XCITIONE™ RMM

www.xcitione.com

Una sola consola para administrar, proteger y demostrar el estado de toda infraestructura tu TI

Inventario, parches, vulnerabilidades, AV/EDR, filtrado web, control de dispositivos, control remoto, automatización, mesa de ayuda y cumplimiento ISO 27001 / NIST CSF. Multi-tenant desde el primer día.

ISO 27001 **ISO 27001:2022** **ISO 37001:2016**

7 consolas abiertas para responder una pregunta

El inventario vive en una herramienta, los parches en otra, el antivirus en la del fabricante y los tickets en un tercero. El reporte del cliente se arma a mano el último viernes del mes, y cuando por fin está listo nadie sabe si los números son de hoy o de hace seis semanas.

Inventario

Parches

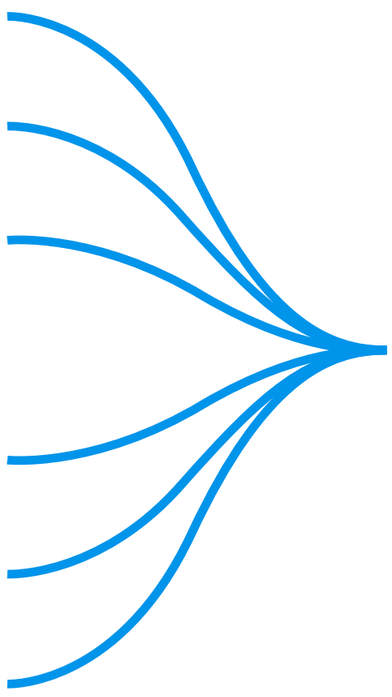
Antivirus

Backup

Filtrado Web

Inventario

Hoja de cálculo



Xcitione reemplaza ese recorrido por una sola pantalla

Un backend, un agente, un tablero. Todos los clientes a la vez o uno por uno, con el mismo lenguaje de datos en cada módulo y el mismo modelo de permisos.

27 vistas **1 agente** **multi-tenant**

El dato que ves es el dato que hay

Cada panel declara la antigüedad de su información y se autocalifica como dato al día, antiguo o muy antiguo. Si un equipo lleva 48 días sin reportar, la consola lo dice en la cara en lugar de pintarlo de verde. Toda métrica se muestra con su denominador: 1 de 7, 4 de 6, 7 de 7.

dato del día **dato antiguo** **dato de hace 48d** **sin datos**

Estados Diferenciados

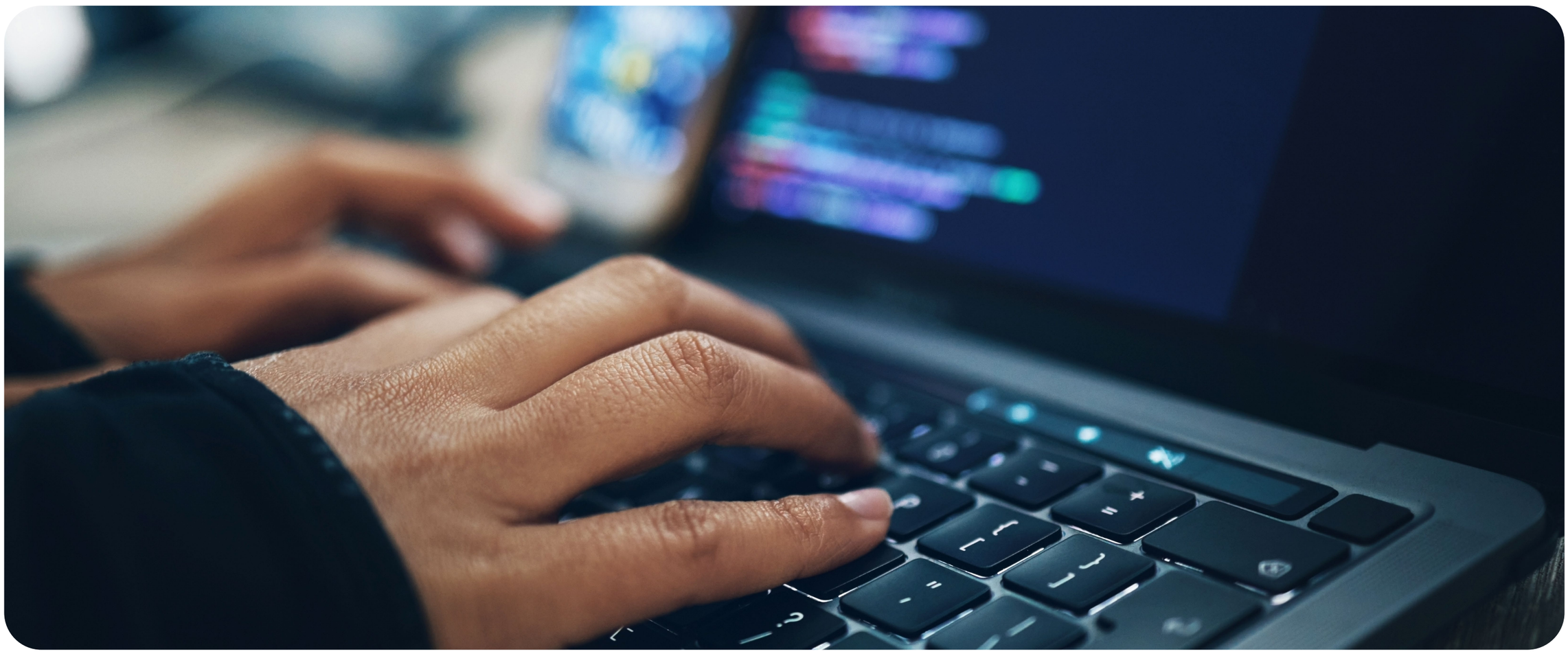
Desconectado, sin reportar, sin dato y no aplica son cuatro cosas distintas y se muestran distinto.

Limites Declarados

El módulo de respaldo advierte que la cobertura es estimada por inventario y que incronizar no es respaldar.

Nota Metodológica

Cada panel explica cómo se calcula y cada gráfico tiene su tabla equivalente en texto.



De 89 vulnerabilidades
a 4 acciones

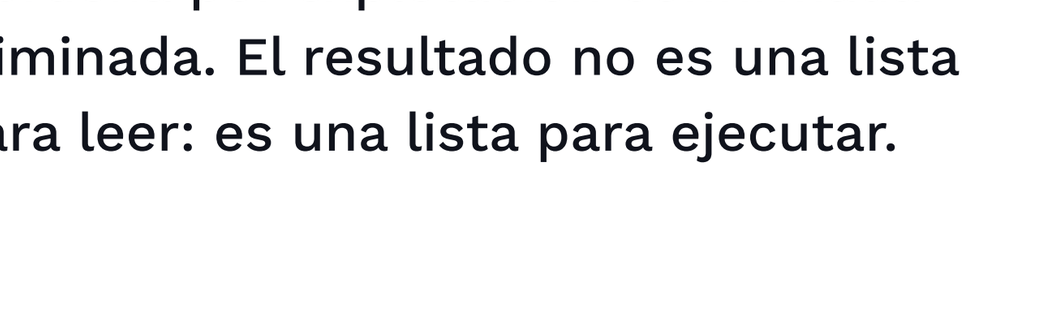
La consola cruza tu inventario contra una base curada de CVE, el catálogo CISA KEV y NVD en vivo. Después agrupa por producto normalizado sin arquitectura ni versión y ordena por explotación confirmada eliminada. El resultado no es una lista para leer: es una lista para ejecutar.

Hallazgos Crudos

2 KEV

89 CVE

59 CRÍTICAS Y ALTAS



ROJO = EXPLOTACIÓN CONFIRMADA

01 **Actualizar navegador Chrome** — 1 CLIC
2 equipos - Elimina 31 CVE - 2KEV

02 **Actualizar Node.js** — 1 CLIC
3 equipos - Elimina 18 CVE

03 **Actualizar WinRAR** — 1 CLIC
1 equipo - Elimina 9 CVE

04 **Aplicar KB pendientes de Windows** — 1 CLIC
4 equipos - Reinicio requerido

Cada acción trae el comando exacto de remediación, los equipos afectados y el botón para ejecutarla sobre todos ellos a la vez.

Clasificación CVSS v3.1

Crítica ≥ 9,0 · Alta 7,0–8,9 · Media 4,0–6,9 · Baja < 4,0. Marca KEV independiente del puntaje, porque lo que se explota hoy manda sobre lo que puntúa alto.

Parches de Windows

KB faltantes consolidados, instalaciones pendientes, reinicios en cola, reparto por días desde la última actualización y ranking de equipos más atrasados.

Aplicaciones de terceros

Catálogo monitoreado con versión objetivo, presencia real en la flota y equipos rezagados por aplicación, con despliegue desde la consola.

LA REUNIÓN MENSUAL CON EL CLIENTE YA ESTÁ HECHA

Matriz de riesgo por cliente sobre seis dominios —parches, KEV, backup, AV/EDR, check-in y fin de soporte—, índice de salud con tendencia de 30 días y 23 plantillas de reporte sobre 13 módulos. Ejecutivo, técnico, SOC, auditoría, ISO 27001 y NIST CSF. Programables por tenant y frecuencia, con entrega a Slack, Teams o Discord.

23 PLANTILLAS

13 MODULOS

18 PANELES

2 MARCOS

AUTOMATIZACIÓN QUE NINGÚN AUDITOR TE VA A DISCUTIR

La potencia de ejecutar scripts en toda la flota solo sirve si queda demostrada. Por eso la política de automatización es parte del producto, no una recomendación.

- **Scripts versionados y aprobados,** con alcance global o por tenant.
- **Entrega al agente verif icada por hash,** con timeout máximo.
- **Motivo obligatorio** en cada ejecución y aprobación previa para riesgo alto o crítico.
- **Lista de comandos bloqueados y** lenguajes permitidos declarados.
- **Ticket requerido** en acciones críticas.
- **Lista de comandos bloqueados y** lenguajes permitidos declarados.

MULTI-TENANT REAL, NO UNA VISTA FILTRADA.

Cada cliente se implementa como un tenant con dominio propio del tipo tenant.rmm.xcitione.com, en modo MSP o Enterprise, con su propio token de enrolamiento con vigencia, renovación y regeneración. Opera 40 clientes desde una sola pestaña o entra al de uno solo.

Aislamiento

Datos por tenant y clave de cifrado propia por cliente en la bóveda.

Enrolamiento

Token con caducidad, HTTPS /443 obligatorio y certificado distribuible por GPO.

Jerarquía

Tenant, grupos de endpoints con arrastrar y soltar, y equipo.

HIGIENE DEL AGENTE

Un agente no está “viejo”: está a cierta distancia de la última versión de su propia rama.

Rama Go 1.1.xy rama PowerShell heredada 0.6.x conviven y se miden por separado . La co nso la actualiza el agente y separa el check-in de la instantánea de inventario , con frescura independiente para cada uno.

RAMA ACTUAL

Go 1.1.55

HEREDADA - PS 0.6.35

27 vistas en 7 grupos.
Un solo agente.

La navegación de la consola es también el mapa del producto. Todo lo que sigue corre sobre el mismo backend, el mismo inventario y el mismo modelo de permisos.

INICIO

- Dashboard con 18 paneles reordenables.
- Vistas guardadas por operador.
- Copilot con contexto de flota.
- Exportación del informe a PDF

MONITOREO

- Monitoreo de actividad (UAM) con consentimiento.
- Uptime y certificados SSL.
- Alertas con umbral explícito.

OPERACIÓN

- Automatización, runbooks y tareas programadas.
- Mesa de ayuda con tickets.
- PSA: SLA, horas facturables y facturación

ANÁLISIS

- Reportes · 23 plantillas
- Reportes programados por tenant y frecuencia

ACTIVOS

- Endpoints.
- Inventario de hardware (21 secciones).
- Gestión de aplicaciones, vulnerabilidades y parches.
- Descubrimiento de red.
- Directorio.
- Geolocalización.

PROTECCIÓN

- AV / EDR.
- Seguridad y score de riesgo.
- Filtrado web (69 categorías).
- Control de dispositivos.
- Vault de credenciales.
- Postura de backup.

SISTEMA

- Integraciones: ChatO ps a Slack, Teams y Discord; Shodan; inventario cloud de AWS, Azure y Huawei Cloud; webhook a SIEM/SO C; conector de IA.
- Ajustes, roles, MFA por TO TP y capacidades gestionada activables.

TRANSVERSAL

- Control remoto con tres modos de consentimiento, transferencia de archivos e impresión remota.
- Búsqueda global de endpoint, alerta y ticket - tema claro y oscuro interfaz en español.

FILTRADO WEB

69

Categorías en 6 familias, 3 plantillas y simulador de política.

CONTROL DE DISPOSITIVOS

USB

Por clase, dispositivo Vo serie, con vigencia y lockdown de pánico.

VAULT

AES-256

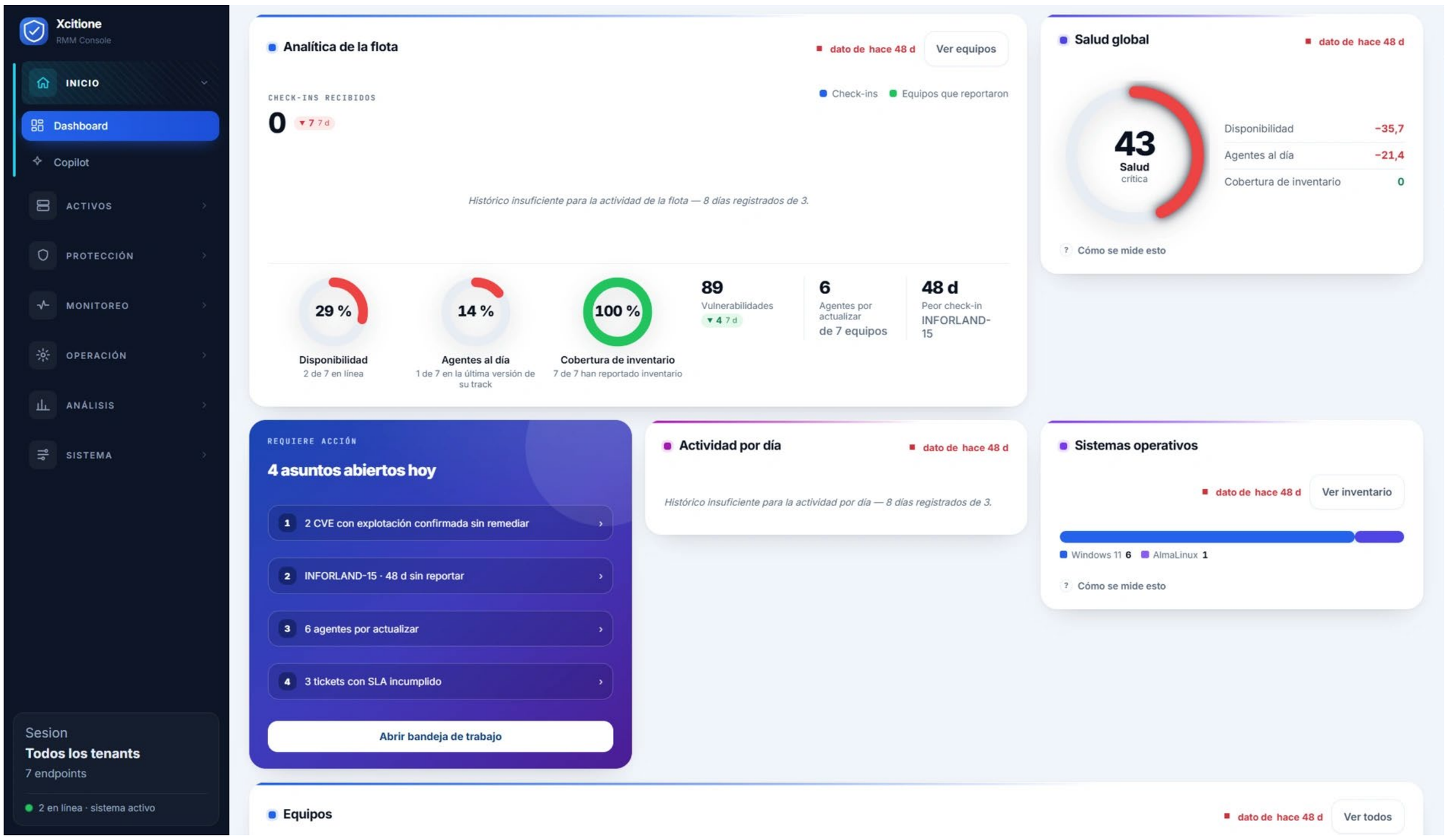
GCM con clave por cliente y auditoría de cada revelación.

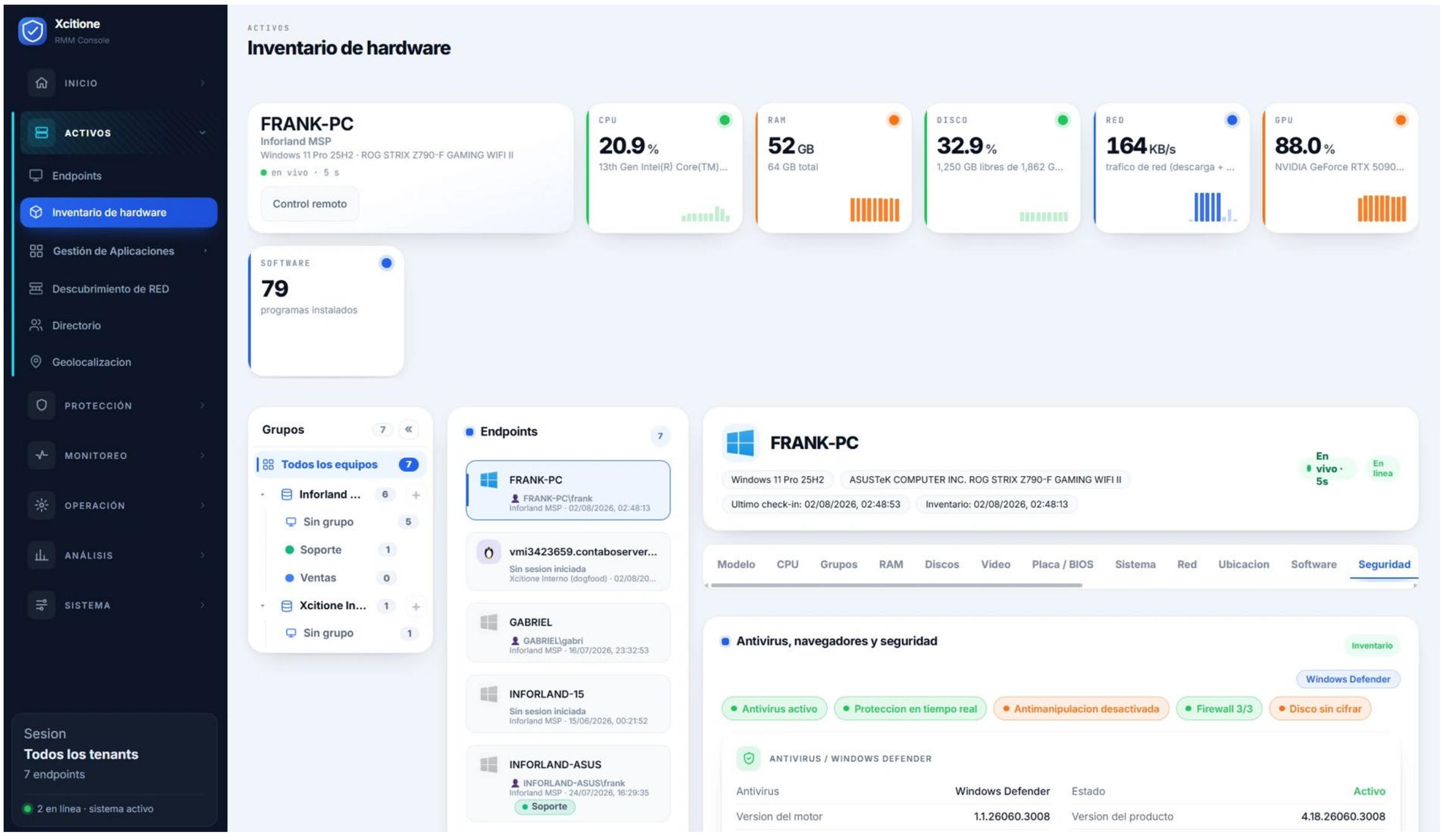
DESCUBRIMIENTO

5

Sondas: TCP, SNMP, ARP/MAC, DNS y SSDP/mDNS.

Diseñada para leerse rápido y sostener una auditoría





POTENCIA CON FRENO DE MANO

Una consola que puede ejecutar scripts, ver pantallas y abrir credenciales necesita controles del mismo tamaño. Están dentro del producto y dejan rastro.

BÓVEDA DE CREDENCIALES

- Cifrado AES-256-GCM con clave por cliente y rotación de claves.
- Revelar un secreto exige motivo y verificación de identidad.
- Versionado por ítem y retención de auditoría de 365 días.

MONITOREO DE ACTIVIDAD CONFORME

- Consentimiento por usuario, con jurisdicción y modo de aviso para Europa y Perú.
- Las capturas se descartan hasta que el usuario acepta, y la revocación detiene la captura.
- Redacción de datos sensibles, requisito de DPIA y auditoría de accesos al material.

CUMPLIMIENTO MEDIBLE

- Hallazgos mapeados a controles de ISO/IEC 27001 Anexo A y a NIST CSF, con score por marco.
- Índice de salud operativa: 50% disponibilidad, 25% agentes al día, 25% cobertura de inventario.
- Score de riesgo continuo de 0 a 100 por equipo, separado del índice de salud.

CONTROL REMOTO CON TESTIGO

- Tres modos de consentimiento, incluido preguntar y denegar por defecto.
- El usuario ve quién se conectó y puede cortar la sesión.
- Reporte de auditoría con operador, consentimiento, duración y motivo.

Coherentes con el principio del producto, estas son las fronteras actuales de la plataforma. Se declaran aquí antes de que las pregunte el área de TI del cliente.

Verificación de respaldo

Hoy la postura de backup se infiere del inventario de software y se muestra con nivel de confianza. El último respaldo exitoso y el RPO llegan con la telemetría de agente prevista.

Windows y Linux

Windows 10 y 11, incluido 25H2, y Linux verificado sobre AlmaLinux 10.x. Consultar disponibilidad paraotras plataformas.

Requieren recolección

Las tendencias de 7, 30 y 90 días necesitan días de datos: la consola avisa cuántos lleva registrados en lugar de dibujar una curva incompleta.

XCITIONE™ RMM

www.xcitione.com

Traiga sus veinte equipos más olvidados. La demo empieza por ahí.

Piloto sobre su propio parque: enrolamos un grupo de equipos, dejamos que reporten y a la semana revisamos juntos las acciones de mayor impacto, la matriz de riesgo y el reporte ejecutivo que saldría hacia su dirección. Sin datos de ejemplo.

ISO 27001 **ISO 27001:2022** **ISO 37001:2016**

ventas@xcitione.com

994444344