cp<r>
CHECK POINT RESEARCH

SECURITY REPORT IBERIA 2026

ÍNDICE

01

INTRODUCCIÓN

INTRODUCCIÓN

La ciberseguridad vive un momento de inflexión. Si en los últimos años hablábamos de transformación digital, hoy hablamos de transformación impulsada por Inteligencia Artifcial. La IA ya no es una promesa futura ni una herramienta puntual: es el nuevo sistema operativo de las organizaciones. Está presente en aplicaciones internas y externas, en chatbots, en navegadoresy en sistemas autónomos que toman decisiones a velocidad de máquina. Y, como ocurre con toda revolución tecnológica, amplía de forma exponencial la superficie de ataque.

En Check Point Software creemos que la pregunta ya no es si las empresas adoptarán la IA, sino cómo lo harán de forma segura. El reto no está únicamente en proteger infraestructuras tradicionales, sino en salvaguardar todo el ecosistema digital donde interactúan datos, usuarios, aplicaciones y agentes autónomos. El navegador se ha convertido en una nueva superficie crítica; los empleados utilizan herramientas de IA generativa en su día a día; los modelos LLM procesan información sensible; y los entornos híbridos combinan data centers, cloud, dispositivos móviles y trabajo remoto. La seguridad debe ser preventiva, en tiempo real y capaz de operar en arquitecturas complejas y distribuidas.

La adquisición de Lakera, referente mundial en seguridad nativa para IA agéntica, nos permite ofrecer una protección para todo el ciclo de vida de la inteligencia artificial: modelos, agentes y datos. Lakera aporta capacidades de evaluación, protección en tiempo de ejecución y red teaming continuo que elevan el estándar de seguridad en LLM y aplicaciones generativas.

A esta apuesta se suman las recientes adquisiciones de Cyata, Cyclops y Rotate, que refuerzan nuestra estrategia en cuatro pilares: protección de redes híbridas, seguridad del espacio de trabajo digital, gestión integral de la superficie de exposición y seguridad específica para entornos impulsados por IA. Con ellas, ampliamos nuestras capacidades en gestión de identidad de agentes de IA, visibilidad avanzada de activos y protección de entornos gestionados y SaaS, integradas dentro de nuestra arquitectura Infinity.

Nuestro objetivo es claro: ofrecer a las organizaciones en España y Portugal una plataforma escalable y abierta que permita combinar múltiples piezas, (data center, aplicaciones web, usuarios en remoto o móviles), sin sacrificar seguridad ni eficiencia. No existe una única solución válida para todos los entornos; la resiliencia exige combinaciones cruzadas, integración y capacidad de crecimiento sin necesidad de reemplazar infraestructuras existentes.

La seguridad del futuro no será reactiva. Será predictiva, integrada y diseñada desde el origen para proteger entornos impulsados por inteligencia artificial. En Check Point Software estamos preparados para liderar esta nueva etapa.

MARIO GARCÍA

COUNTRY MANAGER CHECK POINT SOFTWARE EN ESPAÑA Y PORTUGAL

02

TENDENCIAS QUE REDEFINIERON EL PANORAMA EN 2025

MÁS ALLÁ DEL CORREO ELECTRÓNICO: INGENIERÍA SOCIAL MULTICANAL

En 2025 la ingeniería social dejó de estar asociada casi exclusivamente al phishing por correo electrónico para convertirse en un conjunto de técnicas combinadas, distribuidas en múltiples canales y apoyadas en dinámicas psicológicas cada vez más refinadas.

A lo largo de 2025 se consolidaron campañas que combinaban mensajes en redes sociales, llamadas telefónicas, plataformas de mensajería instantánea, entornos de colaboración empresarial y flujos legítimos de autenticación en la nube.

ClickFix: la ingeniería social que traslada la ejecución al usuario

ClickFix, detectada inicialmente en 2024, aumentó un 500% su actividad en 2025 y estuvo presente en casi la mitad de las campañas de malware documentadas.

Se basa en la manipulación del usuario para que ejecute voluntariamente una serie de instrucciones que simulan ser la resolución de un CAPTCHA, validar un error del sistema o completar un proceso aparentemente necesario para continuar navegando.

Durante 2025 fue utilizado tanto por grupos criminales asociados a campañas de infostealers como por actores más sofisticados, incluidos algunos vinculados a operaciones patrocinadas por Estados.

Ingeniería social basada en voz: el arma preferida en ataques de alto impacto económico

Otra de las transformaciones más relevantes en 2025 fue el auge de la suplantación telefónica en entornos empresariales. Lo que tradicionalmente se asociaba al fraude minorista o a estafas dirigidas a particulares evolucionó hacia un vector de acceso inicial en intrusiones corporativas complejas.

En 2025, actores altamente organizados utilizaron llamadas dirigidas a servicios de soporte técnico, departamentos de TI o proveedores externos para solicitar restablecimientos de credenciales, modificación de factores de autenticación o concesión de accesos temporales. La suplantación por voz introdujo un elemento diferencial: el componente emocional y la presión en tiempo real. A diferencia del phishing por correo electrónico, la llamada permite insistir, generar urgencia y adaptarse dinámicamente a las respuestas de la víctima.

> CLICKFIX, DETECTADA INICIALMENTE EN 2024, AUMENTÓ UN 500% Y ESTUVO EN CASI LA MITAD DE LAS CAMPAÑAS DE MALWARE

Incidentes de ciberseguridad más destacados en Iberia en 2025

España y Portugal afrontaron en 2025 un contexto de amenazas digitales en crecimiento, con un aumento sostenido de incidentes y varios casos de alto impacto que afectaron tanto a administraciones públicas como a grandes empresas y pymes.

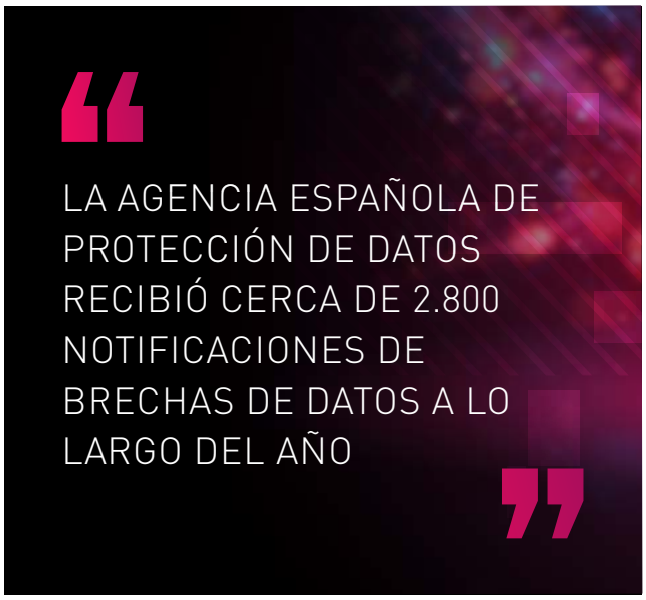
En España, el Instituto Nacional de Ciberseguridad (INCIBE) gestionó 122.223 incidentes, un 26 % más que en 2024. El incremento estuvo marcado por el phishing, el malware y el ransomware, que siguieron siendo los vectores predominantes.

Entre los casos más relevantes destacó la filtración de datos de aproximadamente 180.000 miembros de la Guardia Civil, las Fuerzas Armadas y personal del Ministerio de Defensa, cuyos correos electrónicos y usuarios aparecieron en foros clandestinos. En el ámbito institucional, el grupo NoName057 lanzó ataques de denegación de servicio contra webs de diputaciones y ayuntamientos. El Ayuntamiento de Badajoz fue víctima de un ransomware que paralizó servicios digitales y trámites administrativos, mientras que la Federación de Asociaciones de Autónomos (ATA) confirmó la exposición de 240.000 registros de asociados.

A nivel agregado, España se situó entre los países europeos más afectados por ransomware, y la Agencia Española de Protección de Datos recibió cerca de 2.800 notificaciones de brechas de datos personales a lo largo del año.

El ransomware también tuvo presencia destacada. A finales de 2025, el grupo Nova reivindicó un ataque contra la organización sindical de profesores SPZC, con amenazas de publicar información sensible.

En conjunto, 2025 confirmó que la Península Ibérica se enfrenta a un escenario de riesgo estructural creciente, con una combinación de ataques oportunistas, campañas coordinadas y vulnerabilidades en infraestructuras esenciales que obligan a reforzar capacidades de prevención y respuesta en todos los sectores.



Actividad de ingeniería social en plataformas de comunicación empresarial

Durante 2025 también se observó un desplazamiento hacia plataformas de mensajería corporativa como Microsoft Teams o Slack.

En varios casos documentados, los atacantes se hicieron pasar por personal de soporte interno y persuadieron a empleados para instalar herramientas de acceso remoto. A partir de ahí, el compromiso avanzó hacia fases más destructivas.

EL ECOSISTEMA DEL RANSOMWARE EN 2025

En 2025, el ransomware alcanzó niveles sin precedentes pese a la reconfiguración del ecosistema criminal. El año comenzó con una campaña masiva de explotación por parte de Cl0p y continuó con la desaparición de varios grandes grupos de ransomware como Servicio, lo que abrió espacio a nuevos actores sin frenar la actividad.

Las cifras son especialmente relevantes: más de 7.960 víctimas en todo el mundo vieron sus datos publicados en sitios de filtración gestionados por grupos de doble extorsión, lo que supone un aumento del 53% respecto al año anterior. Solo en el primer trimestre se registraron 2.289 víctimas, un aumento del 134% nteranual, impulsadas por la explotación de vulnerabilidades de día cero. Ese récord fue superado en el cuarto trimestre, que cerró con 2.473 víctimas, el dato más alto registrado en la historia de Check Point Software.

Reconfiguración a mitad de año y reajuste de afiliados

En el segundo trimestre de 2025, varios programas relevantes de Ransomware como Servicio desaparecieron de forma repentina, aunque el volumen de víctimas siguió muy por encima de los niveles de 2024.

8Base y Phobos fueron desarticulados en operaciones internacionales que incluyeron la incautación de sus sitios y la detención de operadores. Otros grupos como BianLian, Hunters y Cactus cambiaron de marca, evolucionaron hacia modelos centrados solo en la extorsión de datos o dejaron de publicar víctimas. RansomHub, que había difundido más de 760 víctimas desde 2024, cerró sin previo aviso en abril de 2025.

Este vacío fue aprovechado por Qilin y DragonForce, que reclutaron a antiguos afiliados de RansomHub y LockBit. En el tercer trimestre ya estaban entre los operadores más activos. Qilin fue el gran beneficiado del proceso: incrementó de forma sostenida el número de víctimas publicadas y, a mediados de 2025, se situó entre los actores de RaaS más activos, superando a varias marcas históricas.

Proliferación de grupos independientes de doble extorsión

El número de marcas activas en sitios de filtración pasó de unas 90 a finales de 2024 a 140 en 2025, un incremento superior al 50 %. Muchos de estos nuevos actores operaban sin programas formales de afiliados, con estructuras reducidas y menor infraestructura que los grandes esquemas de Ransomware como servicio. Qilin recuperó protagonismo, Akira intensificó su actividad, Cl0p reapareció con nuevas campañas masivas y LockBit regresó bajo la marca LockBit 5.0.

Actividad en España y Portugal

La actividad de doble extorsión en España y Portugal durante 2025 mostró una concentración clara en un número limitado de actores, aunque con un ecosistema fragmentado en su conjunto.

Qilin fue el grupo con mayor peso en la región, representando el 20% del total de organizaciones publicadas en sitios de filtración vinculadas a España y Portugal. Muy por detrás se situó Akira, con un 9%, seguido por Space Bears y Nova, ambos con un 4%.

El conjunto de otros grupos menores acumuló el 46 % restante, lo que refleja un mercado todavía fragmentado, con múltiples actores de menor tamaño operando bajo marcas efímeras o de reciente creación.

Estos datos evidencian que, aunque el ecosistema global experimentó una proliferación de marcas durante el año, la actividad efectiva en la Península Ibérica estuvo dominada por un número reducido de grupos con capacidad operativa consolidada, mientras que casi la mitad de los incidentes se distribuyó entre actores menos conocidos o emergentes.

Qilin: el operador dominante

Qilin fue el grupo de Ransomware como Servicio más activo de 2025, con más de 1.000 víctimas publicadas en su sitio de filtración tras negarse a pagar. Activo desde 2022, aprovechó la desaparición de RansomHub y la inactividad de LockBit para ganar terreno.

Tras el colapso de RansomHub en abril, reclutó a numerosos afiliados y casi triplicó su actividad mensual: de unas 35 víctimas en el primer trimestre a más de 150 en el cuarto. Según los datos disponibles, lideró de forma sostenida el número de víctimas publicadas, por delante de Akira, DragonForce y Play.

Perfil de objetivos e incentivos para afiliados

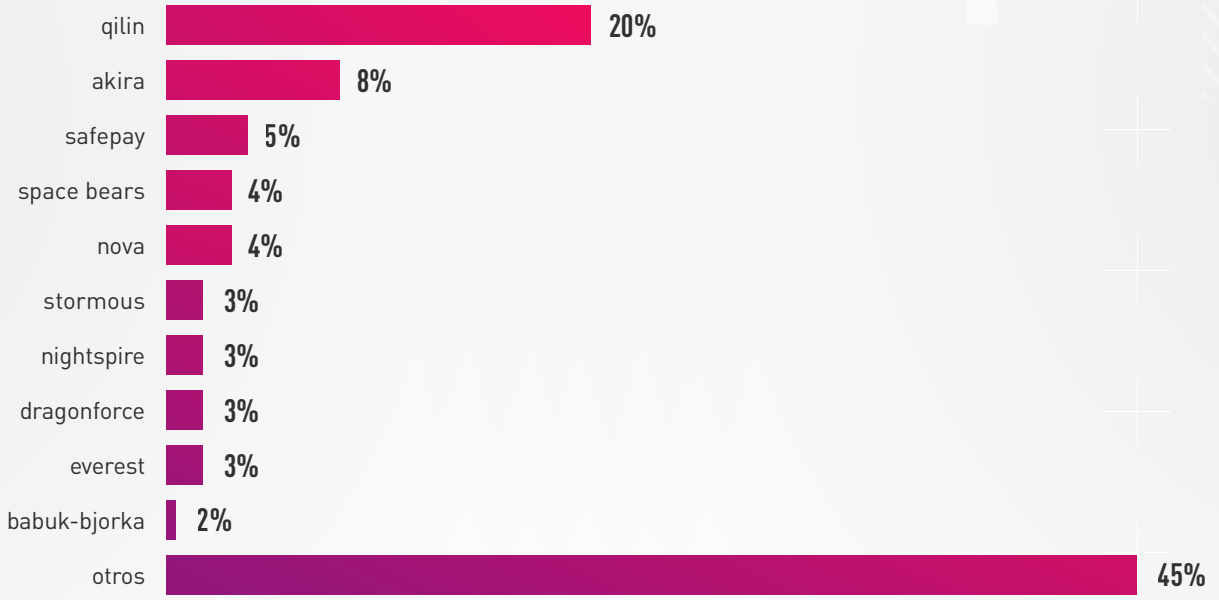
Aunque Qilin se presenta como un grupo "idealista" con motivaciones patrióticas, su actividad es global —con la excepción de países de la Comunidad de Estados Independientes—, no se limita a ningún sector concreto y responde claramente a fines económicos.

El grupo ofrece a sus afiliados un reparto de beneficios muy competitivo, entre el 80 % y el 85 %, lo que lo convirtió en una opción especialmente atractiva frente a otros programas de Ransomware como Servicio en un año marcado por la reubicación masiva de afiliados.

ClOp: la excepción basada en zero-day

ClOp fue uno de los protagonistas del ransomware en 2025. A diferencia de otros grupos, basó sus campañas en la explotación estratégica de vulnerabilidades de día cero en software empresarial para robar datos y extorsionar sin recurrir al cifrado.

En febrero atacó las soluciones de transferencia de archivos de Cleo mediante dos fallos de ejecución remota de código, lo que dejó más de 335 víctimas, sobre todo en manufactura, retail y logística en Norteamérica, y disparó las cifras del primer trimestre.



Top 10 de operadores en base al porcentaje de víctimas de ransomware publicadas - España y Portugal

Entre el tercer y cuarto trimestre explotó vulnerabilidades en Oracle E-Business Suite (CVE-2025-61882 y CVE-2025-61884), activas desde agosto antes de que existieran parches. La posterior filtración del código en octubre permitió que otros actores replicaran los ataques y amplió el alcance del incidente.

El regreso de LockBit

Tras un periodo de inactividad significativo, LockBit reapareció en 2025 con una versión renovada de su infraestructura. Su retorno evidenció que las "marcas" consolidadas conservan capacidad de atracción para afiliados cuando ofrecen estabilidad y continuidad operativa.

La reaparición confirma el carácter cíclico del ecosistema: caída, rebranding y regreso bajo nueva identidad.

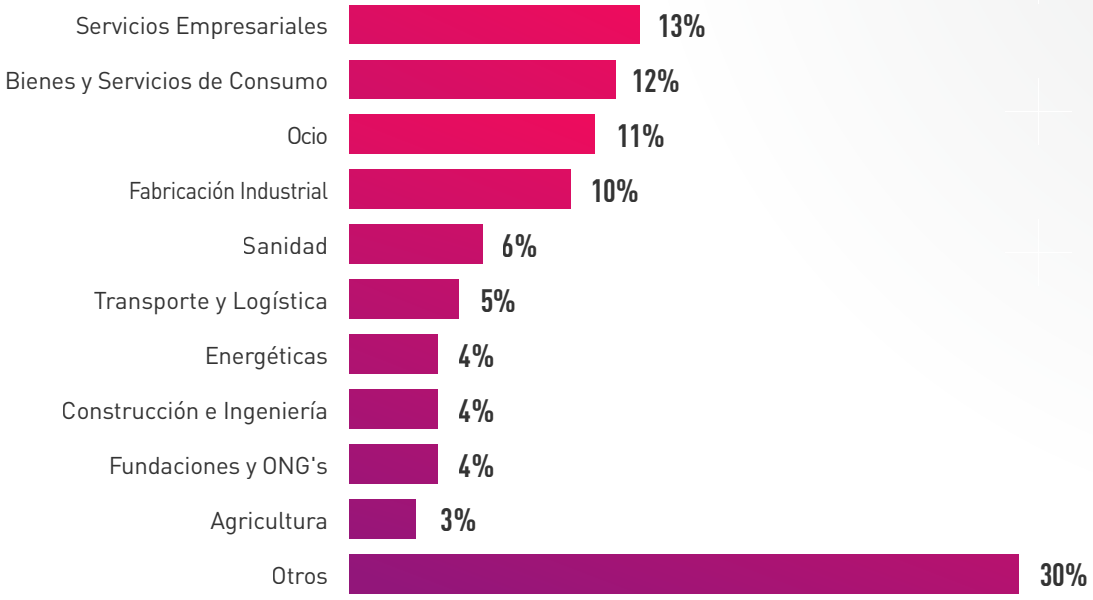
Restricciones al pago y obligación de reporte

El crecimiento sostenido de víctimas de ransomware en 2025 confirma que las operaciones policiales contra grandes grupos de Ransomware como Servicio no lograron reducir el volumen global de ataques. Los afiliados se reagruparon bajo nuevas marcas o migraron a otras plataformas, lo que llevó a los gobiernos a centrar su estrategia en limitar los incentivos financieros que sostienen este modelo criminal.

La Directiva NIS2 de la Unión Europea impuso plazos estrictos de comunicación de incidentes, incluyendo información sobre posibles pagos. En conjunto, el enfoque político se orienta a reducir la rentabilidad del ransomware mediante transparencia y restricciones financieras.

En España y Portugal, los sectores más afectados fueron servicios empresariales (13%), bienes y servicios de consumo (12%), ocio (11%) e industria manufacturera (10%). Sanidad representó el 6%, transporte el 5%.Esta distribución confirma que los atacantes priorizan organizaciones privadas con mayor probabilidad de pago, mientras que el menor peso del sector público se alinea con las crecientes restricciones regulatorias sobre el pago de rescates.

> LOS SECTORES MÁS AFECTADOS FUERON SERVICIOS EMPRESARIALES, BIENES Y SERVICIOS DE CONSUMO, OCIO E INDUSTRIA MANUFACTURERA



Top 10 de sectores en base al porcentaje de víctimas de ransomware publicadas - España y Portugal

DEL RECONOCIMIENTO AL CONTROL DEL RELATO: EL IMPACTO OPERACIONAL DEL CIBERESPECIO EN LOS CONFLICTOS DE 2025

En 2025 las ciber operaciones dejaron de percibirse como acciones accesorias dentro de los conflictos geopolíticos para consolidarse como un componente integrado de la estrategia militar, política e informativa. El informe no analiza el ciberespacio como un escenario aislado, sino como un dominio que interactúa de forma constante con operaciones físicas, decisiones políticas y campañas de influencia.

La actividad observada durante el año puede agruparse en funciones recurrentes que, lejos de ser fases estrictamente secuenciales, se superponen y se refuerzan entre sí. En este apartado se analizan cuatro conflictos activos durante 2025: Rusia-Ucrania, Irán-Israel, India-Pakistán y Tailandia-Camboya.

Actividad de posicionamiento y preparación

La actividad de posicionamiento y preparación constituye la base sobre la que se apoyan fases posteriores del conflicto. En este estadio, el objetivo no es necesariamente provocar una interrupción visible, sino establecer acceso persistente, mapear infraestructuras críticas y comprender dependencias estratégicas.

En el conflicto entre Rusia y Ucrania, se documentó acceso el sostenido a redes logísticas, sistemas de transporte e infraestructuras energéticas. La obtención de visibilidad sobre cámaras conectadas a Internet, nodos de telecomunicaciones y sistemas asociados permitió a los operadores mantener una comprensión casi en tiempo real de movimientos y actividad en zonas estratégicas.

Este tipo de posicionamiento no busca necesariamente un impacto inmediato. Su valor reside en la acumulación de opciones operativas. El acceso puede permanecer latente hasta que el contexto lo haga oportuno.

Actividad de apoyo operacional

En el enfrentamiento entre Israel e Irán, infraestructuras civiles previamente comprometidas fueron utilizadas para obtener visibilidad operativa. En junio de 2025, operadores iraníes accedieron a cámaras de seguridad en torno al Instituto Weizmann, monitorizando movimientos antes y durante un ataque con misiles, convirtiendo dispositivos de consumo en herramientas de reconocimiento.

En el conflicto ruso-ucraniano también se observó esta integración. Un ataque vinculado a Ucrania afectó la infraestructura utilizada para distribuir firmware de drones rusos, dificultando su despliegue. Por su parte, el grupo APT44 (Sandworm), vinculado a Rusia, operó en paralelo a bombardeos, atacando redes energéticas y logísticas ucranianas, a menudo acompañado de campañas de desinformación y ataques DDoS.

Durante la confrontación entre India y Pakistán en mayo de 2025, las operaciones cibernéticas —incluyendo DDoS, intrusiones de malware y suplantación GPS— coincidieron con intercambios de drones y misiles, contribuyendo a degradar la conciencia situacional?. De forma similar, tras un choque fronterizo entre Tailandia y Camboya, grupos alineados intensificaron ataques contra redes gubernamentales y militares.

Estos casos reflejan cómo, en 2025, las operaciones cibernéticas funcionaron cada vez más como habilitadores en tiempo real de acciones militares y políticas, apoyadas en fases previas de posicionamiento digital. Las operaciones cinéticas y cibernéticas se coordinan en una integración multidominio en un contexto de guerra híbrida en la cual se necesita no solamente la superioridad física sino también cibernética y en el espectro electromagnético.

Actividad de modelado narrativo

En 2025, la configuración narrativa se consolidó como un eje central de las operaciones cibernéticas, con efectos a menudo más duraderos que la disrupción técnica. El objetivo fue moldear percepciones, señalar capacidades e influir en audiencias nacionales e internacionales. La visibilidad y la interpretación pública resultaron tan importantes como el impacto técnico.

Las campañas de influencia, filtraciones selectivas y reivindicaciones públicas fueron frecuentes. Rusia mantuvo una estrategia sostenida de amplificación narrativa mediante redes digitales y generación automatizada de contenido, donde el daño técnico funcionó principalmente como mecanismo de señalización.

El ataque de ransomware contra el Shamir Medical Center en Israel ilustra esta dinámica. Aunque inicialmente atribuido a criminalidad convencional vinculada a Qilin, posteriores investigaciones lo relacionaron con actores alineados con Irán, subrayando su dimensión política.

Durante la escalada entre Irán e Israel, se difundieron alertas falsas y mensajes fraudulentos diseñados para erosionar la confianza en los sistemas de emergencia. Las autoridades israelíes registraron más de 1.200 operaciones de ingeniería social dirigidas a la población. En las tensiones entre Tailandia y Camboya, ataques masivos contra plataformas gubernamentales y filtraciones de datos buscaron generar presión informativa más que efectos tácticos directos.

Rusia también intensificó campañas de saturación informativa tras ataques cinéticos, destacando el crecimiento de redes como Pravda, capaces de publicar miles de artículos diarios con apoyo de IA.

En conjunto, los conflictos de 2025 mostraron que la actividad cibernética ya no actúa como herramienta aislada, sino como componente integrado de la guerra moderna: prepara el entorno antes de la escalada, acompaña las operaciones y ejerce presión psicológica sostenida, explotando la incertidumbre y moldeando la percepción pública.

Qué cambiará en 2026: negar la persistencia, no solo la intrusión

La defensa en 2026 no debe centrarse únicamente en impedir el acceso inicial, sino en impedir que ese acceso se consolide.

La persistencia prolongada es el elemento que transforma una intrusión en una amenaza estructural. Si el atacante puede permanecer, observar y expandirse sin generar alertas críticas, el riesgo se multiplica.

Por ello, negar la persistencia implica reforzar controles de identidad, supervisar infraestructuras tradicionalmente menos visibles y validar de forma continua la integridad de servicios críticos.

> LA DEFENSA EN 2026 NO DEBE CENTRARSE ÚNICAMENTE EN IMPEDIR EL ACCESO INICIAL, SINO EN IMPEDIR QUE ESE ACCESO SE CONSOLIDE

03

PANORAMA DE LA IA EN LA CIBERSEGURIDAD

DE LA INTEGRACIÓN A LA AUTONOMÍA

En 2025 la inteligencia artificial quedó tan profundamente integrada en la actividad digital que distinguir entre ataques "relacionados con IA" y operaciones convencionales se volvió cada vez más complejo. A diferencia de 2023 y 2024, cuando el uso de IA por parte de los atacantes era fácilmente reconocible, en 2025 su presencia se normalizó hasta diluirse en el trasfondo operativo.

La IA se utiliza en prácticamente todas las fases de la actividad cibernética y, sin embargo, rara vez es visible. La mayoría de los resultados maliciosos no permiten saber si un modelo participó en su creación o ejecución. El informe State of AI in Cyber Security publicado en abril de 2025, ya advertía que, a medida que los modelos se integraran en el trabajo diario, la frontera entre amenazas habilitadas por IA y ataques tradicionales acabaría desdibujándose. A finales de ese mismo año, esa previsión se había materializado.

La inteligencia artificial sustenta hoy el desarrollo de software, la ingeniería social, el diseño de malware, la minería de datos, las operaciones de influencia, el reconocimiento, el descubrimiento de vulnerabilidades e incluso la post-explotación. Paralelamente, los actores de amenaza no solo ampliaron su uso de estas capacidades, sino que comenzaron a dirigir ataques contra el propio ecosistema de IA. La adopción de marcos agentivos, servidores MCP y modelos desplegados localmente abrió nuevas superficies de exposición.

LOS SERVICIOS DE IA COMO SUPERFICIE DE ATAQUE

La integración de asistentes y agentes inteligentes en correo electrónico, calendarios, documentos y bases de conocimiento internas ha ampliado su acceso a datos sensibles y sistemas conectados. Esa confianza implícita ha convertido a la IA en una superficie de ataque relevante.

Ataques de inyección directa e indirecta de prompts

Lakera observó en su revisión del cuarto trimestre de 2025 que los ataques indirectos solían requerir menos intentos que los directos, al aprovechar supuestos operativos normales del agente en lugar de intentar anular sus salvaguardas. También se identificaron muestras de malware que incorporaban instrucciones en lenguaje natural destinadas a engañar herramientas de detección basadas en LLM, señal de que los motores de defensa impulsados por IA ya son considerados objetivos.

LOS LLM COMO VECTOR DE FUGA DE DATOS SENSIBLES

La adopción masiva de IA generativa en entornos corporativos abrió otro frente de riesgo. La integración cotidiana de estos servicios difumina la frontera entre datos internos y plataformas externas.

Nuestros datos de GenAI Protect correspondientes al cuarto trimestre de 2025 muestran que el 89% de las empresas se vio afectado mensualmente por prompts considerados de riesgo. Uno de cada 41 fue clasificado como de alto riesgo, lo que representa un incremento del 97% respecto al primer trimestre del año. Las exposiciones más frecuentes incluyeron información personal identificable, artefactos internos de red y código fuente.

USO DE LA IA EN INGENIERÍA SOCIAL Y ROBO DE IDENTIDAD

La generación automática de texto alcanzó plena madurez operativa. Campañas de phishing, sextorsión, fraude BEC e influencia política se desarrollaron en múltiples idiomas y con adaptación cultural precisa, sin repetir estructuras evidentes. La automatización eliminó la necesidad de operadores humanos con dominio lingüístico específico.

Deepfakes de audio: suplantación en tiempo real y llamadas autónomas

La clonación de voz en tiempo real, posible con apenas minutos de audio disponible en redes sociales, se utilizó para suplantar figuras públicas y familiares con fines de fraude financiero. Surgieron sistemas de llamadas automatizadas basadas en IA capaces de gestionar conversaciones adaptativas, recopilar códigos OTP y operar sin intervención humana directa.

Suplantación en vídeo: del deepfake pregrabado al intercambio facial en directo

Los deepfakes pregrabados se emplearon en estafas de inversión y campañas de influencia. Paralelamente, herramientas de intercambio facial en directo alcanzaron calidad suficiente para operar en videollamadas reales con hardware convencional. Se documentaron entrevistas laborales fraudulentas vinculadas a actores patrocinados por estados. La combinación de clonación de voz y manipulación facial en tiempo real permitió replicar identidades audiovisuales completas durante interacciones en vivo.

Identidades sintéticas y fraude en procesos KYC

Las identidades generadas por IA se convirtieron en un método habitual para superar procesos de verificación de identidad. El mercado clandestino ofrece desde imágenes faciales sintéticas de bajo coste hasta paquetes KYC (Know Your Customer) completos adaptados a regiones específicas. En 2025, autoridades de Hong Kong arrestaron a varios sospechosos acusados de utilizar deepfakes para eludir sistemas de verificación bancaria y abrir cuentas fraudulentas.

La identidad, tradicionalmente asociada a apariencia y voz, se consolidó como uno de los elementos más frágiles del ecosistema digital

PERSPECTIVA

A finales de 2025, la inteligencia artificial dejó de ser únicamente una herramienta de apoyo y pasó a actuar como participante activo en operaciones cibernéticas. Modelos, datos e integraciones distribuidas amplían la superficie de ataque, mientras los adversarios utilizan IA para escalar ingeniería social, acelerar el desarrollo de malware y optimizar la explotación de vulnerabilidades.

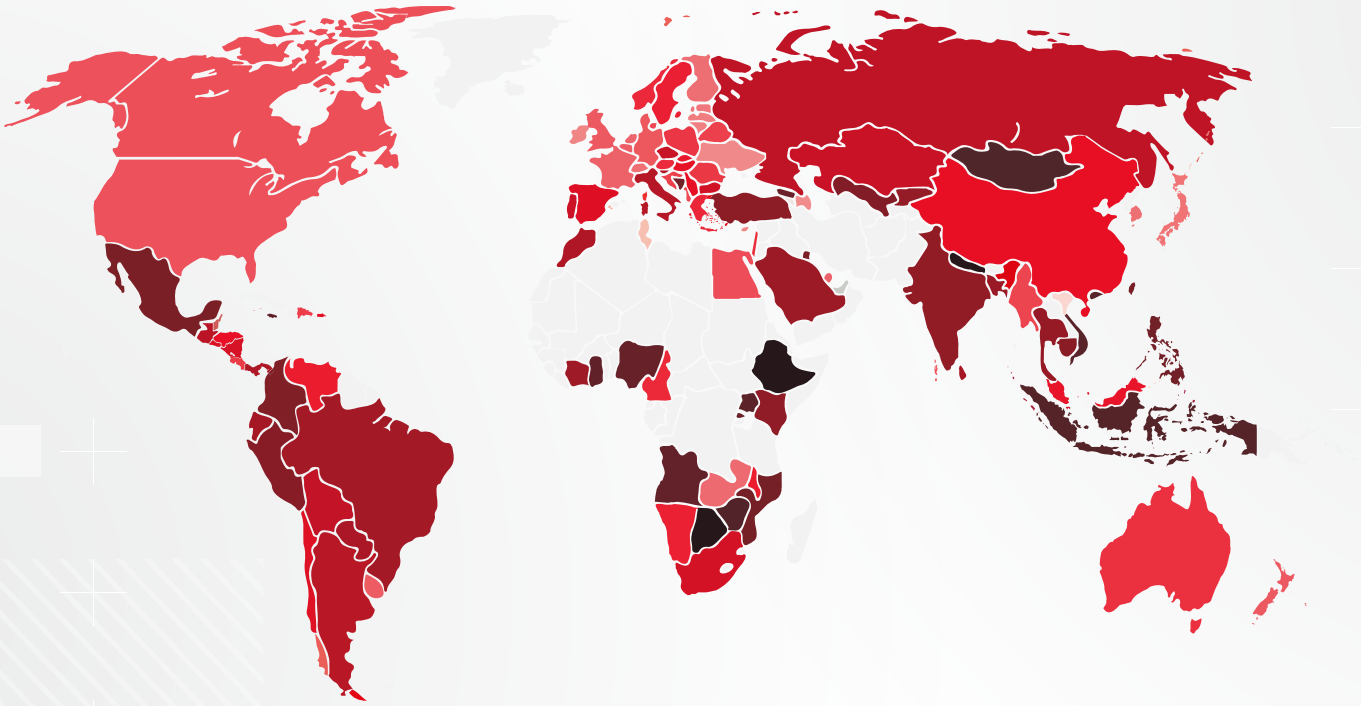
La IA ya no es un elemento separado dentro de la ciberseguridad. Está entrelazada en todo el entorno digital y redefine el equilibrio entre automatización, control y riesgo.

04

ANÁLISIS GLOBAL Y REGIONAL

MAPA GLOBAL DE ÍNDICE DE AMENAZAS

El mapa global del índice de amenazas muestra el nivel de riesgo cibernético en las distintas regiones del mundo y permite identificar las áreas con mayor exposición. La visualización refleja la distribución del riesgo en función de la actividad detectada y sitúa en niveles más elevados a aquellas zonas donde la presión ofensiva es más intensa.



Riesgo máximo

Riesgo mínimo

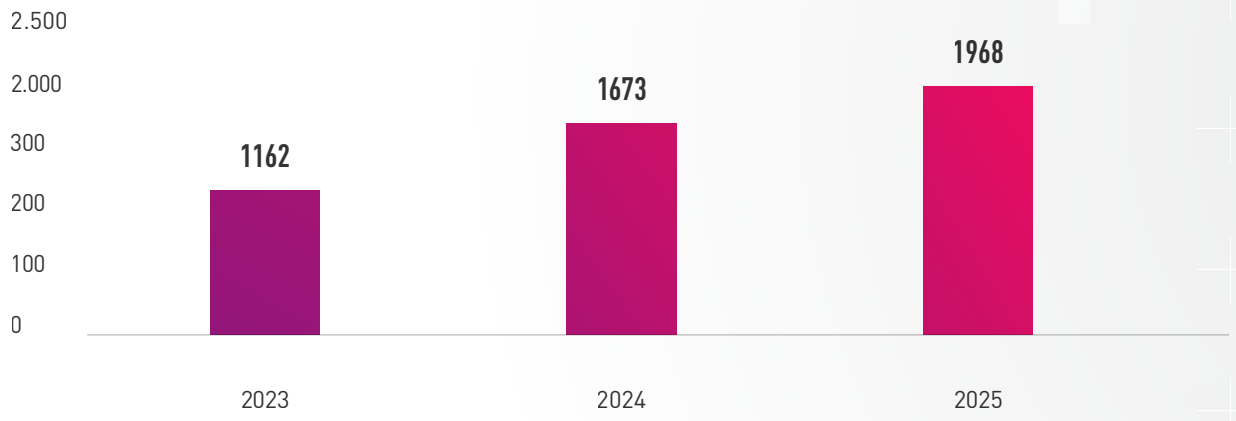
Datos insuficientes

Mapa global del índice de amenazas de ciberataques

ATAQUES POR EMPRESA

La telemetría global de Check Point muestra un aumento sostenido de los ciberataques semanales por empresa. Tras un fuerte repunte en 2024, la tendencia continuó al alza en 2025, alcanzando el nivel más alto registrado en el periodo analizado.

En 2025, las organizaciones sufrieron una media de 1.968 ataques semanales, lo que supone un incremento interanual del 18 % y cerca de un 70 % más que en 2023. Las cifras reflejan una escalada continuada de la actividad maliciosa a escala global.



Media mensual de ciberataques por empresa, 2023-2025

ATAQUES SEMANALES POR REGIÓN

El incremento en el número medio de ciberataques por empresa no se distribuyó de manera uniforme entre regiones. En 2025, Norteamérica registró un aumento interanual del 23 %, mientras que Europa experimentó un crecimiento del 20 %. América Latina y la región de Asia-Pacífico mostraron subidas más moderadas, del 13 % y del 10 %, respectivamente. África siguió siendo la región más afectada en términos de volumen absoluto, con más de 3.000 ataques semanales por organización, aunque su crecimiento interanual fue el más contenido, con un 5 %.

ATAQUES SEMANALES POR INDUSTRIA Y REGIÓN

GLOBAL

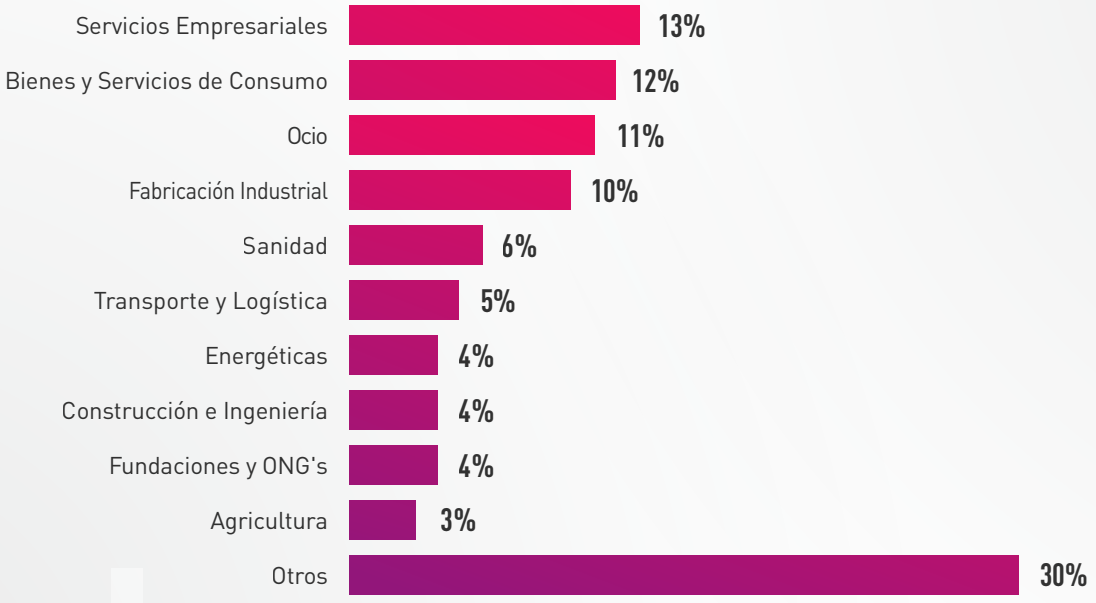
En 2025, la actividad de ataque creció en prácticamente todos los sectores. Educación volvió a situarse como el ámbito más atacado, con una media de 4.352 ataques semanales por empresa, un 22% más que el año anterior. **Gobierno, Telecomunicaciones y Sanidad** alcanzaron también sus niveles más elevados desde que existen registros comparables.

A medida que los ciberdelincuentes ampliaron su foco, las infraestructuras críticas y los sectores industriales experimentaron una escalada significativa. **Energía y Utilities, Automoción y Aeroespacial y Defensa** registraron incrementos interanuales que oscilaron entre el 21% y el 3 %. Se trata de sectores que sustentan servicios esenciales y capacidades estratégicas, lo que los convierte en objetivos prioritarios tanto para campañas oportunistas como para operaciones alineadas con intereses geopolíticos.

ESPAÑA Y PORTUGAL

En España y Portugal, la distribución sectorial del ransomware muestra un patrón específico. Los Servicios Empresariales concentran el 13 % de los incidentes publicados, seguidos de Bienes y Servicios de Consumo, con un 12 %, y Hostelería, Viajes y Ocio, con un 11%. La Industria Manufacturera representa el 10%, mientras que Sanidad y Servicios Médicos alcanzan el 6%.

Transporte y Logística supone el % del total, Energía y Utilities el 4 %, al igual que Construcción e Ingeniería y ONGs. Este reparto refleja la exposición de un tejido empresarial donde los servicios y la actividad turística tienen un peso estructural relevante, junto con una base industrial y logística significativa.



Top 10 de sectores en base al porcentaje de víctimas de ransomware publicadas - España y Portugal

En cuanto a actores de ransomware, Qilin encabeza la actividad en la región con el 20 % de los casos publicados, seguido por Akira con un 9 % y Safepay con un 5 %. Otros grupos como Space Bears, Nova, Stormous, Nightspire, Dragonforce, Everest y Babuk-Bjorka presentan porcentajes más reducidos, mientras que el conjunto de otros actores representa el 46 % restante.

Desde el punto de vista geográfico, España concentra el 2 % de los incidentes globales de ransomware publicados y Portugal el 0,4 %, lo que sitúa a ambos países en torno al 2,4 % del total mundial.

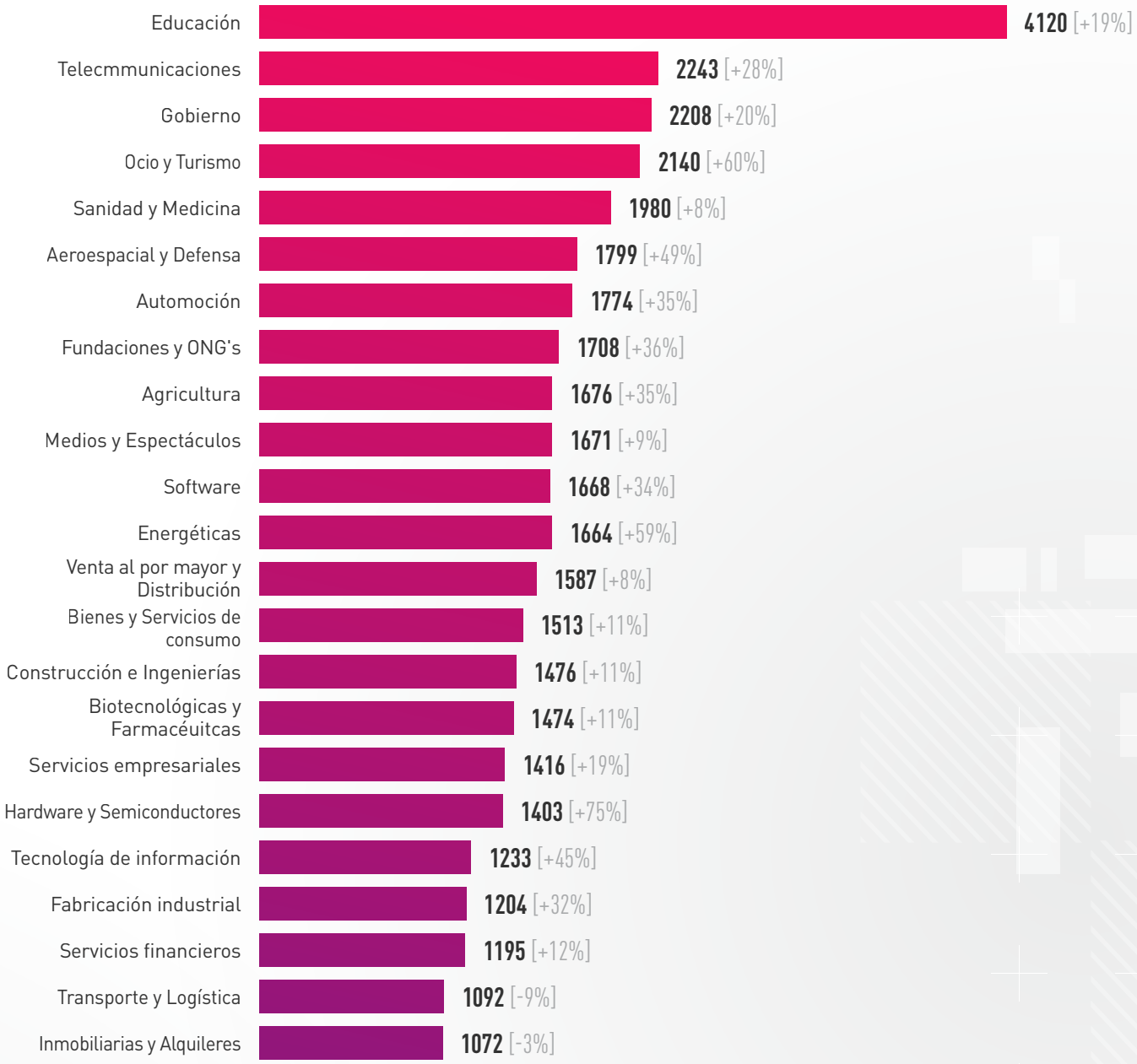
> ESPAÑA Y PORTUGAL CONCENTRAN EN CONJUNTO EN TORNO AL 2,4 % DEL TOTAL MUNDIAL DE LOS INCIDENTES GLOBALES DE RANSOMWARE

PAÍS	% DEL TOTAL
Estados Unidos	52%
Reino Unido	5%
Canadá	4%
Alemania	4%
Francia	2%
Italia	2%
España	2%
Brasil	2%
Australia	2%
India	2%
Japón	1,1%
México	1%
Emiratos Árabes	0,9%
Tailandia	0,8%
Singapur	0,8%
Suiza	0,8%

PAÍS	% DEL TOTAL
Corea del Sur	0,7%
Taiwán	0,7%
Israel	0,6%
Argentina	0,6%
Indonesia	0,6%
Suecia	0,6%
Turquía	0,6%
China	0,5%
Malasia	0,5%
Países Bajos	0,5%
Colombia	0,5%
Sudáfrica	0,4%
Austria	0,4%
Bélgica	0,4%
Portugal	0,4%
Resto del Mundo	9%

Índices globales de ransomware por países en %

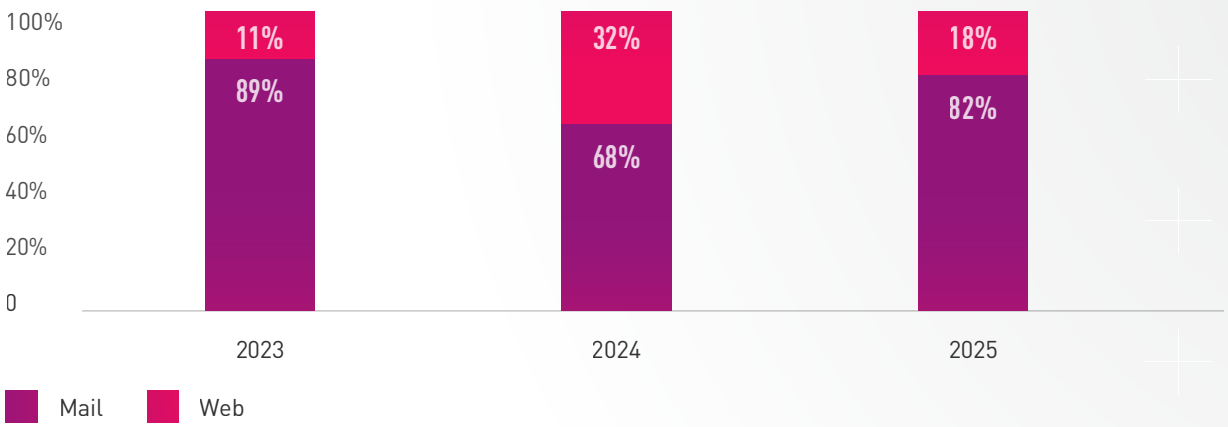
ATAQUES SEMANALES POR SECTOR INDUSTRIAL
EUROPA



Media de ciberataques a empresas clasificados por sector en Europa en 2025 [el % expresa la variación respecto a 2024]

VECTORES DE ATAQUE

Vectores de entrega del ataque: correo electrónico frente a web



Vectores de entrega del ataque (Email frente a Web), 2023-2025

En 2025, los ataques basados en correo electrónico que incluían archivos maliciosos representaron el 82 % de la actividad observada, frente al 18 % de los ataques originados en la web. Esta distribución confirma la preferencia sostenida por el correo electrónico como principal canal de entrega de archivos maliciosos. Según datos de Check Point Harmony Email and Collaboration, aproximadamente uno de cada 68 correos electrónicos con archivos adjuntos recibidos por una organización contiene contenido malicioso.

Aunque en 2024 se registró un descenso temporal, la tendencia desde 2018 muestra un refuerzo progresivo del correo como vector dominante.

EL ECOSISTEMA DE INFOSTEALERS

Tras las operaciones policiales que desmantelaron botnets como Qbot y Emotet en el marco de Operation Endgame y Operation Endgame 2.0, muchos actores que adquirían accesos iniciales a través de estos servicios tuvieron que modificar sus tácticas. Los infostealers se consolidaron como una alternativa prioritaria. Los registros y credenciales robadas comenzaron a circular de forma masiva en foros y canales clandestinos, convirtiéndose en combustible para ataques posteriores.

En 2025, Lumma dominó el panorama de registros de infostealers con el 43 %, seguido por Redline con el 22 %, Meta con el 14 %, Stealc con el 12 % y Vidar con el 5 %. Según los datos analizados, más del 76 % de las máquinas infectadas parecen ser dispositivos no corporativos, frente al 70 % del año anterior. Este aumento evidencia la estrategia de penetrar en entornos empresariales a través de dispositivos menos protegidos, como equipos personales conectados mediante VPN, cuentas de Microsoft 365 o plataformas colaborativas.

En este contexto, **España** representa el 2 % de la actividad observada vinculada a infostealers y **Portugal** el 0,5 %, lo que sitúa conjuntamente a ambos países en torno al 2,5 % del total global.

PAÍS	% DEL TOTAL
Brasil	7%
India	7%
Pakistán	4%
Indonesia	4%
Vietnam	4%
Egipto	4%
Estados Unidos	3%
Filipinas	3%
Argentina	3%
Turquía	3%
Tailandia	2%
México	2%
Colombia	2%
España	2%
Bangladesh	2%
Perú	2%
Argelia	2%
Alemania	1,4%
Francia	1,3%
Marruecos	1,3%

PAÍS	% DEL TOTAL
Chile	1,1%
Reino Unido	1,1%
Polonia	1%
Italia	0,9%
Venezuela	0,9%
Sudáfrica	0,8%
Ecuador	0,8%
Malasia	0,8%
Sri Lanka	0,8%
Iraq	0,8%
Rumanía	0,8%
Bolivia	0,7%
Corea	0,7%
Paises Bajos	0,7%
República Dominicana	0,6%
Kenia	0,6%
Arabia Saudí	0,6%
Nigeria	0,6%
Emiratos Árabes	0,6%
Portugal	0,5%

Índices globales de infostealers por países en %

06

PREDICCIONES DEL SECTOR PARA 2026: EL FUTURO DE LA CIBERSEGURIDAD

1. La IA agentiva pasa de la asistencia a la autonomía operativa

En 2026 la ciberseguridad estará marcada por la consolidación de la inteligencia artificial como elemento estructural tanto en la operativa empresarial como en el propio ámbito de la defensa y el ataque. La IA agentiva dejará de limitarse a funciones de asistencia para asumir autonomía operativa real, gestionando presupuestos, supervisando procesos industriales o redirigiendo operaciones logísticas con mínima intervención humana. Esta capacidad ampliará la eficiencia, pero también generará un riesgo sistémico si no va acompañada de marcos sólidos de gobernanza, auditoría y control, obligando a las organizaciones a implantar consejos de supervisión, límites de política y mecanismos de trazabilidad de decisiones.

2. Inyección de prompts y envenenamiento de datos: los modelos de IA como nuevo "día cero"

Al mismo tiempo, los propios modelos de IA se convertirán en nuevas superficies de ataque. La inyección de prompts y el envenenamiento de datos transformarán a los sistemas de inteligencia artificial en un equivalente al "día cero", donde la integridad ya no depende solo del parcheo sino de una validación y supervisión continuas. La exposición se amplificará en ecosistemas hiperconectados, donde la cadena de suministro digital y los entornos SaaS permitirán que vulnerabilidades en proveedores, bibliotecas de código o credenciales en la nube se propaguen rápidamente a múltiples organizaciones. La respuesta exigirá visibilidad extendida a terceros y cuartos niveles, junto con modelos de acceso Zero Trust y monitorización permanente.

> "LA INYECCIÓN DE PROMPTS Y EL ENVENENAMIENTO DE DATOS TRANSFORMARÁN A LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL EN UN EQUIVALENTE AL "DÍA CERO""

3. La confianza es el nuevo perímetro: deepfakes y fraude conversacional

En paralelo, la confianza se convertirá en el nuevo perímetro de seguridad. La proliferación de deepfakes, clonación de voz e identidades sintéticas impulsadas por IA erosionará los mecanismos tradicionales de autenticación, facilitando fraudes conversacionales y nuevas formas de Business Email Compromise basadas en manipulación emocional. La verificación continua de identidad, contexto e intención será imprescindible en cada interacción digital.

4. El riesgo cuántico pasa de preocupación a acción inmediata

Otro eje clave será el riesgo cuántico, que pasará de preocupación teórica a acción práctica. Ante la amenaza de "harvest now, decrypt later", gobiernos y empresas acelerarán la migración hacia criptografía poscuántica, inventariando algoritmos y certificados y exigiendo planes claros de transición a sus proveedores. La protección de los datos actuales dependerá de decisiones adoptadas hoy.

5. La IA se convierte en motor estratégico de decisión

En este contexto, la IA también se consolidará como motor estratégico de decisión en ciberseguridad. Atacantes y defensores emplearán capacidades de aprendizaje continuo y análisis en tiempo real, desplazando la seguridad hacia modelos más automatizados y consistentes. Sin embargo, tras la adopción acelerada de los últimos años, muchas organizaciones entrarán en una fase de recalibración: deberán abordar riesgos derivados de la "shadow AI", API expuestas y lagunas de cumplimiento, avanzando desde el entusiasmo inicial hacia marcos formales de aseguramiento, explicabilidad y responsabilidad algorítmica.

> ANTE LA AMENAZA DE "HARVEST NOW, DECRYPT LATER", GOBIERNOS Y EMPRESAS ACELERARÁN LA MIGRACIÓN HACIA CRIPTOGRAFÍA POSCUÁNTICA

6. Regulación y rendición de cuentas: la resiliencia como licencia para operar

Finalmente, la regulación endurecerá el entorno operativo. Normativas como NIS2, el Reglamento Europeo de IA y las exigencias de divulgación de incidentes en Estados Unidos convergerán en un principio común: la resiliencia debe ser medible y demostrable en tiempo real. El cumplimiento anual dará paso a monitorización automatizada, atestaciones continuas y analítica de riesgo basada en IA. En 2026, la resiliencia dejará de ser una declaración documental para convertirse en una condición operativa y estratégica para mantener la licencia para operar en un entorno digital cada vez más interdependiente.

CONTACTO

SEDE CORPORATIVA ESPAÑA

Check Point Software Technologies (Iberica) S.A.

Via de las Dos Castillas 33. Edificio Ática 7. Planta Baja. Oficina 1

28824 Pozuelo de Alarcón, Madrid, España

E-mail: info_iberia@checkpoint.com

Tel: +34 91 799 27 14

www.checkpoint.com