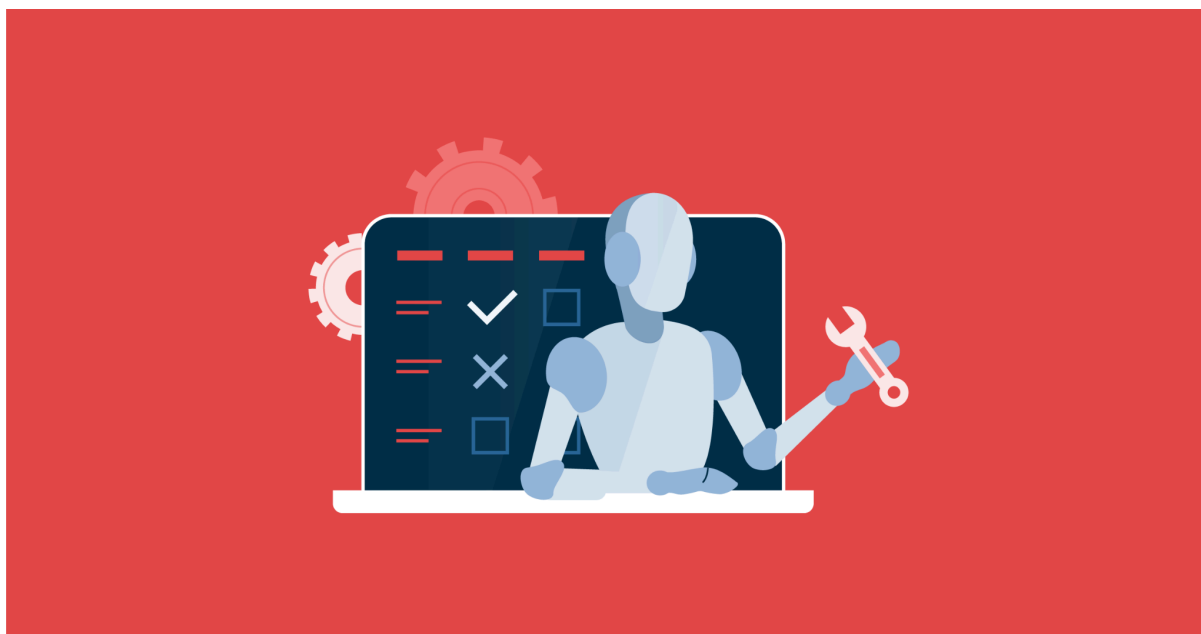


EL 61 % DE LOS EJECUTIVOS SENIOR HAN SIDO OBJETIVO DE CIBERATAQUES EN LOS ÚLTIMOS 18 MESES

- Según la última encuesta realizada por Capterra, los ataques dirigidos a este colectivo han aumentado un 57 % en los últimos tres años, de acuerdo con aquellos empleados en cuyas empresas ha habido uno o varios ciberataques a ejecutivos en los últimos 18 meses.
- España se sitúa entre los países donde más se han incrementado, por encima de Canadá, Italia, Brasil, Japón y México.



Barcelona, 04 de diciembre de 2024 — Los altos ejecutivos de las empresas españolas se han convertido en objetivos prioritarios para los ciberdelincuentes, según un reciente [estudio](#) elaborado por [Capterra](#), la plataforma líder de descubrimiento y reseñas de software. La encuesta, realizada a profesionales de TI y ciberseguridad en todo el mundo, revela que el 61 % de estos profesionales afirma que los ejecutivos de nivel senior en España han sufrido al menos un intento de ciberataque en los últimos 18 meses.

Que existe una exposición creciente frente a amenazas digitales es un hecho. Y es que los ataques dirigidos a este grupo han aumentado un 57 % en los últimos tres años. En este sentido, el estudio pone de manifiesto que los directivos de pequeñas y medianas empresas son especialmente vulnerables, dado que suelen manejar información crítica de

la compañía en sus dispositivos, convirtiéndose en objetivos estratégicos para los atacantes.

Así, España es el sexto país de los países encuestados donde más han incrementado los ciberataques a ejecutivos a escala internacional en los últimos tres años. Por encima, se sitúan Australia (69 %), Estados Unidos (69 %), Francia (66 %), Alemania (65 %) y Reino Unido (59 %). Por debajo, Canadá (56 %), Italia (55 %), Brasil (53 %), Japón (52 %) y México (37 %).



Conductas de riesgo comunes entre los ejecutivos

Actualmente, las empresas se apoyan en el software de seguridad, como antivirus (73 %), firewalls (72 %), sistemas de copia de seguridad (66 %), redes privadas virtuales (VPN) (65

%) y gestores de contraseñas (55 %). Sin embargo, se dan conductas de riesgo que facilitan los ciberataques, según los profesionales encuestados. Entre las más comunes se encuentran la descarga de archivos de origen no confiable (41 %), la falta de formación en ciberseguridad (38 %) y el uso de contraseñas débiles o poco seguras (34 %).

En cuanto a los tipos de ciberataques más frecuentes a ejecutivos senior, el 46 % de encuestados que trabajan en empresas donde ha habido ciberataques a ejecutivos en los últimos 18 meses señala que el phishing ha afectado a los directivos, convirtiéndose en la técnica más utilizada. Le siguen los ataques de malware (42 %), ransomware (36 %), robo de contraseñas (32 %), y la manipulación de registros DNS (25 %). Además, amenazas emergentes como los deepfakes, utilizados para falsificar identidades mediante inteligencia artificial, ya afectan al 15 % de los directivos, mientras que un 13 % ha sido víctima de ataques de intermediario o “man-in-the-middle”, donde el cibercriminal intercepta los datos enviados entre dos empresas.

Ante este escenario, las empresas españolas han incrementado su inversión en ciberseguridad. Según el estudio, un 76 % de los encuestados afirma que su empresa ha destinado más recursos a esta área en los últimos 18 meses, priorizando medidas clave como el fortalecimiento de la seguridad de las contraseñas (49 %), la mejora de la seguridad de la red (46 %), la actualización más frecuente del software (45 %) y la formación específica para ejecutivos en temas de seguridad (42 %).

Acciones que implementan las empresas para **contrarrestar los ciberataques**



Fuente: Encuesta de Capterra sobre Ciberseguridad para Ejecutivos 2024.

Pregunta: ¿Qué medidas o políticas ha puesto en marcha o ha mejorado su empresa en los últimos 18 meses para protegerse frente a los ciberataques? Seleccione todas las opciones que correspondan.

n: 149

Nota 1: Se muestran las 6 principales respuestas de 14 posibles.

Nota 2: Solo contestaron a esta pregunta aquellos encuestados que previamente indicaron que los ejecutivos de sus empresas han recibido ciberataques en los últimos 18 meses.



"La ciberseguridad es un imperativo para los altos cargos que manejan datos críticos", ha afirmado Alejandra Aranda, Content Analyst en Capterra. "Implementar medidas como una autenticación fuerte para usuarios con privilegios debe ser una prioridad en cualquier estrategia de seguridad. Es fundamental proteger la infraestructura de una organización, pero también reforzar la confianza en sus procesos internos".

La formación en ciberseguridad, una estrategia clave para reducir riesgos

Asimismo, la formación de los empleados sigue siendo una de las estrategias más efectivas para prevenir incidentes de seguridad. El informe revela que el 77 % de encuestados en España afirma que, al menos una vez al año, los empleados de su empresa reciben formación en ciberseguridad. Sin embargo, solo en el 40 % de casos se imparte formación específica sobre ingeniería social, una técnica cada vez más utilizada por los atacantes para manipular a las víctimas y obtener información confidencial.

En términos de contenido formativo, las áreas más comunes incluyen ciberseguridad general (75 %), privacidad de datos (68 %), seguridad en instalaciones físicas (42 %),

directrices sobre el uso seguro de redes sociales (37 %) y políticas de uso aceptable de recursos tecnológicos (33 %).

La falta de formación específica para los altos ejecutivos es un factor determinante en su exposición a estas amenazas. Aunque un 52 % de los encuestados afirma que los ejecutivos senior reciben formación avanzada en ciberseguridad, un 41 % indica que no se les imparte ningún tipo de capacitación adicional respecto al resto de los empleados. Entre las razones de esta carencia destacan la falta de tiempo o recursos (31 %), la percepción de que no es una prioridad (31 %), la creencia de que los ejecutivos ya tienen conocimientos suficientes (29 %), y la resistencia de estos a participar debido a sus agendas ocupadas (26 %).

Acerca de Capterra

Capterra ayuda a las empresas de todo el mundo a encontrar el software adecuado a sus necesidades. Fundada en 1999, la plataforma de opiniones de usuarios verificados, estudios independientes y herramientas de comparación adaptadas, ofrece cada mes a más de 5 millones de compradores de software una experiencia de descubrimiento que genera confianza. Para obtener más información, visita capterra.es.

Además de su plataforma de comparación de software, Capterra también publica estudios independientes sobre diversos temas. Nuestros informes anteriores están disponibles aquí: www.capterra.es/blog

Contacto de prensa

Capterra

pr@capterra.es

TEAM LEWIS

Noelia Iglesias / Clara Casanovas

T. + 34 935 228 600

capterra@teamlewis.com