CRONUP
CIBERSEGURIDAD

VULNERABILIDADES
EN FABRICANTES DE CIBERSEGURIDAD
LO QUE EL MARKETING NO TE CUENTA

2026

INTRODUCCIÓN

RIESGO POTENCIAL EN PRODUCTOS DE CIBERSEGURIDAD: MÁS ALLÁ DE LA NARRATIVA DEL MERCADO

El año 2025 confirmó una realidad incómoda para muchas organizaciones: la estrategia de ciberseguridad no falla solo cuando faltan controles, sino también cuando se confía ciegamente en ellos. Mientras empresas de todos los sectores continúan incrementando su inversión en soluciones para la ciberseguridad; firewalls de nueva generación, plataformas EDR/XDR y controles de seguridad en la nube, igualmente los incidentes de alto impacto siguen ocurriendo, incluso en entornos considerados “bien protegidos”.

Este aparente contrasentido plantea una pregunta estratégica clave para la alta dirección: ¿Qué tan confiables son en la práctica los productos de ciberseguridad sobre los que se construye la defensa digital de la organización?

El presente estudio aborda esta pregunta desde una perspectiva técnica, basada en evidencia proveniente de bases públicas de vulnerabilidades. A partir del análisis de 881 vulnerabilidades registradas durante 2025, correspondientes a 28 de los fabricantes más relevantes de la industria de ciberseguridad, se identifican patrones estructurales que permiten comprender mejor dónde se concentra el riesgo real, cómo evoluciona la exposición y por qué ciertos productos, aun siendo líderes de mercado, se transforman con frecuencia en vectores de ataque.

Lejos de cuestionar la validez de las tecnologías analizadas, esta investigación busca poner en perspectiva la percepción de seguridad asociada a marcas, rankings o posicionamiento comercial, contrastándola con datos objetivos provenientes de divulgaciones de vulnerabilidades, inteligencia de amenazas y evidencia de explotación activa.

SEGURIDAD, INVERSIÓN Y PERCEPCIÓN DEL RIESGO

RESUMEN EJECUTIVO

La ciberseguridad se ha consolidado como una prioridad estratégica para las organizaciones. Sin embargo, la toma de decisiones en esta materia suele apoyarse en marcos de referencia ampliamente aceptados y en la adopción de tecnologías reconocidas como una vía para reducir el riesgo, en un contexto donde la narrativa, el posicionamiento y la maquinaria comunicacional de la industria influyen de manera significativa en la percepción de seguridad. Si bien este enfoque aporta estructura y facilita la comparación de alternativas, no garantiza por sí solo una disminución efectiva de la exposición real.

Los resultados de este estudio muestran que el riesgo no depende únicamente de la tecnología adquirida, sino de cómo esta se integra y opera dentro de la organización. La exposición emerge de la combinación entre arquitectura, configuraciones, dependencias operativas y contexto, lo que explica por qué organizaciones con soluciones similares pueden presentar niveles de riesgo significativamente distintos. En la práctica, la superficie de ataque relevante no está determinada por la cantidad de vulnerabilidades conocidas, sino por aquellos puntos donde convergen exposición directa, interés del adversario y ausencia de mitigaciones efectivas. Son estas condiciones las que explican la materialización de incidentes relevantes, incluso en entornos con altos niveles de inversión y cumplimiento.

Un aspecto clave para la alta dirección es comprender que los atacantes actúan antes de que el riesgo sea evidente para los modelos convencionales. La investigación identifica señales tempranas de actividad maliciosa a través de inteligencia de amenazas (CTI), incluso cuando las métricas técnicas o predictivas, como EPSS, que estima la probabilidad de explotación de una vulnerabilidad, aún no reflejan un riesgo elevado.

En términos simples, cuando el riesgo aparece en los reportes tradicionales, la amenaza ya puede encontrarse en una etapa avanzada. Este desfase genera una falsa sensación de control y extiende la ventana de exposición al riesgo.

Organizaciones con buenas evaluaciones y altos niveles de inversión pueden sentirse protegidas mientras su exposición real aumenta de forma silenciosa.

El desafío estratégico no es invertir más, sino invertir mejor, orientando los recursos hacia los puntos donde el riesgo efectivamente se está configurando.

En este contexto, **Alerta Temprana de Riesgos Cibernéticos**– ATRc® ofrece un enfoque complementario para la toma de decisiones estratégicas, apoyando al Directorio y a la alta administración en la identificación temprana de riesgos relevantes mediante la incorporación de contexto, comportamiento adversario y exposición real, antes de que estos se traduzcan en impactos operativos, reputacionales o regulatorios.

Para el Directorio, la pregunta clave deja de ser únicamente: "¿Contamos con las herramientas adecuadas?" y pasa a ser: "¿Estamos anticipando correctamente dónde se está formando el riesgo que puede afectar al negocio?"

La capacidad de responder esta pregunta marca la diferencia entre una organización que cumple y una que gobierna activamente su riesgo.

CRONUP
CIBERSEGURIDAD

Cyber Threat Intelligence (ATRc®)

INTELIGENCIA DE AMENAZAS EN TIEMPO REAL:
DETECTA, CONTEXTUALIZA Y NEUTRALIZA RIESGOS
ANTES DE QUE IMPACTEN TU NEGOCIO

RESULTADOS DEL ESTUDIO

Para este análisis se seleccionaron 28 fabricantes con alta presencia en entornos empresariales, representativos de las principales capas de la arquitectura de ciberseguridad. La selección considera tanto su despliegue en entornos operacionales críticos como su relevancia en escenarios de evaluación de ciberseguridad, como ejercicios de red teaming y simulaciones de ataque.

Las tecnologías analizadas se agrupan en las siguientes categorías, con el objetivo de identificar patrones de vulnerabilidad y exposición a través de distintos componentes de la infraestructura de ciberseguridad.

Categoría	Fabricantes
Seguridad de Red y Perímetro (Network / Perimeter Security)	Fortinet, Palo Alto Networks, F5, Cisco, Check Point, SonicWall, Citrix, Cloudflare, Akamai, Thales-Imperva
Seguridad de Identidad y Cloud (Identity & Cloud Security)	Zscaler, Okta
Seguridad de Endpoints (Endpoint Security - EDR/XDR)	Microsoft Defender, CrowdStrike, SentinelOne, Sophos, Trend Micro, ESET, Kaspersky, Trellix
Seguridad de Aplicaciones y Gestión de Vulnerabilidades (Application & Vulnerability Security)	Tenable, Rapid7, Qualys, Snyk
Analítica de Seguridad y Monitoreo (Security Analytics & Monitoring)	Splunk, IBM Security, Darktrace
Protección de Email y Datos (Email & Data Protection)	Proofpoint

Este estudio busca comprender cómo se construye realmente el riesgo en entornos protegidos por tecnologías líderes, y qué factores explican por qué ciertas vulnerabilidades se convierten en incidentes mientras muchas otras nunca llegan a ser explotadas.

HALLAZGOS CLAVE

28
Fabricantes Líderes evaluados

24
Fabricantes Reportaron Vulnerabilidades

881
Vulnerabilidades Analizadas en 2025

78%
Se concentran en productos de red y perímetro

Para cada fabricante incluido en el estudio, se recopilaron las vulnerabilidades divulgadas durante el año 2025, obtenidas desde repositorios oficiales de vulnerabilidades, principalmente el National Vulnerability Database (NVD), basado en registros del sistema CVE.

En total, se identificaron **881 vulnerabilidades**, que constituyen la base cuantitativa del análisis.

Sin embargo, el enfoque no se limita a su contabilización, sino que evalúa su relevancia operativa incorporando múltiples dimensiones, como severidad técnica, probabilidad de explotación, evidencia de ataques reales e inteligencia de amenazas. Este enfoque permite comprender el riesgo cibernético desde una perspectiva más amplia, considerando no sólo la existencia de vulnerabilidades, sino su probabilidad de materialización y su impacto potencial en entornos operacionales.

CONSIDERACIONES METODOLÓGICAS

FABRICANTES SIN VULNERABILIDADES REPORTADAS:

Del total de 28 fabricantes seleccionados inicialmente, 4 no registraron vulnerabilidades con CVE publicados durante 2025: Darktrace, SentinelOne, Thales-Imperva y Snyk. En consecuencia, el análisis se centra en los 24 fabricantes restantes que sí reportaron vulnerabilidades durante el período evaluado.

Es importante señalar que Darktrace, Thales-Imperva y Snyk sí registraron vulnerabilidades en 2024, lo que indica que su ausencia en 2025 no implica una ausencia estructural de vulnerabilidades, sino una variación temporal en su divulgación pública. SentinelOne, por su parte, no registró CVEs públicos en ninguno de los dos períodos analizados.

Esta variabilidad interanual refuerza la necesidad de monitoreo continuo, independientemente del perfil de vulnerabilidades observado en períodos anteriores.

NOMENCLATURA CVE Y FECHA DE PUBLICACIÓN:

Algunos identificadores CVE incluyen el año 2024 en su nomenclatura (por ejemplo, CVE-2024-xxxxx), a pesar de haber sido publicados durante 2025. Esto ocurre porque el identificador CVE se asigna en el momento de su reserva, que puede preceder a su publicación oficial por semanas o incluso meses.

En este estudio, el criterio utilizado corresponde a la fecha de publicación oficial de la vulnerabilidad, y no al año indicado en su identificador. Por tanto, todos los CVE incluidos en el análisis fueron efectivamente publicados durante el año 2025.

LIMITACIONES DEL ESTUDIO

Como toda investigación basada en fuentes públicas y análisis de vulnerabilidades, este estudio presenta ciertas limitaciones que deben ser consideradas al interpretar sus resultados.

En primer lugar, **el análisis se basa exclusivamente en vulnerabilidades divulgadas públicamente durante el año 2025**. Esto implica que vulnerabilidades no reportadas, aquellas sujetas a acuerdos de confidencialidad o divulgadas posteriormente al período analizado, no forman parte del dataset. En consecuencia, el estudio refleja la visibilidad pública del riesgo, pero no necesariamente su totalidad.

En segundo lugar, la evidencia de explotación activa y las señales de inteligencia de amenazas (CTI) están sujetas a disponibilidad y publicación de información por parte de la comunidad de ciberseguridad. **Algunas vulnerabilidades pueden no presentar evidencia de explotación al momento del análisis**, pero ser utilizadas posteriormente en campañas reales.

Asimismo, el modelo de priorización utilizado combina múltiples dimensiones, como severidad técnica, probabilidad de explotación, inteligencia de amenazas y disponibilidad de contramedidas, mediante ponderaciones definidas con base en criterios técnicos y experiencia práctica. Si bien este enfoque permite una evaluación más contextual del riesgo, no constituye un modelo predictivo determinístico, sino una aproximación orientada a la priorización operativa.

Adicionalmente, la selección de fabricantes se basa en su presencia en entornos empresariales y en el volumen de vulnerabilidades divulgadas durante el período analizado. Si bien esto permite capturar una muestra representativa del ecosistema de ciberseguridad, no incluye la totalidad de fabricantes existentes ni refleja necesariamente su participación de mercado global.

Finalmente, es importante considerar que la relación entre vulnerabilidad, exposición y explotación es dinámica. El riesgo asociado a una vulnerabilidad puede cambiar rápidamente en función de nuevos descubrimientos, desarrollo de exploits o cambios en el contexto de amenaza. Por esta razón, los resultados de este estudio deben interpretarse como una fotografía del riesgo en un momento determinado, y no como una condición estática.

LAS MÉTRICAS QUE IMPORTAN

Para evaluar cada vulnerabilidad utilizamos seis dimensiones complementarias del riesgo asociado a cada una de ellas:

01 CVSS Base Score

Métrica estándar que evalúa la severidad técnica de una vulnerabilidad (0-10), clasificada en cinco niveles: Crítico (9.0-10.0), Alto (7.0-8.9), Medio (4.0-6.9), Bajo (0.1-3.9) e Informacional (0.0).

02 EPSS (Exploit Prediction Scoring System)

Probabilidad estimada de explotación en los próximos 30 días, calculada mediante modelo estadístico desarrollado por FIRST. Crucial para priorizar más allá del CVSS: Por ejemplo, una vulnerabilidad crítica con baja probabilidad de explotación puede representar un menor riesgo operativo que una vulnerabilidad de severidad alta con alta probabilidad de explotación.

03 Estado de Explotabilidad

Clasificación en cuatro categorías (Atacado, Prueba de concepto, No probado, No está definido) que indica si existe evidencia de explotación activa o código público disponible.

04 CTI (Cyber Threat Intelligence)

Indicador de presencia en fuentes de inteligencia de amenazas. La aparición de una vulnerabilidad en reportes de investigación o análisis técnicos puede indicar interés del adversario y su posible evolución hacia escenarios de explotación.

05 Estado de Contramedidas

Nivel de disponibilidad de las mitigaciones por parte del fabricante, incluyendo parche oficial, mitigación alternativa o ausencia de solución definida.

06 CVE

Identificador único utilizado para referenciar y correlacionar vulnerabilidades a través de distintas fuentes y sistemas de seguridad.

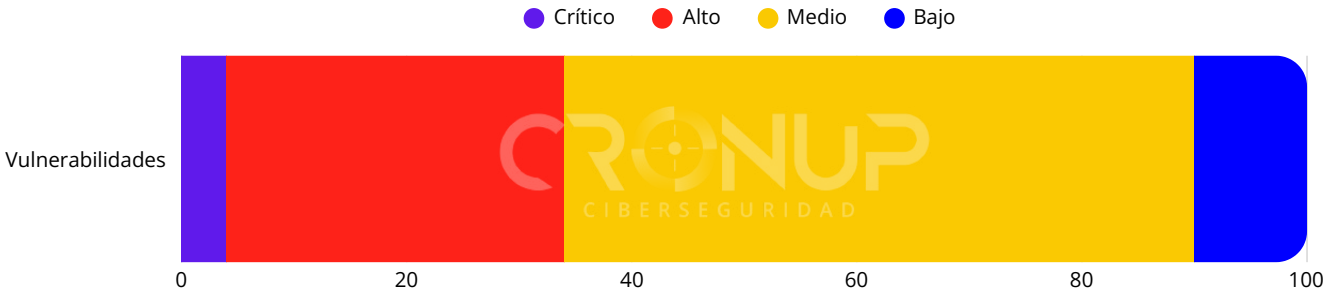
PREDOMINIO DE VULNERABILIDADES MEDIAS Y ALTAS, CON UN SUBCONJUNTO CRÍTICO DE ALTO IMPACTO

Del total de 881 vulnerabilidades analizadas, la distribución se concentra en severidades media (56%) y alta (30%). Las vulnerabilidades críticas representan el 4% del total (35), mientras que las de severidad baja alcanzan el 10%.

Aunque el 4% de vulnerabilidades críticas parece marginal, su impacto no lo es. Estas principalmente afectan tecnologías ampliamente desplegadas en entornos empresariales, y su explotación puede tener consecuencias significativas para la seguridad de una organización.

Este perfil indica que los equipos de seguridad enfrentan un flujo constante de vulnerabilidades de severidad media y alta, mientras deben mantener capacidad de respuesta para un subconjunto reducido, pero potencialmente más crítico, desde el punto de vista del riesgo operativo.

Distribución Porcentual de Vulnerabilidades por Nivel de Severidad



Fuente: Elaboración propia CronUp Ciberseguridad

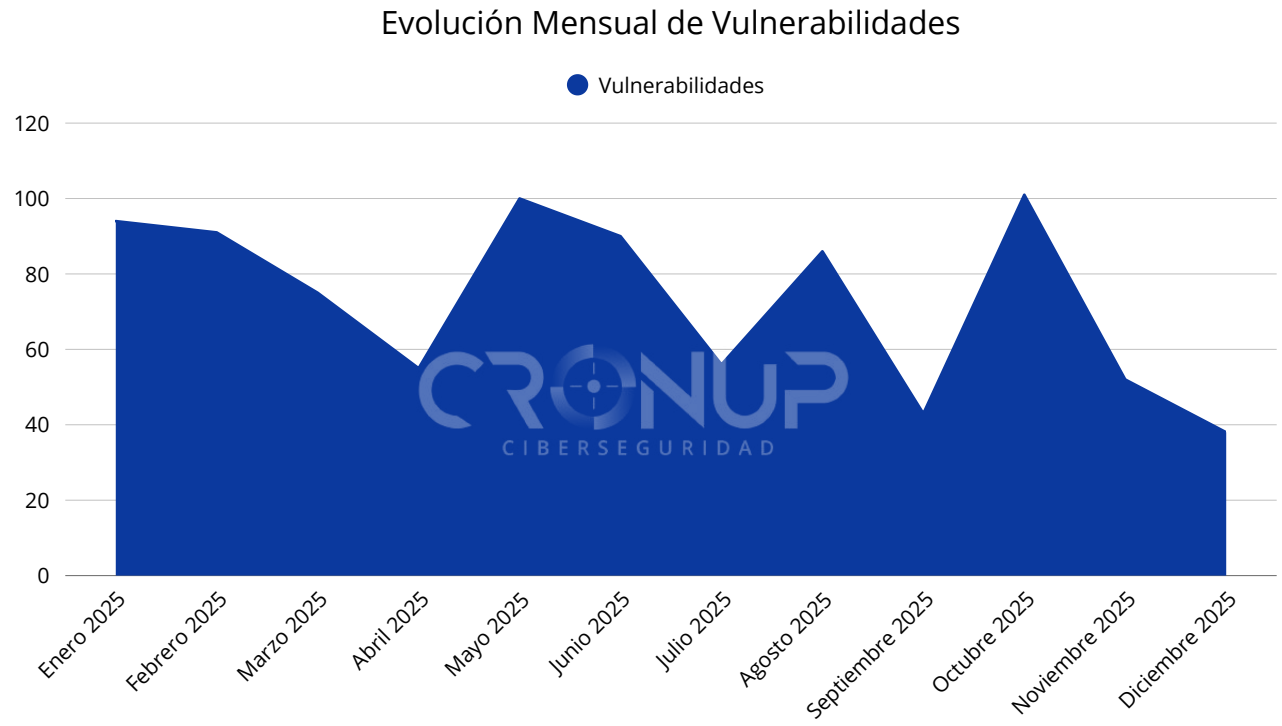
UNA ÚNICA VULNERABILIDAD CRÍTICA EXPLOTADA PUEDE TENER UN IMPACTO SIGNIFICATIVO EN LA SEGURIDAD DE UNA ORGANIZACIÓN

OCTUBRE: MAYOR NÚMERO DE VULNERABILIDADES REPORTADAS

El análisis revela una distribución irregular, con un aumento pronunciado en el mes de octubre, donde se registraron 101 vulnerabilidades. Este valor se sitúa por sobre el promedio mensual de 73,4 vulnerabilidades, lo que sugiere la existencia de períodos de concentración que pueden tensionar las capacidades operativas de los equipos de ciberseguridad.

En contraste, diciembre presenta un menor número de vulnerabilidades (38), lo que debe interpretarse con cautela. Es habitual que los últimos meses del año presenten rezagos entre el descubrimiento de vulnerabilidades, la asignación del identificador CVE y su publicación oficial.

Desde una perspectiva operativa, esta variabilidad mensual tiene implicancias directas en la gestión del riesgo. Los equipos de ciberseguridad no enfrentan un flujo constante y predecible de vulnerabilidades, sino olas de divulgación que pueden concentrar vulnerabilidades de severidad media, alta y crítica en un mismo período.



Fuente: Elaboración propia CronUp Ciberseguridad

Esto exige una capacidad de respuesta flexible y escalable, capaz de absorber estos incrementos sin degradar los procesos de análisis, priorización y remediación. Más aún, la limitada predictibilidad de estos eventos reduce la efectividad de modelos de planificación rígidos.

Las organizaciones que dependen exclusivamente de ventanas periódicas de parchado o de ciclos fijos de revisión se exponen a **ventanas de exposición al riesgo** ampliadas durante estos períodos de alta divulgación. En este contexto, la capacidad de adaptación se convierte en un factor clave de resiliencia.

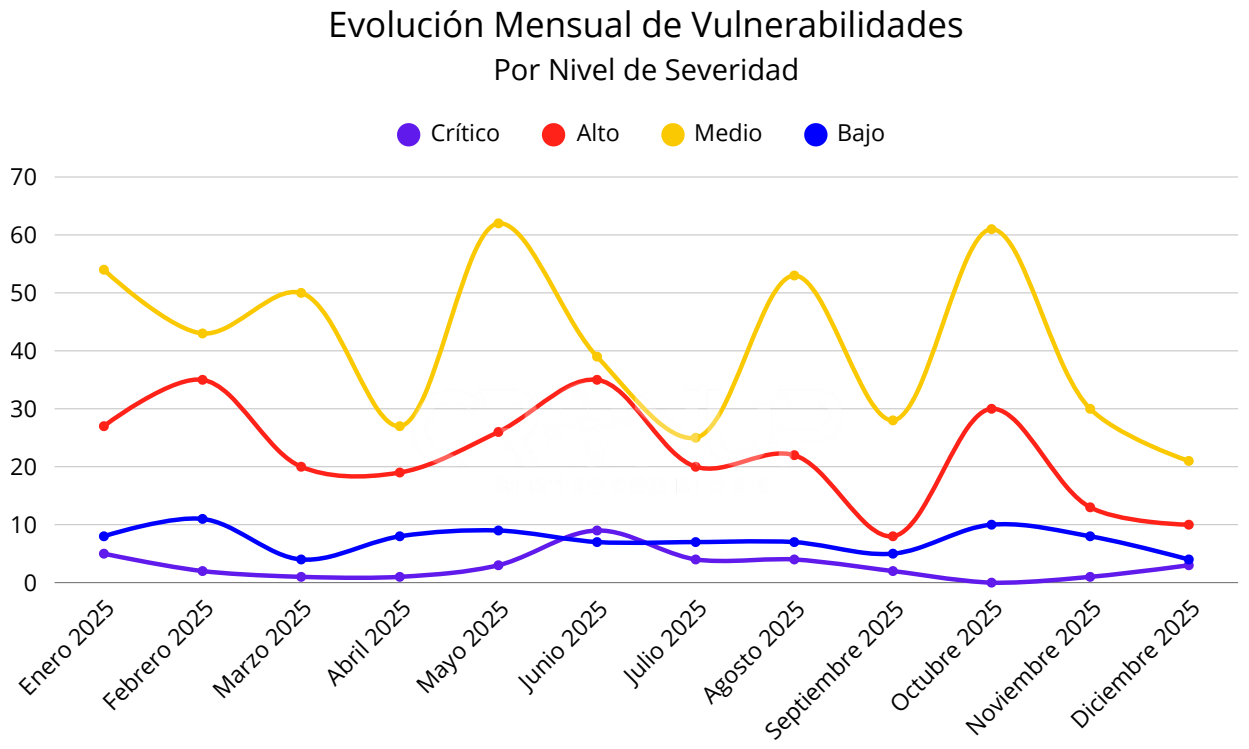
MOVIMIENTO SINCRONIZADO CON ALZAS DIFERENCIADAS

Aunque las vulnerabilidades críticas alcanzaron su máximo en junio (9), las de severidad alta en febrero (35) y las de severidad media en mayo (62), el análisis temporal revela un patrón relevante: las distintas severidades tienden a evolucionar de forma conjunta.

Al observar las curvas de evolución, se identifica que incrementos en vulnerabilidades de severidad media suelen coincidir con aumentos en vulnerabilidades altas y críticas, lo que sugiere la existencia de factores comunes que influyen en su divulgación.

Entre los factores que pueden explicar este comportamiento se encuentran ciclos de auditorías de ciberseguridad, campañas de investigación coordinadas, programas de bug bounty, actualizaciones relevantes de productos y divulgaciones agrupadas por parte de fabricantes o investigadores independientes, que resultan en la publicación simultánea de múltiples vulnerabilidades.

Fuente: Elaboración propia CronUp Ciberseguridad



Fuente: Elaboración propia CronUp Ciberseguridad

El año muestra una distribución irregular con un máximo marcado en octubre (101 vulnerabilidades). Diciembre registra hasta el momento 38 vulnerabilidades, aunque este dato probablemente se incrementará en las próximas semanas debido al rezago natural entre descubrimiento y publicación de CVEs.

LOS CICLOS DE DIVULGACIÓN AFECTAN DE MANERA TRANSVERSAL A TODOS LOS NIVELES DE SEVERIDAD

VULNERABILIDADES

240
CISCO

236
FORTINET

Esta concentración no necesariamente indica menor madurez de seguridad, sino carteras robustas y y presencia significativa en entornos empresariales.

36,7
Promedio
Por fabricante

CRONUP
CIBERSEGURIDAD

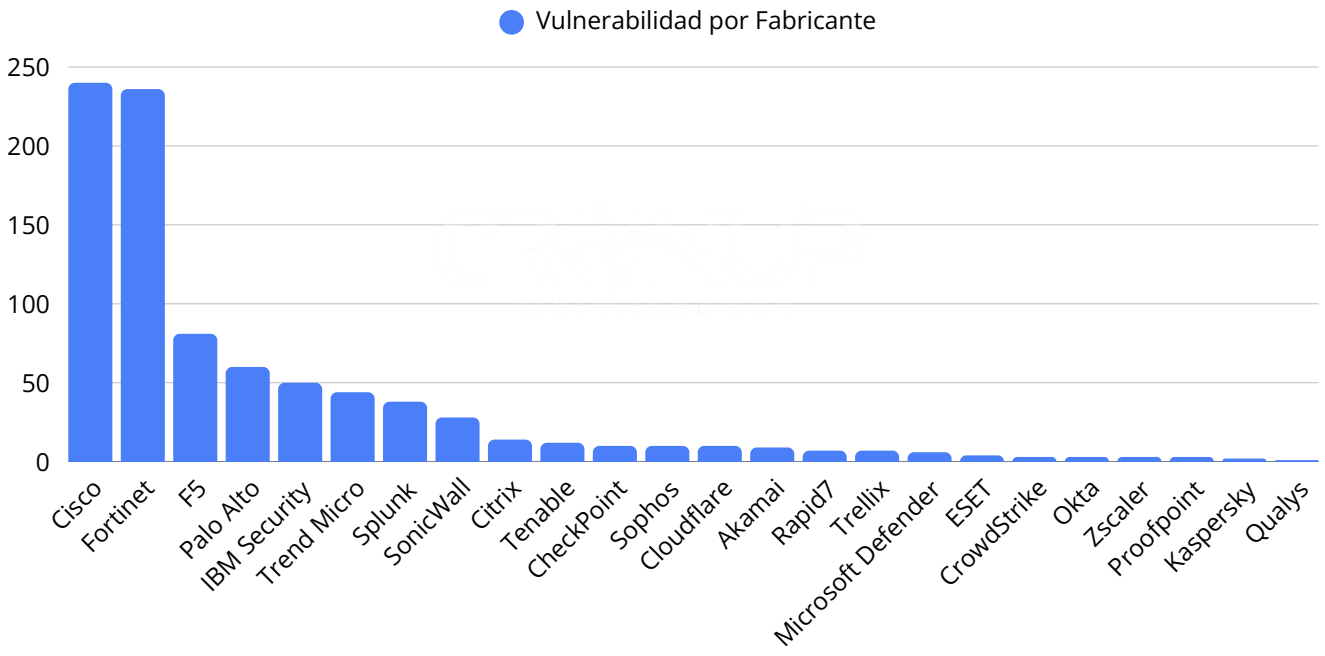
ANÁLISIS COMPARATIVO

Cisco y Fortinet concentran el mayor volumen

El análisis de distribución por fabricante muestra una alta concentración en soluciones de seguridad de red. **Cisco registra 240 vulnerabilidades**, seguido por **Fortinet con 236**.

En conjunto, ambos fabricantes concentran más de la mitad del total de vulnerabilidades analizadas, distanciándose significativamente del resto del ecosistema.

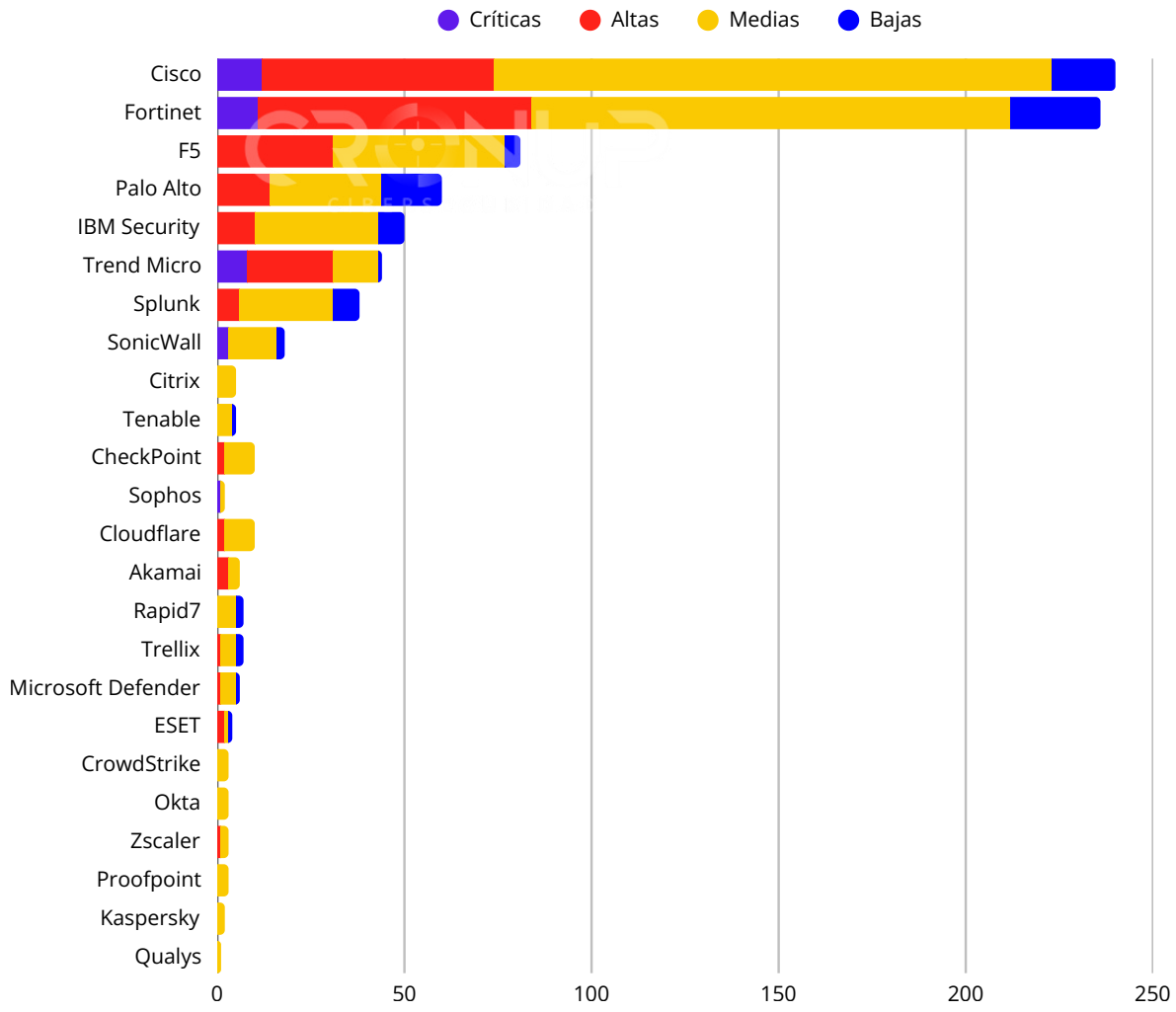
Esta concentración está alineada con la exposición estructural de las tecnologías de red y perímetro, que representan la mayor superficie de ataque dentro de la arquitectura de ciberseguridad empresarial.



Fuente: Elaboración propia CronUp Ciberseguridad

El tercer y cuarto lugar ya muestran una caída pronunciada, sin superar las 100 vulnerabilidades, y a partir de ahí la distribución se vuelve más dispersa. En el extremo opuesto, Qualys registró una única vulnerabilidad durante 2025.

Vulnerabilidades por Fabricante según severidad



Fuente: Elaboración propia CronUp Ciberseguridad

¿MÁS PRODUCTOS IMPLICAN MÁS VULNERABILIDADES?

La disparidad es notable: mientras el promedio por fabricante se ubica en 36,7 vulnerabilidades, la mediana es de 10. Esta diferencia sugiere que un número reducido de fabricantes concentra un volumen desproporcionado de reportes, mientras la mayoría presenta cifras significativamente menores.

Esta concentración, particularmente en algunos fabricantes, no necesariamente indica una menor madurez en ciberseguridad. En muchos casos, responde a la amplitud de sus portafolios de productos y a su despliegue en entornos empresariales de gran escala, lo que incrementa el interés tanto de investigadores de ciberseguridad como de actores de amenaza.

Asimismo, la existencia de programas de bug bounty consolidados y comunidades activas de investigación puede favorecer una mayor divulgación pública de vulnerabilidades.

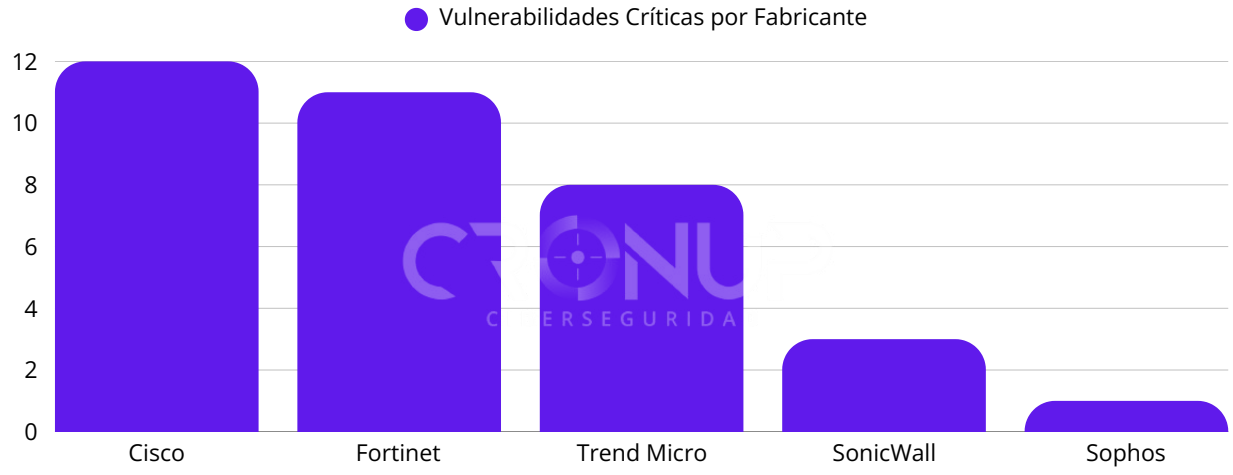
En este contexto, el volumen absoluto de vulnerabilidades debe interpretarse considerando factores como el tamaño del portafolio, el nivel de adopción de las tecnologías y los procesos de divulgación de cada fabricante. Por sí solo, este indicador no refleja necesariamente el nivel de riesgo al que están expuestas las organizaciones.

El volumen absoluto de vulnerabilidades debe interpretarse considerando el tamaño del portafolio de productos, la cuota de mercado y la transparencia en procesos de divulgación de cada fabricante.

VULNERABILIDADES CRÍTICAS: CONCENTRADAS EN UN NÚMERO REDUCIDO DE FABRICANTES

De las 35 vulnerabilidades críticas identificadas, solo 5 fabricantes las concentraron. Esta concentración significativa contrasta con el comportamiento general observado: mientras la mayoría de los fabricantes presenta vulnerabilidades de severidad media, las vulnerabilidades críticas se concentran en un subconjunto acotado de fabricantes.

Este patrón refuerza la idea de que el riesgo más relevante no se distribuye de manera uniforme, sino que tiende a concentrarse en determinados componentes o tecnologías dentro del ecosistema de ciberseguridad.



Fuente: Elaboración propia CronUp Ciberseguridad

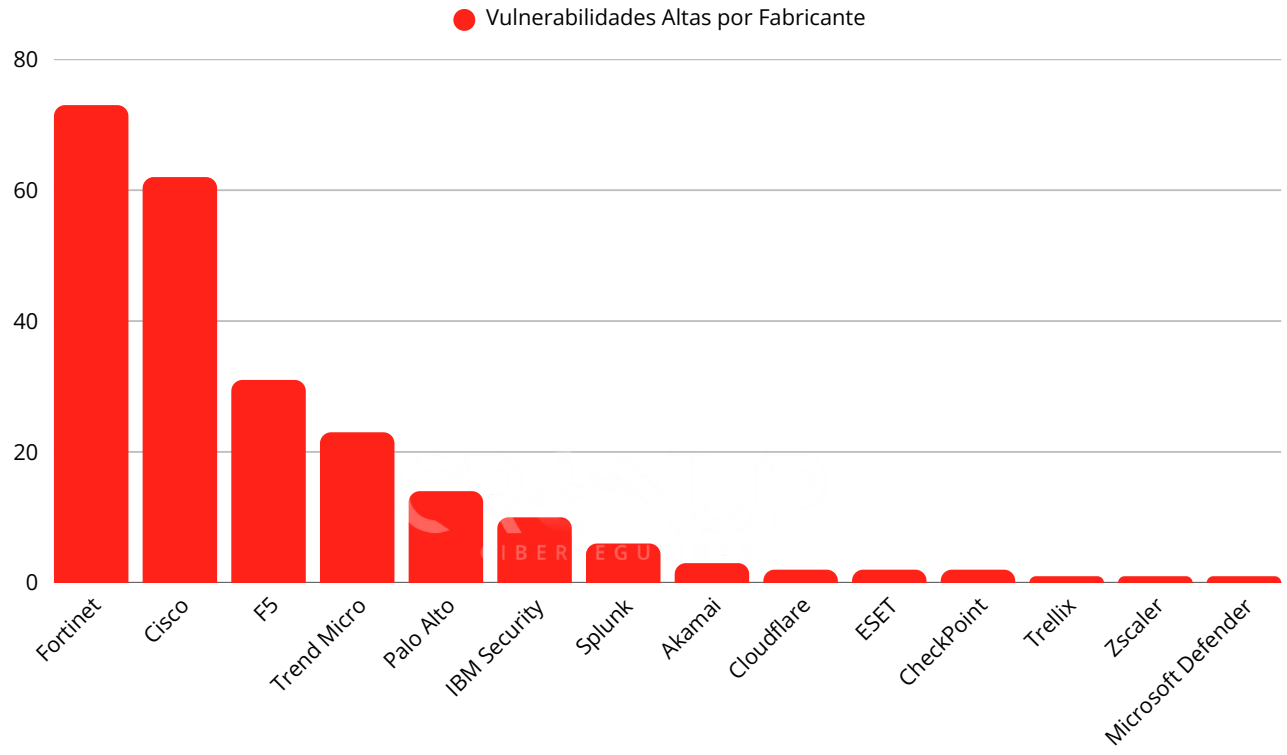
*LOS PRODUCTOS DE RED Y PERÍMETRO, POR SER LA "**PRIMERA LÍNEA DE DEFENSA**" EXPUESTA A INTERNET, SE TRANSFORMAN EN OBJETIVOS DE ALTO VALOR.*

VULNERABILIDADES ALTAS: DISTRIBUCIÓN AMPLIA, CON DIFERENCIAS ENTRE FABRICANTES

Las 265 vulnerabilidades de severidad alta se distribuyen entre 18 de los 24 fabricantes analizados. A diferencia de las vulnerabilidades críticas, las de severidad alta constituyen un fenómeno transversal, presente en la mayoría de los fabricantes, aunque con distribuciones heterogéneas en términos de volumen.

Esta distribución más amplia sugiere que la gestión de vulnerabilidades de severidad alta forma parte de la operación habitual de la mayoría de las organizaciones, independientemente de la combinación de tecnologías implementadas.

Desde una perspectiva operativa, este tipo de vulnerabilidades representa una carga constante para los equipos de ciberseguridad, que deben evaluarlas y priorizarlas en función de su contexto de explotación y exposición.



Fuente: Elaboración propia CronUp Ciberseguridad

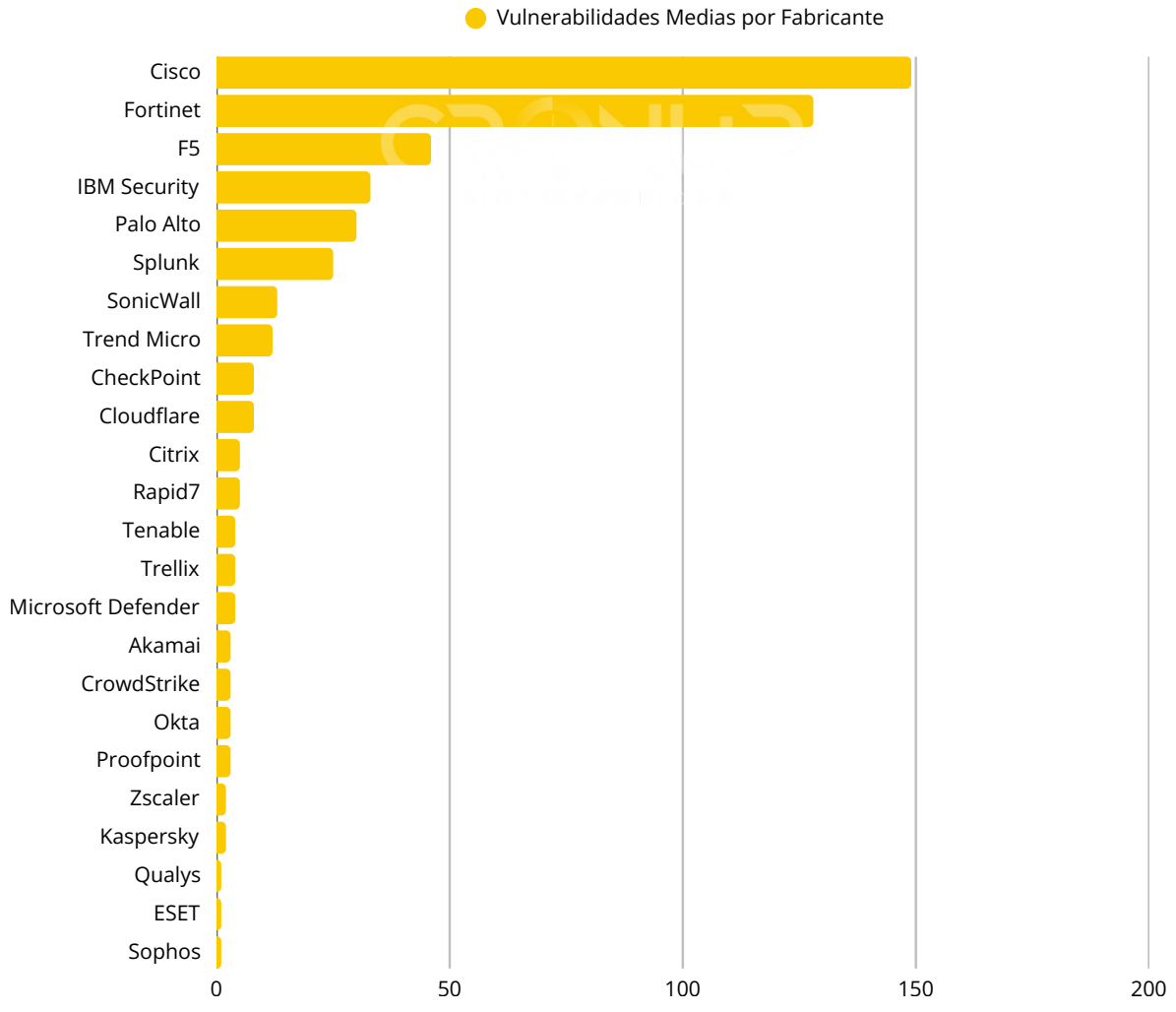
LAS VULNERABILIDADES ALTAS SON UN FENÓMENO TRANSVERSAL QUE AFECTA A TRES CUARTOS DE LA INDUSTRIA, AUNQUE CON VOLÚMENES MUY DISPARES ENTRE FABRICANTES.

VULNERABILIDADES MEDIAS: EL DENOMINADOR COMÚN ENTRE LOS FABRICANTES ANALIZADOS

Con 493 vulnerabilidades de severidad media, distribuidas entre todos los fabricantes con vulnerabilidades, esta categoría representa el flujo base de la gestión de vulnerabilidades.

Este tipo de vulnerabilidades se observa en todos los fabricantes analizados, lo que sugiere que forma parte del ciclo normal de desarrollo y mantenimiento del software.

El volumen absoluto (56% del total) posiciona la gestión eficiente de vulnerabilidades medias como un elemento clave de la operación continua, a diferencia de la urgencia táctica que caracteriza a las vulnerabilidades críticas.

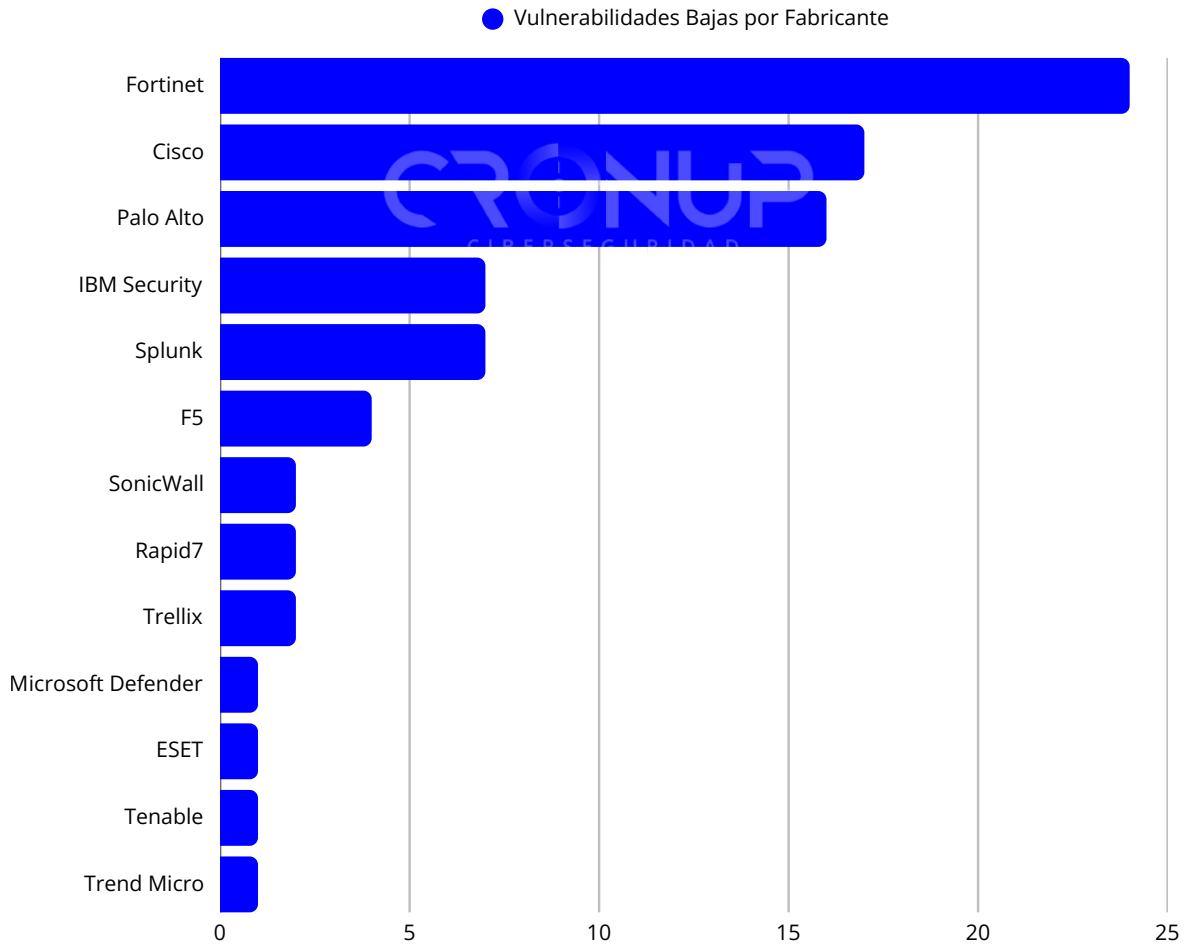


Fuente: Elaboración propia CronUp Ciberseguridad

VULNERABILIDADES BAJAS: PRESENTES, CON MENOR DISTRIBUCIÓN ENTRE FABRICANTES

Las 88 vulnerabilidades de severidad baja se distribuyen en 14 fabricantes, mostrando una cobertura menos extendida que la observada en vulnerabilidades medias, pero más amplia que la de las vulnerabilidades críticas.

Aunque presentan menor severidad técnica, su gestión no debe ser descartada en los procesos de evaluación de riesgo. En escenarios de ataque encadenado, este tipo de vulnerabilidades puede actuar como punto de entrada o facilitar la progresión hacia compromisos de mayor impacto.



Fuente: Elaboración propia CronUp Ciberseguridad

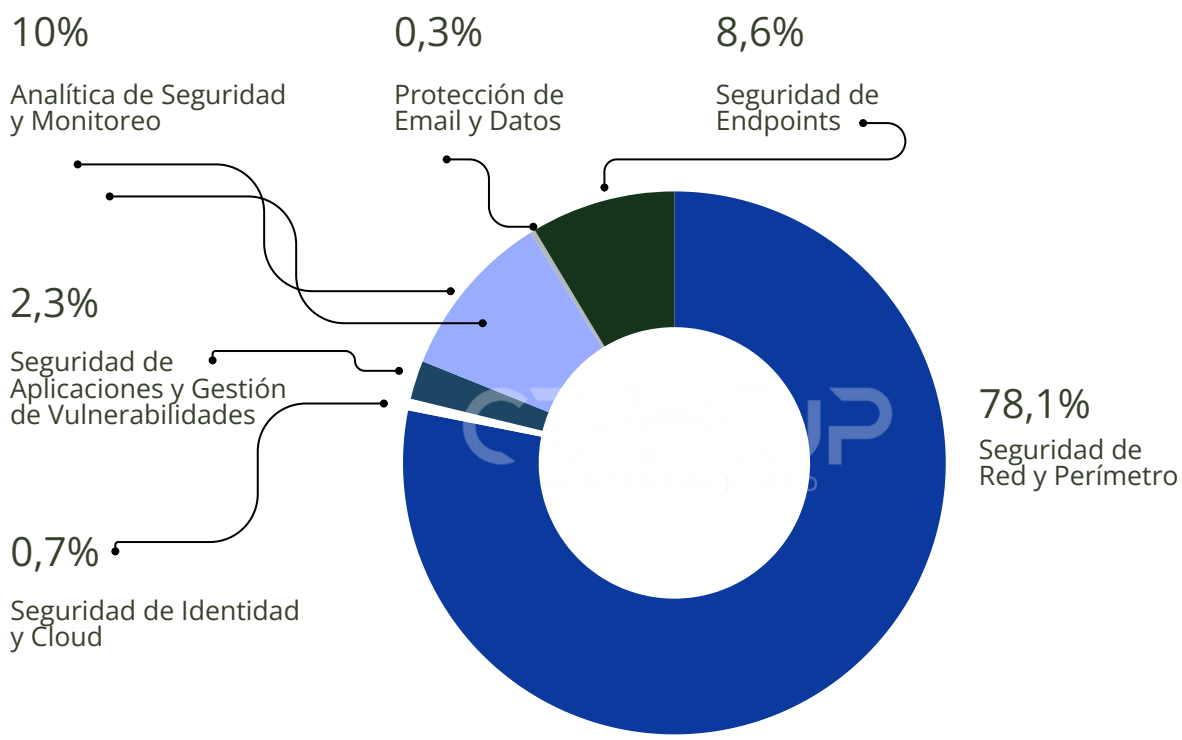
SEGURIDAD DE RED Y PERÍMETRO CONCENTRA LA MAYOR PROPORCIÓN DE VULNERABILIDADES

La distribución de vulnerabilidades por categoría de producto muestra una alta concentración en soluciones de seguridad de red y perímetro, que representan el 78,1% del total (688 vulnerabilidades). Esta categoría no solo presenta el mayor volumen absoluto, sino que además concentra una mayor densidad de vulnerabilidades de severidad media y alta.

El resto de las categorías presenta volúmenes significativamente menores: analítica de seguridad y monitoreo (10%), seguridad de endpoints (8,6%) y seguridad de aplicaciones y gestión de vulnerabilidades (2,3%). Las categorías de seguridad de identidad y cloud, así como protección de email y datos, registran una participación marginal, con menos del 1% del total.

Esta distribución refleja la exposición estructural de las tecnologías de red y perímetro, que operan como puntos de entrada críticos dentro de la arquitectura de ciberseguridad empresarial y, por tanto, concentran una mayor superficie de ataque.

Distribución de Vulnerabilidades



Fuente: Elaboración propia CronUp Ciberseguridad

La mayor intensidad de vulnerabilidades de severidad media y alta responde a factores estructurales más allá del volumen. Las tecnologías de red y perímetro operan como componentes directamente expuestos a Internet dentro de la arquitectura de seguridad, lo que las posiciona como puntos de alto interés tanto para investigadores de seguridad como para actores de amenaza.

Esta concentración debe interpretarse considerando que Cisco y Fortinet, los fabricantes con mayor volumen de vulnerabilidades en el análisis, pertenecen precisamente a la categoría de seguridad de red y perímetro. Asimismo, esta categoría agrupa el mayor número de fabricantes con vulnerabilidades (10 de 24), lo que contribuye a amplificar su representación en el total.

Este patrón responde a la posición estructural de estas tecnologías dentro de la arquitectura de seguridad, más que a diferencias inherentes en la calidad de los productos.

CRONUP
CIBERSEGURIDAD

DETECCIÓN Y RESPUESTA AUTOMATIZADA 24/7

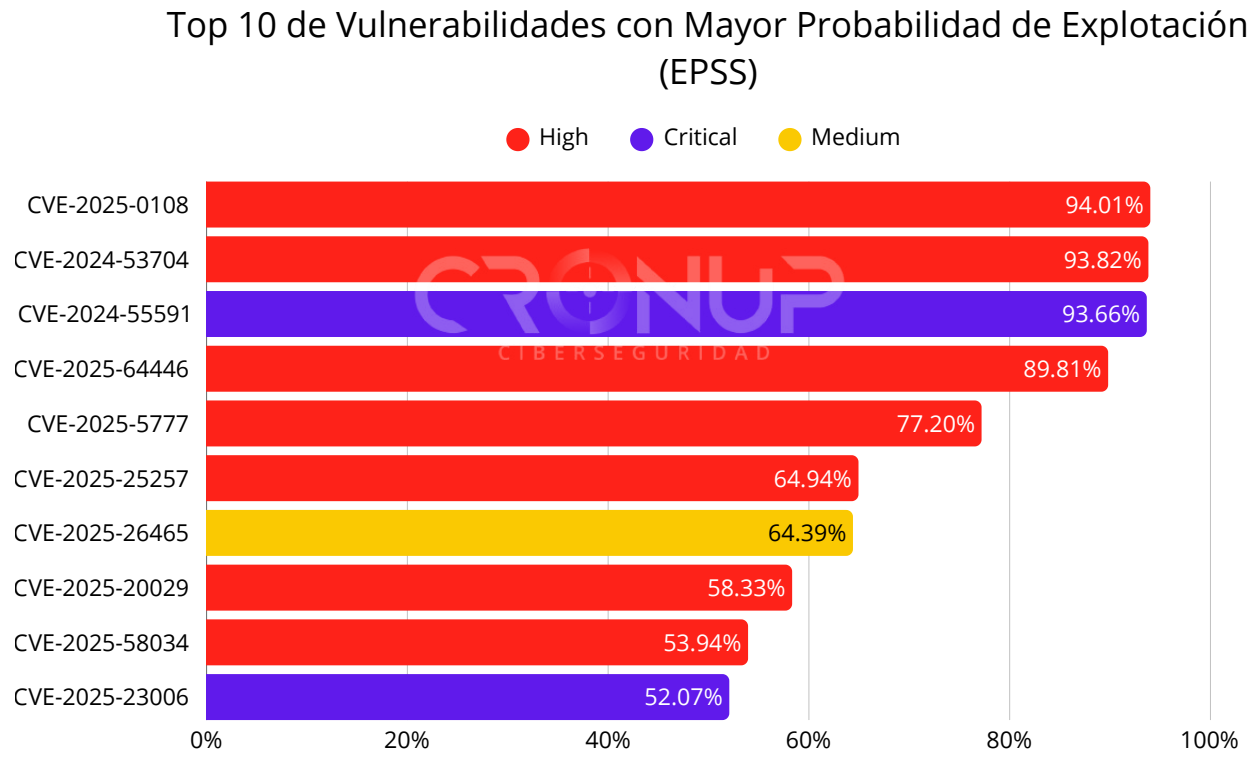
Conversemos y conoce el nivel
de riesgo de tu empresa

EVALUACIÓN DEL RIESGO Y ACTIVIDAD DE AMENAZAS

Top 10 por EPSS: vulnerabilidades con mayor probabilidad de explotación

Utilizando el puntaje EPSS, que estima la probabilidad de explotación de una vulnerabilidad en el mundo real, se identificaron las 10 vulnerabilidades con mayor probabilidad de materialización desde una perspectiva operativa.

Este enfoque permite complementar las métricas tradicionales de severidad técnica, priorizando aquellas vulnerabilidades que, independientemente de su CVSS, presentan mayor probabilidad de ser utilizadas en escenarios reales de ataque.



Fuente: Elaboración propia CronUp Ciberseguridad

Tres vulnerabilidades superan el 93% de probabilidad de explotación en los próximos 30 días:

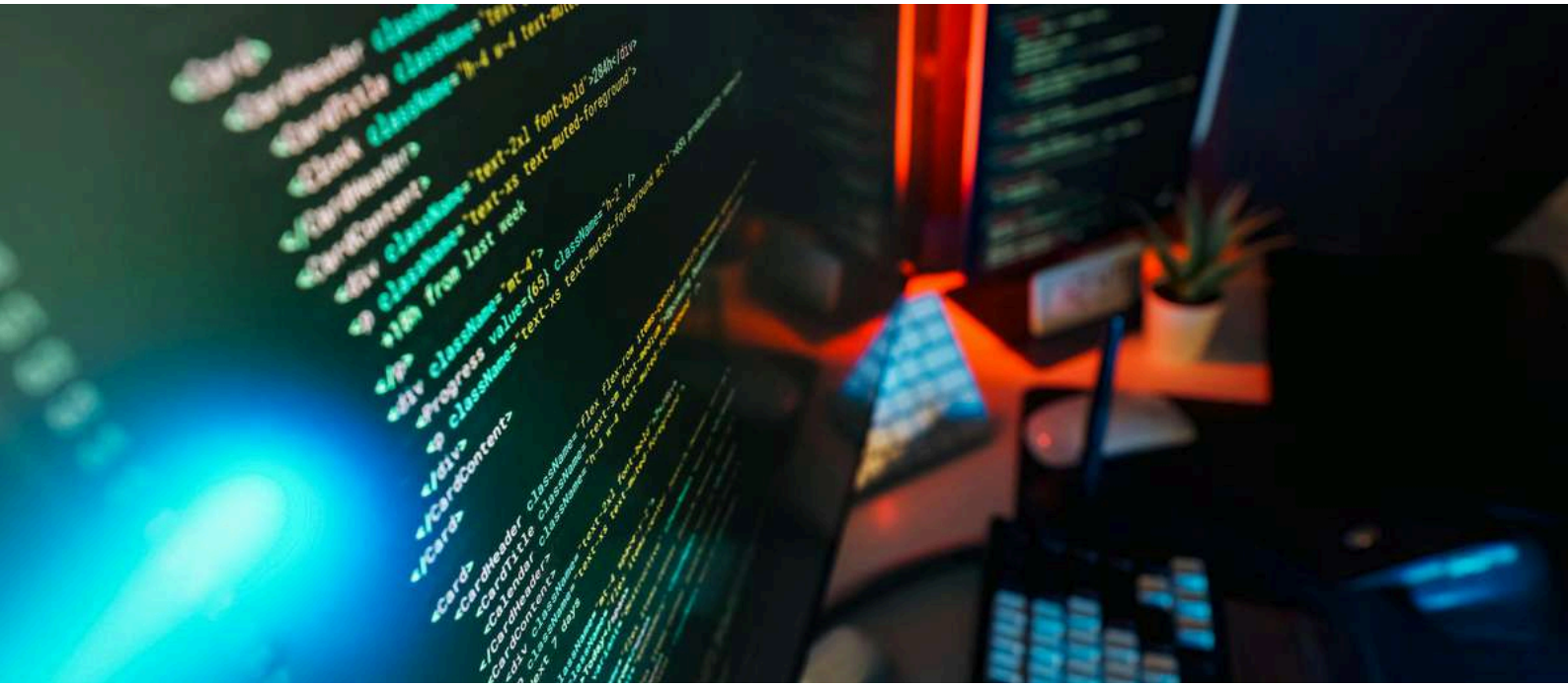
CVE-2025-0108 (Palo Alto, 94.01%), CVE-2024-53704 (SonicWall, 93.82%) y CVE-2024-55591 (Fortinet, 93.66%). Estos valores reflejan un nivel muy elevado de probabilidad de explotación en escenarios reales, lo que las posiciona como prioritarias desde una perspectiva operativa.

De las 10 vulnerabilidades con mayor probabilidad de explotación, 5 corresponden a Fortinet:

Esta concentración debe interpretarse en el contexto de la exposición de estas tecnologías, su despliegue en entornos empresariales y su relevancia dentro de la superficie de ataque.

El Top 10 se distribuye entre 4 fabricantes: Fortinet (5), SonicWall (2), Palo Alto (1), F5 (1) y Citrix (1):

Todas estas vulnerabilidades pertenecen a la categoría de seguridad de red y perímetro, lo que refuerza el patrón observado en el análisis: las tecnologías directamente expuestas a Internet concentran no solo el mayor volumen de vulnerabilidades, sino también aquellas con mayor probabilidad de explotación.

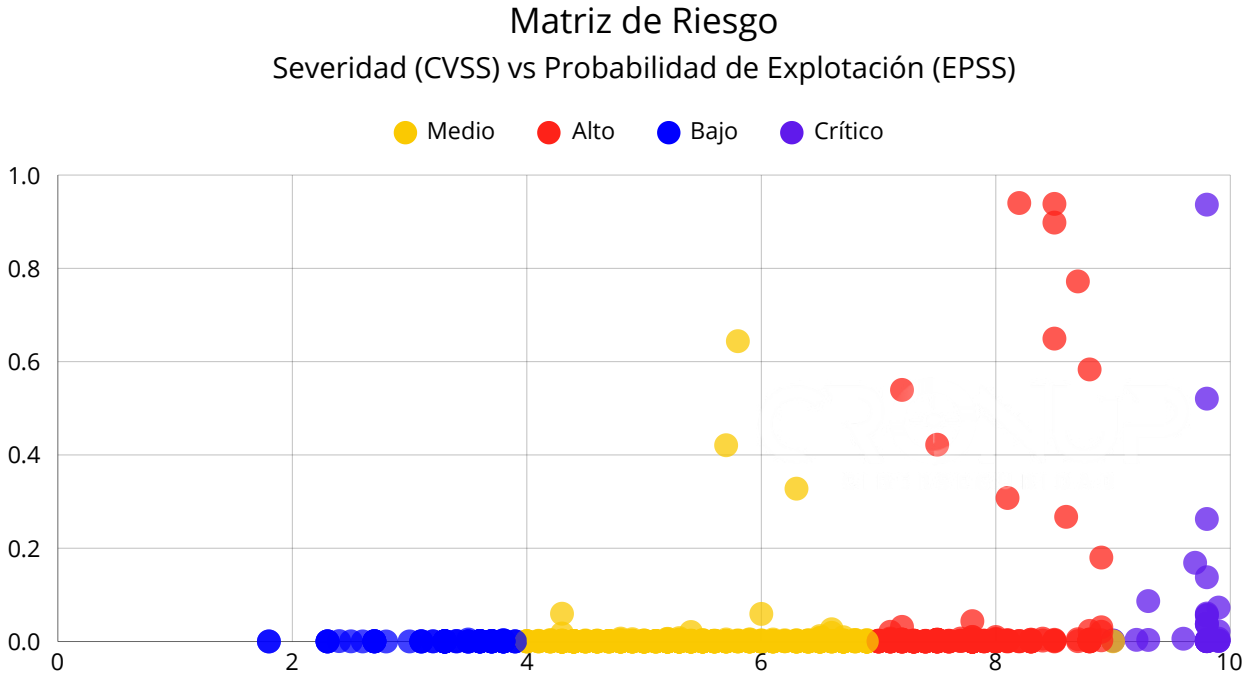


Más allá de la severidad técnica

El análisis anterior permitió identificar las vulnerabilidades con mayor probabilidad de explotación. A continuación, se analiza cuáles de estas vulnerabilidades también presentan alta severidad técnica.

Este enfoque permite identificar el conjunto de vulnerabilidades de mayor riesgo operativo, definido por la combinación de impacto técnico elevado y alta probabilidad de explotación.

La matriz de riesgo permite visualizar esta intersección, posicionando cada vulnerabilidad según su severidad técnica (CVSS) en el eje horizontal y su probabilidad de explotación (EPSS) en el eje vertical.



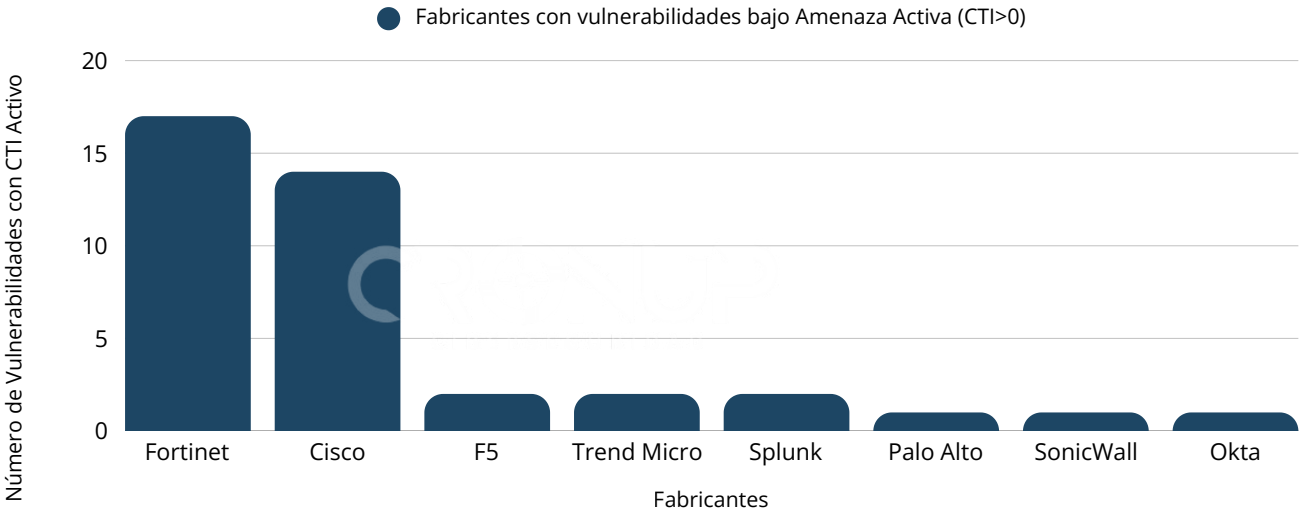
Fuente: Elaboración propia CronUp Ciberseguridad

- La gran mayoría de las vulnerabilidades se concentra en la zona inferior del gráfico (EPSS < 10%), formando una banda densa que atraviesa todos los niveles de CVSS. Este patrón refuerza un hallazgo clave: en términos generales, la mayoría de las vulnerabilidades presenta una baja probabilidad de explotación, independientemente de su severidad técnica.
- El cuadrante superior derecho (definido por CVSS ≥ 7.0 y EPSS > 10%) es notablemente reducido y contiene 16 vulnerabilidades (1,8% del total). Esta zona representa el escenario de mayor riesgo operativo, donde convergen impacto técnico elevado y mayor probabilidad de explotación.

- Se observan vulnerabilidades de severidad alta con EPSS superior al 90%, lo que indica una probabilidad de explotación muy elevada. En contraste, múltiples vulnerabilidades críticas permanecen por debajo del umbral del 10%, lo que evidencia que incluso vulnerabilidades con CVSS 9.0+ pueden presentar una baja probabilidad de explotación en escenarios reales.

CTI COMO SEÑAL DE ALERTA TEMPRANA

El indicador de Cyber Threat Intelligence (CTI) permite identificar vulnerabilidades que han sido referenciadas en fuentes de inteligencia de amenazas o en análisis técnicos relevantes. La presencia de indicadores CTI sugiere interés observado en el ecosistema de amenazas y puede anticipar escenarios de explotación.



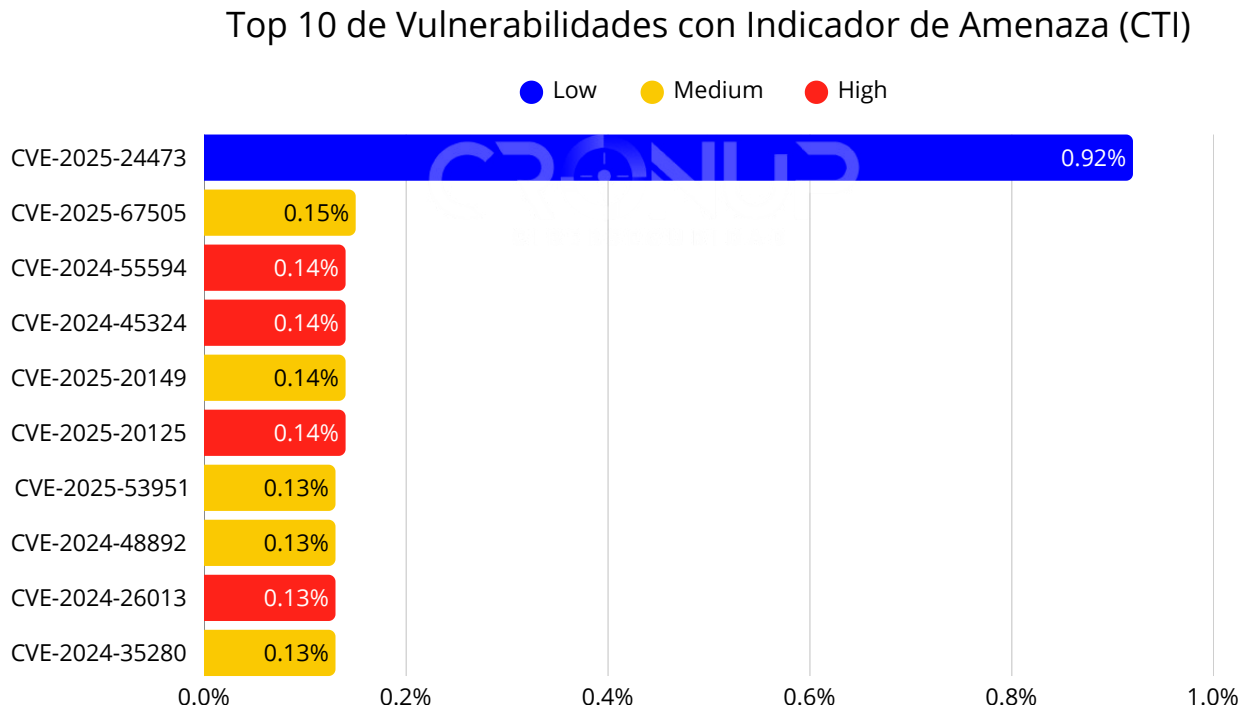
Fuente: Elaboración propia CronUp Ciberseguridad

- Del total de 881 vulnerabilidades analizadas, 40 presentan indicadores de CTI activo (4,5% del total). Aunque representan una fracción menor, corresponden a vulnerabilidades que han sido observadas en contextos reales o en procesos de análisis dentro de la comunidad de ciberseguridad.

Concentración por fabricante

- Fortinet registra 17 vulnerabilidades con indicadores de CTI activo, seguido por Cisco con 14. En conjunto, ambos fabricantes concentran el 77,5% de estas vulnerabilidades. El resto se distribuye entre F5, Trend Micro y Splunk (2 cada uno), y Palo Alto, SonicWall y Okta (1 cada uno).
- Este comportamiento es consistente con la mayor presencia de estas tecnologías en entornos empresariales y su rol dentro de la arquitectura de seguridad. Su amplia adopción incrementa su exposición tanto a investigación de ciberseguridad como a actividad adversaria, lo que favorece la identificación y seguimiento de vulnerabilidades en estos productos.

Las 10 vulnerabilidades con mayor score de CTI revelan un patrón notable.



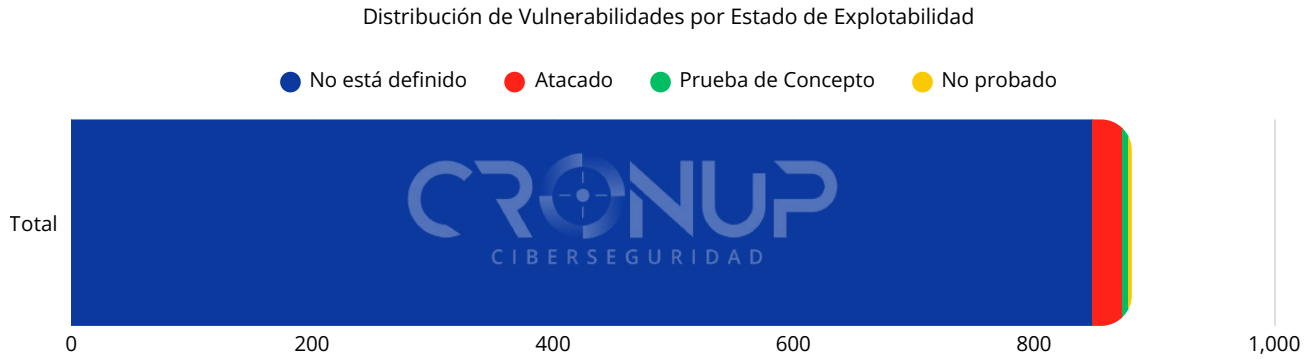
Fuente: Elaboración propia CronUp Ciberseguridad

- Las 10 vulnerabilidades con mayor puntuación de CTI revelan un patrón relevante. CVE-2025-24473 de Fortinet presenta el valor más alto (CTI 0.92), a pesar de tener un CVSS de 3.7 (bajo) y un EPSS cercano a cero. Este caso evidencia que la actividad observada en inteligencia de amenazas puede no estar alineada con la severidad técnica ni con los modelos predictivos de explotación. Aunque el impacto técnico estimado es bajo, la vulnerabilidad ha sido referenciada en fuentes de inteligencia de amenazas.
- El resto del Top 10 muestra una mayor alineación con la severidad técnica: 5 de las 10 vulnerabilidades corresponden a nivel Alto, mientras que 4 se clasifican como Medias.

- Fortinet concentra 7 de las 10 posiciones, mientras que Cisco y Okta aparecen con una vulnerabilidad cada uno. En estos casos, los valores de EPSS se mantienen cercanos a cero, lo que sugiere que estas vulnerabilidades han sido identificadas en fuentes de inteligencia antes de que modelos predictivos como EPSS reflejen una probabilidad elevada de explotación.
- Este comportamiento refuerza el valor del CTI como indicador de alerta temprana, permitiendo identificar señales de interés adversario en etapas previas a su priorización por métricas tradicionales.

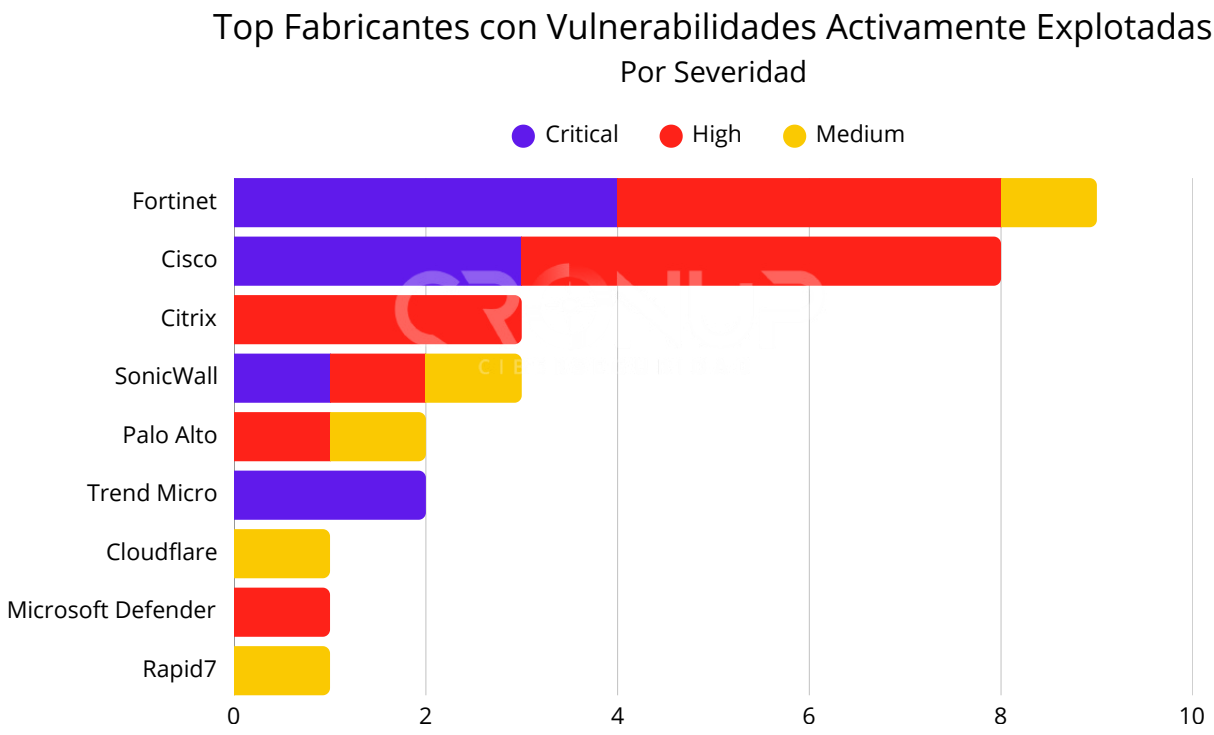
LA BRECHA ENTRE VULNERABILIDAD Y ATAQUE REAL

La mayoría de las vulnerabilidades publicadas no llega a ser explotada. El análisis de explotabilidad evidencia una diferencia relevante entre el volumen total de vulnerabilidades y aquellas que representan un riesgo operativo efectivo.



Fuente: Elaboración propia CronUp Ciberseguridad

- El 96,3% de las vulnerabilidades analizadas (848 de 881) presenta estado “No definido”, lo que indica ausencia de evidencia pública de explotación o de código de prueba de concepto disponible. Esta proporción elevada sugiere que la mayoría de las vulnerabilidades permanece sin evidencia observable de explotación en el momento del análisis.
- Solo el 3,4% de las vulnerabilidades (30 en total) se ubica en categorías con evidencia más directa de explotación: 25 presentan actividad de ataque observada (2,8%) y 5 cuentan con prueba de concepto pública (0,6%). Estas vulnerabilidades reflejan escenarios donde existe evidencia de explotación o de desarrollo de capacidades asociadas. Adicionalmente, 3 vulnerabilidades se clasifican como “No probado” (0,3%), lo que indica que no existe evidencia de explotación, pero tampoco se ha descartado su viabilidad.
- Las 30 vulnerabilidades con evidencia de explotación o desarrollo de exploits no se distribuyen de manera uniforme, sino que se concentran en un subconjunto específico de fabricantes, con diferencias relevantes en volumen y composición de severidad.



Fuente: Elaboración propia CronUp Ciberseguridad

- Entre las vulnerabilidades con evidencia de explotación activa, Fortinet registra el mayor número (9), distribuidas en 4 críticas, 4 altas y 1 media. Cisco le sigue con 8 vulnerabilidades: 3 críticas y 5 altas. En conjunto, ambos fabricantes concentran aproximadamente dos tercios de las vulnerabilidades bajo explotación activa.
- Las vulnerabilidades explotadas no se limitan a la categoría crítica. El análisis muestra una distribución que incluye severidades crítica, alta y media, lo que sugiere que la selección de vulnerabilidades por parte de los atacantes no se basa exclusivamente en la severidad técnica (CVSS), sino también en factores como la facilidad de explotación, la exposición de la tecnología y el valor del objetivo.

LAS 30 VULNERABILIDADES EXPLOTABLES NO SE DISTRIBUYEN UNIFORMEMENTE: SE CONCENTRAN EN UN SUBCONJUNTO ESPECÍFICO DE FABRICANTES, CON DISPARIDADES MARCADAS EN VOLUMEN Y COMPOSICIÓN DE SEVERIDAD.

PRIORIZACIÓN DE REMEDIACIÓN

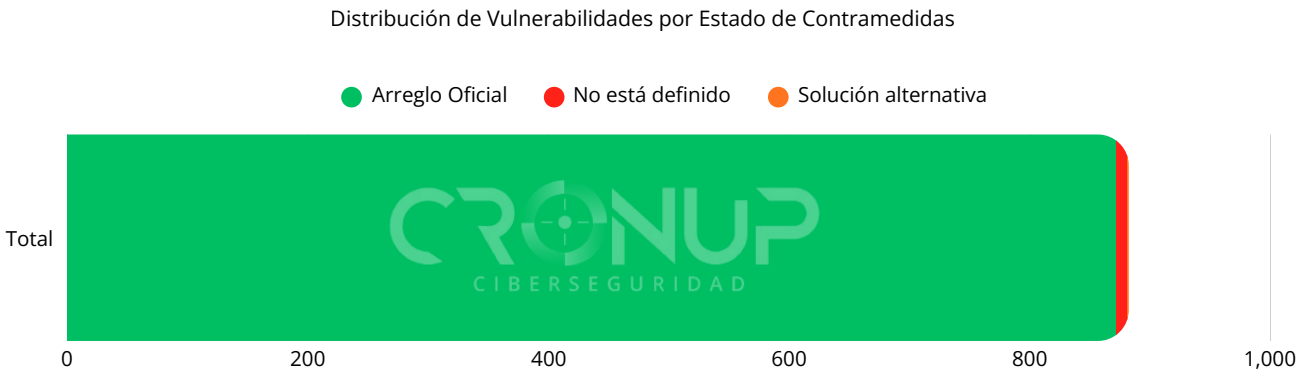
La remediación efectiva de vulnerabilidades requiere más que identificar amenazas: necesita entender qué soluciones están disponibles y cuáles vulnerabilidades demandan atención urgente ante la ausencia de parches.

PANORAMA FAVORABLE DE REMEDIACIONES

Comprender las soluciones disponibles y determinar cuáles vulnerabilidades deben ser priorizadas según su nivel de riesgo es crucial para una efectiva remediación de vulnerabilidades, que va más allá de simplemente identificar amenazas.

El entorno es positivo para llevar a cabo remediaciones.

El análisis muestra una alta disponibilidad de contramedidas: el 98.9% de las vulnerabilidades cuenta con arreglo oficial (872 de 881), lo que indica que existen parches o actualizaciones de ciberseguridad para la gran mayoría de los casos analizados durante 2025.



Fuente: Elaboración propia CronUp Ciberseguridad

Solo 9 vulnerabilidades (1,0%) se clasifican como “sin contramedidas disponibles”, correspondientes a casos en los que no se identificaron parches oficiales en fuentes públicas. No obstante, esta clasificación no implica necesariamente la ausencia total de soluciones, ya que algunos parches pueden encontrarse disponibles en portales de soporte con acceso restringido o documentados en advisories no indexados en bases de datos públicas.

Una única vulnerabilidad (0,1%) cuenta con una mitigación alternativa (workaround), lo que indica la existencia de una solución temporal en ausencia de un parche definitivo.

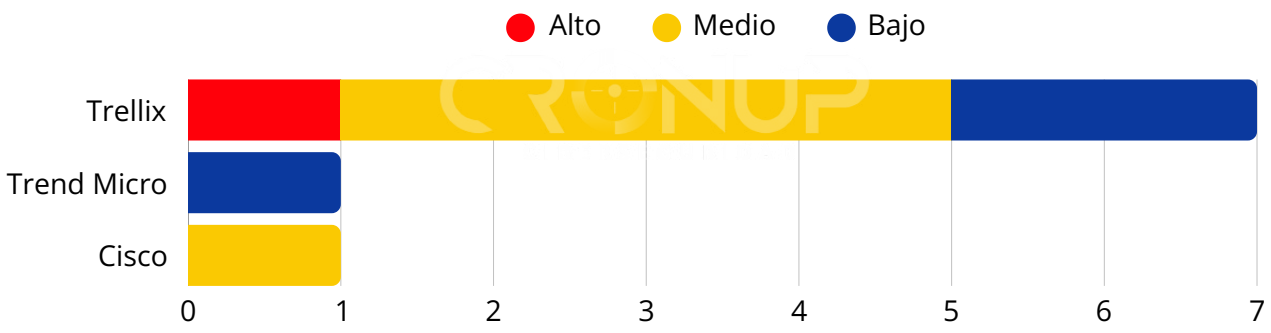
EXPOSICIÓN MARGINAL

Las 9 vulnerabilidades clasificadas como sin contramedidas disponibles se distribuyen entre 3 fabricantes: Trellix (7), Cisco (1) y Trend Micro (1). Estos casos corresponden a situaciones en las que no fue posible identificar parches oficiales en fuentes públicas al momento del análisis.

No se identificaron vulnerabilidades críticas sin contramedidas disponibles en fuentes públicas.

En este contexto, el desafío principal no radica en la disponibilidad de contramedidas, sino en su priorización e implementación oportuna dentro de la organización.

Top 15 Fabricantes con Vulnerabilidades sin Contramedidas - Por severidad



Fuente: Elaboración propia CronUp Ciberseguridad

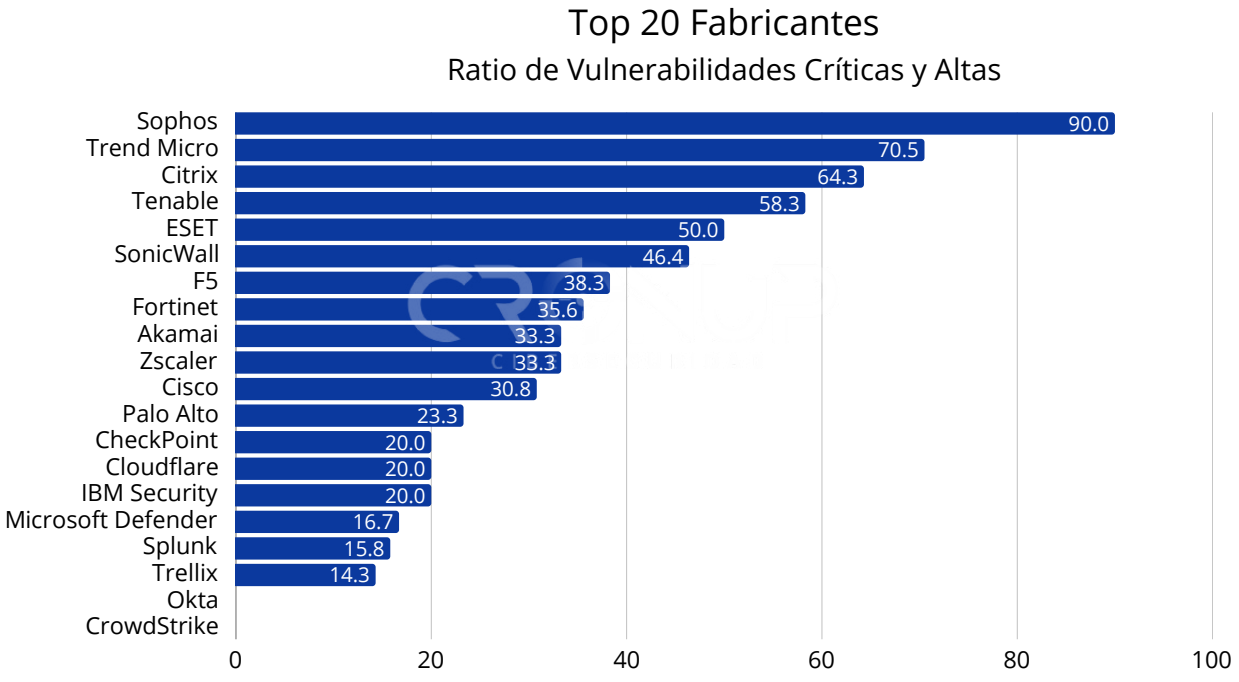
- Trellix registra 7 de las 9 vulnerabilidades sin contramedidas identificadas (1 alta, 4 medias y 2 bajas). La validación de estos casos presentó limitaciones, ya que las publicaciones de seguridad de este fabricante requieren autenticación en su portal de soporte, lo que limita la verificación en fuentes públicas. En este contexto, es posible que algunas de estas vulnerabilidades cuenten con soluciones documentadas en canales restringidos a clientes.
- Cisco (1 vulnerabilidad media) y Trend Micro (1 vulnerabilidad baja) también presentan casos sin confirmación pública de contramedidas en las fuentes analizadas.

¿TU EMPRESA ESTÁ PREPARADA PARA ESTE 2026?

ANÁLISIS DE PROPORCIÓN DE VULNERABILIDADES CRÍTICAS Y ALTAS POR FABRICANTE

El volumen absoluto de vulnerabilidades no refleja completamente el riesgo. Un fabricante con 100 vulnerabilidades donde 10 son críticas presenta un perfil distinto a uno con 10 vulnerabilidades donde 9 son críticas. La proporción de vulnerabilidades críticas y altas permite complementar el análisis, aportando una visión más precisa de la composición de severidad.

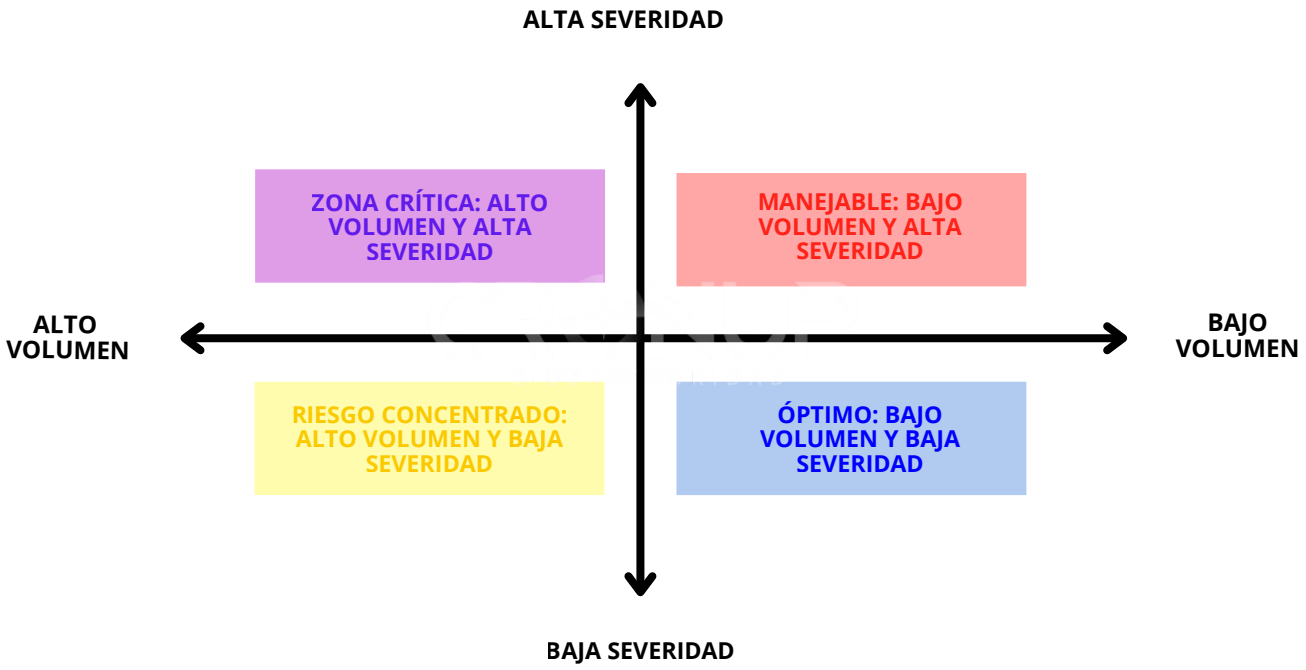
El ratio promedio de vulnerabilidades críticas y altas se ubica en 28,4%, lo que establece una línea base de comparación. Los fabricantes por debajo de este umbral presentan una menor proporción de vulnerabilidades de mayor severidad, mientras que aquellos por encima reflejan una mayor concentración de este tipo de hallazgos, lo que puede requerir un análisis más detallado en función de su contexto y exposición.



Fuente: Elaboración propia CronUp Ciberseguridad

- El volumen absoluto de vulnerabilidades puede no reflejar completamente la composición del riesgo asociado a cada fabricante. El análisis de proporción de vulnerabilidades críticas y altas permite complementar esta visión, evidenciando diferencias relevantes en la distribución de severidad.

- En algunos casos, se observan proporciones elevadas de vulnerabilidades de severidad crítica y alta. Por ejemplo, Sophos presenta una proporción del 90% (9 de 10), mientras que otros fabricantes como Trend Micro (70,5%, 31 de 44), Citrix (64,3%, 9 de 14), Tenable (58,3%, 7 de 12) y ESET (50%, 2 de 4) también muestran concentraciones relevantes.
- Es importante considerar que estas proporciones pueden verse influenciadas por el número total de vulnerabilidades reportadas y el tamaño de la muestra analizada, especialmente en fabricantes con menor volumen total.
- Asimismo, varios de estos casos corresponden a tecnologías de seguridad de endpoints, lo que sugiere la necesidad de analizar en mayor profundidad cómo se distribuye la severidad en distintas categorías de producto, considerando su rol dentro de la arquitectura y su contexto de exposición.



Este modelo permite visualizar cómo distintas combinaciones de volumen y severidad configuran perfiles diferenciados de riesgo. Los fabricantes ubicados en el cuadrante superior derecho (alto volumen y alta severidad) concentran la mayor carga operativa y requieren una priorización más intensiva en la gestión de vulnerabilidades.

Zona Crítica: Fabricantes como Trend Micro (44 vulnerabilidades, 70,5% críticas/altas) combinan alto volumen con alta severidad, creando la mayor carga operacional para equipos de seguridad.

- En contraste, cinco fabricantes registran una proporción de 0% de vulnerabilidades críticas o altas: Okta, CrowdStrike, Kaspersky, Rapid7 y Qualys. En estos casos, todas las vulnerabilidades reportadas en 2025 corresponden a severidades media o baja. Es importante considerar que, en algunos fabricantes, este resultado puede estar influenciado por el bajo número total de vulnerabilidades analizadas (por ejemplo, Qualys con 1 y Kaspersky con 2).
- Analizando los casos con mayor proporción de vulnerabilidades críticas y altas, se observa un patrón relevante en la composición de severidad. Sophos presenta 1 vulnerabilidad crítica y 8 altas, mientras que Trend Micro registra 8 críticas y 23 altas. En contraste, Citrix, Tenable y ESET no presentan vulnerabilidades críticas en el período analizado.
- Este comportamiento sugiere que, en varios casos, una alta proporción de severidad está impulsada principalmente por la acumulación de vulnerabilidades de nivel alto, más que por una concentración de vulnerabilidades críticas.

OKTA

0% CRÍTICAS/ALTAS
GESTIÓN DE IDENTIDAD

CROWDSTRIKE

0% CRÍTICAS/ALTAS
ENDPOINT DETECTION

KASPERSKY

0% CRÍTICAS/ALTAS
2 VULNERABILIDADES TOTALES

RAPID7

0% CRÍTICAS/ALTAS
7 VULNERABILIDADES TOTALES

QUALYS

0% CRÍTICAS/ALTAS
1 VULNERABILIDAD TOTAL

ESTE COMPORTAMIENTO REFLEJA UNA MENOR PROPORCIÓN DE VULNERABILIDADES CRÍTICAS Y ALTAS EN EL PERÍODO ANALIZADO. NO OBSTANTE, ESTE RESULTADO DEBE INTERPRETARSE CONSIDERANDO FACTORES COMO EL VOLUMEN TOTAL DE VULNERABILIDADES, EL ALCANCE DE LOS PRODUCTOS Y EL CONTEXTO DE EXPOSICIÓN.

JUNTANDO TODAS LAS PIEZAS: EL RIESGO REAL

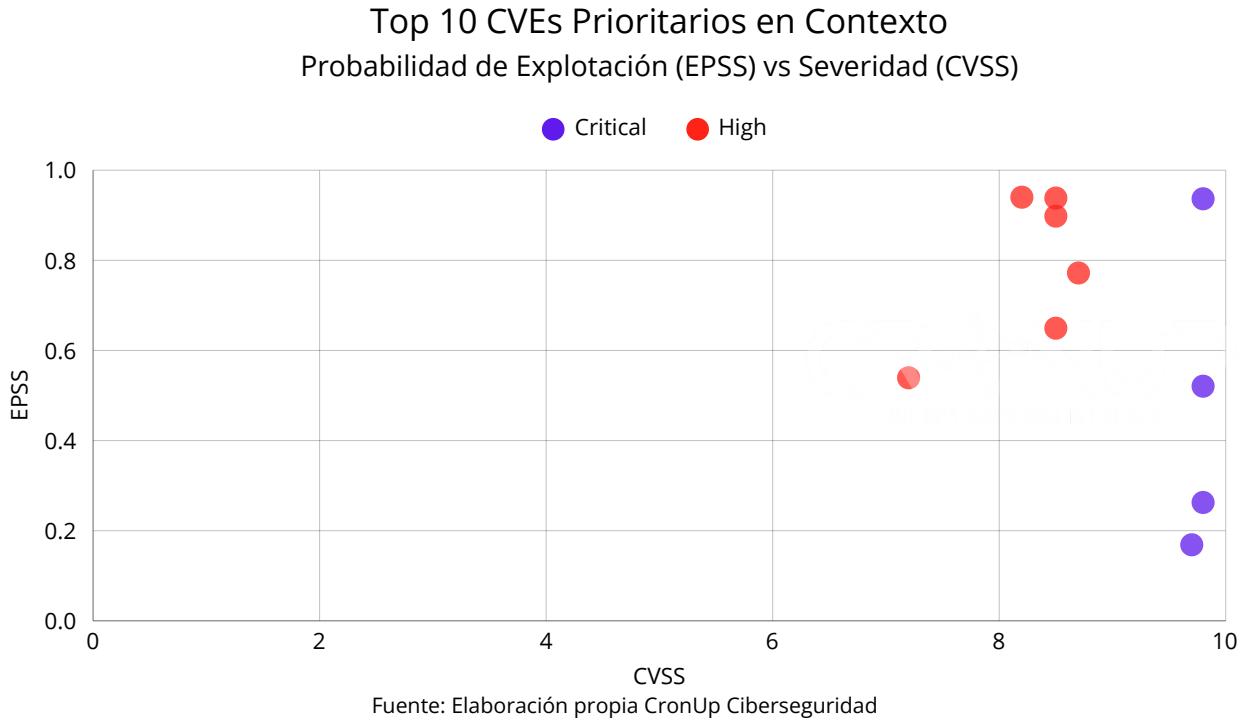
TOP 10 DE VULNERABILIDADES CON MAYOR RIESGO COMBINADO

El siguiente análisis integra las dimensiones evaluadas a lo largo del estudio (CVSS, EPSS, estado de explotabilidad, CTI y disponibilidad de contramedidas) mediante un modelo de scoring ponderado, con el objetivo de identificar las vulnerabilidades con mayor riesgo combinado desde una perspectiva operativa.

Metodología del *Priority Score*

El modelo asigna pesos relativos a cada dimensión, reflejando su contribución al riesgo real:

- CVSS Base Score (30%): severidad técnica de la vulnerabilidad
- EPSS (25%): probabilidad estimada de explotación en escenarios reales
- Estado de Explotabilidad (25%): evidencia de explotación o disponibilidad de código
- CTI (10%): presencia en fuentes de inteligencia de amenazas
- Contramedidas (10%): disponibilidad de parches o mitigaciones



Fuente: Elaboración propia CronUp Ciberseguridad

Del análisis a la realidad: CVEs que se materializaron durante el año 2025

El modelo de priorización presentado en este estudio no es un ejercicio académico, sino que se alinea con nuestro servicio de Alerta Temprana de Riesgos (ATRc®). La validación de su efectividad llegó cuando varios CVEs identificados en nuestros rankings se materializaron en campañas de ataque reales durante 2025.

Cuando emerge un 0-day, nuestro equipo inicia inmediatamente un proceso de análisis multidimensional: validamos si está siendo explotado activamente, cruzamos con el inventario tecnológico de nuestros clientes, evaluamos la exposición real, y en casos críticos, ejecutamos validaciones técnicas para confirmar si sistemas específicos son vulnerables. Esta Inteligencia de Vulnerabilidades (no solo datos de CVE) es lo que permite anticipar situaciones de riesgo antes de que las amenazas materialicen sus ataques.

A continuación, algunos casos que investigamos, monitoreamos y reportamos durante 2025:

CVE-2025-0108 (Palo Alto)

Actores maliciosos explotaron esta vulnerabilidad crítica en PAN-OS, eludiendo autenticación para ejecutar scripts PHP y obtener acceso no autorizado. Con CVSS 8.2, EPSS del 94.01% y sin contramedidas disponibles al momento inicial, este CVE ejemplificó el escenario "tormenta perfecta". Ante los reportes de explotación activa, validamos inmediatamente la exposición en inventarios de clientes y alertamos sobre el encadenamiento con **CVE-2024-9474** y **CVE-2025-0111** que atacantes estaban utilizando para elevar privilegios. Las organizaciones afectadas recibieron recomendaciones de mitigación antes de que la explotación se generalizara.

CVE-2025-64446 (Fortinet)

Este **0-day en FortiWeb bajo explotación masiva** permitió elusión de autenticación y path traversal para crear usuarios administradores sin credenciales. Con CVSS 8.5, EPSS 89.81% y sin CVE asignado inicialmente, la ventana crítica dejó a miles de dispositivos expuestos. Mediante nuestro monitoreo continuo de superficie de ataque, detectamos actividad maliciosa activa e identificamos múltiples dispositivos vulnerables en Chile y la región, incluyendo instancias con alta probabilidad de compromiso. Paralelamente, validamos exposición en inventarios de clientes con FortiWeb, proporcionando recomendaciones e iniciando la respuesta al incidente mientras Fortinet liberaba FortiWeb 8.0.2 como versión corregida.

CVE-2025-5777 (Citrix)

"**Citrix Bleed**" permite filtrar memoria sensible y comprometer tokens de sesión, facilitando accesos no autorizados y movimientos laterales. Con CVSS 8.7, EPSS 77,2% y evidencia de explotación activa: la amenaza era inmediata. Durante labores de Inteligencia de Vulnerabilidades, detectamos al menos cinco empresas estratégicas del ecosistema nacional con exposición activa, incluso más de 30 días después de la liberación del parche oficial. La persistencia de esta exposición en infraestructuras clave representó un riesgo inaceptable. Validamos técnicamente que la ventana de exposición se mantuvo abierta no por ausencia de parches, sino por aplicación incorrecta o configuraciones erróneas que mantuvieron las brechas activas bajo una falsa sensación de seguridad.

Caso Cisco: Explotación Coordinada de Múltiples CVEs

CVE-2025-20333, **CVE-2025-20362** y **CVE-2025-20352 fueron explotadas simultáneamente** en dispositivos Cisco ASA, Firepower Threat Defense e IOS/IOS XE, afectando hasta 2 millones de dispositivos globalmente. Asociadas a la campaña ArcaneDoor vinculada a espionaje estatal, permitieron implantación de malware y ejecución remota de comandos. Identificamos exposición de servicios Cisco vulnerables en clientes y aplicamos threat hunting especializado para búsqueda de IoCs asociados a la campaña, confirmando que Cisco demanda monitoreo continuo para anticipar convergencias de múltiples vectores de ataque.

Caso F5: Convergencia de Vulnerabilidades en Productos Enterprise

La exposición crítica de F5 se materializó cuando actores estatales vinculados a China (UNC5221) comprometieron sistemas internos del fabricante, exfiltrando código fuente y vulnerabilidades no divulgadas de BIG-IP. El impacto fue sistémico: más de 269,000 dispositivos F5 expuestos globalmente, con cuatro CVEs bajo ataque simultáneo (CVE-2025-53868, CVE-2025-61955, CVE-2025-57780, CVE-2025-60016). Este caso reveló la falsa sensación de seguridad en productos enterprise y la necesidad de verificación independiente de fabricantes, independientemente de su reputación. Ante la directiva de emergencia de CISA, validamos exposición en clientes y correlacionamos IoCs asociados a UNC5221 para identificar posibles compromisos en la cadena de suministro.

La correlación entre el modelo predictivo y los incidentes observados no es coincidencia**:** es el resultado de integrar Cyber Threat Intelligence, análisis continuo de exposición y validación técnica en tiempo real. Las vulnerabilidades que aparecen en los rankings de máxima urgencia no son ejercicios hipotéticos, son amenazas que monitoreamos activamente, validamos contra inventarios tecnológicos reales, y sobre las cuales alertamos antes de que materialicen compromisos.

Los tres CVEs con mayor puntuación en el modelo de riesgo combinado reflejan la convergencia de múltiples dimensiones: alta severidad técnica, elevada probabilidad de explotación y evidencia de actividad en escenarios reales.

CVE-2024-55591

(FORTINET, 77.8 PUNTOS)

CVSS 9.8 (crítico), EPSS 93.66% y evidencia de explotación activa. Aunque actualmente cuenta con parche oficial, la combinación de alta severidad y elevada probabilidad de explotación lo posiciona entre los casos de mayor riesgo operativo.

CVE-2024-53704

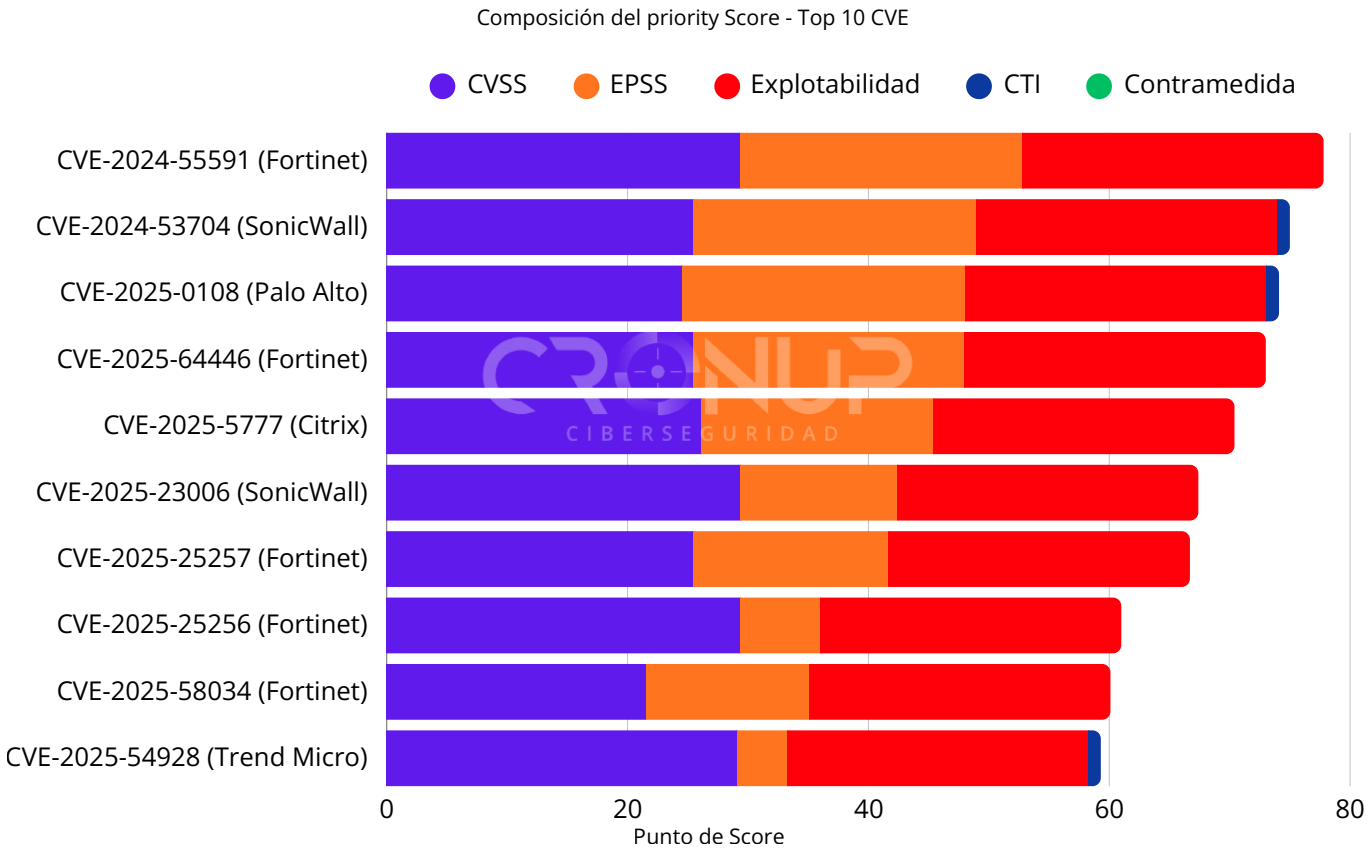
(SONICWALL, 74.6 PUNTOS)

CVSS 8.5, EPSS 93.82% y actividad de ataque observada. Corresponde a un caso asociado a SSL VPN, donde la combinación de exposición y probabilidad de explotación incrementa su relevancia operativa. El parche se encuentra disponible.

CVE-2025-0108

(PALO ALTO, 73.5 PUNTOS)

CVSS 8.2, EPSS 94.01% y evidencia de explotación activa. Aunque no alcanza nivel crítico en términos de CVSS, su alta probabilidad de explotación y estado de actividad lo posicionan dentro de las vulnerabilidades de mayor riesgo combinado. El parche se encuentra disponible.



Fuente: Elaboración propia CronUp Ciberseguridad

- De las 10 vulnerabilidades con mayor riesgo combinado, 5 corresponden a Fortinet. SonicWall aparece en 2 casos, mientras que Palo Alto, Citrix y Trend Micro registran 1 cada uno.
- Todas las vulnerabilidades incluidas en este conjunto presentan evidencia de explotación activa, lo que indica que no se trata únicamente de escenarios potenciales, sino de casos con actividad observada en el ecosistema de amenazas.
- Tras la validación de datos, las 10 vulnerabilidades cuentan con contramedidas disponibles. Si bien esto permite su remediación, la presencia de explotación activa refuerza la necesidad de una gestión oportuna en función del contexto de exposición de cada organización.
- En términos de severidad, 6 corresponden a nivel Alto y 4 a nivel Crítico. El score promedio del Top 10 es de 68.3 puntos, reflejando la convergencia de severidad técnica, probabilidad de explotación y evidencia de actividad adversaria.

CVE utilizados en ataques de Ransomware

Según el catálogo **Known Exploited Vulnerabilities (KEV)** de **CISA**, múltiples grupos de ransomware han aprovechado vulnerabilidades conocidas y activamente explotadas como vector inicial de acceso. Estas fallas, muchas de ellas con exploits públicos o de fácil weaponización, permiten a los atacantes comprometer sistemas expuestos sin necesidad de técnicas avanzadas, facilitando la intrusión inicial, el movimiento lateral y el despliegue de cargas de ransomware.

Del contraste entre el inventario de vulnerabilidades analizado en el presente estudio y el catálogo KEV, se identificaron 22 CVEs con explotación activa confirmada en entornos reales. De este conjunto, 5 presentan uso confirmado en campañas de ransomware según la atribución de CISA, todos correspondientes a productos de seguridad de red y perímetro: CVE-2024-55591 y CVE-2025-24472 de Fortinet, CVE-2025-23006 y CVE-2024-53704 de SonicWall, y CVE-2025-5777 de Citrix. Los tres primeros destacan además por sus valores de EPSS, con CVE-2024-55591 (93.7%), CVE-2024-53704 (93.8%) y CVE-2025-23006 (52.1%), lo que indica que su explotación no solo está confirmada sino que se mantiene activa y sostenida en el tiempo.

A continuación se presentan los CVEs identificados en el presente estudio con uso confirmado en campañas de ransomware según la atribución del catálogo KEV de CISA.

CVE	Vendor	Producto	Severidad	EPSS	CTI	Uso en Ransomware
CVE-2024-53704	SonicWall	SonicOS SSLVPN	Alta	0.93819	0.06	Conocido (sin atribución específica)
CVE-2024-55591	Fortinet	FortiOS/ FortiProxy	Crítica	0.93661	0.00	Conocido (sin atribución específica)
CVE-2025-5777	Citrix	NetScaler ADC/ Gateway	Alta	0.77205	0.00	Conocido (sin atribución específica)
CVE-2025-23006	SonicWall	SMA1000	Crítica	0.52066	0.00	Conocido (sin atribución específica)
CVE-2025-24472	Fortinet	FortiOS/ FortiProxy	Alta	0.04369	0.07	Conocido (sin atribución específica)

CONCLUSIONES DEL ESTUDIO

El análisis de 881 vulnerabilidades reportadas durante 2025 en 24 de los 28 fabricantes evaluados revela un panorama que desafía los enfoques tradicionales de gestión de vulnerabilidades basados exclusivamente en severidad técnica.

LA SEVERIDAD TÉCNICA NO CUENTA TODA LA HISTORIA.

Aunque el 4% de las vulnerabilidades corresponde a nivel crítico y el 30% a nivel alto, solo el 3,4% presenta evidencia de explotación activa. Esta diferencia entre severidad potencial y riesgo observable refuerza la necesidad de incorporar métricas complementarias: EPSS permite estimar la probabilidad de explotación, CTI identifica señales de interés en el ecosistema de amenazas, y el estado de contramedidas contribuye a definir la prioridad operativa.

Priorizar únicamente en función del CVSS puede llevar a destinar esfuerzos a vulnerabilidades críticas sin evidencia de explotación, mientras se postergan vulnerabilidades de severidad alta con alta probabilidad de explotación y actividad observada.

LA EXPOSICIÓN SE CONCENTRA EN TECNOLOGÍAS DE RED Y PERÍMETRO

Esta categoría representa el 78% de todas las vulnerabilidades reportadas, lo que refleja tanto la amplitud de sus portafolios como su posición como componentes directamente expuestos a Internet dentro de la arquitectura de seguridad. Las organizaciones con infraestructuras de red complejas (firewalls, balanceadores de carga, VPNs y WAFs) tienden a enfrentar una mayor carga en la gestión de vulnerabilidades, particularmente en rangos de severidad media y alta. Esta concentración responde a factores estructurales propios de la naturaleza y función de estos productos.

EXPOSICIÓN CONCENTRADA EN FABRICANTES CON ALTA PRESENCIA EN ENTORNOS EMPRESARIALES

Algunos fabricantes presentan una mayor concentración de vulnerabilidades en distintas dimensiones del análisis. Por ejemplo, Fortinet registra 236 vulnerabilidades totales, 17 con indicadores de CTI y 5 apariciones en el Top 10 de riesgo combinado. Cisco, por su parte, presenta 240 vulnerabilidades totales, con presencia en análisis de explotabilidad y CTI.

Para las organizaciones que utilizan este tipo de tecnologías, la gestión de vulnerabilidades no es una actividad puntual, sino un proceso continuo que requiere capacidades de monitoreo, priorización y respuesta adaptativa, incorporando además análisis contextual y señales tempranas del comportamiento adversario para anticipar riesgos antes de su materialización.

Este comportamiento refuerza que la superficie de ataque no se distribuye de forma uniforme, sino que se concentra en componentes críticos de la arquitectura.

LA PROPORCIÓN DE SEVERIDAD COMPLEMENTA EL ANÁLISIS POR VOLUMEN

El análisis de proporción de vulnerabilidades críticas y altas aporta una dimensión adicional al volumen total. En algunos casos se observan concentraciones elevadas de severidad, por ejemplo, Sophos (90%), Trend Micro (70,5%) y Citrix (64,3%), que contrastan con fabricantes de mayor volumen pero menor proporción de hallazgos de alta severidad.

Esta diferencia sugiere que, dependiendo de la tecnología utilizada, una nueva vulnerabilidad puede tener mayor probabilidad de corresponder a niveles de severidad elevados, independientemente del volumen total observado.

En consecuencia, la proporción de severidad constituye un elemento relevante para la toma de decisiones, complementando el análisis por volumen al evaluar la composición del riesgo y orientar la asignación de esfuerzos de remediación en función del contexto operativo.

LA DISPONIBILIDAD DE CONTRAMEDIDAS ES ALTA, PERO DEPENDE DE SU IMPLEMENTACIÓN OPORTUNA.

El 98,9% de las vulnerabilidades analizadas cuenta con una mitigación oficial. En el Top 10 de riesgo combinado, todas las vulnerabilidades presentan evidencia de explotación activa y, al mismo tiempo, cuentan con parches disponibles.

Este comportamiento sugiere que la disponibilidad de soluciones técnicas no es suficiente por sí sola para reducir el riesgo, sino que su efectividad depende de su implementación oportuna y adecuada dentro de la organización.

En este contexto, la ventana entre la disponibilidad del parche y su aplicación se convierte en un punto crítico donde puede materializarse el riesgo, especialmente en escenarios de explotación activa.

EL CONTEXTO DE AMENAZA ES DINÁMICO

La presencia de indicadores de Cyber Threat Intelligence (CTI) sugiere interés observado en el ecosistema de amenazas y constituye una señal relevante para la priorización, independientemente de la severidad técnica (CVSS) o de la probabilidad estimada de explotación (EPSS).

Cuando una vulnerabilidad es referenciada en fuentes de inteligencia de amenazas o en análisis técnicos, la ventana de exposición al riesgo tiende a reducirse, ya que puede anticipar escenarios de explotación antes de que estos se reflejen en métricas tradicionales.

En este contexto, este tipo de vulnerabilidades requiere una evaluación oportuna, especialmente cuando existen contramedidas disponibles, dado que su relevancia puede evolucionar rápidamente en función de la actividad adversaria observada.

LA GESTIÓN EFECTIVA DE VULNERABILIDADES REQUIERE INTEGRACIÓN DE MÚLTIPLES FACTORES.

Ninguna métrica individual es suficiente para capturar el riesgo real. El análisis muestra que ningún CVE aparece simultáneamente en los Top 10 de EPSS, CTI y Priority Score. Mientras 8 vulnerabilidades coinciden entre EPSS y Priority Score, el conjunto identificado por CTI presenta una composición distinta, incorporando amenazas emergentes que aún no se reflejan en patrones de explotación más amplios.

Este comportamiento evidencia que la priorización basada en una sola dimensión puede generar puntos ciegos. El modelo de riesgo combinado permite integrar severidad técnica, probabilidad de explotación, inteligencia de amenazas y disponibilidad de contramedidas en una única perspectiva operativa.

En este contexto, un enfoque multidimensional contribuye a una asignación más precisa de recursos de remediación, especialmente en organizaciones con entornos complejos o alta exposición al riesgo.

EL 80% DE BRECHAS COMIENZAN POR UN CLICK:
ENTRENAMIENTO CONTINUO = TU PRIMERA LÍNEA DE DEFENSA

Evalúa tus riesgos antes que el atacante

CRONUP
CIBERSEGURIDAD

Vulnerabilidades en Fabricantes de Ciberseguridad

CronUp Ciberseguridad

Alerta Temprana de Riesgos Cibernéticos | Cyber Threat Intelligence

Conversa con nosotros y conoce la postura de tu empresa frente a las ciberamenazas:
contacto@cronup.com

CronUp Ciberseguridad es una empresa chilena especializada en ciberinteligencia, seguridad ofensiva y gestión del riesgo cibernético. A través de inteligencia de amenazas, análisis técnico y simulación controlada de ataques, ayudamos a las organizaciones a identificar, priorizar y reducir riesgos reales que puedan afectar su continuidad operacional, reputación y confianza de clientes.

Nuestras capacidades integran Threat Intelligence, protección digital de marca, análisis continuo de superficie de ataque, ejercicios de Red Team y capacidades de respuesta a incidentes (DFIR), permitiendo identificar exposición real, validar escenarios de ataque y fortalecer la resiliencia de las organizaciones frente a adversarios avanzados.
Este enfoque se articula mediante ATRc® (Alerta Temprana de Riesgos Cibernéticos), una metodología que combina inteligencia contextual, monitoreo continuo y validación ofensiva para anticipar amenazas y priorizar riesgos antes de que el adversario actúe.

Conversemos

contacto@cronup.com
www.cronup.com

© 2026 CronUp Ciberseguridad. Todos los derechos reservados. Este contenido está protegido por la Ley Nº 17.336.
Se permite su uso informativo citando la fuente y enlazando el artículo original. Su reproducción o uso sin atribución constituye infracción.

CRONUP
CIBERSEGURIDAD