Aitamit

Manual de Usuario

Plataforma europea de Gestión de Activos TI

European Digital Stores SL

Agosto de 2026 · aitamit.com

Índice

1. Bienvenida a AITAMIT

AITAMIT es la plataforma de **Gestión de Activos TI (ITAM)** de European Digital Stores SL. Su misión es responder, en todo momento y con evidencia verificable, a las cuatro preguntas que toda organización debería poder contestar sobre su parque informático: **qué activos tengo**, **en qué estado están**, **qué software ejecutan y con qué licencias**, y **hasta qué punto cumplen** las normativas que le aplican.

Para conseguirlo, AITAMIT combina un **agente ligero** que se instala en cada equipo con una **consola web** desde la que se gobierna todo el parque. El agente recopila el inventario de forma continua y la plataforma lo convierte en información accionable: licencias sin usar, equipos fuera de política, controles de seguridad incumplidos, recomendaciones priorizadas y, cuando hace falta actuar, comandos y despliegues remotos con un modelo de seguridad Zero-Trust.

1.1 Qué hace AITAMIT por usted

- **Inventario continuo**: hardware, software, discos, red y usuarios de cada equipo, actualizado cada 15 minutos sin intervención manual.
- **Gobierno de licencias (SAM)**: qué software hay instalado, qué licencias se han contratado y dónde no cuadran las cuentas.
- **Postura de seguridad**: controles ponderados que puntúan cada equipo y el conjunto de la organización.
- **Cumplimiento normativo**: evaluación frente a NIS2, ENS, ISO 27001 y DORA con informes firmados listos para auditoría.
- **Operación remota Zero-Trust**: comandos, paquetes, despliegues y políticas sin abrir un solo puerto en sus equipos.
- **Móviles gestionados (MDM)**: inventario y gestión de iPhone, iPad y Android (bloqueo, borrado remoto, apps, restricciones), con enrolamiento directo o conectando su Jamf/Intune existente.
- **Control remoto de escritorio**: tome el control de cualquier equipo Windows, macOS o Linux para dar soporte sin desplazarse, con consentimiento y auditoría.
- **Asistente de IA**: pregunte a su parque en lenguaje natural y reciba diagnósticos y recomendaciones accionables.

1.2 Conceptos básicos

Concepto	Qué significa
Tenant	Su organización dentro de AITAMIT. Todos sus datos están aislados del resto de clientes y su consola vive en su propio subdominio (suempresa.aitamit.com).
Activo	Cada equipo gestionado: un portátil, un servidor, un TPV, un móvil Android…

Concepto	Qué significa
Agente	El programa ligero instalado en cada activo que reporta el inventario y ejecuta las acciones aprobadas.
Token de instalación	La credencial que vincula un agente recién instalado con su organización. Se genera y revoca desde la consola.
Postura	La puntuación de seguridad de un activo calculada a partir de controles ponderados.
Framework	Un marco normativo (NIS2, ENS, ISO 27001, DORA) contra el que AITAMIT evalúa su parque.

Nota: AITAMIT es un producto **soberano europeo**: sus datos se alojan y procesan íntegramente en la Unión Europea, sin sub-procesadores fuera de la UE.

2. Alta y primer acceso

2.1 Crear la cuenta de su organización

1. Entre en **aitamit.com** y pulse «Probar AITAMIT».
2. Elija el plan que mejor encaje con su organización (puede cambiarlo más adelante).
3. Rellene el formulario: nombre de la empresa, su nombre, email corporativo y contraseña. El **identificador (slug)** se propone automáticamente a partir del nombre de la empresa y determina la dirección de su consola: suempresa.aitamit.com. El formulario comprueba en vivo que esté disponible.
4. Al enviar, AITAMIT crea su organización, su usuario administrador y su primer token de instalación, y le muestra la pantalla de bienvenida con los tres primeros pasos.

2.2 Verificar el email

Recibirá un correo de verificación en su idioma. Hasta que confirme la dirección, algunas funciones permanecen limitadas. Si no llega en unos minutos, revise la carpeta de spam o solicite el reenvío desde la pantalla de acceso.

2.3 Acceder a la consola

Su consola vive en **https://suempresa.aitamit.com** (también puede entrar por console.aitamit.com). El acceso usa el sistema de identidad corporativa de la plataforma; tras cinco intentos fallidos la cuenta se bloquea temporalmente por protección contra fuerza bruta.

> **Importante:** La contraseña del primer usuario da control total sobre su organización. Guárdela en su gestor de contraseñas corporativo y active usuarios adicionales con roles limitados para el trabajo diario (capítulo 23).

3. Desplegar el agente en su parque

El agente de AITAMIT es un binario ligero (menos de 8 MB) que se ejecuta como servicio del sistema, consume recursos insignificantes y **solo genera tráfico saliente HTTPS**: nunca abre puertos ni acepta conexiones entrantes. Cada instalación necesita un **token de instalación** vigente, disponible en Consola → Instalar.

3.1 Linux (x86_64 y ARM64)

```
curl -fsSL https://aitamit.com/install.sh | INSTALL_TOKEN=SU_TOKEN bash
```

El instalador detecta la arquitectura, verifica el checksum SHA-256 del binario, instala el servicio systemd y arranca el agente. En menos de dos minutos el equipo aparece en el inventario con su hardware, software, discos, interfaces y usuarios.

3.2 Windows

```
powershell -ExecutionPolicy Bypass -c "iwr https://aitamit.com/install.ps1 -
UseBasicParsing | iex" -Token SU_TOKEN
```

Se instala como servicio de Windows «AitamitAgent» con recuperación automática ante fallos. Ejecute la consola de PowerShell como administrador.

3.3 macOS (Intel y Apple Silicon)

```
curl -fsSL https://aitamit.com/install-mac.sh | INSTALL_TOKEN=SU_TOKEN bash
```

El instalador registra un LaunchDaemon (com.aitamit.agent) que arranca con el sistema. Existen binarios nativos para Intel, Apple Silicon y un binario universal.

3.4 Android

El agente de Android está disponible en **Google Play** (busque «AITAMIT Agent») y también como **APK** para instalación manual desde la sección de descargas de la consola. Tras instalarlo, introduzca el **token de instalación** y pulse «Iniciar». La app funciona como servicio en primer plano: reporta identificación del dispositivo, sistema, almacenamiento, red y aplicaciones instaladas, y se rearma sola tras cada reinicio. Para grandes flotas puede distribuirse de forma centralizada con **Android Enterprise / Managed Google Play**.

3.5 iPhone y iPad (iOS / iPadOS)

Apple **no permite instalar un agente** de inventario en iPhone o iPad: la vía soportada por el sistema es **MDM** (gestión de dispositivos móviles). AITAMIT actúa como su **propio servidor MDM**, así que puede incorporar sus dispositivos Apple de dos formas según su situación.

Opción A — Enrolar directamente con AITAMIT (si no usa otro MDM)

1. En la consola, vaya a **Móviles** → **«Enrolar dispositivo»**. Obtendrá una URL de enrolamiento (y un código QR).
2. En el iPhone o iPad, abra esa URL en **Safari**. El sistema descargará un **perfil de configuración**.

3. Instálelo en **Ajustes → General → VPN y gestión de dispositivos**. En segundos el dispositivo aparece en el inventario con su modelo, versión de iOS, almacenamiento y aplicaciones.

Para grandes flotas, el enrolamiento puede ser **automático y sin intervención del usuario (zero-touch)** mediante **Apple Business Manager**; la puesta en marcha se describe en el Manual de Administrador.

Opción B — Si ya gestiona sus iOS con Jamf Pro o Microsoft Intune

Apple no permite **dos perfiles MDM** en el mismo dispositivo, de modo que no necesita (ni puede) re-enrolarlos. En su lugar, **conecte su MDM existente en modo solo lectura**: AITAMIT inventaría su flota iOS a través de la API de Jamf o Intune **sin tocar los dispositivos** y la muestra junto al resto del parque. El conector se configura una vez en **Móviles → «Conectar Jamf / Intune»** (ver Manual de Administrador).

> **Nota:** Con iOS obtiene inventario y las **acciones de gestión que permite Apple**: bloquear, borrado remoto, instalar o quitar apps y perfiles, y restricciones. El **control remoto interactivo de la pantalla NO es posible en iOS** — Apple lo prohíbe a nivel de sistema para cualquier fabricante (tampoco TeamViewer o AnyDesk pueden). Para ver y controlar la pantalla, esa capacidad está disponible en equipos de escritorio y en Android (capítulos 16 y 17).

3.6 Comprobar que todo funciona

- El equipo aparece en **Inventario** con un punto verde (en línea) en menos de 2 minutos.
- La ficha del activo muestra hardware y software completos tras el primer ciclo de inventario (máximo 15 minutos).
- Si no aparece: compruebe la salida a Internet por HTTPS del equipo, la vigencia del token y vuelva a ejecutar el instalador.

4. El Dashboard

El Dashboard es la portada operativa de su organización y responde de un vistazo a «¿cómo está mi parque hoy?». Sus indicadores se calculan en tiempo real sobre el inventario vivo.

- **Activos**: total gestionado, en línea y sin reportar. Un activo que lleva horas sin latido merece atención: puede estar apagado, sin red o con el agente detenido.
- **Postura**: la puntuación media de seguridad y su tendencia. La meta razonable es mantenerla por encima de 80.
- **Cumplimiento**: porcentaje de controles superados en los frameworks activos.
- **Licencias**: desviaciones detectadas entre lo instalado y lo contratado.
- **Actividad reciente**: últimos cambios de inventario, comandos ejecutados y alertas.

Si su organización acaba de estrenarse y aún no hay activos, el Dashboard muestra el asistente de despliegue del primer agente.

5. Inventario de activos

5.1 La lista de activos

Inventario muestra todos los equipos de la organización con su estado en vivo. Puede **filtrar** por sistema operativo, estado (en línea / sin reportar), texto libre sobre nombre y usuario, y combinaciones de ambos; y **ordenar** por cualquier columna. La búsqueda es instantánea y no distingue mayúsculas.

5.2 La ficha del activo

Cada activo tiene una ficha completa con pestañas:

- **Resumen**: identificación, SO y versión, hardware (CPU, memoria, modelo), último latido y última actualización de inventario.
- **Software**: todas las aplicaciones instaladas con versión y editor. Este listado alimenta el módulo de licencias.
- **Discos y red**: volúmenes con capacidad y ocupación; interfaces con MAC e IP.
- **Usuarios**: cuentas locales presentes en el equipo.
- **Postura**: el detalle de cada control evaluado en este equipo, con su peso y su resultado.
- **Historial**: los cambios detectados entre inventarios (software instalado o eliminado, hardware modificado, usuarios nuevos).

5.3 Cambios

La vista **Cambios** agrega el historial de todo el parque en una línea temporal: qué se instaló, qué se desinstaló y qué cambió, en qué equipo y cuándo. Es la primera parada para responder «¿qué ha cambiado esta semana?» y para detectar software no autorizado recién aparecido.

6. Catálogo de software

El catálogo consolida todo el software detectado en el parque en una vista única normalizada: cada producto con sus versiones, el número de instalaciones y los equipos donde está presente. Desde aquí se decide qué productos requieren licencia y se conecta el inventario con el módulo de licencias.

- Identifique **software no autorizado** revisando los productos recién llegados al catálogo (combínelo con la vista Cambios).
- Detecte **versiones obsoletas** de productos críticos: navegadores, ofimática, runtimes.
- Priorice: los productos con más instalaciones son los que más impacto tienen en licencias y seguridad.

7. Licencias (SAM)

7.1 Registrar licencias

Dé de alta cada contrato de licencia con el producto del catálogo al que aplica, el número de puestos adquiridos, el coste y las fechas de vigencia. AITAMIT no necesita que registre nada en los equipos: el lado «instalado» de la ecuación ya lo aporta el inventario.

7.2 Reconciliación automática

AITAMIT cruza continuamente **instalado ↔ contratado** y clasifica cada producto:

Situación	Qué significa	Qué hacer
Conforme	Instalaciones ≤ puestos contratados.	Nada. Todo en orden.
Sobre-despliegue	Hay más instalaciones que licencias.	Regularizar: comprar puestos o desinstalar (puede hacerlo con un despliegue remoto, cap. 14).
Infrautilización	Hay bastantes menos instalaciones que licencias.	Ahorrar: reducir puestos en la próxima renovación.

Cada situación de riesgo genera además una entrada en **Recomendaciones** con su impacto estimado, de modo que las oportunidades de ahorro no se pierdan de vista.

8. Postura de seguridad

La postura es la respuesta de AITAMIT a «¿cómo de bien configurado está mi parque?». Cada activo se evalúa contra un conjunto de **controles cross-platform** — cifrado de disco, cortafuegos activo, actualizaciones automáticas, antivirus, bloqueo de pantalla, cuentas sin contraseña, etc. — y cada control tiene un **peso** acorde a su criticidad.

- La **puntuación del activo** (0–100) pondera los controles superados por su peso.
- La **puntuación de la organización** agrega las de todos los activos y es el número que verá en el Dashboard.
- El detalle por activo (ficha → Postura) muestra exactamente **qué control falla y por qué**, que es la información que necesita el técnico para corregirlo.

La forma más eficaz de subir la puntuación global es atacar primero los controles de mayor peso en los equipos donde fallan de forma masiva; la vista de postura agrupa los incumplimientos por control para que ese diagnóstico sea inmediato.

9. Cumplimiento normativo

9.1 Frameworks disponibles

Framework	Ámbito	Para quién
NIS2	Ciberseguridad de entidades esenciales e importantes en la UE.	Energía, transporte, banca, sanidad, digital, AAPP y sus cadenas de suministro.
ENS (nivel Alto)	Esquema Nacional de Seguridad español.	Administraciones públicas españolas y sus proveedores.
ISO/IEC 27001	Gestión de la seguridad de la información.	Cualquier organización que certifique o quiera certificar su SGSI.
DORA	Resiliencia operativa digital del sector financiero de la UE.	Entidades financieras y sus proveedores TIC críticos.

9.2 Cómo funciona

Cada framework define **controles** que AITAMIT mapea automáticamente a los datos del inventario y de la postura. La evaluación es continua: no hay que lanzar nada. La vista de cumplimiento muestra el porcentaje de superación por framework, el detalle de cada control (superado, fallido, no aplicable) y los activos afectados por cada fallo.

9.3 Evidencia para auditoría

Desde Cumplimiento → Informes se genera el **informe de evidencia** de cada framework: un documento con el resultado de cada control en el momento de la generación, **firmado con SHA-256**. Cualquier tercero puede verificar la integridad del informe en la página pública de verificación. Es exactamente el artefacto que un auditor espera recibir.

> **Nota:** AITAMIT aporta la evidencia técnica del parque. El cumplimiento completo de una norma incluye además procesos, documentación y gobierno que quedan fuera del alcance de una herramienta ITAM — desconfíe de quien le prometa lo contrario.

10. Informes

- **Tipos**: inventario completo, cumplimiento por framework, postura, licencias.
- **Generación**: desde la vista Informes, eligiendo tipo y alcance. El informe queda archivado con fecha, autor y firma.
- **Firma SHA-256**: cada informe lleva su hash; la página pública de verificación confirma que el documento no ha sido alterado desde su emisión.
- **Historial**: los informes emitidos quedan en la plataforma, formando la línea temporal de evidencia de su organización.

11. Recomendaciones

El motor de recomendaciones convierte los hallazgos de todos los módulos en una **lista priorizada de acciones**: regularizar un sobre-despliegue, cerrar un control de postura masivamente incumplido, actualizar un producto obsoleto, revisar un equipo que lleva días sin reportar. Cada recomendación explica el porqué, estima el impacto y enlaza con el módulo donde ejecutarla. Márquelas como completadas o descártelas con justificación; ambas cosas quedan en la auditoría.

12. Asistente de IA

El asistente responde en lenguaje natural con el **contexto completo de su parque**: inventario, licencias, postura y cumplimiento. Ejemplos de lo que puede preguntarle:

- «¿Qué equipos tienen menos de un 20 % de disco libre?»
- «¿Dónde está instalado el producto X y en qué versiones?»
- «¿Qué tres acciones subirían más mi puntuación de postura?»
- «Redáctame un resumen del estado del parque para el comité de dirección.»

Las conversaciones se guardan por usuario y pueden retomarse. El asistente **no ejecuta acciones**: propone, explica y diagnostica; la ejecución siempre pasa por los módulos correspondientes con sus permisos y su auditoría.

13. Comandos remotos

Los comandos permiten actuar sobre los equipos sin desplazarse: ejecutar un script, recabar un diagnóstico, forzar una actualización. El modelo es **Zero-Trust y pull**: la plataforma nunca se conecta al equipo; es el agente quien, en su siguiente latido (máximo 60 segundos), recoge el comando pendiente, lo ejecuta y devuelve el resultado.

- **Estados**: pendiente → entregado → completado / fallido. La vista de detalle muestra la salida completa de la ejecución.
- **Por lotes**: un mismo comando puede dirigirse a una selección de activos o a un filtro (p. ej., todos los Windows).
- **Auditoría**: quién ordenó qué, en qué equipos, cuándo y con qué resultado — todo queda en el registro encadenado.

Importante: Un comando se ejecuta con los privilegios del agente. Restrinja el permiso de crear comandos a los roles adecuados y revise la auditoría periódicamente.

14. Paquetes y despliegues

Los **paquetes** definen software instalable (instalador + parámetros silenciosos por sistema operativo). Los **despliegues** llevan un paquete a un conjunto de activos: seleccione el paquete, el alcance (activos concretos o filtro) y lance. El progreso se sigue en vivo: pendientes, en curso, completados y fallidos, con el detalle de error de cada fallo.

Los despliegues también sirven para **desinstalar** (paquete con comando de desinstalación), que es la vía rápida para regularizar un sobre-despliegue de licencias detectado en el capítulo 7.

15. Políticas declarativas

Una política declara un **estado deseado** — «el cortafuegos debe estar activo», «este software debe estar presente», «esta configuración debe tener este valor» — y AITAMIT la evalúa continuamente en los activos de su alcance. La diferencia con un comando es la persistencia: el comando es una acción puntual; la política es una regla que vigila la deriva de configuración en el tiempo.

- Cada evaluación deja resultado por activo: conforme / no conforme, con el detalle del porqué.
- Las no conformidades alimentan postura y recomendaciones.
- Use políticas para los mínimos exigibles del parque y comandos/despliegues para las correcciones.

16. Control remoto de escritorio

El control remoto le permite **ver la pantalla de un equipo y manejarlo con su ratón y teclado** para dar soporte sin desplazarse — el caso de uso típico de una empresa de soporte IT que resuelve la incidencia de un cliente en remoto. Está disponible para equipos **Windows, macOS y Linux** con el agente instalado.

16.1 Iniciar una sesión

1. Abra la ficha del equipo en **Inventario** (debe estar en línea).
2. Pulse el botón **«Control remoto»**. Se abre el visor a pantalla completa.
3. En unos segundos el agente del equipo acepta la sesión y verá su pantalla en vivo. A partir de ahí, su ratón y su teclado actúan sobre el equipo remoto.

El visor incluye contador de imágenes por segundo, botón **Ctrl+Alt+Supr**, conmutador de captura de teclado y botón de desconexión. Al cerrar la ventana, la sesión termina.

16.2 Cómo funciona y seguridad

- **Sin abrir puertos**: es el agente quien inicia la conexión saliente hacia AITAMIT; funciona detrás de NAT y cortafuegos sin exponer el equipo.
- **Cifrado y con ticket de un solo uso**: cada sesión usa una credencial temporal que se invalida al terminar.
- **Auditado**: el inicio y el fin de cada sesión de control remoto, con operador y equipo, quedan en el registro de auditoría encadenado.

> **Nota:** El control remoto interactivo **no está disponible en iPhone/iPad**: Apple lo prohíbe a nivel de sistema. En **Android** sí es posible (capítulo 17).

17. Móviles: iPhone, iPad y Android (MDM)

Además del inventario, AITAMIT **gestiona** los dispositivos móviles desde la vista **Móviles** de la consola. El alcance depende de lo que permite cada sistema operativo.

17.1 Qué puede hacer con iPhone y iPad

Sobre los dispositivos Apple enrolados (capítulo 3.5) dispone de las acciones que Apple habilita vía MDM, desde la ficha del dispositivo:

- **Bloquear** el dispositivo y **borrado remoto** (wipe) si se pierde o se da de baja a un empleado.
- **Instalar o quitar aplicaciones** y **perfiles de configuración** (Wi-Fi, VPN, correo…).
- **Restricciones**: por ejemplo, deshabilitar la cámara, impedir la instalación de apps o forzar copia de seguridad cifrada.
- **Quitar el código** o **reiniciar** (en dispositivos supervisados).

> **Importante:** El **control remoto de la pantalla** (ver y tocar) **no es posible en iOS/iPadOS** por decisión de Apple, común a todos los fabricantes. Sí lo es en Android.

17.2 Android

Los dispositivos Android con el agente instalado (capítulo 3.4) reportan su inventario como cualquier otro activo. La visualización y el control remoto de la pantalla en Android requieren que el usuario del dispositivo conceda el permiso de captura y active el servicio de accesibilidad, tal y como exige Android a cualquier herramienta de este tipo.

17.3 Conectar un MDM existente (Jamf / Intune)

Si su organización ya gestiona los iOS con Jamf Pro o Microsoft Intune, no re-enrole: conecte ese MDM en **modo solo lectura** desde **Móviles** → **«Conectar Jamf / Intune»** y AITAMIT inventariará su flota a través de su API, sin tocar los dispositivos. Los detalles de configuración (credenciales de API) están en el Manual de Administrador.

18. Auditoría

Todo lo que ocurre en AITAMIT — accesos, cambios de configuración, comandos, despliegues, cambios de licencias, generación de informes — queda registrado en la **auditoría encadenada**: cada entrada incluye el hash de la anterior, de modo que cualquier manipulación del histórico rompería la cadena y sería detectada. La vista permite filtrar por usuario, acción y fecha, y el botón «Verificar integridad» valida la cadena completa al momento.

19. Integraciones

Lleve las alertas y novedades de AITAMIT a las herramientas donde su equipo ya trabaja:

Integración	Qué hace
Slack / Microsoft Teams / Discord	Notificaciones de alertas y eventos en el canal que elija.
Jira	Creación de incidencias a partir de hallazgos y recomendaciones.
Email	Resúmenes y alertas por correo a las direcciones configuradas.

Cada integración se configura con sus credenciales en Integraciones y puede probarse con un evento de test antes de activarla.

20. Marketplace

El marketplace reúne extensiones instalables con un clic: paquetes de reglas adicionales, plantillas de políticas e integraciones. Cada elemento indica qué añade y qué permisos necesita; lo instalado puede desinstalarse desde el mismo lugar.

21. Para desarrolladores: API y webhooks

21.1 API keys

En Desarrolladores → API keys puede emitir claves para automatizar cualquier operación de la consola vía API REST. Las claves tienen el prefijo **ait_** y el secreto **solo se muestra al crearlas**: guárdelo en su gestor de secretos. Revoque inmediatamente cualquier clave comprometida.

```
curl -H "Authorization: Bearer ait_…" https://api.aitamit.com/api/v1/assets
```

21.2 Webhooks

Los webhooks envían eventos de AITAMIT (nuevo activo, alerta de postura, desviación de licencias…) a la URL que indique, **firmados con HMAC** para que su receptor verifique el origen. Configure la URL y el secreto en Desarrolladores → Webhooks y valide la firma en cada entrega.

La referencia completa de endpoints está en la documentación técnica del producto (docs/API.md).

22. Transparencia: SBOM y página de estado

- **SBOM**: AITAMIT publica el inventario de componentes de su propia plataforma en formato SPDX — la misma transparencia que le pedimos a su parque, aplicada a nosotros mismos.
- **Página de estado**: el estado operativo de la plataforma es público y consultable en todo momento.

23. Configuración de la organización

23.1 Usuarios y roles

Rol	Permisos
admin	Control total del tenant: usuarios, configuración, todos los módulos.
manager	Operación completa de los módulos sin administración de usuarios.
worker	Operación técnica del día a día (inventario, comandos, despliegues).
employee	Lectura de la información de su ámbito.

23.2 Tokens de instalación

Emita tokens distintos por oleada de despliegue u oficina: podrá revocarlos de forma independiente sin afectar a los agentes ya registrados. Un token revocado no expulsa a los agentes existentes; solo impide nuevas altas con él.

23.3 BYOK (Bring Your Own Key)

Si su política de seguridad lo exige, aporte su propia clave de cifrado **AES-256-GCM** para los datos sensibles de su tenant. Configúrela en Configuración y valide su funcionamiento con la prueba integrada antes de activarla. La custodia de la clave pasa a ser responsabilidad de su organización: sin ella, esos datos no son recuperables.

24. Planes y facturación

- Su plan vigente, el número de agentes y el estado de la suscripción se consultan en Configuración → Plan.
- Los importes y condiciones de cada plan están siempre actualizados en **aitamit.com/precios**.
- El cobro se realiza con tarjeta a través de Stripe; las facturas llegan por email y quedan descargables.
- Los cambios de plan se aplican con prorrateo; el detalle exacto se muestra antes de confirmar cualquier cambio.

25. Resolución de problemas

Síntoma	Causa probable y solución
Un equipo no aparece tras instalar el agente	Sin salida HTTPS a Internet, token caducado o revocado. Verifique conectividad, genere un token nuevo y reinstale.
Un activo lleva horas «sin reportar»	Equipo apagado, sin red, o servicio del agente detenido. Arranque el servicio (systemd / services.msc / launchctl) y revise su log local.
El inventario de un equipo se ve incompleto	El primer ciclo completo tarda hasta 15 minutos. Si persiste, reinicie el servicio del agente.
No llega el email de verificación	Revise spam y la dirección introducida; solicite reenvío desde la pantalla de acceso.
Acceso bloqueado tras varios intentos	Protección de fuerza bruta: espere al desbloqueo automático o contacte con su administrador.
Un comando queda «pendiente» mucho tiempo	El activo destino no está en línea. El comando se entregará en su siguiente latido.
Un despliegue falla en algunos equipos	Abra el detalle del despliegue: cada fallo incluye el error exacto devuelto por el equipo.

26. Glosario

Término	Definición
Agente	Servicio ligero instalado en cada activo que reporta inventario y ejecuta acciones aprobadas.
BYOK	Bring Your Own Key: cifrado de datos sensibles con una clave aportada y custodiada por el cliente.
Framework	Marco normativo evaluado automáticamente (NIS2, ENS, ISO 27001, DORA).
Hash encadenado	Técnica de auditoría en la que cada registro incluye el hash del anterior, haciendo evidente cualquier manipulación.
ITAM	IT Asset Management: gestión del ciclo de vida de los activos TI.
MDM	Mobile Device Management: gestión de móviles (iOS/iPadOS/Android) mediante perfiles y comandos del sistema operativo.
Enrolamiento	Alta de un dispositivo móvil en AITAMIT instalando el perfil MDM (manual por Safari o automático con Apple Business Manager).
Conector MDM	Integración de solo lectura con un MDM existente (Jamf Pro, Microsoft Intune) para inventariar sus móviles sin re-enrolarlos.
Control remoto	Ver y manejar la pantalla de un equipo de escritorio (Windows/macOS/Linux) o Android para dar soporte sin desplazarse.
Postura	Puntuación de seguridad basada en controles ponderados.
Reconciliación	Cruce automático entre software instalado y licencias contratadas.
RMM	Remote Monitoring & Management: monitorización y operación remota del parque.
SAM	Software Asset Management: gestión de activos de software y licencias.
SBOM	Software Bill of Materials: inventario de componentes de un software.
Slug	Identificador corto de su organización que forma su subdominio.
Tenant	Espacio aislado de una organización dentro de la plataforma.
Token de instalación	Credencial revocable que autoriza el alta de nuevos agentes.
Zero-Trust	Modelo en el que la plataforma jamás abre conexiones hacia los equipos; toda comunicación la inicia el agente.