# Ivanti Neurons for Risk-Based Vulnerability Management (RBVM)

**Convierta su estrategia de gestión de vulnerabilidades en un enfoque basado en riesgos con Ivanti Neurons for RBVM. Gracias a esta solución SaaS, podrá priorizar de forma eficiente y eficaz las vulnerabilidades y puntos débiles que plantean un mayor riesgo de corrección para una mejor protección frente a las filtraciones de datos, el secuestro informático y otras ciberamenazas.**

## Es hora de adoptar un nuevo enfoque para la gestión de la vulnerabilidad

Se conocen más de 270 000 vulnerabilidades.[1] Afortunadamente, las empresas no necesitan corregir todas las vulnerabilidades y puntos débiles que aparecen en sus entornos informáticos. Sin embargo, para las empresas que utilizan métodos tradicionales de gestión de vulnerabilidades, la identificación de aquellas vulnerabilidades o puntos débiles que suponen un riesgo importante es un proceso lento y susceptible de errores.

Antes de que estas empresas puedan siquiera priorizar las vulnerabilidades y puntos débiles para su corrección, primero deben recopilar una serie de datos dispares—desde los resultados de los escáneres hasta la información sobre amenazas—, normalizarlos y prepararlos para su uso. Cuando se realizan manualmente, estos procedimientos pueden tardar días, semanas o meses en completarse, y con llevan un error humano.

El proceso de priorización no es mejor. Considere las vulnerabilidades del programa de secuestro informático. El 74% no están consideradas críticas según CVSS v3 y 156 no aparecen en el catálogo de vulnerabilidades explotadas conocidas (KEV) de CISA. Además, tres escáneres muy populares todavía no han añadido complementos ni firmas de detección para un total de 20 vulnerabilidades de *ransomware*.[2]


Además de esto, los responsables de la seguridad y las TI señalan la falta de cooperación entre sus equipos como el mayor desafío al que se enfrentan en la defensa contra los ciberataques.[3] Esta discrepancia entre las partes interesadas en la gestión de vulnerabilidades puede ralentizar la corrección y dejar a la empresa expuesta a los ataques.

## Capacidades principales

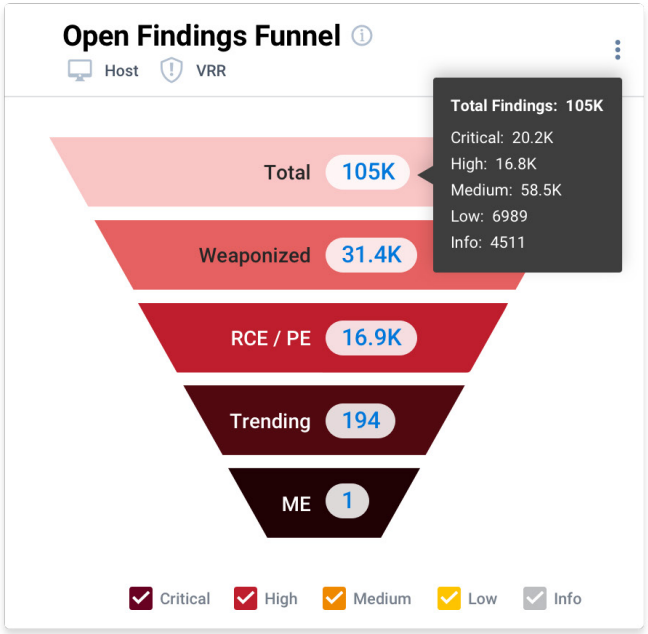
### Priorizar acciones inmediatas basadas en el riesgo de las amenazas

Pase de la detección de vulnerabilidades y debilidades a la corrección en cuestión de minutos (y no de meses) con un punto de vista contextualizado y basado en el riesgo de su enfoque de ciberseguridad. Ivanti Neurons for RBVM mide el riesgo y prioriza las actividades de corrección a través de un proceso que implica la correlación continua de la infraestructura de una organización con:

- Datos sobre vulnerabilidad interna y externa.
- Inteligencia de amenazas.
- Manual de pruebas y resultados basados en la investigación.
- Criticidad de los activos empresariales.

Y lo mejor de todo: se llega a un plan de ataque totalmente informado sin apenas esfuerzo manual.

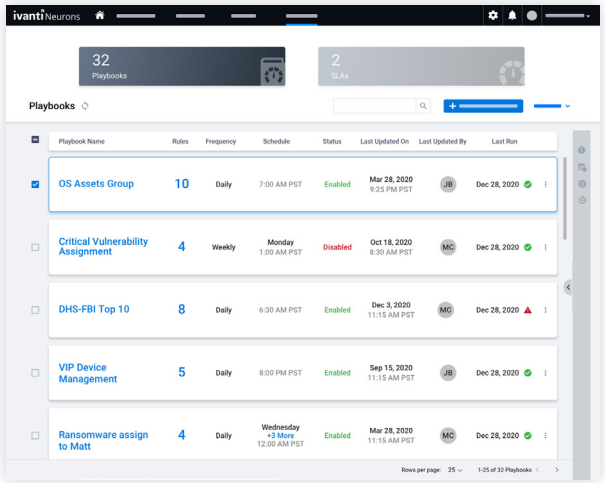
Además, a diferencia del CVSS, la calificación de riesgo de vulnerabilidad (VRR) de Ivanti permite a las empresas medir con precisión el impacto y determinar la probabilidad de que se explote una vulnerabilidad. Ivanti Neurons for RBVM identifica de forma específica la ejecución remota de código, la escalada de privilegios, el programa de secuestro informático (*ransomware*) y las vulnerabilidades activas y de tendencia. Esta información ayuda a las empresas a centrarse en las vulnerabilidades que les suponen un mayor riesgo.




## Centrarse en la corrección, no en la administración

Aumente su estrategia de ciberseguridad de ciberseguridad sin perder tiempo, invertir esfuerzo y cometer los errores que suelen asociarse a este proceso gracias a una serie de automatizaciones y otras funciones que mejoran
la eficacia:

- Cree playbooks para automatizar tareas comunes o repetitivas de las que tradicionalmente se encargan los analistas de seguridad.
- Establezca fechas de vencimiento de cierre de vulnerabilidades automáticamente si lo desea con automatizaciones de acuerdos de nivel de servicio.
- Reciba alertas casi en tiempo real fuera del producto que enlazan con una página del producto que contiene información relacionada con el evento reportado.
- Filtre fácilmente los anfitriones y los hallazgos de anfitriones por criterios de tendencias que revelan su exposición a las principales vulnerabilidades críticas—como secuestro informático y CVE de tendencia—, mediante vistas del sistema impulsadas por el equipo de seguridad Ivanti.
- Entregue las vulnerabilidades priorizadas directamente a Ivanti Neurons for Patch Management para su corrección: se acabó el envío de CSV de ID de CVE por correo electrónico y chat.

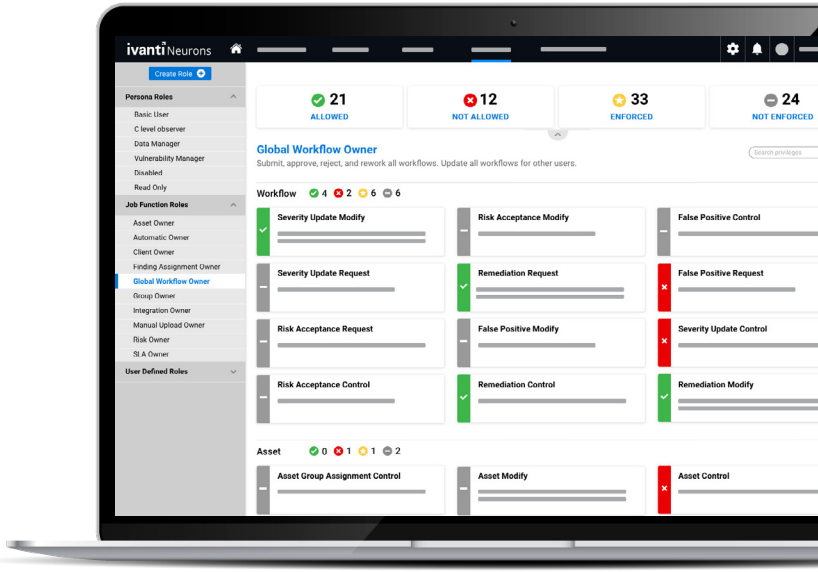



## Permita una mejor colaboración entre los responsables de seguridad

Cultive la comunicación y la cooperación entre las partes interesadas en la seguridad de toda la empresa, proporcionándoles información actualizada y pertinente para sus funciones. Ivanti Neurons for RBVM aplica un control de acceso basado en funciones (RBAC) para que todo el personal pueda acceder al producto de forma segura.

Cuando están dentro del producto, los usuarios tienen acceso a cuadros de mando diseñados para el personal, desde el SOC hasta la C-suite. Pueden modificar estos cuadros de mando para adaptarlos a casos de uso más específicos, o incluso aprovechar los *widgets* de usuario para crear cuadros de mando personalizados que satisfagan las necesidades exactas de las distintas funciones y equipos.

Además, el producto cuantifica el perfil de riesgo de una empresa en forma de puntuación Ivanti RS3. Esta puntuación garantiza que todas las partes interesadas en la seguridad estén de acuerdo con el nivel de seguridad general de la empresa. Las integraciones bidireccionales con sistemas de incidencias como Ivanti Neurons for ITSM mejoran la coordinación entre quienes trabajan para mejorar ese nivel de seguridad.



## Características y funciones

| Característica | Función |
|---|---|
| **Diversas fuentes de datos** | Alcance una amplia visión del ciberriesgo con una plataforma que recopila datos de escáneres de red, puntos finales, bases de datos y dispositivos IoT, hallazgos de vulnerabilidad de más de 100 fuentes independientes, hallazgos manuales de equipos de investigación y pruebas de penetración, y fuentes de datos personalizadas. |
| **Motor de amenazas** | Obtenga información inigualable sobre las vulnerabilidades, como las relacionadas con el *ransomware*, a través de la inteligencia sobre amenazas generada por humanos e impulsada por la IA, procedente de Ivanti Neurons for Vulnerability Knowledge Base. |
| **Vulnerability Risk Rating (VRR)** | Determine rápidamente el riesgo que supone una vulnerabilidad con puntuaciones numéricas de riesgo que tienen en cuenta los atributos intrínsecos de la vulnerabilidad más su contexto de amenaza en el mundo real. |
| **Ivanti RS³** | Obtenga una visión cuantificada del perfil de riesgo de su empresa mediante una metodología de puntuación propia que tiene en cuenta el VRR, la criticidad empresarial de los activos, la información sobre amenazas y la accesibilidad externa. |
| **Automatización** | Sustituya una serie de tareas manuales por otras automatizadas para que los empleados puedan centrarse en tareas de reparación e iniciativas estratégicas en lugar de en la administración. |
| **Alertas y notificaciones** | Infórmese al instante de los acontecimientos pertinentes mediante alertas casi en tiempo real enviadas desde un motor de notificaciones. Del mismo modo, dirija a otros usuarios a información importante dentro del producto utilizando enlaces profundos. |
| **Organización de datos personalizable** | aplicaciones de usuario que permiten la creación de cuadros de mando personalizados, además de la posibilidad de pivotar datos en vistas de listas. |
| **Paneles de control** | Descubra rápidamente cómo se manifiestan en su entorno las principales vulnerabilidades críticas, como Log4j y las asociadas a las versiones del *Patch Tuesday*, utilizando vistas basadas en amenazas. También puede crear y compartir sus propios filtros personalizados. |
| **Puntos de vista basados en las amenazas** | Descubra rápidamente cómo se manifiestan amenazas específicas como BlueKeep, WannaCry o las 10 principales vulnerabilidades explotadas por el FBI/DHS/CISA en el entorno de su organización utilizando filtros basados en amenazas. También puedes crear y compartir tus propios filtros personalizados. |
| **Integración de Neurons** | Combine Ivanti Neurons for RBVM con Ivanti Neurons for ASPM para ampliar la gestión de vulnerabilidades basada en riesgos a una mayor área de su superficie de ataque. Aproveche las integraciones listas para usar con Ivanti Neurons for ITSM e Ivanti Neurons for Patch Management para potenciar a los profesionales de la gestión de vulnerabilidades de toda la organización a realizar sus tareas con mayor eficiencia y eficacia. |

## Sobre Ivanti

Ivanti mejora y asegura el «Everywhere Work» para que las personas y las empresas puedan prosperar. Logramos que la tecnología trabaje para las personas, no al revés. Los empleados actuales utilizan una amplia gama de dispositivos corporativos y personales para acceder a aplicaciones y datos de TI a través de múltiples redes y seguir siendo productivos dondequiera y comoquiera que trabajen. Ivanti es una de las únicas empresas tecnológicas que encuentra, gestiona y protege cada activo de TI y punto final de una empresa. Más de 40 000 clientes, incluidos 88 de las 100 empresas de Fortune, confían en Ivanti para que les ofrezca una excelente experiencia digital a sus empleados y mejore la productividad y eficiencia de los equipos de TI y seguridad. En Ivanti, nos esforzamos por crear un entorno en el que se escuchen, respeten y valoren todas las perspectivas, y estamos comprometidos con un futuro más sostenible para nuestros clientes, socios, empleados y el planeta.

Para más información, entre en www.ivanti.es y siga a @GoIvanti.



ivanti neurons

ivanti.es/neurons
+34 91 049 66 76
contact@ivanti.es

1. Datos extraídos de Ivanti Neurons for Vulnerability Knowledge Base el 29 de junio de 2023
2. Cyber Security Works, Cyware, Ivanti, Securin, «2023 Spotlight Report: Ransomware Through the Lens of Threat and Vulnerability Management», 16 de febrero de 2023. https://www.securin.io/ransomware/
3. ExtraHop, "Cyber Confidence Index 2022", 1 de marzo de 2022. https://www.extrahop.com/resources/papers/cyber-confidence-index-2022/