

SEGURIDAD

Seguridad en Oktavia y Argos

Vulnerabilidades

Hardening

Argos

11 de octubre de 2026 · 10 minutos de lectura

La seguridad de una red no se resuelve con una lista de CVE ni con un puntaje. Se resuelve sabiendo qué equipo está expuesto y por qué, qué se cambia para corregirlo, y con la certeza de que la herramienta que lo encontró no se convirtió en un riesgo nuevo. Este artículo explica cómo lo hacen Oktavia y su asistente, Argos.

Cientos de CVE y ninguna decisión

Cualquier escáner le entrega cientos de vulnerabilidades por cada versión de sistema operativo. Ordenadas por puntaje CVSS, la lista dice que todo es urgente, y cuando todo es urgente nada lo es. Lo que el responsable de red necesita saber es otra cosa: cuáles se están explotando hoy, en qué equipos, a qué versión hay que subir y si esa versión ya es parte del estándar.

Lo mismo pasa con la configuración. Un hallazgo de «SSH expuesto» sin la línea que lo sustenta, ni el cambio que lo corrige, es una conversación, no una tarea.

Un hallazgo de seguridad sirve cuando trae su evidencia, su prioridad real y su corrección.

Vulnerabilidades por versión de software

Oktavia toma la plataforma y la versión que el descubrimiento obtuvo de cada equipo, y las cruza con tres catálogos públicos:

- **NVD (CVE API 2.0)**, la base del NIST: los CVE que afectan esa versión, con su severidad y las versiones que los corrigen.
- **CISA KEV**: el catálogo de vulnerabilidades que se están explotando activamente.
- **FIRST EPSS**: la probabilidad estimada de que una vulnerabilidad se explote en los próximos treinta días.

El orden de prioridad es explícito: primero lo que está en KEV, luego la severidad, la probabilidad de explotación y el puntaje. De ahí sale una calificación por equipo, por sitio y por organización, y la explicación de cada una: cuántas vulnerabilidades explotadas activamente, cuántas críticas, cuál es la probabilidad más alta.

Para cada equipo, Oktavia sugiere la versión mínima segura dentro del mismo tren de software —no le propone saltar de IOS a IOS XE para corregir un CVE— y dice cuántas de las vulnerabilidades graves corrige. Esa versión mínima se puede llevar, con una acción explícita, a la norma de software por modelo, y desde entonces el cumplimiento la evalúa en cada auditoría como cualquier otra regla.

- **Imágenes de laboratorio y nodos virtuales.** Se marcan como aproximados: su versión no permite un cruce exacto y no representan exposición real, así que se listan pero no cuentan en la calificación.
- **Cuándo corre.** Con cada auditoría completa y a diario con el programador de tareas. Un reemplazo de equipo cambia la versión, y el análisis se actualiza en la auditoría siguiente.
- **Qué sale de su red.** A los catálogos sólo se consulta producto y versión, o identificadores de CVE. Nada que identifique a su organización ni a sus equipos.
- **Reporte imprimible.** Un reporte de CVE por red o por sitio, listo para imprimir a PDF, con los equipos ordenados por exposición. El envío semanal automático estará disponible próximamente.

Postura de seguridad con evidencia

La postura de seguridad se calcula sobre la configuración recolectada, de forma determinista, por equipo y por sitio, en cuatro dominios:

DOMINIO	QUÉ REvisa
Perímetro	Qué entra y sale sin filtro: políticas demasiado permisivas, listas de acceso abiertas, servicios expuestos a internet.
Plano de gestión	SSH y HTTPS alcanzables desde la WAN, telnet o HTTP habilitados, líneas virtuales sin lista de acceso, SNMP con valores por omisión.
Identidades	Cuentas de administración sin origen restringido o sin segundo factor, cuentas privilegiadas con contraseña sin cifrar.
Segmentación	Zonas sin protección, políticas sin registro, puertos de acceso sin endurecer, objetos huérfanos.

Cada hallazgo trae la línea o el objeto que lo sustenta y la recomendación concreta. En FortiGate y Junos se agrega el análisis de políticas de firewall: reglas permisivas y qué queda expuesto hacia internet. La cobertura es multivendor: Cisco IOS e IOS XE, FortiGate, Junos, FortiSwitch y Cisco SD-WAN, cada uno leído con su propio modelo, no con una traducción común.

Hardening por rol, como intención

Detectar una debilidad es la mitad del trabajo. La otra mitad es que no vuelva. Por eso en Oktavia el hardening no es un documento aparte: es un estándar por rol que vive en la misma intención que el resto de la configuración, y que un equipo nuevo hereda al darse de alta.

- **Línea base.** Lo mínimo por plataforma: acceso de gestión restringido, servidores de tiempo y de registro, SNMP sin valores por omisión, tiempos de sesión.

- **Valores débiles.** Lo que el estándar declara y contradice la línea base, como telnet en las líneas virtuales, con su corrección.
- **Excepciones.** Los equipos que se apartan del estándar de su rol, visibles para decidir si se justifican o se limpian.
- **Líneas prohibidas en IOS.** Configuración que no debe existir en el equipo, aunque nadie la haya declarado. Es la única configuración de más que el cumplimiento señala.

Guardar el estándar no toca la red. Llevarlo a los equipos pasa por el mismo ciclo cerrado que cualquier cambio: gemelo digital, aprobación, aplicación y verificación. Oktavia nunca propone secretos: comunidades, usuarios, contraseñas y llaves los define una persona.

Argos: salud de la red y diagnóstico sin ticket

Argos, el asistente de Oktavia, junta en un solo análisis la salud de un sitio, de un equipo o de toda la red, en cinco dimensiones: estado de la red, recursos, hardware y software (incluidos CVE y KEV), seguridad, y configuración contra la intención.

Lo que lo hace útil es la correlación. Cada falla de estado se cruza con la configuración y se clasifica en una de tres causas:

- **La configuración del propio equipo** se desvió de la intención en el servicio que falla.
- **La configuración de un vecino** explica la falla: el otro extremo del túnel o del vecino BGP.
- **Operación:** la configuración está bien y la causa es el enlace, el proveedor o el equipo remoto.

Con eso Argos arma un diagnóstico que no necesita un ticket para empezar: agrupa las fallas en incidentes con una causa y varios síntomas, y los ordena por impacto —sitio aislado, usuarios afectados, redundancia degradada, sin impacto en usuarios—. Cada incidente propone lo que sigue: cerrar el ciclo donde está la causa, probar conectividad o diagnosticar el equipo.

Todo esto es determinista. La inteligencia artificial entra sólo cuando la persona la pide, y sólo sobre un resumen acotado del equipo o del sitio. Nunca recibe configuraciones completas ni secretos.

Que la herramienta no sea el riesgo

Una plataforma que entra a todos los equipos de la red es, por definición, un objetivo atractivo. Las decisiones que la protegen:

- **Credenciales en una bóveda,** con precedencia por equipo, sitio u organización. En la red de pruebas, el día 0 lleva sólo el hash de la contraseña.
- **Aislamiento por organización.** Cada organización ve sólo su inventario, sus resultados y sus análisis.

- **Verificación de la identidad SSH.** Las llaves conocidas se guardan por organización, y una llave que cambió se rechaza hasta que el operador la confirma.
- **Exportaciones sin secretos.** Las exportaciones a CSV omiten las líneas que llevan contraseñas, comunidades o llaves, y los paquetes de baja de un equipo se archivan sin secretos.
- **Nada sensible al modelo de lenguaje.** Sólo resúmenes acotados, y sólo a petición.

✓ Los principios detrás

- **Cambio mínimo.** Se corrige lo que falta o lo que está prohibido, no se reescribe la configuración completa.
- **Aprobación humana.** Ningún cambio llega a la red sin que una persona revise el diferencial exacto.
- **Trazabilidad.** Cada cambio queda como un ticket del gemelo digital, con lo propuesto, lo aprobado, lo aplicado y la verificación.
- **Ningún secreto a la IA.** Lo que el modelo no recibe, no lo puede filtrar.

Seguridad con evidencia, corrección por el mismo ciclo que todo lo demás, y una herramienta que no agrega superficie de ataque.

¿Sabe hoy qué equipos corren una versión con vulnerabilidades explotadas activamente?

Si la respuesta tarda más de un minuto, vale la pena verlo en su propia red. Para cotizar sólo necesitamos saber aproximadamente cuántos equipos administra.

Acerca de Oktanet

Oktanet es una empresa mexicana de automatización de redes con enfoque en operaciones controladas, trazables y escalables para entornos empresariales en Latinoamérica.

[LinkedIn](#) · [YouTube](#)

© 2026 Oktanet · Oktavia · Artículo público, sin información confidencial de clientes.