EN CIFRAS:

El panorama moderno de vulnerabilidades

ninjaOne

Los CVE han aumentado un

275 % desde 2024

El informe DBIR de Verizon de 2025 registró un impresionante aumento del 180 % en la explotación exitosa de vulnerabilidades en 2024. Posteriormente, su informe publicado el 23 de abril de 2025 mostró otro aumento del 34 %.

Esto se traduce en **132 nuevos CVE** cada día, con el **33 % de los CVE** clasificados como altos o críticos

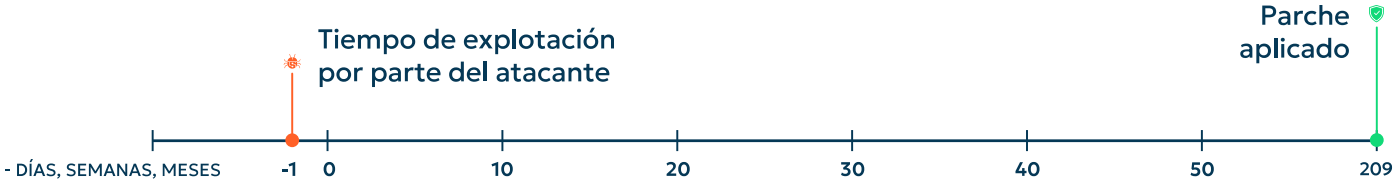
Verizon informa:

Solo el **54 %** de las vulnerabilidades se corrigen en un plazo de **32 días**.

Lo más preocupante es que el tiempo medio de aplicación de parches es de **209 días**.

El software empresarial representó el **44 %** de todos los días cero en 2024 y el **48 %** en 2025.

Entre el 50 % y el 61 % de las nuevas vulnerabilidades se explotan en las primeras 48 horas tras su divulgación



El momento cero es cuando un parche está disponible. Los atacantes suelen explotar vulnerabilidades antes de que existan parches, mientras que las organizaciones tardan hasta **209 días** en desplegarlos.

Vectores de ataque

La explotación de vulnerabilidades se ha vuelto tan común como el phishing o los ataques de contraseñas. De hecho, Verizon señala:

la explotación de vulnerabilidades se multiplicó casi

8 veces del **3 %** al **22 %**.

Una mejor forma

NinjaOne Vulnerability Management, con evaluación en tiempo real, elimina por completo los ciclos de escaneo, proporcionando información de vulnerabilidades siempre actualizada sin interrumpir los endpoints. Combinado con NinjaOne Autonomous Patch Management, crea un sistema de remediación de ciclo cerrado. La información de vulnerabilidades fluye directamente hacia flujos de trabajo de parches impulsados por IA. Esto acelera la remediación y reduce el riesgo operativo.

Más información en
ninjaone.com/vulnerability-management/