**Chile sufrió 27.600 millones de intentos de ciberataques en 2024**

*El reporte de Fortinet sobre amenazas reveló un aumento récord de ciberataques automatizados a medida que los adversarios utilizan IA y nuevas técnicas como armas.*

*El informe de FortiGuard Labs sobre el panorama global de amenazas de 2025 destaca un auge del ciberdelito como servicio en la dark web, lo que impulsa un mercado lucrativo de credenciales, exploits y accesos.*

**SUNNYVALE, California- April, 2025**

**Resumen**

[Fortinet](https://www.fortinet.com/content/fortinet-com/en_us)® (NASDAQ: FTNT), el líder global en ciberseguridad impulsando la convergencia de redes y seguridad, anunció hoy el lanzamiento de su reporte de [FortiGuard Labs sobre el panorama global de amenazas de 2025](https://www.fortinet.com/resources/reports/threat-landscape-report). Sobre Chile, el informe indica que el país sufrió 27.600 millones de intentos de ciberataques en 2024, frente a los 6.000 millones del año anterior.

El último reporte anual es una mirada hacia el panorama de amenazas actual y las tendencias, incluyendo un análisis integral de las tácticas utilizadas en los ciberataques, como se describe en el marco MITRE ATT&CK. Los datos revelan que los actores de amenazas están utilizando de manera exponencial la automatización, las herramientas mercantilizadas e inteligencia artificial (IA) para erosionar de manera sistemática las ventajas antes sostenidas por los defensores.

“Nuestro último reporte de FortiGuard Labs sobre el panorama global de amenazas de 2025 deja una cosa clara: los cibercriminales están acelerando sus esfuerzos, utilizando IA y automatización para operar a niveles sin precedentes de rapidez y escala”, aseguro Derek Manky, jefe de Estrategia de Seguridad y VP global de Inteligencia de Amenazas de FortiGuard Labs de Fortinet. “El manual tradicional de seguridad ya no es suficiente. Las organizaciones deben tomar una estrategia proactiva enfocada en inteligencia e impulsada por IA, confianza cero y manejo continuo de exposición a amenazas, para poder mantenerse a la vanguardia del panorama de amenazas actual que está cada vez más evolucionado”.

**Los principales hallazgos del último reporte de FortiGuard Labs sobre el panorama global de amenazas incluyen:**

* **El escaneo automatizado alcanza picos récord al tiempo que los atacantes buscan identificar objetivos expuestos con anticipación:** para capitalizar las vulnerabilidades recién descubiertas, los cibercriminales están desplegando escaneo automatizado a escala global. El escaneo activo en el ciber espacio alcanzó niveles sin precedente en 2024, con un incremento de 16,7% año con año a nivel mundial, resaltando una colección masiva y sofisticada de información en infraestructura digital expuesta. FortiGuard Labs observó mil millones de escaneos mensuales -el equivalente a 36.000 escaneos por segundo- lo que revela un foco en mapear servicios expuesto como SIP, RDP y protocolos de IT/OT como ModbusTCP.
* **Los mercados de la dark web facilitan el acceso a kits de explotación cuidadosamente empaquetados:** en 2024, los foros de ciberdelincuentes funcionaron cada vez más como sofisticados mercados de kits de explotación, con más de 40.000 nuevas vulnerabilidades añadidas a la Base de datos nacional de vulnerabilidades, un aumento del 39% con respecto a 2023. Además de las vulnerabilidades de día cero que circulan en la dark web, los intermediarios ofrecen cada vez más credenciales corporativas (20%), accesod RDP (19%), paneles de administración (13%) y shells web (12%). Asimismo, FortiGuard Labs observó un aumento del 500% durante el último año en los registros disponibles de sistemas comprometidos por malware de robo de información, con 1.700 millones de registros de credenciales robadas compartidos en estos foros clandestinos**.**
* **El cibercrimen impulsado por IA está escalando de manera rápida:** los actores de amenazas están aprovechando la inteligencia artificial para mejorar el realismo del phishing y evadir los controles de seguridad tradicionales, lo que hace que los ciberataques sean más efectivos y difíciles de detectar. Herramientas para crear amenazas como FraudGPT, BlackmailerV3 y ElevenLabs están impulsando campañas más escalables, creíbles y efectivas, sin las restricciones éticas de las herramientas de IA disponibles públicamente.
* **Se intensifican los ataques dirigidos a sectores críticos:** industrias como manufactura, salud y servicios financieros continúan experimentando un aumento de ciberataques personalizados, con adversarios que despliegan exploits específicos para cada sector. En 2024, los sectores más atacados fueron manufactura (17%), servicios empresariales (11%), construcción (9%) y comercio minorista (9%). Tanto los actores de los estados-nación como los operadores de ransomware como servicio (RaaS) concentraron sus esfuerzos en estos sectores, siendo Estados Unidos el más afectado (61%), seguido del Reino Unido (6%) y Canadá (5%).
* **Los riesgos en nube e IoT escalan:** los ambientes de nube continúan siendo uno de los principales objetivos, con adversarios explotando debilidades persistentes como depósitos de almacenamiento abiertos, identidades con permisos excesivos y servicios mal configurados. En el 70 % de los incidentes observados, los atacantes obtuvieron acceso mediante inicios de sesión desde ubicaciones desconocidas, lo que destaca el papel crucial del monitoreo de identidades en la defensa de la nube.
* **Las credenciales son la moneda de cambio del cibercrimen:** durante 2024, los ciberdelincuentes compartieron más de 100.000 millones de registros comprometidos en foros clandestinos, un aumento interanual del 42%, impulsado principalmente por el auge de las "listas combinadas" que contienen nombres de usuario, contraseñas y direcciones de correo electrónico robadas. Más de la mitad de las publicaciones en la dark web involucraban bases de datos filtradas, lo que permitió a los atacantes automatizar ataques de robo de credenciales a gran escala. Grupos conocidos de ciberdelincuentes como BestCombo, BloddyMery y ValidMail fueron los más activos durante este periodo y continúan reduciendo la barrera de entrada al empaquetar y validar estas credenciales, lo que impulsa un aumento en el robo de cuentas, el fraude financiero y el espionaje corporativo.

**Fortalecimiento de las ciberdefensas contra las amenazas emergentes**

El reporte de Fortinet sobre el panorama global de amenazas ofrece información detallada sobre las últimas tácticas y técnicas de los atacantes, además de ofrecer recomendaciones prescriptivas e información práctica. Diseñado para capacitar a los CISOs y a los equipos de seguridad, el informe ofrece estrategias para contrarrestar a los actores de amenazas antes de que ataquen, ayudando a las organizaciones a anticiparse a las ciberamenazas emergentes.

El informe de este año incluye una “Guía del CISO para la defensa contra adversarios” que destaca algunas áreas estratégicas en las cuales centrarse:

* **Transición de la detección tradicional de amenazas a la gestión continua de la exposición a amenazas:** este enfoque proactivo prioriza la gestión continua de la superficie de ataque, la emulación del comportamiento del adversario en situaciones reales, la priorización de la remediación basada en riesgos y la automatización de las respuestas de detección y defensa. El uso de herramientas de simulación de brechas y ataques (BAS) para evaluar periódicamente las defensas de los endpoints, la red y la nube contra escenarios de ataque reales garantiza la resiliencia contra el movimiento lateral y la explotación.
* **Simulación de ataques reales:** realizando ejercicios de emulación de adversarios, trabajando en equipo rojo y morado, y aprovechando MITRE ATT&CK para probar las defensas contra amenazas como ransomware y campañas de espionaje.
* **Reducción de riesgos en la exposición de la superficie de ataque:** implementando herramientas de gestión de la superficie de ataque (ASM) para detectar activos expuestos, credenciales filtradas y vulnerabilidades explotables mientras monitorea continuamente los foros de la dark web en busca de amenazas emergentes.
* **Priorizar vulnerabilidades de alto riesgo:** enfocando los esfuerzos de remediación en las vulnerabilidades que están siendo discutidas por los grupos cibercriminales, aprovechando marcos de priorización basados ​​en riesgos como EPSS y CVSS, para una gestión eficaz de parches.
* **Aprovechar la inteligencia en la dark web:** supervisando los mercados de la dark web en busca de servicios de ransomware emergentes y hacer un seguimiento de los esfuerzos de coordinación de los hacktivistas para mitigar de forma preventiva amenazas como los ataques DDoS y de desfiguración web.

Descubra cómo los [Servicios de Asesoría de FortiGuard Labs](https://www.fortinet.com/lat/solutions/enterprise-midsize-business/security-as-a-service/respond) combinan tecnología de vanguardia y servicios expertos para ayudar a las organizaciones a fortalecer su seguridad antes de que surjan amenazas. En caso de incidente, FortiGuard Labs ofrece una respuesta rápida y eficaz, así como un análisis forense exhaustivo para minimizar el impacto y prevenir futuras intrusiones, brindando protección integral en el panorama digital actual, cada vez más volátil.

**Recursos Adicionales**

* Descargue una copia del [Reporte del Panorama Global de Amenazas 2025 de FortiGuard Labs](https://www.fortinet.com/resources/reports/threat-landscape-report).
* Conozca más sobre la inteligencia de amenazas e investigación de [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs) y las [Outbreak Alerts,](https://www.fortinet.com/fortiguard/outbreak-alert) que brindan pasos oportunos para mitigar ataques cibernéticos de última hora.
* Obtenga más información sobre [**FortiAI**](https://www.fortinet.com/lat/solutions/enterprise-midsize-business/fortiai) y las innovaciones impulsadas por IA de Fortinet.
* Obtenga más información acerca de [**Fortinet Security Fabric**](https://www.fortinet.com/lat/solutions/enterprise-midsize-business/security-fabric)
* Visite [**fortinet.com/trust**](https://www.fortinet.com/lat/trust) para obtener información sobre la innovación de Fortinet, los socios colaboradores, los procesos de seguridad de productos y los productos de nivel empresarial.
* Lea acerca de cómo los [**clientes de Fortinet**](https://www.fortinet.com/lat/customers) están protegiendo sus organizaciones.
* Obtenga información sobre [**el compromiso de Fortinet con la seguridad e integridad de los productos**](https://www.fortinet.com/content/dam/fortinet/assets/flyer/flyer-fortinet-commitment-to-product-security-and-integrity.pdf), incluido su enfoque y políticas responsables de desarrollo de productos y divulgación de vulnerabilidades.
* Siga a Fortinet en [**Twitter**](https://www.x.com/fortinetlatam), [**LinkedIn**](https://www.linkedin.com/company/fortinet), [**Facebook**](https://www.facebook.com/FortinetLATAM), e [**Instagram**](https://www.instagram.com/fortinet/). Suscríbase a nuestro [**blog**](https://www.fortinet.com/lat/blog) y [**canal de YouTube**](https://www.youtube.com/FortinetLATAM).

 **Acerca de Fortinet**

[**Fortinet**](https://www.fortinet.com/lat) (Nasdaq: FTNT) es una fuerza impulsora en la evolución de la ciberseguridad y la convergencia de las redes y la seguridad. Nuestra misión es proteger a las personas, los dispositivos y los datos en todas partes, y hoy ofrecemos ciberseguridad donde nuestros clientes la necesitan con la cartera integrada más grande de más de 50 productos de grado empresarial. Más de medio millón de clientes confía en las soluciones de Fortinet, que se encuentran entre las más implementadas, patentadas y validadas de la industria. El Instituto de capacitación  de Fortinet,  uno de los programas de capacitación más grandes y amplios de la industria, se dedica a poner a disposición de todos la capacitación en ciberseguridad y nuevas oportunidades profesionales. [**Fortinet**](https://www.fortinet.com/lat/nse-training)Colaboración con  [**organizaciones apreciadas**](https://www.fortinet.com/lat/trust?tab=trusted%20partners)  de los sectores público y privado, incluyendo Equipos de respuesta a emergencias informáticas (“CERTS”), entidades gubernamentales, y el mundo académico, es un aspecto fundamental del compromiso de Fortinet de mejorar la ciberresiliencia a nivel mundial. [**FortiGuard Labs**](https://www.fortinet.com/lat/fortiguard/labs), La organización de investigación e inteligencia frente a amenazas de élite de Fortinet, desarrolla y utiliza tecnologías de aprendizaje automático e IA de vanguardia para proporcionar a los clientes una protección oportuna y consistentemente mejor calificada e inteligencia frente a amenazas procesable. Obtenga más información en  [**https://www.fortinet.com**](https://www.fortinet.com/lat)el blog  Fortinet [y **FortiGuard Labs**](https://www.fortinet.com/lat/fortiguard/labs).[**Fortinet**](https://www.fortinet.com/blog).

*Copyright © 2025 Fortinet, Inc. Todos los derechos reservados. Los símbolos ® y ™ denotan, respectivamente, marcas comerciales registradas a nivel federal y marcas comerciales legales comunes de Fortinet, Inc., sus subsidiarias y filiales. Las marcas comerciales de Fortinet incluyen, entre otras, las siguientes: Fortinet, el logotipo de Fortinet, FortiGate, FortiOS, FortiGuard, FortiCare, FortiAnalyzer, FortiManager, FortiASIC, FortiClient, FortiCloud, FortiMail, FortiSandbox, FortiADC, FortiAI, FortiAIOps, FortiAgent, FortiAntenna, FortiAP, FortiAPCam, FortiAuthenticator, FortiCache, FortiCall, FortiCam, FortiCamera, FortiCarrier, FortiCASB, FortiCentral, FortiCNP, FortiConnect, FortiController, FortiConverter, FortiCSPM, FortiCWP, FortiDAST, FortiDB, FortiDDoS, FortiDeceptor, FortiDeploy, FortiDevSec, FortiDLP, FortiEdge, FortiEDR, FortiExplorer, FortiExtender, FortiFirewall, FortiFlex FortiFone, FortiGSLB, FortiGuest, FortiHypervisor, FortiInsight, FortiIsolator, FortiLAN, FortiLink, FortiMonitor, FortiNAC, FortiNDR, FortiPAM, FortiPenTest, FortiPhish, FortiPoint, FortiPolicy, FortiPortal, FortiPresence, FortiProxy, FortiRecon, FortiRecorder, FortiSASE, FortiScanner, FortiSDNConnector, FortiSIEM, FortiSMS, FortiSOAR, FortiSRA, FortiStack, FortiSwitch, FortiTester, FortiToken, FortiTrust, FortiVoice, FortiWAN, FortiWeb, FortiWiFi, FortiWLC, FortiWLM, FortiXDR y Lacework FortiCNAPP. Otras marcas comerciales pertenecen a sus respectivos dueños. Fortinet no ha verificado de manera independiente las declaraciones o certificaciones aquí atribuidas a terceros; además, Fortinet no respalda de manera independiente dichas declaraciones. Sin perjuicio de cualquier disposición en contrario en el presente documento, nada de lo que aquí figura constituye una garantía, un contrato, una especificación vinculante u otro compromiso vinculante por parte de Fortinet o cualquier indicación de intención relacionada con un compromiso vinculante, y la información de desempeño y otras especificaciones en el presente documento puede ser única para ciertos entornos.*