

SELF-HOSTED · MULTI-PLATAFORMA · MULTI-TENANT

# Monitoreo de endpoints, control de ejecución y análisis de *actividad*.

Especificación técnica y funcional de la plataforma: arquitectura, capacidades del agente, analítica de presencia, seguridad y modelo de datos. Un agente liviano y un dashboard web multi-tenant para administrar políticas, auditar comportamiento y aplicar bloqueo selectivo de aplicaciones.

---

PLATAFORMAS

macOS · Windows · Linux

VENDOR · VERSIÓN

VectoraIQ · v1.0 · julio 2026

CONTROL

DLP Light

PRESENCIA

Auditable

MODELO

Multi-tenant

DOCUMENTO

IUM-DS-2026 · ES

# Visibilidad, control y auditoría de la *flota corporativa* — desde un solo panel.

IUM Personnel Intelligence combina un agente liviano — production-ready en Windows y macOS — con un dashboard web multi-tenant que permite administrar políticas, auditar comportamiento y aplicar bloqueo selectivo de aplicaciones a nivel organizacional, por departamento o por equipo individual.

## CASOS DE USO PRINCIPALES

### Visibilidad de aplicaciones

Qué aplicaciones se ejecutan en la flota corporativa, en vivo e histórico.

### Bloqueo no autorizado · DLP Light

Granularidad global, por departamento o por equipo.

### Presencia real, medible y defendible

Actividad vs. ausencia con criterio auditable.

### Atribución multi-usuario

Equipos compartidos: RDP, Fast User Switching.

### Reportes de uso

Hardware y aplicaciones con histórico de 7 días.

### Trazabilidad geográfica + cumplimiento

Ubicación de equipos y audit trail completo.

## PRINCIPIO DE DISEÑO EN MÉTRICAS DE PERSONAL

IUM mide **señales verificables** y las expone con su significado explícito. No infiere presencia ni ausencia por heurísticas: la ausencia confirmada (AFK) se mide por input real de hardware, y las señales que podrían malinterpretarse — tiempo en una sola ventana, video en reproducción — se reportan como dimensiones separadas y rotuladas, nunca mezcladas dentro del número de ausencia. *La interpretación final queda en manos de una persona, con el contexto a la vista.*

# Detrás de cualquier red corporativa.

*Push-first.*

El agente reporta saliendo hacia el backend — sin puertos entrantes abiertos, compatible con cualquier red corporativa o NAT. Un canal de control persistente y saliente habilita comandos remotos como captura de pantalla y gestión de cifrado.

| COMPONENTE       | ROL                                                               |
|------------------|-------------------------------------------------------------------|
| Agente           | Captura datos del equipo, aplica políticas y reporta al backend   |
| Backend          | Concentra la API, la lógica de control y la persistencia de datos |
| Dashboard        | Interfaz administrativa: flota, políticas, reportes y auditoría   |
| Mapeo geográfico | Visualización de la ubicación de la flota                         |

MODO PUSH

**NAT-friendly**

El agente reporta saliendo. No requiere puertos entrantes abiertos.

MODO PULL

**Opcional**

El dashboard consulta al agente si hay alcance entrante. Métricas en vivo.

CANAL DE CONTROL

**Persistente**

Conexión saliente continua para comandos remotos seguros.

| MODO          | PRIVILEGIOS       | RESPONSABILIDAD                                                     |
|---------------|-------------------|---------------------------------------------------------------------|
| Modo servicio | Nivel sistema     | Bloqueo, inventario y canal de control. Independiente de la sesión. |
| Modo usuario  | Por sesión activa | Análisis de actividad, capturas y contexto de aplicaciones.         |

El servicio es la **única autoridad de bloqueo** del equipo. La instancia por usuario solo hace telemetría — evita acciones duplicadas en escenarios multi-usuario.

En macOS el agente se distribuye como **binario universal** (Apple Silicon e Intel en un solo archivo) y corre como una sola instancia en la sesión gráfica del usuario — requisito del sistema para leer la ventana activa y capturar pantalla. Los permisos del sistema (Grabación de Pantalla y Accesibilidad) se autorizan una única vez durante la instalación guiada y persisten entre actualizaciones.

|                                                                                                         |                                                                                           |                                                                       |                                                                                                      |
|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <b>TENANT</b><br>Organización cliente.<br>Aislamiento completo de datos, usuarios, agentes y políticas. | <b>DEPARTAMENTO</b><br>Subdivisión del tenant.<br>Delega permisos sin perder aislamiento. | <b>AGENTE</b><br>Equipo físico con identificador estable a renombres. | <b>AUTO-ENROLLMENT</b><br>El equipo se auto-registra en el tenant correcto, sin intervención manual. |
|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|

Cada usuario tiene un rol con alcance acotado. La visibilidad de cada funcionalidad se controla de forma granular.

| ROL         | ALCANCE            | CAPACIDADES CLAVE                                                           |
|-------------|--------------------|-----------------------------------------------------------------------------|
| root        | Toda la plataforma | Administrar tenants. Acceso a cualquier dato.                               |
| super_admin | Tenant completo    | Políticas globales, usuarios, departamentos, todas las features del tenant. |
| operator    | Tenant (técnico)   | Hardware/procesos histórico, install windows. No edita políticas.           |
| dept_leader | Su departamento    | Agentes de su dept, reglas allow/block segmentadas, actividad.              |

VISIBILIDAD GRANULAR POR ROL

| FUNCIONALIDAD                    | SUPER_ADMIN | OPERATOR | DEPT_LEADER |
|----------------------------------|-------------|----------|-------------|
| CPU / Memoria / Procesos en vivo | ✓           | ✓        | ✗           |
| Histórico de hardware (7 días)   | ✓           | ✓        | ✗           |
| Histórico de procesos (top apps) | ✓           | ✓        | ✗           |
| Classifier de actividad          | ✓           | ✗        | ✗           |
| Blocking policy                  | ✓           | ✗        | ✗           |
| Catálogo de Apps (vista)         | ✓           | ✓        | su dept     |
| Crear reglas allow/block         | global      | ✗        | dept        |
| Install Window                   | ✓           | ✓        | ✗           |
| Gestión de cifrado de disco      | ✓           | ✗        | ✗           |
| Gestión de usuarios              | ✓           | ✗        | ✗           |
| Activity / Screenshots / Browser | ✓           | ✓        | ✓           |
| Mapa · Inventario · Reports      | ✓           | ✓        | ✓           |

## § 05.1 · RECOLECCIÓN DE DATOS

## QUÉ CAPTURA EL AGENTE

|                            |                                                                                  |
|----------------------------|----------------------------------------------------------------------------------|
| Métricas de hardware       | CPU global y por core, memoria, swap, discos por volumen, red RX/TX por interfaz |
| Top procesos               | Procesos con mayor consumo: nombre, uso de CPU, memoria                          |
| Inventario de aplicaciones | Aplicaciones instaladas con nombre, versión, vendor y ubicación                  |
| Actividad de ventanas      | Ventana en primer plano, título, proceso, duración                               |
| Contexto de navegador      | URL y dominio activo en navegadores comunes — sin extensión de navegador         |
| Atribución por monitor     | Cada evento se etiqueta con el display donde ocurrió                             |
| Geolocalización            | Lookup por IP pública (cada 30 min)                                              |
| File system watching       | Detección de archivos eliminados en paths sensibles                              |

## § 05.1.1 · SEÑALES DE PRESENCIA

## TRES SEÑALES INDEPENDIENTES

IUM captura tres señales independientes sobre la presencia del usuario. Se reportan por separado y **nunca se fusionan en un único número**.

| SEÑAL                     | CÓMO SE MIDE                                                                                   | QUÉ SIGNIFICA                                                                            |
|---------------------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| AFK · ausencia real       | Input idle de mouse/teclado medido por hardware. Umbral configurable por tenant (default 60 s) | <b>Ausencia confirmada.</b> El dato duro del que dependen los reportes de presencia      |
| Video / media en foco     | Señal de energía del sistema operativo sostenida por un navegador o reproductor                | El usuario consume video (capacitación, videollamada). Se superpone al AFK sin alterarlo |
| Presencia falsa · juggler | Escaneo de la totalidad de procesos contra un catálogo de herramientas anti-idle               | Hay software simulando actividad. Marca las métricas del período como no confiables      |

## POR QUÉ IMPORTA LA SEÑAL DE VIDEO

Un detector basado solo en input clasifica como «ausente» a quien mira una capacitación de 40 minutos sin tocar el teclado — técnicamente correcto, operativamente injusto. IUM no resuelve esto falseando el AFK (eso destruiría su valor probatorio), sino **exponiendo el contexto en paralelo para que un humano decida**. La señal usa la información de energía del sistema operativo, no heurísticas sobre títulos de ventana; el audio solo (música, podcast) no la activa: detecta video.

§ 05.2 · CONTROL DE EJECUCIÓN · DLP LIGHT

WINDOWS

### Bloqueo de procesos en tiempo real

Termina procesos que coinciden con reglas de bloqueo, con verificación continua. El watcher de archivos pone en cuarentena extensiones bloqueadas en carpetas vigiladas (Descargas, Escritorio, temporales y medios removibles).

### MODO AUDITORÍA

Reporta qué se habría bloqueado sin actuar. Calibración previa al rollout.

### ACCIÓN POR DEFECTO CONFIGURABLE

**allow** (permisivo: solo bloquea reglas explícitas) o **block** (lockdown: bloquea todo lo no pre-aprobado).

COINCIDENCIA MULTI-CAPA

nombre + vendor

ubicación de instalación

nombre del ejecutable

prefijo de ruta

huella del archivo

§ 05.3 · ANTI-TAMPER

RESILIENCIA DEL AGENTE

|                          |                                                                                                                                     |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Watchdog mutuo           | Dos componentes se vigilan entre sí; si uno se detiene, el otro lo relanza automáticamente.                                         |
| Relanzamiento automático | Tareas redundantes con reintentos ante detención.                                                                                   |
| Servicio independiente   | No depende de la sesión de usuario; sobrevive cierre de sesión y reinicios. En macOS, el sistema relanza el agente automáticamente. |

§ 05.4 · DEPLOYMENT

INSTALACIÓN A ESCALA

|                                 |                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Instalador silencioso (Windows) | Desplegable vía Group Policy, Microsoft Intune, cualquier RMM estándar o doble-click.                                                    |
| Script tenant-aware             | Descargable del dashboard con la organización pre-configurada: limpieza previa + instalación + verificación. El cliente solo lo ejecuta. |
| Instalador guiado (macOS)       | Instalación idempotente que limpia versiones previas y abre los paneles de permisos del sistema automáticamente.                         |
| Upgrade automático              | Nueva versión sobre versión anterior sin pérdida de configuración.                                                                       |
| Desinstalación estándar         | Vía el mecanismo nativo de cada sistema; remueve todos los componentes.                                                                  |

Integraciones de despliegue: Microsoft Intune, Group Policy y RMMs estándar (NinjaOne, Atera, Kaseya, ConnectWise, entre otros).

**Gestión de flota**

Tarjetas con status online/offline robusto sobre NAT, métricas en vivo y ubicación. Asignación a departamentos drag-and-drop.

**Catálogo de Apps**

Todas las apps de la flota agrupadas por nombre y vendor. Decisión allow/block/audit por scope global, departamento o agente. Precedencia: agente > dept > global.

**Histórico de Hardware**

CPU, memoria, disco y red — 7 días con visualización adaptativa según el rango consultado.

**Histórico de Procesos**

Top apps por CPU con promedio y pico de CPU/RAM, y gráfico de evolución apilado.

**Mapa de Geolocalización**

Clustering de agentes, track histórico por equipo y alertas de cambio de zona (>50 km o país). Modo claro/oscuro.

**Análisis de Actividad**

Resumen diario, línea de tiempo en franja de 24 h, filtro de jornada laboral y atribución multi-usuario.

**Screen Viewer**

Captura on-demand vía canal de control, optimizada. Histórico opcional.

**Block Events Feed**

Lista cronológica de bloqueos con acción, fuente, archivo y severidad. Filtros por agente, severidad y rango.

**Install Window**

Ventana temporal de instalación (15–120 min) por agente. Extender, revocar, countdown en vivo. Audit completo.

**Gestión de cifrado de disco**

Estado y gestión remota del cifrado en Windows; lectura de estado en macOS. Solo roles altos.

**Reports Builder**

Dimensiones y métricas combinables, export a PDF y reportes pre-armados de actividad, productividad, top apps y bloqueos.

**Deploy Agent**

Descarga del instalador por plataforma y generación del script tenant-aware desde el dashboard.

**Reporte de Conexión**

Tiempo activo, AFK, sesión y % de actividad por usuario, agente, día o departamento — con fórmula explícita y alcance por rol aplicado server-side.

**Inicio con permisos**

Landing con widgets según el rol real del usuario. Navegación protegida: fuera de alcance redirige, nunca error.

**Centro de Ayuda integrado**

33 artículos en español, contextuales a la pantalla activa y filtrados por rol. Accesible con ⌘K / Ctrl+K.

| MÉTRICA               | DEFINICIÓN                                      | INTERPRETACIÓN                                                                          |
|-----------------------|-------------------------------------------------|-----------------------------------------------------------------------------------------|
| Tiempo activo         | Ventanas en primer plano con interacción        | Uso efectivo del equipo                                                                 |
| Ausente (AFK)         | Sin input de mouse/teclado sobre el umbral      | Única ausencia confirmada. Base de los reportes de presencia                            |
| Sin eventos (gaps)    | Períodos sin actividad reportada entre sesiones | Suspensión, apagado o agente detenido                                                   |
| Sin cambio de ventana | Misma ventana por más de 2 min                  | Techo máximo de inactividad posible, no ausencia: incluye lectura y trabajo concentrado |
| Video/media en foco   | Video reproduciéndose en primer plano           | Dimensión separada; se superpone al AFK y no lo altera                                  |

RECONCILIACIÓN CONTRA RELOJ DE PARED

Los totales del día se ajustan a su ventana real (primera a última actividad). **El AFK se preserva como dato duro y el tiempo activo se deriva**, no al revés. Además: deduplicación de eventos, exclusión de apps de sistema en pantalla de bloqueo, y acotamiento a 24 h por día preservando la medición de ausencia.

Determina si cada app, dominio o ventana es **productivo / neutral / improductivo**. Es independiente de las métricas de presencia: una responde «¿estuvo?» y la otra «¿en qué?».

|                     |                                                                                                                                             |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Campos de una regla | Campo a evaluar (app, dominio, URL, título), tipo de coincidencia (exacta, contiene, empieza con, regex), patrón, clasificación y prioridad |
| Prioridad           | Orden de evaluación, no importancia: gana la primera regla que coincide. Una regla específica puede prevalecer sobre una general            |
| Taxonomía N-aria    | Categorías anidables sin límite de profundidad, definidas por cada organización                                                             |

FALLBACK CON LLM · OPCIONAL

Cuando ningún patrón coincide, el evento se clasifica automáticamente con IA y el resultado queda **cacheado por dominio** — se consulta una vez y nunca más, con el razonamiento auditable. Deshabilitable para entornos sin internet.

|                 |                                                                                                      |
|-----------------|------------------------------------------------------------------------------------------------------|
| Autenticación   | Usuario/contraseña con hash seguro. Rate limiting: 5 intentos fallidos en 15 min → bloqueo temporal. |
| Sesiones        | Token con expiración configurable (default 8 h).                                                     |
| Autorización    | RBAC granular. Aislamiento estricto entre tenants verificado en cada endpoint.                       |
| Tenant override | Solo respetado para rol root.                                                                        |
| Comunicación    | HTTPS obligatorio en producción; canal de control cifrado.                                           |

7.4 · AUDIT TRAIL

Log completo de cada acción administrativa, con:

- Timestamp ISO
- Acción (login, alta de usuario, regla de catálogo, ventana de instalación...)
- Usuario + rol
- Detalles específicos
- Organización (tenant)

Con rotación y retención configurable.

| DATO                       | RETENCIÓN DEFAULT           | CONFIGURABILIDAD         |
|----------------------------|-----------------------------|--------------------------|
| Hardware metrics           | 7 días                      | Fijo por diseño          |
| Process metrics (top apps) | 7 días                      | Fijo por diseño          |
| Activity events            | 30 días                     | Vía Platform Settings UI |
| Block events               | 30 días                     | Vía Platform Settings UI |
| Inventory snapshots        | Hasta uninstall del agente  | Sin cleanup automático   |
| Geolocation history        | Solo cambios significativos | Sin retención automática |
| Audit log                  | Rotación por tamaño         | Configurable             |
| Install windows            | Audit permanente            | Limpieza manual si crece |

Frecuencia de muestreo configurable por métrica, ajustable según las necesidades del cliente.

Windows y macOS production-ready; Linux en beta. Todas las plataformas comparten el mismo modelo de gestión y el mismo dashboard.

| CAPACIDAD                              | WINDOWS | MACOS     | LINUX     |
|----------------------------------------|---------|-----------|-----------|
| Métricas de hardware                   | ✓       | ✓         | ✓         |
| Actividad de ventanas + duración       | ✓       | ✓         | ✓         |
| URL y dominio del navegador            | ✓       | ✓         | ~         |
| Detección de ausencia (AFK)            | ✓       | ✓         | ✓         |
| Video/media en foco                    | roadmap | ✓         | roadmap   |
| Detección de presencia falsa (jiggler) | ✓       | ✓         | ✓         |
| Atribución por monitor                 | ✓       | ✓         | ✓         |
| Captura de pantalla on-demand          | ✓       | ✓         | ✓         |
| Inventario de aplicaciones             | ✓       | ✓         | ✓         |
| Bloqueo de ejecución (DLP Light)       | ✓       | ✗         | ✗         |
| Cuarentena de archivos                 | ✓       | ✗         | ✗         |
| Cifrado de disco                       | gestión | lectura   | ✗         |
| Anti-tamper                            | ✓       | relanzado | relanzado |

✓ Soportado   ~ Parcial   ✗ No disponible

ESCALABILIDAD

Flota objetivo de **50–500 agentes por tenant** en deployment típico, con frecuencia de muestreo configurable por métrica según las necesidades de cada cliente.

VENDOR · VECTORAIQ

cesar@vectoraiq.dev

Solicita una demostración guiada y un plan de PoC adaptado a tu flota. Soporte técnico según contrato cliente.

IUM-DS-2026  
v1.0 · julio 2026  
ES