumentaron un 122 %, un porcentaje ligeramente inferior a la media mundial, lo que puede indicar que las multas impuestas en el marco del RGPD ya se habrían pagado en años anteriores.

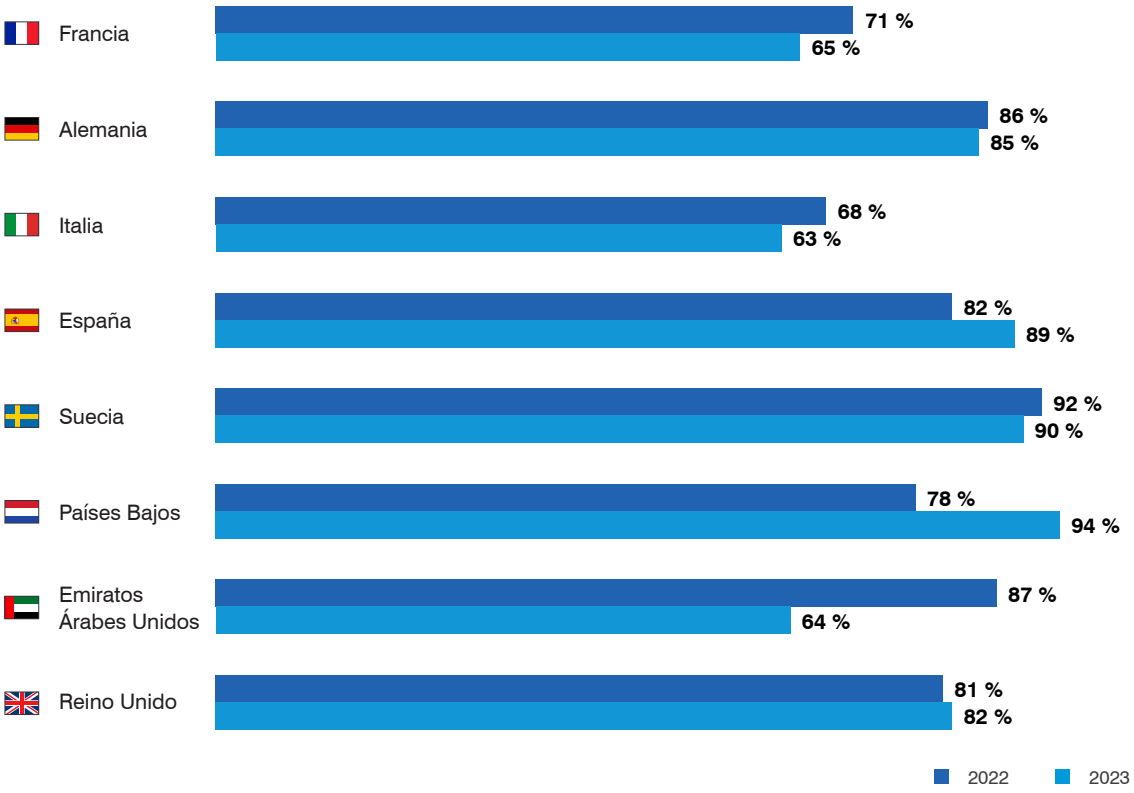
Porcentaje de organizaciones afectadas por ataques dirigidos



Ransomware

El ransomware sigue siendo una grave amenaza para las empresas de la región. El número de ataques e infecciones ha aumentado en el último año. Sin embargo, los detalles varían de un país a otro.

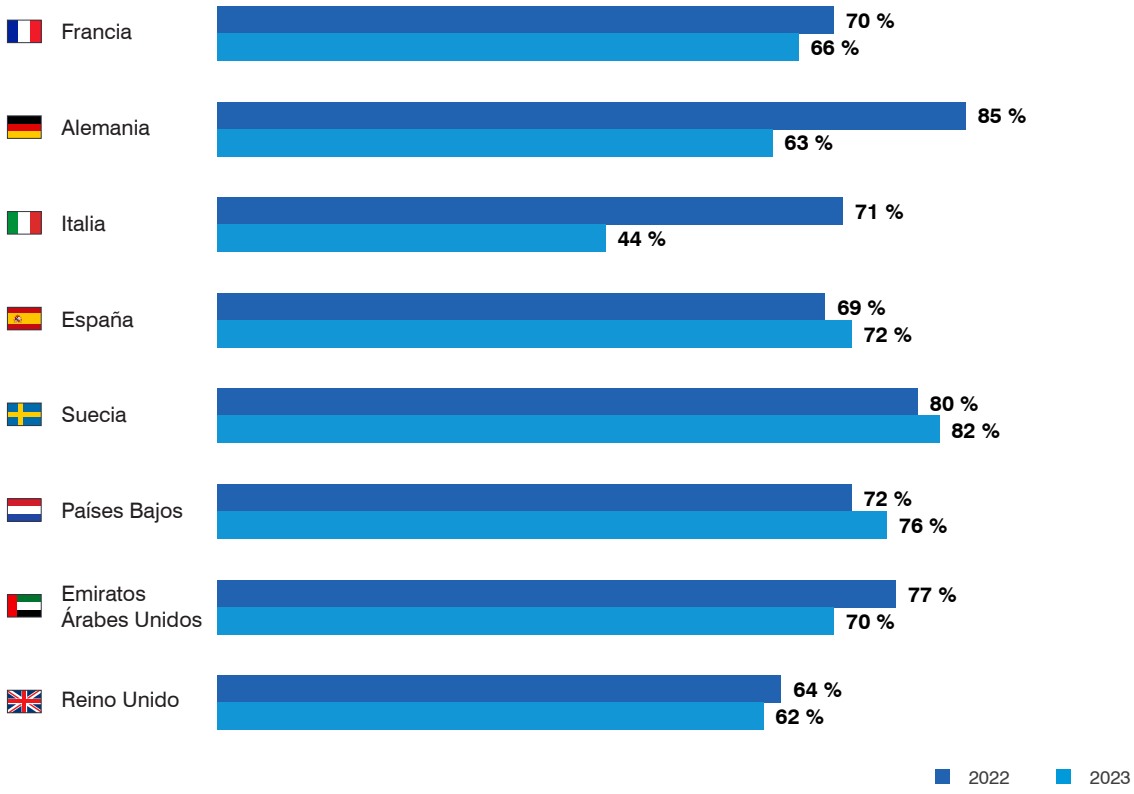
Ataques de ransomware por correo electrónico



Por ejemplo, las empresas italianas han experimentado el mayor aumento en el número de infecciones con éxito de ransomware, pasando del 44 % en 2022 al 71 % en 2023, a pesar de enfrentarse al mismo volumen de ataques que las empresas de otros países. Esto llevó a las autoridades italianas a emitir una advertencia en junio sobre el creciente número de ataques de ransomware que aprovechan un error de VMware.

Suecia registró el mayor porcentaje de intentos de ataques de ransomware del mundo, con un 92 % de sus organizaciones atacadas. Esto podría estar relacionado con el hecho de que, en una encuesta anterior, el 74 % de los encuestados suecos citaron el robo de credenciales de inicio de sesión como la principal causa de fugas de los datos. Dar prioridad a la defensa contra estos ataques podría reducir la probabilidad de actividades secundarias, como el despliegue de ransomware.

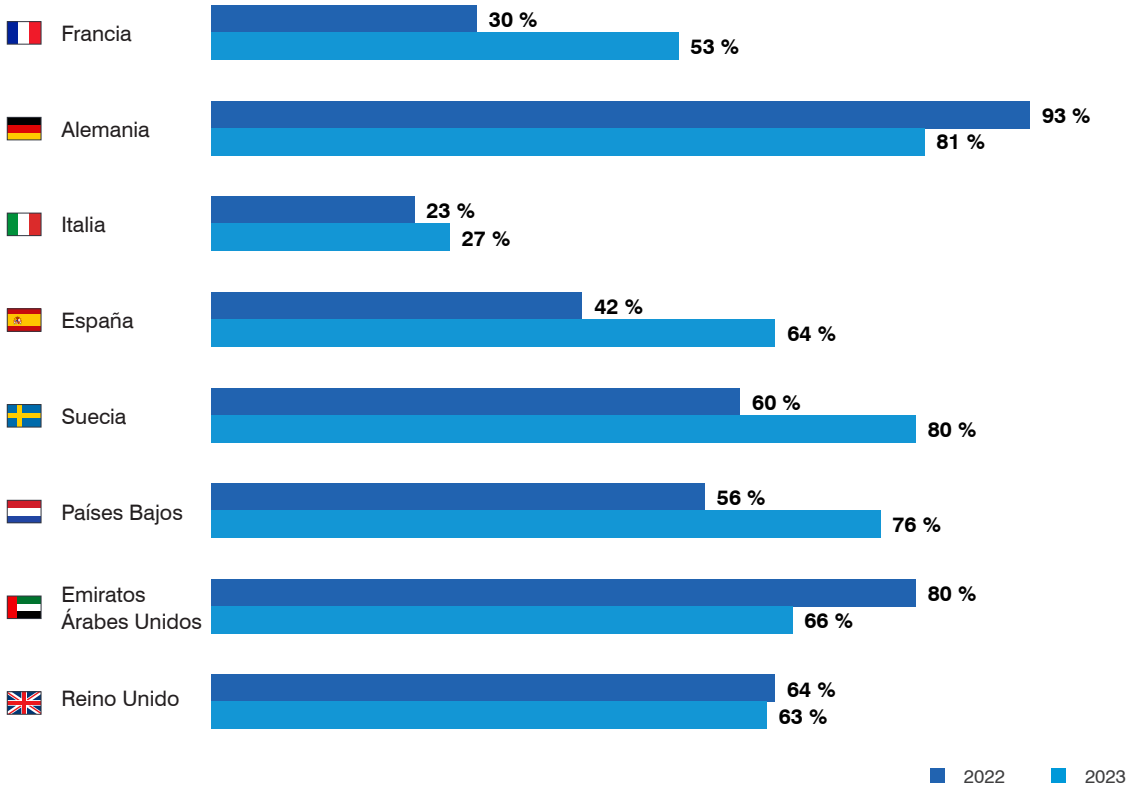
Infecciones de ransomware



Por otra parte, solo tres países (Alemania, Emiratos Árabes Unidos y Reino Unido) mostraron una mayor disposición a pagar. Alemania también registró el mayor porcentaje de empresas que pagaron un rescate (93 % frente a la media mundial del 54 %).

Esta estrategia pareció funcionar para las empresas alemanas y emiratíes, que tenían muchas más probabilidades de recuperar sus sistemas y datos tras un único pago. El hecho de que el 85 % de las empresas alemanas declararan haber sido víctimas de una infección con éxito de ransomware, el porcentaje más alto de la región, sugiere una relación entre su disposición a pagar y la intensidad del ataque.

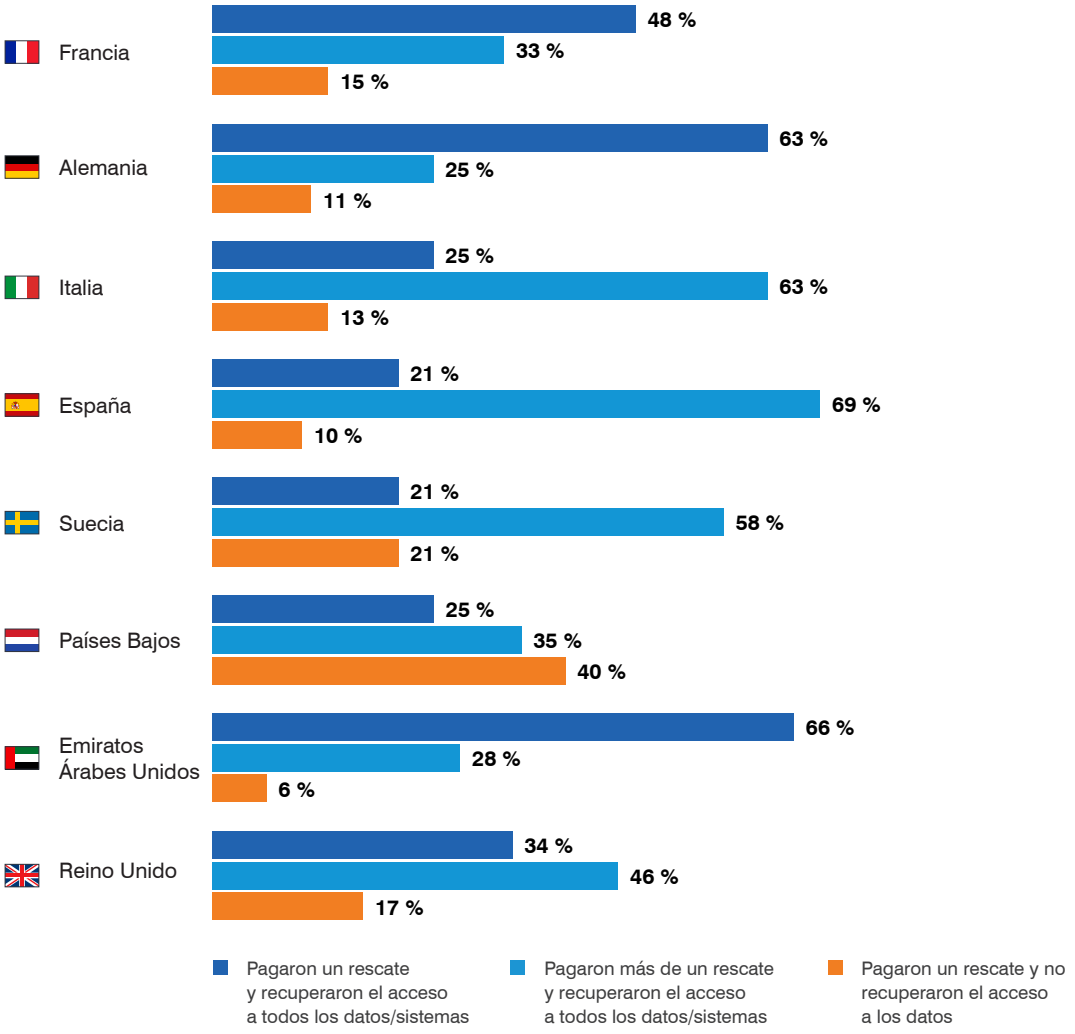
Porcentaje de organizaciones que han pagado un rescate



A las empresas británicas no les fue tan bien. De hecho, registraron el mayor porcentaje de infecciones repetidas. Casi el 14 % de ellas sufrieron 10 o más infecciones, frente a una media mundial del 5 %. Esto demuestra que el pago de rescates no garantiza la inmunidad contra futuros ataques, e incluso puede fomentarlos.

Las empresas holandesas fueron las que menos resultados positivos obtuvieron tras un pago. El 40 % afirmó no haber recuperado nunca sus datos, frente al 16 % en todo el mundo. Esto sugiere que algunos grupos de ransomware pueden no cumplir sus promesas, o no siempre ser capaces de restaurar los datos.

Resultados tras el pago de un rescate



Como nota positiva, los niveles de cobertura de los contratos de ciberseguro han mejorado, ofreciendo cierto alivio financiero. Francia es una excepción. El porcentaje de empresas parcial o totalmente cubiertas ha caído del 87 % en 2022 al 76 % en 2023. Esto se debe probablemente a que la mayor aseguradora de Francia ha anunciado que dejará de cubrir los ataques de ransomware.

Recomendaciones

Los resultados de nuestra encuesta muestran que los usuarios de Europa y Oriente Medio comprenden que su comportamiento entraña riesgos. Sin embargo, esto no suele bastar para convencerles de que la seguridad sea una prioridad. Algunos dan prioridad a la comodidad o al ahorro de tiempo, mientras que otros simplemente no saben si la seguridad de TI es su responsabilidad.

Para los usuarios que ya han comprendido que la seguridad es su responsabilidad

- Proporcione a los usuarios herramientas que les permitan ser más proactivos. Los botones de denuncia de mensajes de correo electrónico facilitan la denuncia de mensajes sospechosos. Además, las tecnologías de incentivos, como las etiquetas de advertencia de correo electrónico, pueden animar a los usuarios a actuar. Considere también la posibilidad de crear una red de defensores y un sistema de recompensas para animar a estos usuarios a modelar las buenas prácticas y convertirse en defensores de la denuncia ante sus colegas que no saben cómo hacerlo.

Para los usuarios que están seguros o que creen que la seguridad no es su responsabilidad

- Ofrezca formación personalizada y pertinente para cada función y sus responsabilidades. Aumentar el número de comunicaciones de la dirección y los responsables de seguridad para informar mejor a los usuarios de sus responsabilidades y su impacto en la empresa.

También es importante ofrecer formación en seguridad informática, así como capacidades de prevención, detección y respuesta de primer nivel. Las soluciones avanzadas pueden ayudar a encontrar el equilibrio adecuado entre unos controles de seguridad más estrictos y la productividad, reduciendo el número de amenazas a las que se enfrentan los usuarios. Por ejemplo, desplegar una solución de protección del correo electrónico con una eficacia del 99,9 % significa que la mayoría de los usuarios nunca tendrán que decidir cómo reaccionar ante un enlace sospechoso.

Por último, colabore con las partes interesadas de la empresa y dé prioridad a la facilidad de uso a la hora de implantar normas de seguridad. Los usuarios estarán menos inclinados a eludir los sistemas si la seguridad está alineada con sus objetivos. Y es más probable que utilicen un control si es intuitivo y no requiere formación.

MÁS INFORMACIÓN

Para obtener más información sobre cómo le ayuda Proofpoint a conocer sus riesgos asociados a los usuarios, y a mitigarlos con una estrategia de ciberseguridad centrada en las personas, visite **proofpoint.com/es**.

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentra el 85 % del Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.

proofpoint.

0402-001-06-01