ivanti

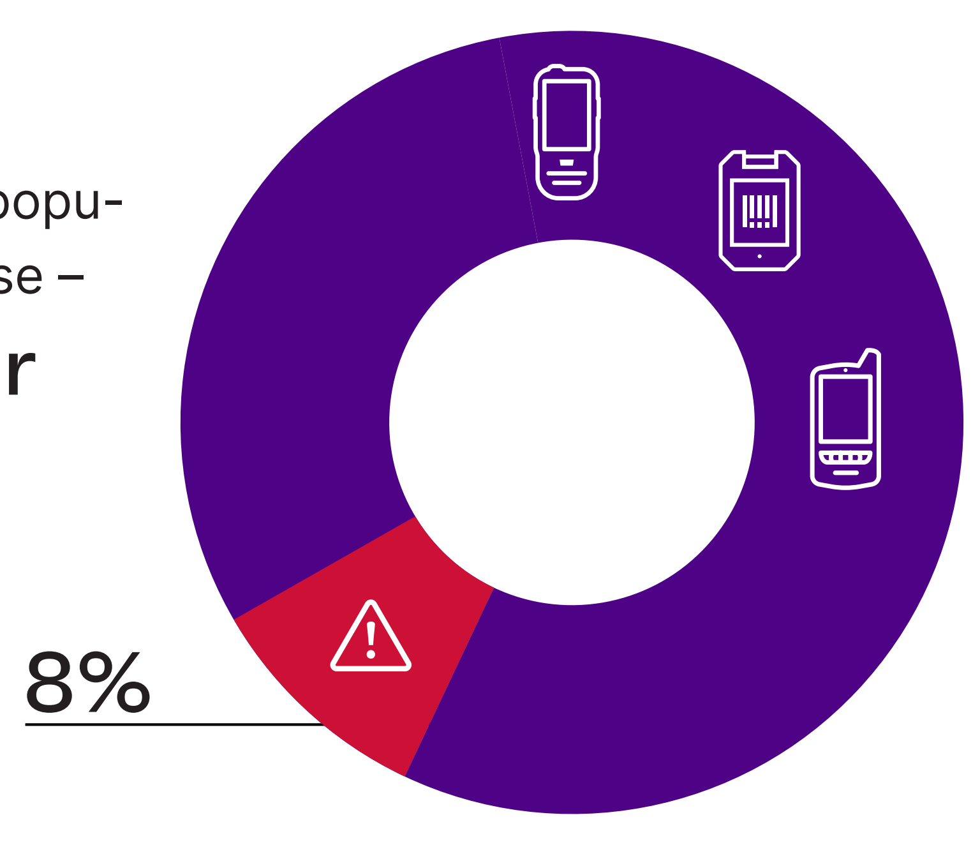
Cinco cosas a mejorar sobre la gestion de vulnerabilidades

1 Sus puntos ciegos de vulnerabilidad

No se puede proteger ni parchear lo que no se ve o no se sabe buscar..

1 de cada 3 empleados de las empresas Fortune 1000 utiliza aplicaciones SaaS basadas en la nube no autorizadas.[i]

Algunos de los escáneres más populares - Nessus, Qualys y Nexpose – **siguen pasando por alto casi el 8%** de las vulnerabilidades de ransomware conocidas.[ii]



2 Falta de ancho de banda del equipo

Imagine intentar parchear cada vulnerabilidad o riesgo existente, o simplemente revisar de forma manual las vulnerabilidades más relevantes para su empresa y entorno.

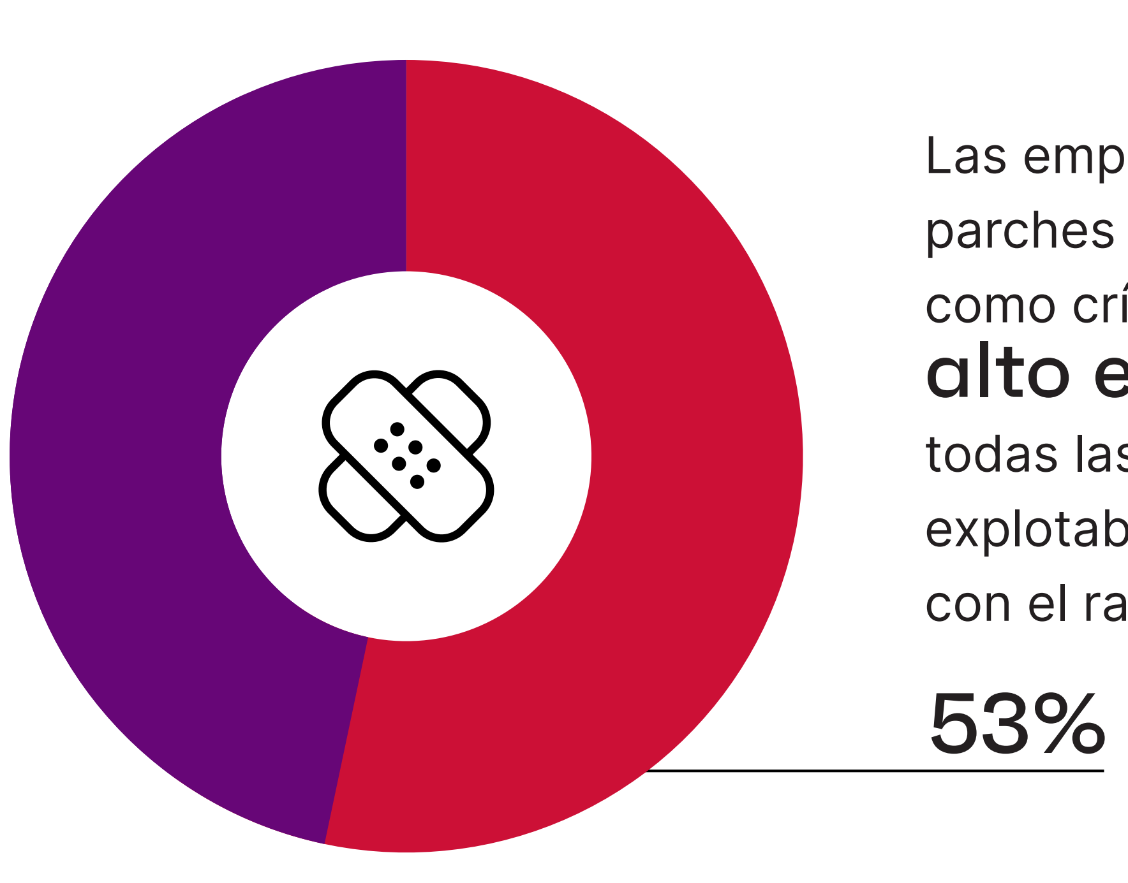
⚠
236,000+
Número total de vulnerabilidades y exposiciones críticas (CVE)

⚠ ⚠
29,000+
CVE armadas

⚠ ⚠ ⚠
9,600+
Más de 9.600 CVE con capacidad de ejecución remota de código (RCE) y/o escalada de privilegios (PE)

3 Exposición a CVE menos "críticas" y más antiguas

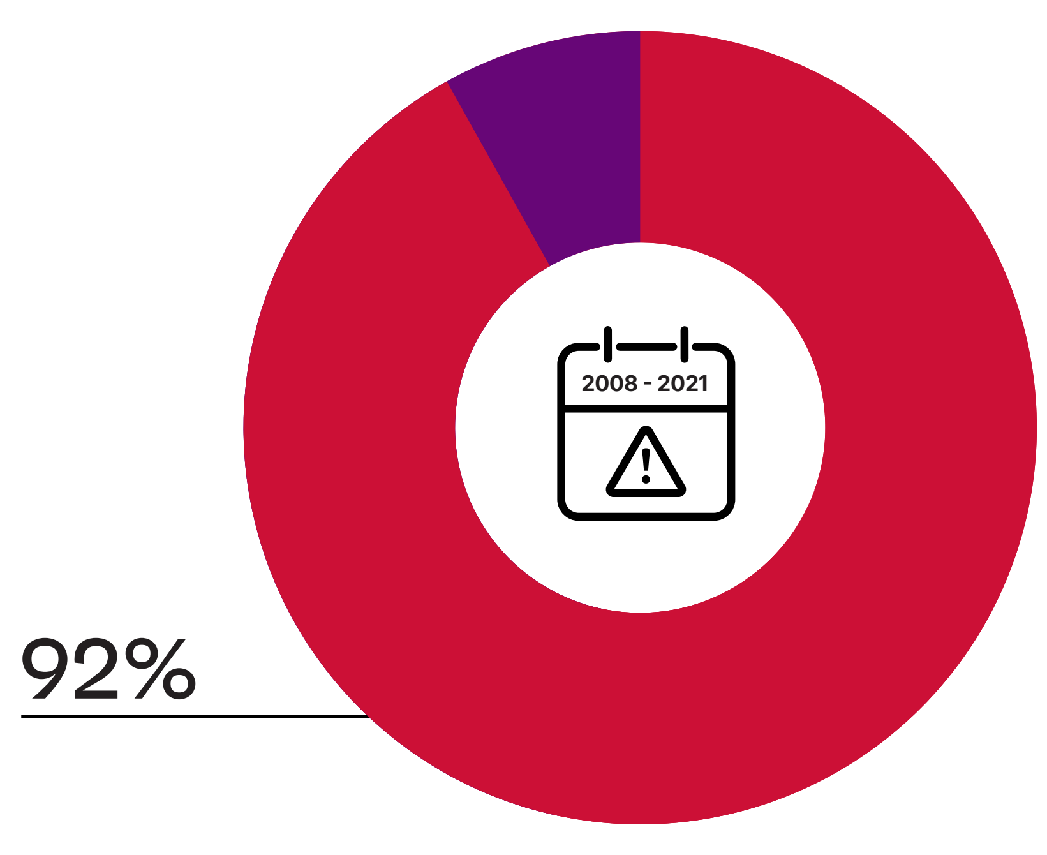
No todas las vulnerabilidades plantean el mismo riesgo y no se puede saber cuál es relevante para su empresa con solo mirar la antigüedad o la criticidad.



Las empresas que solo apliquen parches a los CVE clasificados como críticos pasarán por **alto el 53 % de** todas las vulnerabilidades explotables relacionadas con el ransomware.[iii]

53%

El 92 % de todas las vulnerabilidades que son tendencia activa tienen más de un año de antigüedad, ¡y algunas se publicaron por primera vez en 2008!



4 Pocos recursos para el programa y aceptación interna

RBVM básica

Priorización mediante puntuaciones CVSS y puntuaciones de escáner

Puntos débiles
Depende en gran medida de la calidad de los datos y de la frecuencia de actualización de los escáneres.

Pasar por alto vulnerabilidades de menor puntuación relevantes para los riesgos específicos de la empresas u organización.

Puntos fuertes
La gestión de vulnerabilidades existe

RBVM intermedia

Priorización a través de la probabilidad de explotación de los CVE del año pasado

Puntos débiles
Necesita un ajuste y verificación manuales constantes

Pasa por alto vulnerabilidades antiguas aún relevantes (+1 año)

Puntos fuertes
Prioriza la corrección más allá de la puntuación CVS

Enfatiza los nuevos parches de vulnerabilidad

RBVM avanzada

Priorización mediante inteligencia sobre amenazas de múltiples fuentes y riesgos organizativos contextualizados

Puntos débiles
Requiere un conjunto completo de herramientas para cubrir múltiples fuentes de datos

Puntos fuertes
Contiene todas las fuentes posibles de datos sobre vulnerabilidad

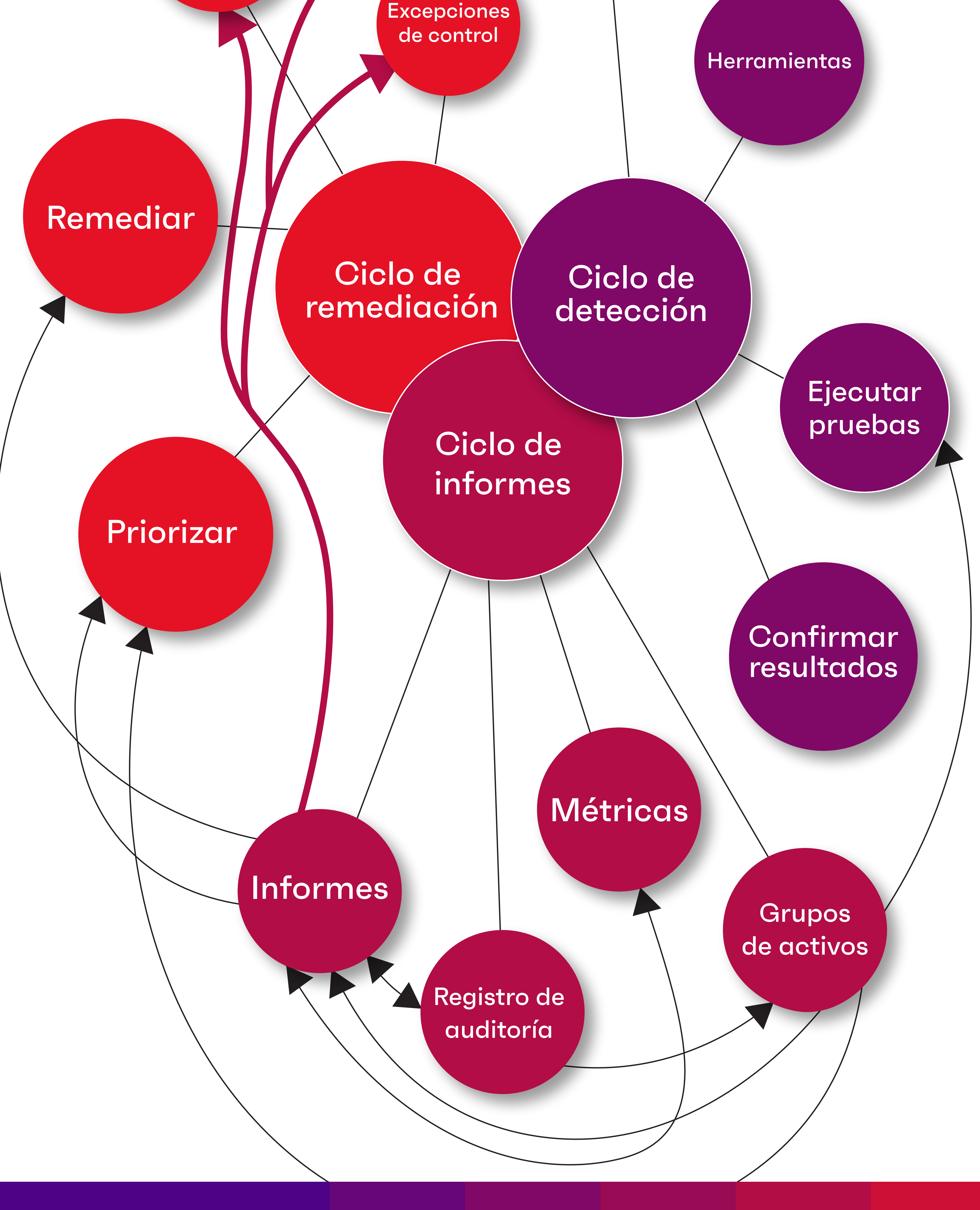
Prioriza en función de los riesgos específicos de cada empresa

Pivota rápidamente para incorporar nuevos contextos y afinar la priorización

5 Informes

Los programas eficaces de gestión de vulnerabilidades pueden crear rápidamente una compleja red de detección, corrección e informes interdepartamentales necesarios para su correcta ejecución.

Sin algún tipo de herramienta de automatización para recopilar, priorizar y mostrar la información y las actividades relacionadas con las vulnerabilidades, su programa de ciberseguridad podría perder su eficacia a causa de los requisitos de presentación de informes antes de empezar.[v]



No tiene por qué ser así. Lea el informe 2022 Spotlight Ransomware Report para conocer las últimas tendencias en vulnerabilidades.

Descargar el informe

---

i “Why shadow IT is the next looming cybersecurity threat” (The Next Web)
ii Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
iii Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
iv Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
v OWASP Vulnerability Management Guide (OVMG) - June 1, 2020

Copyright 2023, Ivanti. All rights reserved. IVI-2706 08/23 PL/FG