



# Manual de usuario

Agente InmunoSec: instalación, portal y respuesta

Esta guía explica cómo contratar InmunoSec, instalar el agente en tus equipos y usar el portal para vigilar lo que pasa en ellos y responder cuando algo no va bien. Está pensada para la persona que administra los sistemas de la empresa; no hace falta ser especialista en seguridad.

Octubre 2026 · agente 0.8 · app Android 0.1 · <https://agentes.inmunosec.store/portal/>

---

## Contenido

1. Qué es InmunoSec
2. Requisitos
3. Crear la cuenta y contratar
4. Instalar el agente
5. El portal, vista por vista
6. Cuando aparece una alerta
7. Actualizaciones de seguridad
8. Red local: dispositivos de tu red
9. Informe por correo
10. Integraciones opcionales
11. Suscripción, facturas y baja
12. Privacidad y seguridad
13. Problemas frecuentes
14. Ayuda

## 1. Qué es InmunoSec

InmunoSec vigila tus servidores y ordenadores aprendiendo cómo se comportan normalmente: qué procesos ejecutan, qué usuarios entran, con quién se conectan y qué software tienen instalado. Cuando algo se sale de lo normal, te lo muestra en el portal, te explica por qué es raro y te propone cómo pararlo.

- **Agente:** un programa ligero que instalas en cada equipo. Observa el sistema y envía lo que ve al portal por una conexión cifrada y autenticada.
- **Portal:** la web donde ves todos tus equipos, sus alertas y las medidas propuestas, en [agentes.inmunosec.store](https://agentes.inmunosec.store).
- **Respuestas:** medidas acotadas y reversibles (poner un fichero en cuarentena, aislar un proceso, bloquear un origen). Por defecto se aplican solo cuando una persona de tu equipo las aprueba.

InmunoSec complementa, no sustituye, tus copias de seguridad, tu antivirus, las actualizaciones y las auditorías. Una alerta no demuestra por sí sola un ataque, y la ausencia de alertas no garantiza que no lo haya.

## 2. Requisitos

| Sistema            | Requisitos                                                                                                                                                                         |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Linux              | Distribución con systemd (Ubuntu, Debian, Red Hat, Rocky, AlmaLinux...), Python 3.12 o superior y acceso root para instalar. Probado en Ubuntu 24.04.                              |
| Windows            | Windows 10, Windows 11 o Windows Server 2019 o posterior, PowerShell como administrador. Si falta Python 3.12, el instalador lo instala con winget.                                |
| Android            | Móviles y tabletas con Android 8 o posterior. La app se instala desde el portal (no está en Google Play).                                                                          |
| macOS (en pruebas) | El soporte para Mac está en fase de pruebas. Si quieres probarlo en tus equipos, escríbenos a <a href="mailto:hola@inmunosec.es">hola@inmunosec.es</a> .                           |
| Red                | Salida a Internet por HTTPS (puerto 443) y al puerto 8443 de <a href="https://agentes.inmunosec.store">agentes.inmunosec.store</a> . No hace falta abrir ningún puerto de entrada. |

## 3. Crear la cuenta y contratar

InmunoSec se contrata solo por empresas y profesionales autónomos. El precio es de 20 € al mes más IVA por cuenta, sin permanencia, y recibes una factura TicketBAI de cada cobro.

- 1 Entra en [agentes.inmunosec.store/portal](https://agentes.inmunosec.store/portal) y pulsa **Crear cuenta**.
- 2 Indica el nombre de tu empresa, tu usuario, una contraseña larga, tu NIF, CIF o NIE (o NIF-IVA si estás en otro país de la UE) y acepta las condiciones de contratación y el encargo del tratamiento.
- 3 Configura la **verificación en dos pasos**: escanea el código QR con una app de autenticación (Google Authenticator, Microsoft Authenticator, 1Password...).
- 4 En **Perfil > Suscripción**, pulsa **Activar suscripción** y completa el pago con tarjeta en Stripe. En unos segundos la cuenta queda activa.

Guarda la contraseña y la app de autenticación: InmunoSec nunca te pedirá estos datos por correo ni por teléfono.

## 4. Instalar el agente

Cada equipo se enlaza a tu cuenta con una **clave de instalación**. El equipo genera su propia identidad durante la instalación; la clave privada no sale nunca de él.

### 4.1 Clave para un equipo

- 1 En **Perfil > Enlazar un servidor**, pulsa **Generar clave de instalación**.
- 2 Copia la orden que aparece para tu sistema (Linux o Windows). La clave es de un solo uso, caduca en 24 horas y solo se muestra una vez.
- 3 Ejecútala en el equipo, como se indica en los apartados siguientes. En menos de un minuto el equipo aparece en **Equipos**.

### 4.2 Linux

En una terminal del servidor, como root o con sudo:

```
curl -fsSL https://agentes.inmunosec.store/install.sh | sudo sh -s -- --key=TU_CLAVE
```

El instalador deja el agente en `/opt/inmunosec` y su configuración en `/etc/inmunosec`, y lo arranca como servicio (*inmunosec*) con un usuario propio sin privilegios de root. También instala el ejecutor de respuestas (*inmunosec-broker*), que solo aplica medidas firmadas por tu cuenta. Si prefieres que el equipo solo detecte y nunca aplique medidas, añade **--sin-respuesta** al final de la orden.

Para comprobar que funciona:

```
systemctl status inmunosec
```

### 4.3 Windows

Abre PowerShell como administrador (clic derecho > Ejecutar como administrador) y pega:

```
& ([scriptblock]::Create((irm https://agentes.inmunosec.store/install.ps1))) -Key TU_CLAVE
```

El agente se instala en «Archivos de programa\InmunoSec», guarda su configuración en «ProgramData\InmunoSec» (solo accesible para el sistema y los administradores) y queda funcionando como la tarea programada **InmunoSec Agent**, que arranca con el equipo y se reinicia sola si se detiene.

### 4.4 Móviles Android

- 1 Desde el móvil, entra en el portal y, en **Perfil**, genera una clave de instalación.
- 2 Pulsa **Descargar la app de Android** e instálala. Android te pedirá permitir instalar apps desde el navegador: acéptalo solo para esta instalación.
- 3 Vuelve al portal y pulsa **Abrir en la app** (o abre la app InmunoSec y pega la clave). Confirma el enlace.
- 4 Acepta las notificaciones y pulsa **Permitir en segundo plano** para que la vigilancia funcione con la pantalla apagada.

La app revisa el móvil cada 15 minutos: bloqueo de pantalla, cifrado, parches de seguridad, root, depuración USB y las apps instaladas con sus privilegios especiales (accesibilidad, administración del

dispositivo, lectura de notificaciones y SMS). Te avisa en el propio móvil y en el portal de lo que deberías corregir, y te explica cómo.

Android aísla cada app: InmunoSec no puede ver dentro de las demás ni leer tus mensajes, fotos, contactos o ubicación, y no lo intenta. Envía solo el estado de seguridad y la lista de apps con su origen y privilegios. Con el móvil en reposo, Android puede espaciar las revisiones; el portal lo tiene en cuenta.

#### 4.5 Muchos equipos: clave de flota

Si vas a instalar el agente en varios equipos (o con Ansible, GPO o scripts), crea una **clave de flota** en **Perfil > Claves de flota**. Sirve para todos los equipos que quieras mientras tu suscripción esté activa; puedes ponerle un nombre y un máximo de equipos. Si se filtra, pulsa **Revocar**: los equipos ya instalados siguen funcionando y nadie más podrá usarla.

#### 4.6 Actualizar o reinstalar

Volver a ejecutar la orden de instalación con una clave válida actualiza el agente y conserva la identidad del equipo.

### 5. El portal, vista por vista

En la columna izquierda eliges la vista; arriba, el equipo que quieres ver. Casi todas las vistas se pueden ver como tabla (con búsqueda, filtros y orden por columnas) o como gráfico. Al pulsar un elemento, a la derecha aparece su detalle.

| Vista      | Qué muestra                                                                                                                                                                                                                                  |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Equipos    | Todos tus equipos con su sistema operativo, estado (sin novedad, avisos, crítico), última señal y si el sensor está sano. Un equipo que deja de informar se marca como silenciado.                                                           |
| Usuarios   | Cuentas del sistema, quién tiene privilegios de administrador y qué cuentas de servicio están haciendo cosas raras.                                                                                                                          |
| Procesos   | Programas en marcha, con su usuario, consumo y conexiones. El árbol muestra quién lanzó a quién.                                                                                                                                             |
| Árbol      | Los ficheros y directorios relevantes que vigila el agente.                                                                                                                                                                                  |
| Paquetes   | Software instalado, si es un servicio en marcha, sus dependencias y los avisos de vulnerabilidades conocidas con su corrección. En un móvil, sus apps, con las instaladas fuera de tienda y las que tienen privilegios especiales señaladas. |
| Redes      | Conexiones entrantes y salientes, puertos en escucha e intentos de exploración, en grafo o en tabla.                                                                                                                                         |
| Red local  | Otros dispositivos de la red de tus equipos (impresoras, móviles, routers...), si activas el inventario.                                                                                                                                     |
| Sistema    | CPU, memoria, tráfico, sesiones abiertas y bases de datos vigiladas. En un móvil, la lista de comprobaciones de seguridad con lo que debes corregir.                                                                                         |
| Respuestas | Medidas propuestas, aprobadas, aplicadas o revertidas, con su motivo.                                                                                                                                                                        |
| Calidad    | Cuánto ruido genera la detección y cómo acierta, según tus decisiones.                                                                                                                                                                       |
| Histórico  | La evolución de las anomalías en el tiempo y el registro de lo que ha ocurrido.                                                                                                                                                              |

| Vista  | Qué muestra                                                                                  |
|--------|----------------------------------------------------------------------------------------------|
| Perfil | Tu cuenta: suscripción, facturas, claves de instalación, informe por correo e integraciones. |

## 6. Cuando aparece una alerta

- 1 Abre el equipo afectado. En el detalle verás **qué** se ha visto (por ejemplo, una cuenta de servicio que abre una consola), **por qué** es raro y el apartado **Qué conviene hacer**.
- 2 Si reconoces la actividad (un despliegue, un cambio de configuración), no hace falta hacer nada: el agente irá aprendiendo que es normal.
- 3 Si no la reconoces, ve a **Respuestas**. Cada medida propuesta indica qué hará, sobre qué y cómo se deshace. Pulsa **Aprobar** o **Rechazar**.
- 4 La medida aprobada se envía firmada al equipo, que la aplica en segundos. Desde el mismo sitio puedes **revertirla** si ha sido un error.

Las medidas más delicadas (como aislar el equipo entero de la red) pueden exigir la aprobación de una segunda persona.

### Respuesta automática

En **Perfil > Respuesta automática** puedes permitir que, ante evidencia fuerte, se apliquen sin esperar las medidas reversibles y acotadas: cuarentena de ficheros, aislar un proceso, cortar una sesión de base de datos que está siendo atacada y bloquear el origen de un ataque de denegación de servicio. Aislar el equipo entero siempre requiere aprobación. Mientras no la actives, el portal te muestra qué habría hecho (modo auditor), para que decidas con datos.

## 7. Actualizaciones de seguridad

Una vez al día, el agente envía la lista de software instalado y InmunoSec la compara con las bases públicas de vulnerabilidades. En **Paquetes > Avisos** verás cada paquete afectado, la versión que lo corrige y su gravedad. Puedes aprobar la actualización desde el portal (el equipo la instala con el gestor de paquetes del sistema) o aplicarla tú.

## 8. Red local: dispositivos de tu red

Activa el inventario en **Red local**. A partir de la siguiente inspección verás los dispositivos que tus equipos ya conocen en su red: IP, dirección MAC, fabricante y qué equipo lo vio. Lo que haya ese primer momento se toma como punto de partida; después, cada dispositivo nuevo genera un aviso.

- **Es mío: marcar como conocido** lo quita de la lista de pendientes.
- **Poner nombre** te ayuda a identificarlo («Impresora oficina»).
- **Olvidar** lo borra; si vuelve a aparecer, se avisará de nuevo.

El inventario es pasivo: el agente lee la tabla de vecinos que el propio sistema ya mantiene y no sondea ni escanea la red. Por eso solo aparecen los dispositivos con los que tus equipos han tenido contacto. Los móviles que cambian su MAC por privacidad se señalan como «MAC aleatoria».

## 9. Informe por correo

En **Perfil > Informe por correo** eliges la frecuencia (diario, semanal los lunes o mensual el día 1) y hasta diez direcciones de correo. Recibirán un PDF con el estado de cada equipo, las alertas del periodo, las actualizaciones pendientes, los dispositivos nuevos de la red y, sobre todo, una lista priorizada de **qué deberías hacer** y cómo. Puedes descargar un PDF de muestra o enviarlo en ese momento para comprobarlo.

## 10. Integraciones opcionales

| Integración    | Para qué sirve                                                                                                                                                        |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Consultor LLM  | Con tu propia clave de un proveedor de IA (Anthropic, OpenAI o Gemini), cada caso incluye una explicación en lenguaje natural. Tiene un límite diario que tú decides. |
| Triaje con Jev | Prioriza los casos con evidencia débil para que revises antes los más probables. Solo recomienda; nunca aprueba.                                                      |
| WPScan         | Si tienes WordPress, consulta las vulnerabilidades de sus plugins y temas.                                                                                            |
| Notificaciones | Envía cada hallazgo, firmado, a la URL que indiques (tu sistema de tickets, Slack, Teams...).                                                                         |

Las claves de terceros se guardan cifradas y solo se envía a cada servicio lo imprescindible.

## 11. Suscripción, facturas y baja

- **Facturas:** en Perfil > Facturas descargas el PDF de cada cobro.
- **Cambiar de tarjeta o darte de baja:** Perfil > Gestionar suscripción. La baja surte efecto al final del mes ya pagado.
- **Si un cobro falla:** se reintenta durante unos días sin cortar el servicio. Si finalmente no se cobra, el portal deja de recibir datos de tus equipos y no se pueden enlazar equipos nuevos. Los agentes guardan lo observado y lo envían si reactivas la suscripción.

## 12. Privacidad y seguridad

- El agente analiza el **comportamiento** del sistema (procesos, usuarios, conexiones, software), no el contenido de tus documentos ni de tus comunicaciones.
- Cada equipo se identifica con su propio certificado y se comunica con InmunoSec por TLS con autenticación mutua.
- En Linux, el agente funciona sin root, con permisos de solo observación; las medidas las aplica un ejecutor aparte que solo acepta órdenes firmadas por tu cuenta.
- Las inspecciones detalladas se conservan 30 días; los datos se alojan en la Unión Europea.
- El acceso al portal exige contraseña y verificación en dos pasos, y cada acción queda registrada.

---

## 13. Problemas frecuentes

| Problema                                             | Qué hacer                                                                                                                                                                                                                        |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| «La clave no es válida o ha caducado»                | Las claves de un equipo duran 24 horas y sirven una vez. Genera otra en Perfil. Comprueba también que la suscripción esté activa.                                                                                                |
| El equipo no aparece en Equipos                      | Espera un minuto y recarga. En Linux revisa «systemctl status inmunosec» y «journalctl -u inmunosec»; en Windows, que la tarea programada InmunoSec Agent esté en ejecución. Comprueba que el equipo puede salir al puerto 8443. |
| Un equipo aparece como silenciado                    | Ha dejado de informar. Si está encendido y nadie ha parado el agente, trátalo como un posible incidente: detener la vigilancia es un paso típico de un atacante.                                                                 |
| Windows: «ejecuta como administrador»                | Abre PowerShell con clic derecho > Ejecutar como administrador y vuelve a pegar la orden.                                                                                                                                        |
| Demasiadas alertas los primeros días                 | Es normal mientras el agente aprende. Rechazar o marcar como esperado lo que reconoces le ayuda; la vista Calidad muestra cómo baja el ruido.                                                                                    |
| He perdido el móvil con la verificación en dos pasos | Escríbenos a <a href="mailto:hola@inmunosec.es">hola@inmunosec.es</a> desde la dirección de la cuenta para verificar tu identidad.                                                                                               |

## 14. Ayuda

Para cualquier duda, escríbenos a [hola@inmunosec.es](mailto:hola@inmunosec.es). Si crees que estás sufriendo un incidente, indícalo en el asunto para que lo atendamos con prioridad.