

Manual de Usuario.

Documentación de producto



OBSERVE | UNDERSTAND | PROTECT



FECHA: 22/09/2026

REFERENCIA: Manual de usuario

VERSIÓN: 2.0

Este documento ha sido creado por Greinfort para su uso exclusivo y su contenido es confidencial. No puede ser divulgado a terceros ni utilizado para fines distintos a aquellos para los que fue entregado sin el permiso previo por escrito de Greinfort. Si se entrega bajo un contrato, su uso y divulgación se limitarán a lo que esté expresamente autorizado en dicho contrato. Greinfort no será responsable de ningún error u omisión en la preparación de este documento.

Índice:

1. Introducción	5
2. Primeros pasos	6
2.1. Acceso a consolas web	6
2.2. Organización de la lista de dispositivos	9
2.3. Análisis de dispositivos inalámbricos	11
2.4. Configuración de reglas.....	11
2.5. Escenarios.....	14
2.6. Escáner activo de dispositivos (opcional).....	14
2.7. Configuración de respuesta activa	14
2.8. Configuración de los informes.....	14
2.9. Exportación de alertas (opcional)	14
2.10. Panel de control continuo (opcional)	15
2.11. Licencias	15
2.12. Control de acceso y funciones	15
2.13. Campos personalizados.....	16
3. Guía rápida.....	16
3.1. Menú	16
3.2. Panel principal	17
3.3. Mapa de red	18
3.4. Lista de dispositivos	20
3.5. Panel de alertas	21
3.6. Lista de comunicaciones.....	22
3.7. Informes.....	23
3.8. Escenarios.....	24
3.8.1. Perfil de usuario.....	24
3.8.2. Preferencias de los usuarios	24
3.8.3. Notificación de alertas.....	25
3.8.4. Gestión de usuarios	26
3.8.5. Configuración de bloqueo de tráfico.....	26
3.8.6. Información.....	27
4. Gestión de aplicación.....	28
4.1. Panel principal	28

4.1.1. Resumen de activos	28
4.1.2. Enlaces rápidos	29
4.1.3. Gráfico de tráfico de red	30
4.1.4. Gráfico de alertas	30
4.1.5. Últimos informes	30
4.2. Mapa de red y lista de dispositivos	31
4.2.1. Mapa de red	31
4.2.2. Lista de dispositivos	32
4.3. Panel de alertas	41
4.3.1. IP pública	44
4.3.2. Política de reputación de IP y bloqueo	45
4.3.3. Lista blanca de IP	47
4.4. Análisis de vulnerabilidades	48
4.4.1. Panel de vulnerabilidades	48
4.4.2. Estadísticas del dispositivo	51
4.4.3. Estadísticas globales	51
4.5. Comunicaciones	51
4.6. Informes	52
4.7. Otros escenarios	52
5. ANEXO I: Clasificación de dispositivos y alertas	54
5.1. Clasificación de dispositivos	54
5.1.1. Según el Estado	54
5.2. Clasificación de alertas	54
5.2.1. Según el Estado	54
5.2.2. Según la gravedad	54
6. ANEXO II: Iconos de Activos y Nivel Purdue	55
7. ANEXO III: Iconos de alertas	57

1. Introducción

Greinfort es una herramienta de detección de activos y de monitorización de anomalías capaz de identificar amenazas de ciberseguridad en entornos industriales. Analiza el tráfico de red, identifica los activos, elabora informes completos y emite alertas mediante reglas estáticas, firmas IDS e inteligencia artificial para facilitar la mitigación de amenazas en la red industrial.

La interfaz de Greinfort es interactiva, fácil de entender y sencilla de utilizar. Además, está disponible en inglés, español, catalán, vasco y gallego.

La interfaz se ha desarrollado con el framework Angular y siguiendo las mejores prácticas y metodologías de seguridad, a fin de garantizar una navegación segura por la información.

La aplicación web ofrece una visión completa de los siguientes aspectos:

- **Panel Continuo:** panel de control autoactualizable para monitorizar los principales aspectos de activos, amenazas e informes 24/7 en un centro de operaciones.
- **Acceso rápido:** a alertas, vulnerabilidades, algoritmos y reglas activas.
- **Gráfico de tráfico de red:** representación del tráfico enviado y recibido durante las últimas 24 horas y comparación con el mismo periodo de siete días antes.
- **Gráfico de alertas:** Gráfico de las alertas recibidas en los últimos 7 días, diferenciadas por color según su nivel de gravedad y la tendencia que siguen a lo largo del tiempo.
- **Mapa de red:** visualización de todos los dispositivos de red, sus conexiones y la estructura de la red de la organización. También permite identificar los dispositivos conectados que no se han considerado legítimos.
- **Gestor de dispositivos:** lista de activos cableados o inalámbricos para su identificación y gestión. Incluye la identificación y el etiquetado de dispositivos, así como su inclusión en la lista negra según el nivel de criticidad. Además, permite definir campos personalizados para clasificar y filtrar los dispositivos de red mediante un inventario virtual que puede organizarse, filtrarse y exportarse.
- **Gestor de alertas:** lista de eventos y alertas de la red OT de la organización, clasificados según el nivel de gravedad. Se muestran mediante códigos de color y se detallan con información dinámica. Se clasifican según su estado (resueltos o silenciados) y se generan a partir de heurísticas, firmas IDS e inteligencia artificial o aprendizaje automático.
- **Integración con sistemas de terceros (SIEM):** Greinfort ofrece la capacidad de enviar las alertas activas generadas a un sistema de terceros como un SIEM (Security Information and Event Management), para su ingesta y correlación con otras fuentes de registro. Para ello, utiliza el protocolo *rsyslog*.
- **Gestor de vulnerabilidades:** Posibilidad de realizar escaneos de vulnerabilidades a petición del cliente y solo a dispositivos seleccionados.
- **Reputación de direcciones IP públicas:** cuando se establecen conexiones con direcciones IP públicas, su reputación se analiza automáticamente y se destacan visualmente aquellas para las que se recomienda una acción activa de mitigación. También es posible cargar una lista de direcciones IP que siempre estarán permitidas.
- **Lista de comunicaciones:** relación de todas las comunicaciones realizadas entre dispositivos de OT de la red de la organización e información sobre estas.
- **Generación de informes:** Compilación de información sobre la red, dispositivos, indicadores, etc., para su análisis y verificación futura tanto a nivel técnico como empresarial.

Además del uso de la aplicación, el servicio requiere una serie de preparativos para el onboarding inicial, entre ellos la recopilación adecuada de datos, el despliegue, la instalación y el fine-tuning de la solución. Estas tareas permiten obtener el máximo rendimiento del servicio y se basan en acciones como las indicadas en la sección siguiente.

2. Primeros pasos

2.1. Acceso a consolas web

En primer lugar, se debe abrir el navegador e introducir la dirección `http://[IP]:9000`, donde IP corresponde a la dirección asignada a la interfaz de gestión.

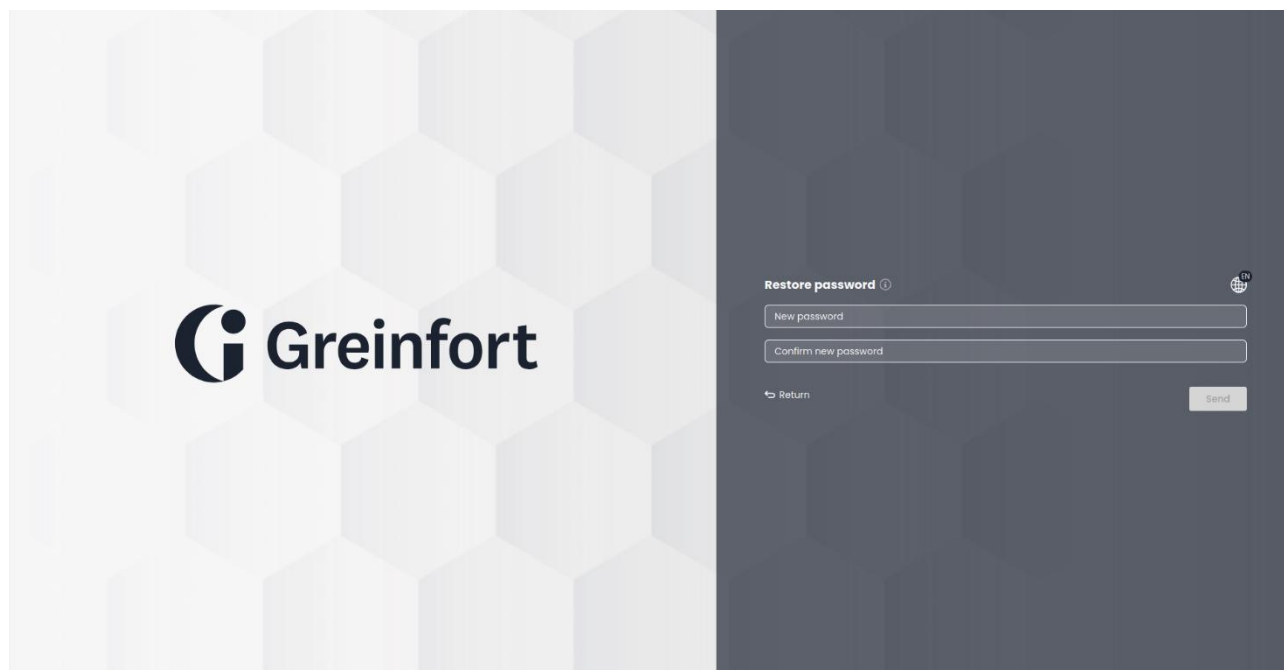


Pantalla de inicio de sesión de Greinfort

El idioma puede seleccionarse en cualquier momento mediante el icono del mapa mundial (inglés, español, catalán, vasco o gallego).

Para autenticarse, se deben introducir el nombre de usuario y la contraseña asignados. Si está activado el segundo factor de autenticación, también se debe introducir el token de un solo uso recibido por correo electrónico en la cuenta asociada al servicio.

Por razones de seguridad, cuando un usuario inicia sesión por primera vez, o cuando un administrador ha marcado la cuenta para requerir un cambio de contraseña, el sistema mostrará automáticamente la pantalla de "Cambiar contraseña" antes de permitir el acceso a la aplicación.



Pantalla obligatoria de cambio de contraseña

En esta pantalla, el usuario debe:

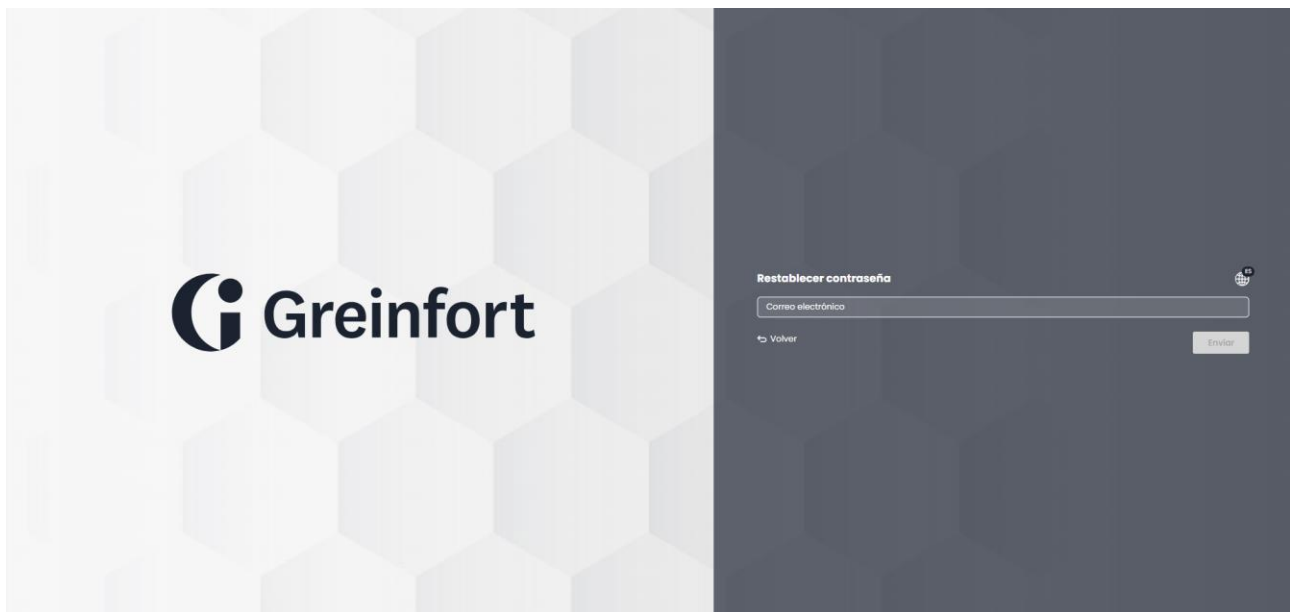
- Introducir la nueva contraseña en el primer campo.
- Confirmar la nueva contraseña en el segundo campo.
- Hacer clic en el botón "Cambiar contraseña" para completar el proceso.

Una vez que la contraseña haya sido cambiada con éxito, se mostrará un mensaje de confirmación y el usuario tendrá acceso a la aplicación. Si la autenticación de dos factores está activada, el usuario también debe introducir el código de verificación recibido por correo electrónico.

El usuario puede ser:

- Administrador: tiene acceso a toda la información presentada por la aplicación y puede realizar las configuraciones necesarias para algoritmos, identificadores de fábrica, modos de producción, etc.
- Operador: tiene el mismo acceso que el administrador, excepto a la configuración específica indicada anteriormente.
- Monitor: dispone exclusivamente de permisos de lectura. Puede descargar manuales e informes, así como exportar resultados de búsqueda y determinadas listas (dispositivos, alertas, vulnerabilidades, comunicaciones, análisis de tráfico, etc.).

En caso de que el usuario haya olvidado o bloqueado su contraseña, tendrá la opción de recuperarla haciendo clic en la opción "He olvidado mi contraseña".

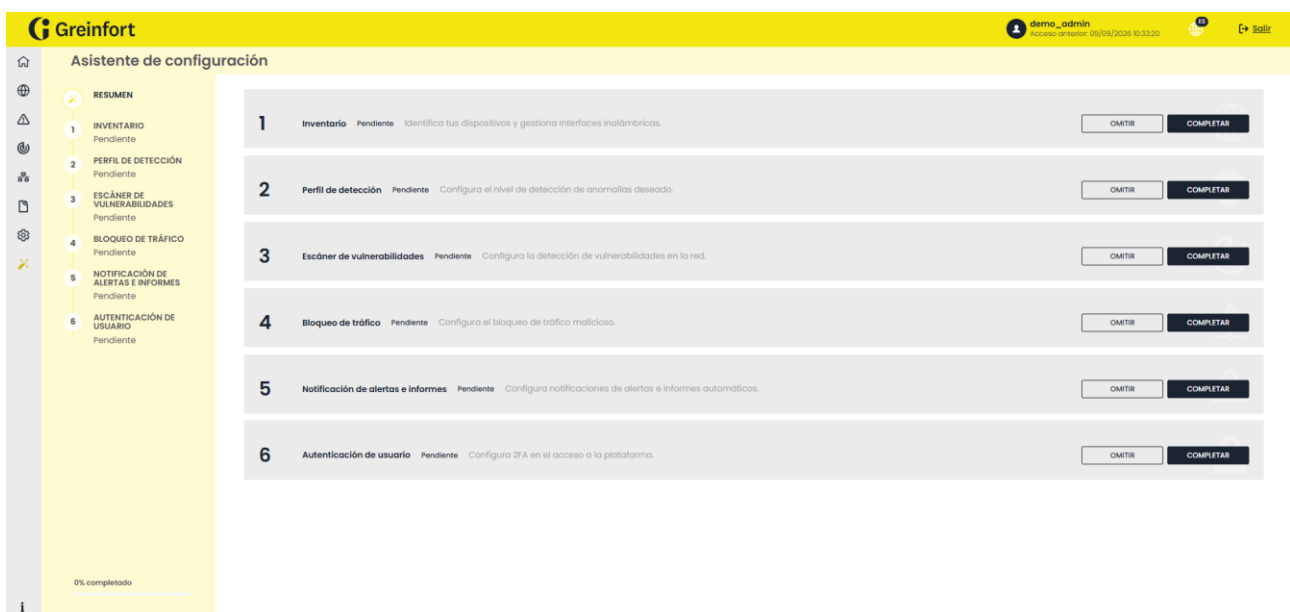


Pantalla de recuperación de contraseña

Al introducir una dirección de correo electrónico válida, se enviará a esa dirección un enlace para restablecer la contraseña de acceso mediante un token de un solo uso.

**Esta funcionalidad, así como otras necesarias para las actualizaciones de software de Greinfort o el acceso remoto, requiere conectividad entre el sistema y determinados servicios de Greinfort o de Internet. Por este motivo, se proporcionará la lista de reglas que deberán aplicarse en el cortafuegos.*

Al iniciar sesión por primera vez, se abre el asistente de configuración de Greinfort, que guía la configuración inicial de la solución. El proceso se divide en seis etapas, cada una de las cuales debe completarse o, alternativamente, omitirse.



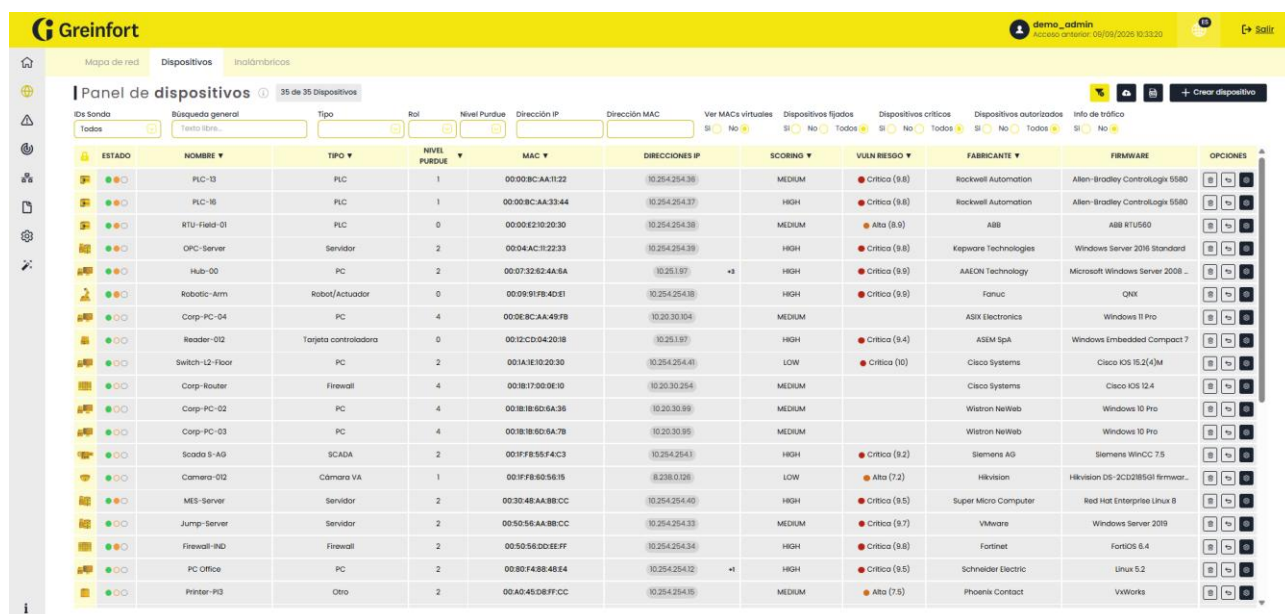
Asistente de configuración inicial

2.2. Organización de la lista de dispositivos

La lista de dispositivos debe organizarse declarando el nombre de cada dispositivo, así como su **nivel PURDUE** (opcional, pues se calculará automáticamente) y su estado (véase Anexo I). Mediante esta declaración, el usuario encontrará más fácil identificar cada dispositivo en las diferentes ventanas de la aplicación y, por tanto, podrá realizar operaciones en cada dispositivo con mayor agilidad, además de extraer más valor del servicio.

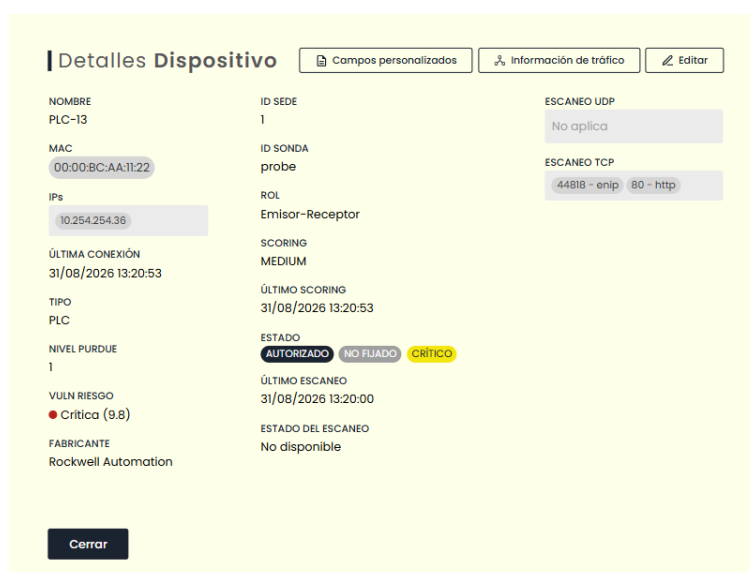
En la primera fase del asistente, se muestra un panel que resume el número de dispositivos no identificados actualmente presentes.

Se debe acceder a la lista de dispositivos haciendo clic en los contadores del asistente. De este modo, se muestra la lista ya filtrada con los dispositivos pendientes de identificación. También se puede acceder a dicha lista mediante el icono del menú y la pestaña "Lista de dispositivos". 



ESTADO	NOMBRE	TIPO	NIVEL PURDUE	MAC	DIRECCIONES IP	SCORE	VULN RIESGO	FABRICANTE	FIRMWARE	OPCIONES
	PLC-13	PLC	1	00:00:BC:AA:11:22	10.254.254.36	MEDIUM	Critica (9.8)	Rockwell Automation	Allen-Bradley ControlLogix 5580	
	PLC-18	PLC	1	00:00:BC:AA:33:44	10.254.254.37	HIGH	Critica (9.8)	Rockwell Automation	Allen-Bradley ControlLogix 5580	
	RTU-Field-01	PLC	0	00:00:E2:10:20:30	10.254.254.38	MEDIUM	Alta (8.9)	ABB	ABB RTU560	
	OPC-Server	Servidor	2	00:04:AC:B2:23:33	10.254.254.39	HIGH	Critica (9.8)	Keypware Technologies	Windows Server 2016 Standard	
	Hub-00	PC	2	00:07:32:82:4A:5A	10.251.197	HIGH	Critica (9.9)	AALON Technology	Microsoft Windows Server 2008 ..	
	Robotic-Arm	Robot/Actuador	0	00:09:91:F8:4D:E1	10.254.254.38	HIGH	Critica (9.9)	Fanuc	ONK	
	Corp-PC-04	PC	4	00:0E:9C:AA:49:F8	10.20.30.104	MEDIUM		ASIX Electronics	Windows 11 Pro	
	Reader-012	Tarjeta controladora	0	00:12:CD:04:20:18	10.251.197	HIGH	Critica (9.4)	ASEM SpA	Windows Embedded Compact 7	
	Switch-L2-Floor	PC	2	00:1A:1E:10:20:30	10.20.30.254	LOW	Critica (10)	Cisco Systems	Cisco IOS 15.2(4)M	
	Corp-Router	Firewall	4	00:1B:17:00:DE:10	10.20.30.254	MEDIUM		Cisco Systems	Cisco IOS 12.4	
	Corp-PC-02	PC	4	00:1B:18:60:5A:36	10.20.30.99	MEDIUM		Wistron NetWeb	Windows 10 Pro	
	Corp-PC-03	PC	4	00:1B:18:60:5A:7B	10.20.30.95	MEDIUM		Wistron NetWeb	Windows 10 Pro	
	Scada S-AG	SCADA	2	00:1F:F8:55:F4:C3	10.254.254.1	HIGH	Critica (9.2)	Siemens AG	Siemens WinCC 7.5	
	Camera-012	Cámara VA	1	00:1F:F8:55:56:15	8.238.0.126	LOW	Alta (7.2)	Hikvision	Hikvision DS-2CD2185G1 firmware...	
	MES-Server	Servidor	2	00:30:4B:AA:8B:CC	10.254.254.40	HIGH	Critica (9.5)	Super Micro Computer	Red Hat Enterprise Linux 8	
	Jump-Server	Servidor	2	00:50:56:AA:8B:CC	10.254.254.33	MEDIUM	Critica (9.7)	VMware	Windows Server 2019	
	Firewall-IND	Firewall	2	00:50:56:D0:EE:FF	10.254.254.34	HIGH	Critica (9.8)	Fortinet	FortiOS 6.4	
	PC Office	PC	2	00:80:F4:9B:4B:E4	10.254.254.12	HIGH	Critica (9.5)	Schneider Electric	Linux 5.2	
	Printer-P13	Otro	2	00:AD:45:D8:FF:CC	10.254.254.16	MEDIUM	Alta (7.5)	Phoenix Contact	VxWorks	

Pantalla de lista de dispositivos



Detalles Dispositivo

Campos personalizados

Información de tráfico

Editar

NOMBRE

PLC-13

ID SEDE

1

ESCANEOP UDP

No aplica

MAC

00:00:BC:AA:11:22

ID Sonda

probe

ESCANEOP TCP

44818 - enip 80 - http

IPs

10.254.254.36

ROL

Emisor-Receptor

ÚLTIMA CONEXIÓN

31/08/2026 13:20:53

SCORE

MEDIUM

TIPO

PLC

ÚLTIMO SCORE

31/08/2026 13:20:53

NIVEL PURDUE

1

ESTADO

AUTORIZADO NO FIJADO CRÍTICO

VULN RIESGO

Critica (9.8)

ÚLTIMO ESCANEOP

31/08/2026 13:20:00

FABRICANTE

Rockwell Automation

ESTADO DEL ESCANEOP

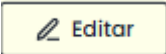
No disponible

Cerrar

Ventana emergente de detalles del dispositivo

Para modificar un dispositivo, se debe hacer clic en el botón correspondiente; a continuación, se abre la pestaña de edición. Después, se debe hacer clic en el botón de edición para modificar el

dispositivo seleccionado.



Editar Dispositivo

[← Ir a detalles](#)

Nombre
PLC-13

Tipo
PLC

Nivel Purdue
Nivel 1

Fijado*
Sí ☐ No ☒

Crítico*
Sí ☒ No ☐

Autorizado*
Sí ☒ No ☐

* Campos obligatorios

Cancelar Guardar

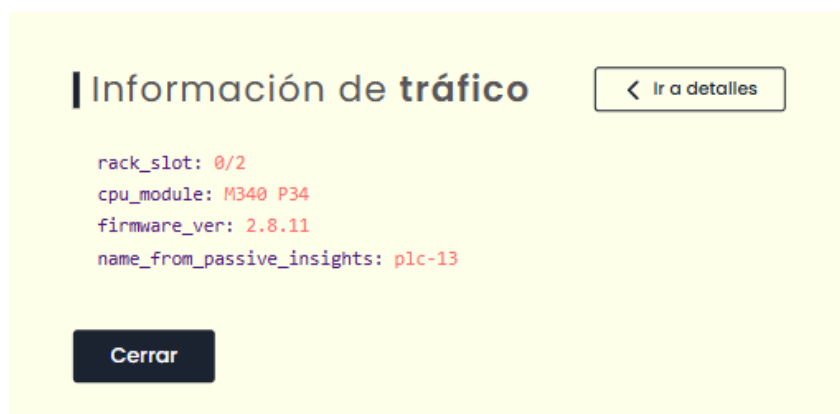
Pantalla de edición de dispositivos

A continuación, se deben completar manualmente el nombre y el nivel Purdue del dispositivo, y seleccionar su estado para indicar si es fijo, crítico o autorizado (véanse las definiciones del Anexo I).

Para hacer cambios masivos de forma más ágil, esta configuración puede hacerse directamente en la lista de activos haciendo clic en el icono del candado y aceptando en la ventana emergente de confirmación.

Una vez hecho esto, se hace clic en el botón "Guardar" para que los cambios sean efectivos en el sistema.

Si el sistema de inventario pasivo está activado en la sonda (opción por defecto), algunos campos de los dispositivos se actualizan automáticamente, bien en la columna correspondiente, bien dentro de una colección denominada "Información de tráfico", accesible desde el menú de cada dispositivo.



Información de tráfico

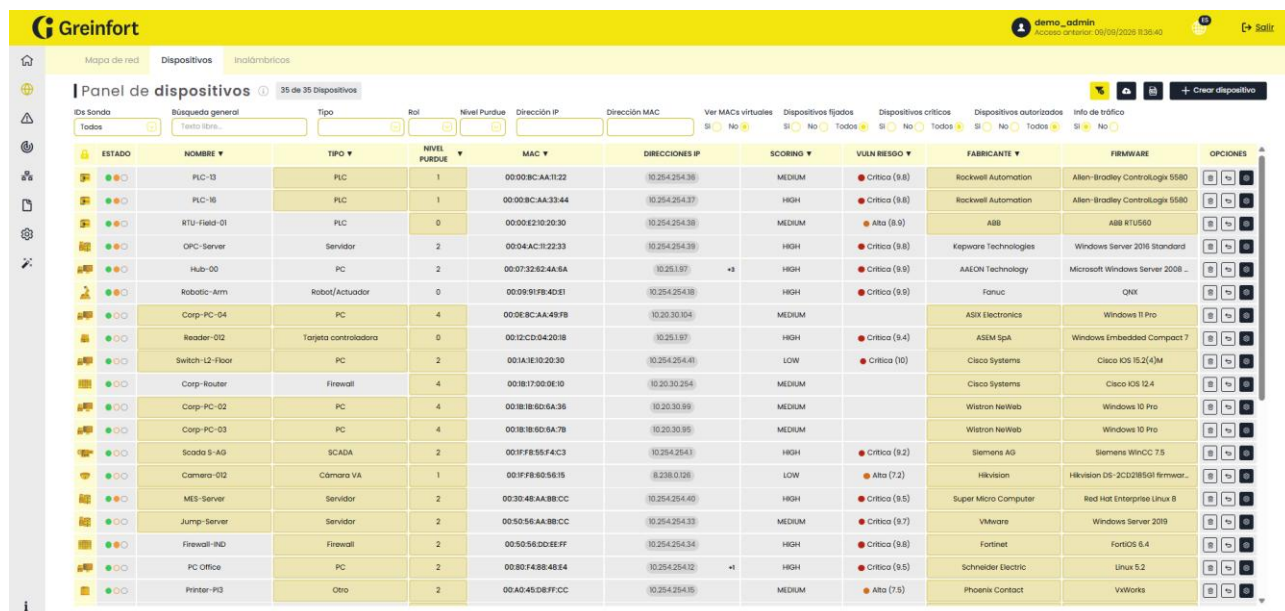
[← Ir a detalles](#)

rack_slot: 0/2
cpu_module: M340 P34
firmware_ver: 2.8.11
name_from_passive_insights: plc-13

Cerrar

Ventana emergente de información de tráfico

Los cambios realizados directamente por el usuario en algunas de las columnas tienen prevalencia con respecto a estas actualizaciones automáticas, que quedarán relegadas a esta colección en caso de conflicto. Existe un filtro en el panel, "Info de tráfico", que permite resaltar qué campos provienen de inferencias hechas por el sistema de inventario pasivo.



ESTADO	NOMBRE	TIPO	NIVEL PUNQUE	MAC	DIRECCIONES IP	SCORING	VULN RIESGO	FABRICANTE	FIRMWARE	OPCIONES
	PLC-13	PLC	1	00:00:8C:AA:11:22	10.254.254.36	MEDIUM	Critico (9.8)	Rockwell Automation	Allen-Bradley ControlLogix 5580	
	PLC-16	PLC	1	00:00:8C:AA:33:44	10.254.254.37	HIGH	Critico (9.8)	Rockwell Automation	Allen-Bradley ControlLogix 5580	
	RTU-Field-01	PLC	0	00:00:E2:10:20:30	10.254.254.38	MEDIUM	Alto (8.9)	ABB	ABB RTU560	
	OPC-Server	Servidor	2	00:04:AC:11:22:33	10.254.254.39	HIGH	Critico (9.8)	Keapware Technologies	Windows Server 2016 Standard	
	Hub-00	PC	2	00:07:32:62:4A:5A	10.251.67	HIGH	Critico (9.9)	AAEON Technology	Microsoft Windows Server 2008 ..	
	Robot-01	Robot/Actuador	0	00:09:91:F8:4D:E1	10.254.254.18	HIGH	Critico (9.9)	Fanuc	QNX	
	Corp-PC-04	PC	4	00:0E:9C:AA:49:F8	10.20.30.104	MEDIUM		ASIX Electronics	Windows 11 Pro	
	Reader-012	Yangeta controladora	0	00:12:CD:04:20:18	10.251.67	HIGH	Critico (9.4)	ASEM SpA	Windows Embedded Compact 7	
	Switch-L2-Floor	PC	2	00:1A:1E:10:20:30	10.254.254.41	LOW	Critico (10)	Cisco Systems	Cisco IOS 15.2(4)M	
	Corp-Router	Firewall	4	00:18:17:00:DE:10	10.20.30.254	MEDIUM		Cisco Systems	Cisco IOS 12.4	
	Corp-PC-02	PC	4	00:18:18:60:6A:36	10.20.30.99	MEDIUM		Wistron NetWeb	Windows 10 Pro	
	Corp-PC-03	PC	4	00:18:18:60:6A:7B	10.20.30.95	MEDIUM		Wistron NetWeb	Windows 10 Pro	
	Scada S-AG	SCADA	2	00:1F:F8:55:F4:C3	10.254.254.1	HIGH	Critico (9.2)	Siemens AG	Siemens WinCC 7.5	
	Camera-012	Cámara VA	1	00:1F:F8:60:56:15	8.238.0.106	LOW	Alto (7.2)	Hikvision	Hikvision DS-2CCD1850G1 firmware..	
	MES-Server	Servidor	2	00:30:4B:AA:8B:CC	10.254.254.40	HIGH	Critico (9.5)	Super Micro Computer	Red Hat Enterprise Linux 8	
	Jump-Server	Servidor	2	00:50:56:AA:8B:CC	10.254.254.33	MEDIUM	Critico (9.7)	VMware	Windows Server 2019	
	Firewall-IND	Firewall	2	00:50:56:D0:EE:FF	10.254.254.34	HIGH	Critico (9.8)	Fortinet	FortiOS 6.4	
	PC Office	PC	2	00:80:F4:8B:4B:E4	10.254.254.12	HIGH	Critico (9.5)	Schneider Electric	Linux 5.2	
	Printer-013	Otro	2	00:AD:45:D6:FF:CC	10.254.254.16	MEDIUM	Alto (7.5)	Phoenix Contact	VWWorks	

Panel de dispositivos con el filtro "Info de tráfico" activado

2.3. Análisis de dispositivos inalámbricos

Si se desea y las sondas de recopilación de tráfico disponen del hardware adecuado, el escaneo inalámbrico de dispositivos puede configurarse en esta primera etapa. Para ello, se deben configurar las interfaces que se van a utilizar; la sonda buscará los dispositivos inalámbricos de su zona de influencia.

Para obtener más detalles, consúltase la sección "Air Watcher" de "Gestión de aplicaciones".

2.4. Configuración de reglas

El sistema Greinfort realiza la detección de amenazas basándose en múltiples criterios de comportamiento, tales como:

- Amenazas basadas en reglas parametrizables predefinidas
- Amenazas basadas en firmas IDS
- Amenazas basadas en algoritmos de IA/ML
- Amenazas de honeypot

A partir de la segunda etapa del asistente de configuración, se puede simplificar la configuración seleccionando uno de los tres perfiles de seguridad predefinidos (modo básico), o editar manualmente las reglas, los parámetros y los filtros a partir de uno de ellos (modo avanzado).

| 2. Perfil de detección

Selecciona el modo de configuración
Elige tu perfil de seguridad (detección de anomalías).

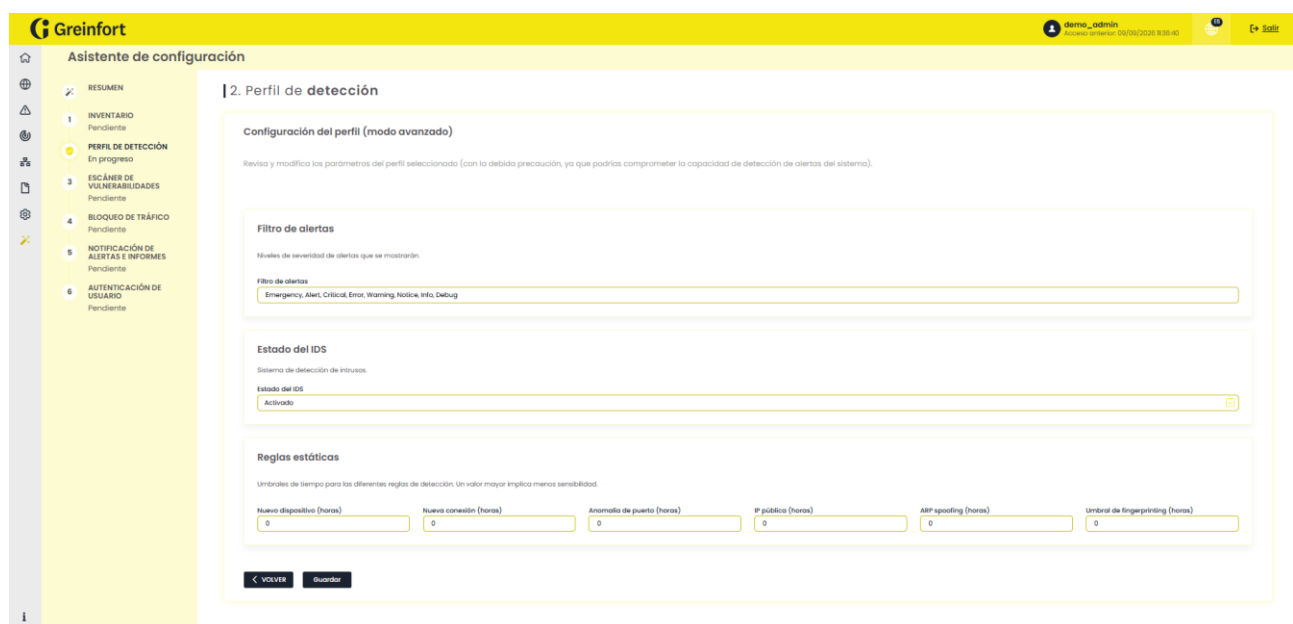
Modo Estándar
Configuración rápida mediante perfiles predefinidos. Ideal para empezar.

Modo Avanzado
Configura los parámetros específicos de cada perfil según tus necesidades.

Selección del perfil de seguridad

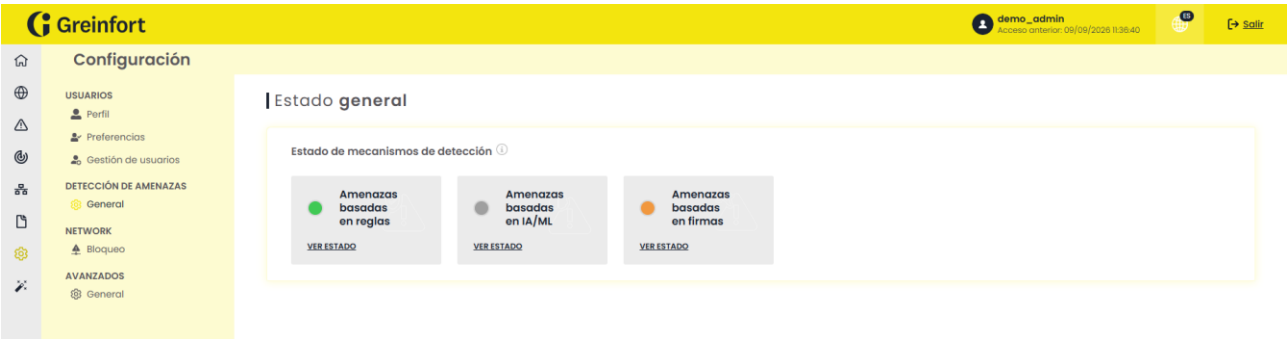
En la edición manual, se deben configurar las reglas que se desea mantener activas para analizar la red de la organización, así como los intervalos de supresión de cada alerta cuando proceda. También se puede establecer un filtro para determinar el nivel de gravedad a partir del cual se envían alertas al portal web.

El intervalo de supresión de una regla permite establecer un umbral temporal durante el cual las reglas configuradas no generan una nueva alerta ante un escenario idéntico. De este modo se evitan advertencias innecesarias sobre situaciones ya conocidas.



Configuración avanzada de reglas

Además, se pueden configurar otros parámetros, que se describen más adelante. Para configurar estos intervalos, se debe abrir el menú lateral y seleccionar Detección de amenazas > General > Amenazas basadas en reglas > VER ESTADO. 



Estado de mecanismos de detección

Motor de reglas ⓘ 6 Reglas ⓘ

	NOMBRE	ESTADO	UMBRALES	OPCIONES
✓	NewDevice	Production	1 ⓘ	✎
✓	ARPAAttack	Production	1 ⓘ	✎
✓	Fingerprinting	Production	5-3-3 ⓘ	✎
✓	PublicIP	Production	1 ⓘ	✎
✓	PortAnomaly	Production	1 ⓘ	✎
✓	NewConnection	Production	1 ⓘ	✎

Motor de reglas

En la columna de umbrales se pueden consultar rápidamente los valores configurados para cada regla.

UMBRALES	OPCIONES
1 ⓘ	✎
1 ⓘ	✎
5-3-3 ⓘ	✎
1 ⓘ	✎
1 ⓘ	✎
1 ⓘ	✎

Umbrales de regla de detección

Estos parámetros se pueden editar desde la columna de acciones.



Edición de reglas

Cuando esté disponible, esta sección también incluirá la configuración de los mensajes asociados a las notificaciones de alertas y a los informes que se desea recibir.

2.5. Escenarios

Los ajustes básicos del perfil de usuario, la seguridad y las preferencias de notificación se encuentran en la sección "Configuración" de la guía rápida. Se recomienda revisarlos y adaptarlos a las necesidades del entorno.

2.6. Escáner activo de dispositivos (opcional)

De forma opcional, en la tercera etapa del asistente se puede activar el motor de consultas de dispositivos y configurar la frecuencia de escaneo para obtener propiedades adicionales de los nodos, como la versión del firmware, los puertos abiertos y los servicios en ejecución. Debe tenerse en cuenta que se trata de un escaneo activo y que puede interferir con determinados dispositivos.

Para obtener más detalles, consúltase la sección "Smart View" de "Gestión de aplicaciones".

2.7. Configuración de respuesta activa

En la cuarta etapa del asistente se pueden configurar el sistema de comprobación de reputación y el bloqueo de tráfico. Es posible activar estas funciones, elegir el modo de funcionamiento y configurar la integración con el cortafuegos para utilizar el bloqueo de tráfico. Los modos y parámetros disponibles se describen más adelante.

2.8. Configuración de los informes

En la etapa siguiente se puede configurar la generación de informes de Greinfort. La funcionalidad puede activarse o desactivarse y también puede definirse la frecuencia de generación.

2.9. Exportación de alertas (opcional)

De forma opcional, en esta misma quinta etapa del asistente se puede habilitar el envío automático de las alertas generadas a un servidor syslog de un SIEM o sistema similar, para su ingesta y correlación* con otras fuentes de registro.

Solo se deben proporcionar la dirección IP y el puerto de destino de los mensajes, así como el protocolo que se utilizará (syslog o syslog cifrado).

* Para estos fines, es importante señalar que todas las marcas de tiempo devueltas por la aplicación web se muestran en UTC.

2.10. Panel de control continuo (opcional)

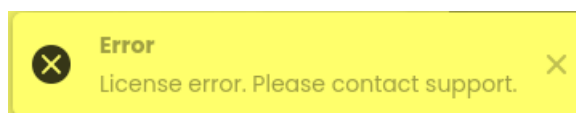
Para consultar de forma permanente el estado de Greinfort y sus indicadores principales (dispositivos no autorizados, tráfico de red, alertas, etc.), el panel principal del aplicativo puede mostrarse en un monitor de la sala de operaciones del cliente, con actualización automática cada cinco minutos.

Para ello, se debe solicitar al servicio de Soporte de Greinfort la creación de un usuario de monitorización.

2.11. Licencias

Permite prestar el servicio Greinfort de forma temporal con fines de prueba y una ventana de uso limitada.

Si se muestra el mensaje "Error de licencia. Contacta con Soporte.", significa que faltan los archivos de licencia o que esta ha caducado.



Detalle del error de licencia

2.12. Control de acceso y funciones

Esta función permite controlar el acceso y las acciones realizadas en el sistema. Su implementación añade una capa de seguridad y privacidad al tratamiento de la información y de los recursos.

Este sistema de control de roles y accesos cuenta con las siguientes características:

- **Roles y permisos predefinidos:** permiten determinar los niveles de acceso y control del sistema.
- **Asignación de permisos a usuarios y grupos:** el sistema permite asignar permisos a usuarios y grupos según sus roles y responsabilidades en la organización.
- **Gestión de grupos de usuarios:** permite asignar permisos a varios usuarios al mismo tiempo y facilita su administración.
- **Control de acceso a recursos:** permite controlar el acceso a los distintos recursos de Greinfort mediante permisos específicos.

Los roles a implementar serán los siguientes:

- **Administrador:** dispone de acceso completo a la configuración, las operaciones del servicio y los registros. También puede alternar entre entornos de entrenamiento y producción, y modificar los conjuntos de algoritmos de IA cuando sea necesario.
- **Operador:** modo de usuario privilegiado de la fábrica. Permite modificar los datos visibles de la interfaz, como los datos de los dispositivos, y marcar las alertas como resueltas o silenciadas.

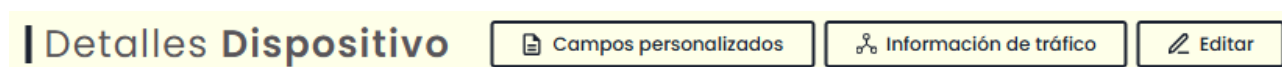
- **Monitor:** modo de usuario estándar de la fábrica, con permisos más restringidos. Solo permite consultar datos y descargar informes o archivos CSV.

2.13. Campos personalizados

Si se necesitan nuevos campos en la lista de dispositivos para mejorar su categorización, pueden definirse en formato clave-valor mediante un archivo CSV.

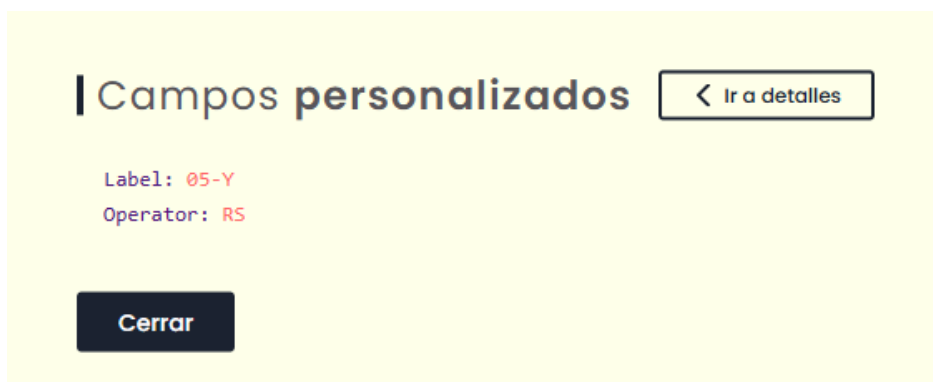
Se debe añadir un archivo desde el botón del panel de dispositivos. Las filas deben incluir los dispositivos que se desee incorporar, junto con los nuevos campos personalizados en cualquiera de los formatos descritos en la sección “Lista de dispositivos” > “Importación mediante CSV” .

Los campos cargados pueden consultarse desde el panel de dispositivos mediante el enlace “Ver Campos personalizados”.



Campos personalizados del dispositivo

Esta acción abre una nueva ventana modal en la que pueden consultarse los campos.



Detalle de los campos personalizados

3. Guía rápida

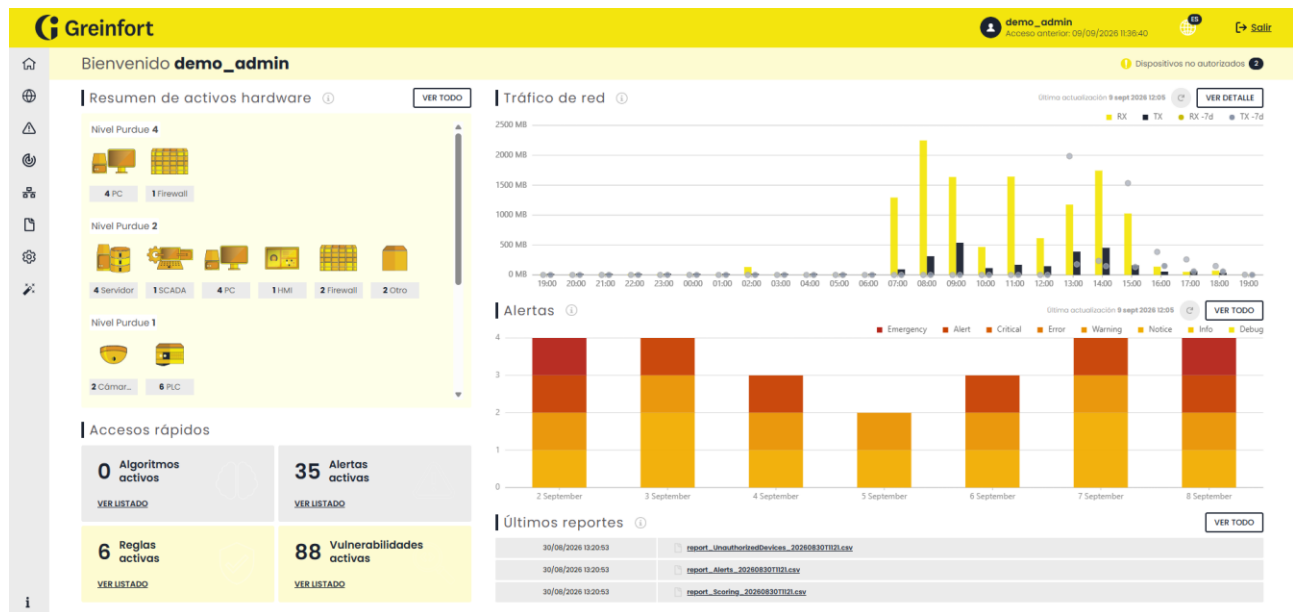
3.1. Menú



Detalle de la ventana de acceso

- 1: Inicio: Panel principal
- 2: Red: Mapa de red y lista de dispositivos
- 3: Alertas: Lista de alertas
- 4: Vulnerabilidades: Lista de vulnerabilidades
- 5: Sesiones de tráfico: Lista de comunicaciones entre dispositivos
- 6: Informes: Lista de informes automáticos
- 7: Configuración: Ventana de configuración de parámetros
- 8: Asistente: guía para realizar la configuración inicial de la solución
- 9: Información: documentación, versión del sistema y registro de cambios

3.2. Panel principal



Vista principal del panel de control

Barra superior:

Tipo de sesión y fecha del acceso anterior.

Idioma de la aplicación.

Cierre de la sesión activa.

Dispositivos no autorizados detectados.

Widget superior izquierdo:

Número de activos en la organización ordenados por [modelo Purdue](#).

Widget superior derecho:

Representación gráfica del tráfico de red enviado y recibido, en bit/s, durante las últimas 24 horas, y comparación con el mismo periodo de siete días antes.

Widget inferior izquierdo:

Atajos a los listados

Vulnerabilidades activas (en construcción)

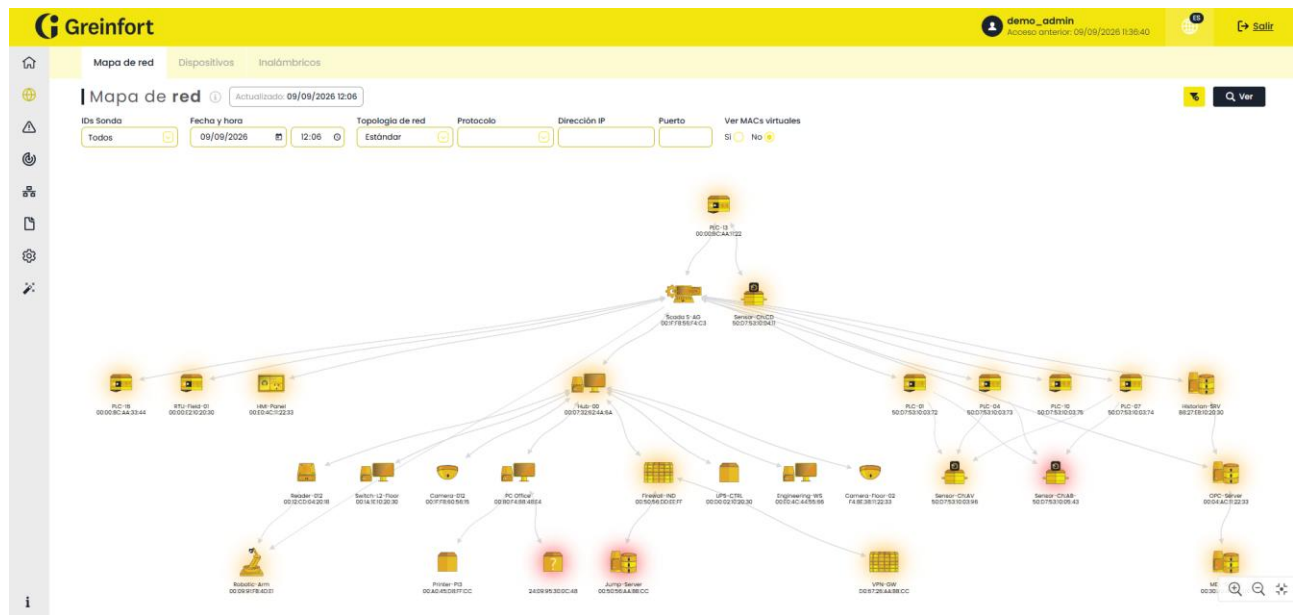
Widgets en la parte inferior derecha:

Representación gráfica del número de alertas según su gravedad.

Acceso a la lista de informes generados

3.3. Mapa de red

El mapa de red presenta dos vistas topológicas: red clásica o por niveles [de PURDUE](#). En el primer caso:



Ventana de mapa de red en vista clásica.

En la parte superior, hay una pestaña para seleccionar la vista del mapa de red, la fecha de la última actualización de la representación gráfica de la topología, así como un botón para hacer efectivos los filtros introducidos.

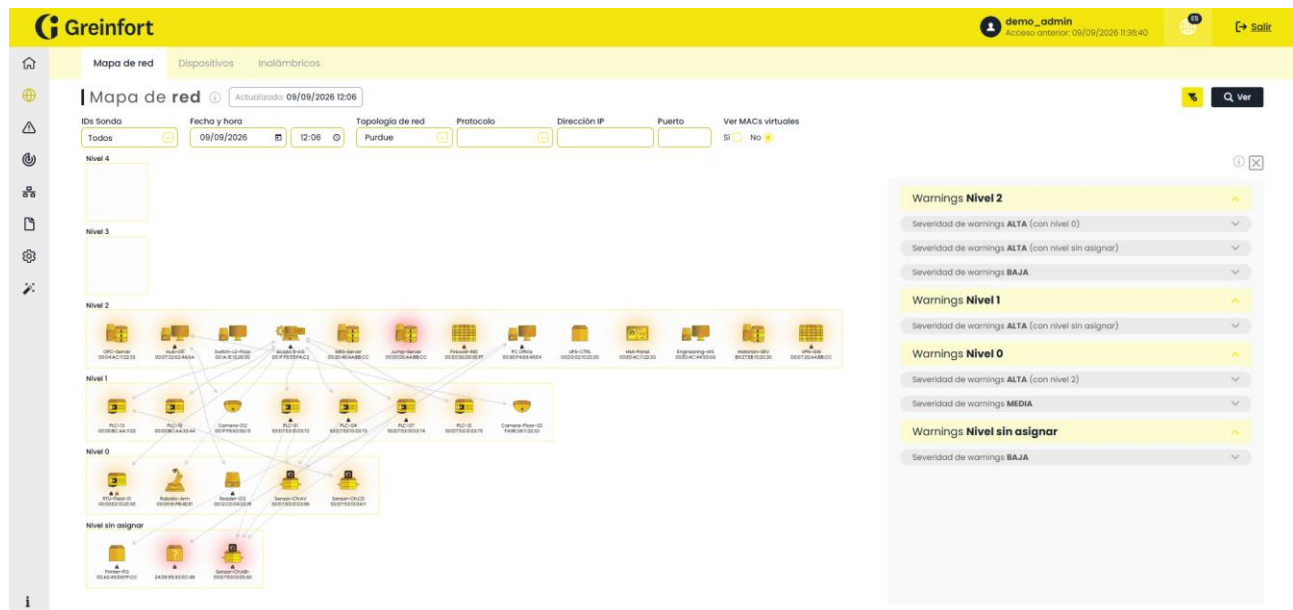
La siguiente fila muestra los posibles filtros para ver los dispositivos de interés en la pantalla.

A continuación se muestran el mapa y la topología de los dispositivos de la red de la organización.

Se debe tener en cuenta lo siguiente:

- Al situar el cursor sobre un nodo o enlace, se muestran sus propiedades.
- Al hacer clic en un nodo o enlace, se accede, respectivamente, a la vista de detalle para editar las propiedades del dispositivo o a la sección de comunicaciones filtrada por el origen del enlace.

En la vista Purdue de la topología, el cumplimiento de las comunicaciones se analiza de acuerdo con la norma ISA/IEC 62443. Las advertencias se clasifican como de gravedad alta (comunicaciones entre niveles no adyacentes), media (asignaciones de niveles Purdue que pueden resultar cuestionables) o baja (niveles sin asignar o recomendación de revisión manual para determinados tipos de dispositivos).



Mapa de red en vista Purdue

En la vista gráfica, situada en el lado izquierdo de la ventana:

- Solo se muestran comunicaciones entre niveles distintos, no aquellas entre dispositivos del mismo nivel.
- Mediante iconos triangulares situados bajo la imagen del dispositivo se indica si este está afectado por alguna advertencia de cumplimiento normativo. Los diferentes colores representan advertencias de gravedad alta, media o baja, según corresponda.
- Se puede hacer clic en los dispositivos para filtrar las advertencias en el lado derecho que se aplican al nodo en cuestión. Si el filtro no está marcado, todos los dispositivos detectados se muestran, en orden descendente de niveles y gravedad.

El resto de las opciones de filtrado son iguales a las de la vista clásica. En el lado derecho de la ventana se muestran las advertencias globales o las asociadas al dispositivo seleccionado.

3.4. Lista de dispositivos

En la pestaña de la lista de dispositivos se muestra, junto al título del panel, el número de dispositivos que cumplen el filtro actual frente al total registrado en la base de datos. En el lado derecho se encuentra el panel de botones para eliminar los filtros, exportar la lista en formato CSV y registrar manualmente un dispositivo.

Panel de dispositivos 35 de 35 Dispositivos											
ESTADO	NOMBRE	TIPO	NIVEL	PURDUE	MAC	DIRECCIONES IP	SCORING	VULN RIESGO	FABRICANTE	FIRMWARE	OPCIONES
	PLC-13	PLC	1	00:00:9C:AA:11:22	10.254.254.36	MEDIUM	Critica (9.8)	Rockwell Automation	Allen-Bradley ControlLogix		
	PLC-16	PLC	1	00:00:9C:AA:33:44	10.254.254.37	HIGH	Critica (9.8)	Rockwell Automation	Allen-Bradley ControlLogix		
	RTU-Field-01	PLC	0	00:00:23:10:20:30	10.254.254.38	MEDIUM	Alta (8.9)	ABB	ABB RTU560		
	OPC-Server	Servidor	2	00:04:AC:11:22:33	10.254.254.39	HIGH	Critica (9.8)	Keypware Technologies	Windows Server 2016 Sta...		
	Hub-00	PC	2	00:07:32:62:AA:5A	10.25.197	HIGH	Critica (9.9)	AAEON Technology	Microsoft Windows Serve...		
	Robotic-Arm	Robot/Actuador	0	00:09:91:F8:4D:E1	10.254.254.18	HIGH	Critica (9.9)	Fanuc	QNX		
	Corp-PC-04	PC	4	00:0E:8C:AA:49:F8	10.20.30.104	MEDIUM		ASIX Electronics	Windows 11 Pro		
	Reader-012	Tarjeta controladora	0	00:12:CD:04:20:18	10.25.197	HIGH	Critica (9.4)	ASEM SpA	Windows Embedded Ca...		
	Switch-L2-Floor	PC	2	00:1A:1E:10:20:30	10.254.254.41	LOW	Critica (10)	Cisco Systems	Cisco IOS 15.2(4)M		
	Corp-Router	Firewall	4	00:1B:17:00:0E:10	10.20.30.254	MEDIUM		Cisco Systems	Cisco IOS 12.4		
	Corp-PC-02	PC	4	00:1B:1B:6D:6A:36	10.20.30.99	MEDIUM		Wistron NetWeb	Windows 10 Pro		
	Corp-PC-03	PC	4	00:1B:1B:6D:6A:76	10.20.30.95	MEDIUM		Wistron NetWeb	Windows 10 Pro		
	Scada S-AG	SCADA	2	00:3F:F8:55:F4:C3	10.254.254.1	HIGH	Critica (9.2)	Siemens AG	Siemens WinCC 7.5		
	Camara-012	Cámara VA	1	00:3F:F8:60:56:15	8.238.0.126	LOW	Alta (7.2)	Hikvision	Hikvision DS-2CD21850I FL		
	MES-Server	Servidor	2	00:30:4B:AA:BB:CC	10.254.254.40	HIGH	Critica (9.5)	Super Micro Computer	Red Hat Enterprise Linux 8		
	Jump-Server	Servidor	2	00:50:56:AA:BB:CC	10.254.254.33	MEDIUM	Critica (9.7)	VMware	Windows Server 2019		

Ventana de lista de dispositivos

La siguiente fila incluye los posibles filtros aplicables para mantener los dispositivos de interés.

La lista de activos contiene información sobre ellos y botones para realizar ciertas acciones (ver detalles, editarlos, eliminarlos o acceder a alertas, comunicaciones o vulnerabilidades presentes). Es posible ordenar los dispositivos alfabéticamente, directa o inversamente, haciendo clic en cualquiera de las columnas.

La tercera pestaña contiene el inventario de dispositivos inalámbricos detectados en las proximidades de los colectores de tráfico (si hay hardware compatible disponible y la funcionalidad está habilitada).

3.5. Panel de alertas

Alertas

</

Sección de alertas

Junto al título de la sección se muestra el número de alertas de la red de la organización que cumplen el filtro frente al total. En el lado derecho se encuentra el panel de botones para eliminar los filtros, exportar la lista en formato CSV o crear manualmente una alerta.

La fila siguiente incluye los filtros disponibles. Debe tenerse en cuenta que el campo de búsqueda general utiliza el criterio CONTAINS y permite buscar en el campo de notas internas de la alerta, visible en "Detalles".

Por último, se muestra la lista de alertas con la información asociada y los botones para actualizar su estado*, acceder a los detalles o añadir notas.

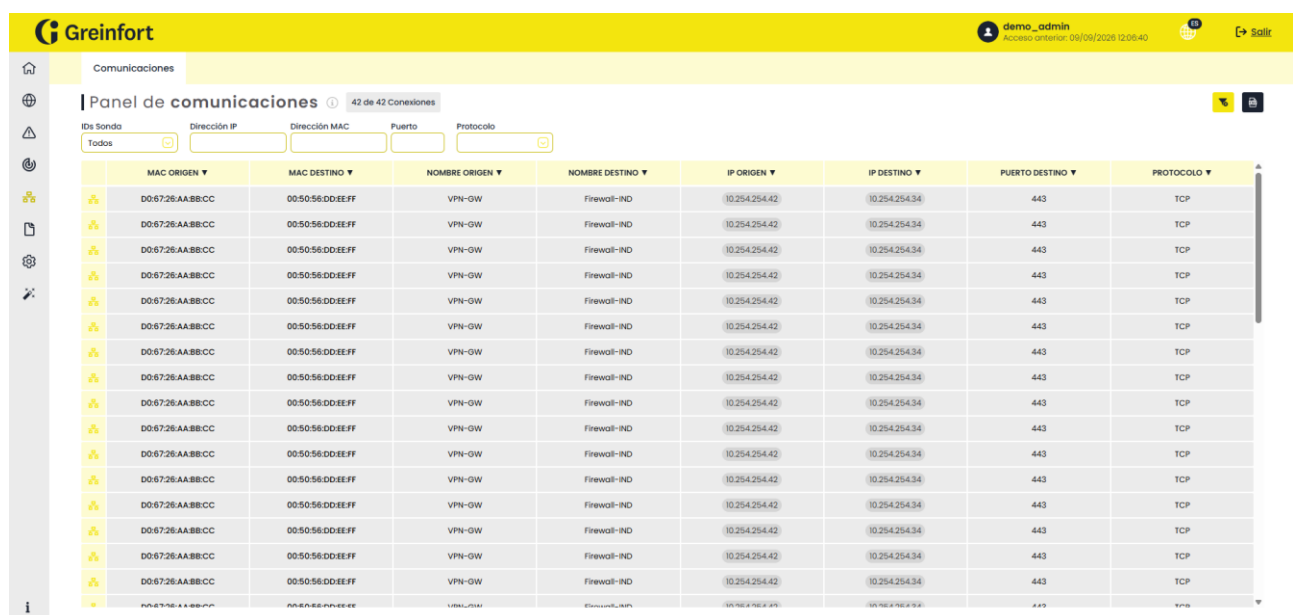
Como se observa en la imagen, cuando un dispositivo tiene un nombre asignado aparece un signo de exclamación junto a la dirección MAC. Al situar el cursor sobre él, se muestra el nombre asociado a esa dirección.

Si la política de bloqueo está activa en cualquiera de sus modos (informativo, manual o automático), las alertas asociadas a direcciones IP públicas clasificadas como maliciosas se resaltan en rojo intenso. El tono se atenúa si la dirección figura en la lista de bloqueo del cortafuegos industrial.

*Para conocer las opciones de cambio de estado, consúltense las definiciones del Anexo I.

3.6. Lista de comunicaciones

Una comunicación se define como un conjunto de conexiones que comparten las direcciones MAC, las direcciones IP y los puertos de origen y destino. Si cambia el protocolo, se considera una comunicación distinta.



MAC ORIGEN	MAC DESTINO	NOMBRE ORIGEN	NOMBRE DESTINO	IP ORIGEN	IP DESTINO	PUERTO DESTINO	PROTOCOLO
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP

Ventana de lista de comunicaciones

En esta sección se muestra, junto al título, el número de comunicaciones que cumplen el filtro actual frente al total registrado en la base de datos. En el lado derecho se encuentran los botones para eliminar los filtros y exportar la lista en formato CSV.

En la fila siguiente se muestran los filtros disponibles para localizar las comunicaciones de interés.

Por último, se muestra la lista de comunicaciones y su información. Las comunicaciones pueden ordenarse alfabéticamente, de forma ascendente o descendente, haciendo clic en cualquiera de las columnas.

3.7. Informes

Esta sección permite descargar informes de varios tipos generados automáticamente por el sistema. Por defecto Greinfort genera informes semanales en archivos CSV descargables de los siguientes ámbitos:

- Dispositivos conectados no autorizados
- Últimas alertas detectadas
- Asociaciones MAC-IP
- IPs públicas (IPs externas conectadas)
- Informe de Puntuación de Riesgo (puntuación)
- Vulnerabilidades

Si el dispositivo tiene un nombre asignado, este sustituye a la dirección MAC en los informes de alertas. En las descargas manuales de búsquedas desde el panel de alertas o la lista de dispositivos, la sección "Últimos informes" muestra ambos campos por separado.

El usuario podrá descargar los informes más recientes generados desde el acceso directo principal del Panel de Control.

Últimos reportes ⓘ		VER TODO
30/08/2026 13:20:53	report_UnauthorizedDevices_20260830T1121.csv	
30/08/2026 13:20:53	report_Alerts_20260830T1121.csv	
30/08/2026 13:20:53	report_Scoring_20260830T1121.csv	

Últimos informes sobre el Panel principal

Además, Greinfort dispone de una sección dedicada a los informes, en la que se puede utilizar el motor de búsqueda para filtrar y descargar el informe de interés:

Greinfort				
		demo_admin	Acceso anterior: 09/09/2026 12:05:40	Salir
Informes				
Panel de reportes ⓘ 7 de 7 Reportes				
Tipo	Fecha y hora de inicio	Fecha y hora de fin		
	dd/mm/yyyy	dd/mm/yyyy		
TIPO DE FICHERO	FECHA DE CREACIÓN		FORMATO	OPCIONES
Dispositivos no autorizados	30/08/2026 13:20		CSV	A
Alertas	30/08/2026 13:20		CSV	A
Scoring	30/08/2026 13:20		CSV	A
IPs públicas	30/08/2026 13:20		CSV	A
MACs & IPs	30/08/2026 13:20		CSV	A
Dispositivos inalámbricos	30/08/2026 13:20		CSV	A
Vulnerabilidades	30/08/2026 13:20		CSV	A

Vista de lista de informes

Junto al título, se muestran el total de informes generados y, a la derecha, el botón de reinicio del filtro.

En la fila siguiente se muestran los distintos filtros de búsqueda.

Por último, está la cuadrícula con los informes disponibles en formato CSV para descargar.

3.8. Escenarios

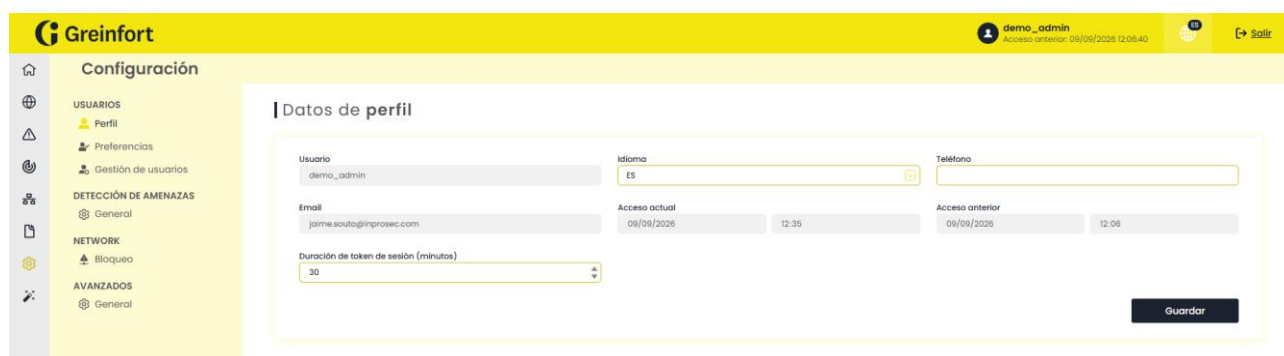
En esta sección se pueden ajustar el perfil y el servicio, así como modificar parámetros relacionados con la detección de amenazas, las alertas y la gestión de usuarios.

A continuación se resumen los aspectos más relevantes a nivel de usuario.

3.8.1. Perfil de usuario

Esta sección muestra información básica como el nombre de usuario, el correo electrónico asociado, la fecha y hora de la última conexión y de la conexión actual, la preferencia de idioma (EN/ES/CAT/EU/GL), el número de teléfono de contacto y la duración del token de sesión en minutos. Los tres últimos campos son editables.

El usuario puede acceder a ella desde  "Configuración" en el menú lateral izquierdo.

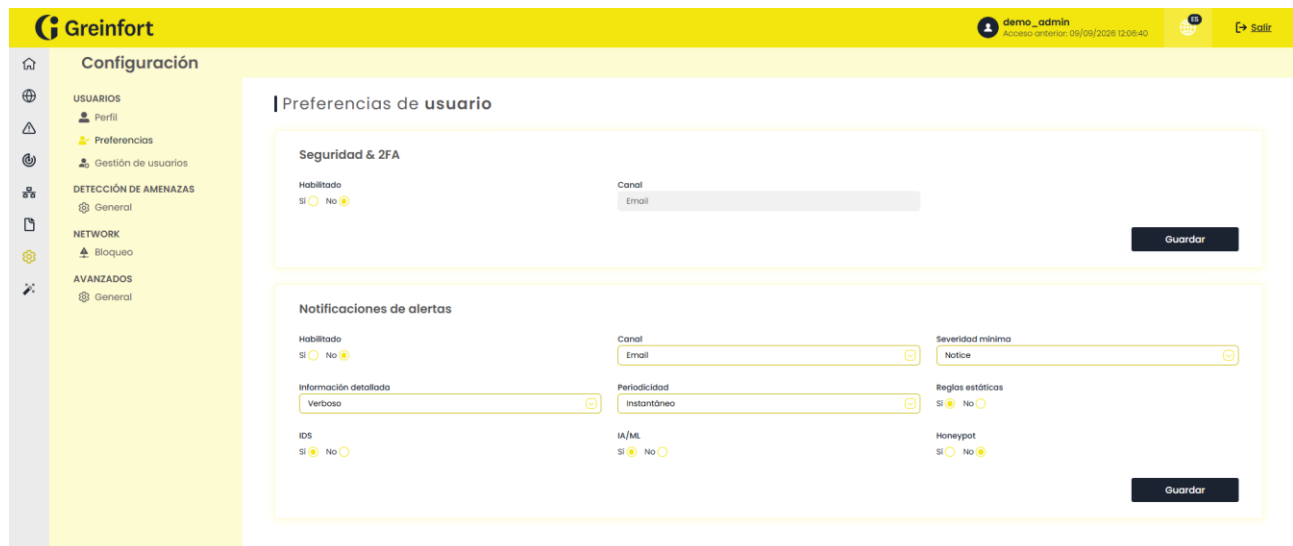


The screenshot shows the Greinfort web interface. The top header is yellow with the Greinfort logo on the left and user information on the right: 'demo_admin', 'Acceso anterior: 06/09/2026 12:06:43', and a 'Salir' button. The left sidebar is yellow and contains a 'Configuración' section with sub-items: 'USUARIOS' (Perfil, Preferencias, Gestión de usuarios), 'DETECCIÓN DE AMENAZAS' (General), 'NETWORK' (Bloqueo), and 'AVANZADOS' (General). The main content area is titled 'Datos de perfil' and contains a form with the following fields: 'Usuario' (demo_admin), 'Idioma' (ES), 'Teléfono' (empty), 'Email' (jaime.souto@inprosec.com), 'Acceso actual' (06/09/2026 12:35), 'Acceso anterior' (06/09/2026 12:06), and 'Duración de token de sesión (minutos)' (30). A 'Guardar' button is at the bottom right of the form.

Vista de datos del perfil de usuario

3.8.2. Preferencias de los usuarios

En Preferencias > Avanzadas, dentro de la sección "Seguridad y MFA", se puede activar el segundo factor de autenticación como mecanismo adicional de seguridad (recomendado) para prevenir el robo de identidad. Tras identificarse con el nombre de usuario y la contraseña, se solicita un token de un solo uso recibido por correo electrónico.



Vista de preferencias del usuario

Debe tenerse en cuenta que se ha implementado un mecanismo de control de acceso basado en roles, con grupos de permisos asociados a tres niveles de usuario, descritos con anterioridad:

- Administrador
- Operador
- Monitor

3.8.3. Notificación de alertas

Si se considera oportuno, pueden configurarse notificaciones proactivas de las alertas generadas por el sistema. Las alertas y advertencias se producen a partir de la detección de anomalías mediante las estrategias implementadas en Greinfort (heurísticas, IA/ML, IDS, honeypot o creación manual).

De este modo, Greinfort avisa de posibles incidentes sin necesidad de comprobar periódicamente la interfaz web.

Se pueden configurar los aspectos siguientes:

- Recepción o no de notificaciones de alertas de seguridad.
- Umbral de gravedad a partir del cual se envían las notificaciones.
- Tipo de alertas: heurísticas, IA/ML, IDS, honeypot o todas.
- Formato de envío:
 - Individual: una notificación por alerta
 - Agrupado: una notificación diaria con el resumen de todas las alertas, seleccionable de lunes a viernes o de lunes a domingo.
 - Si el formato es individual, puede seleccionarse una versión resumida o verbosa.



Vista de notificaciones de alertas

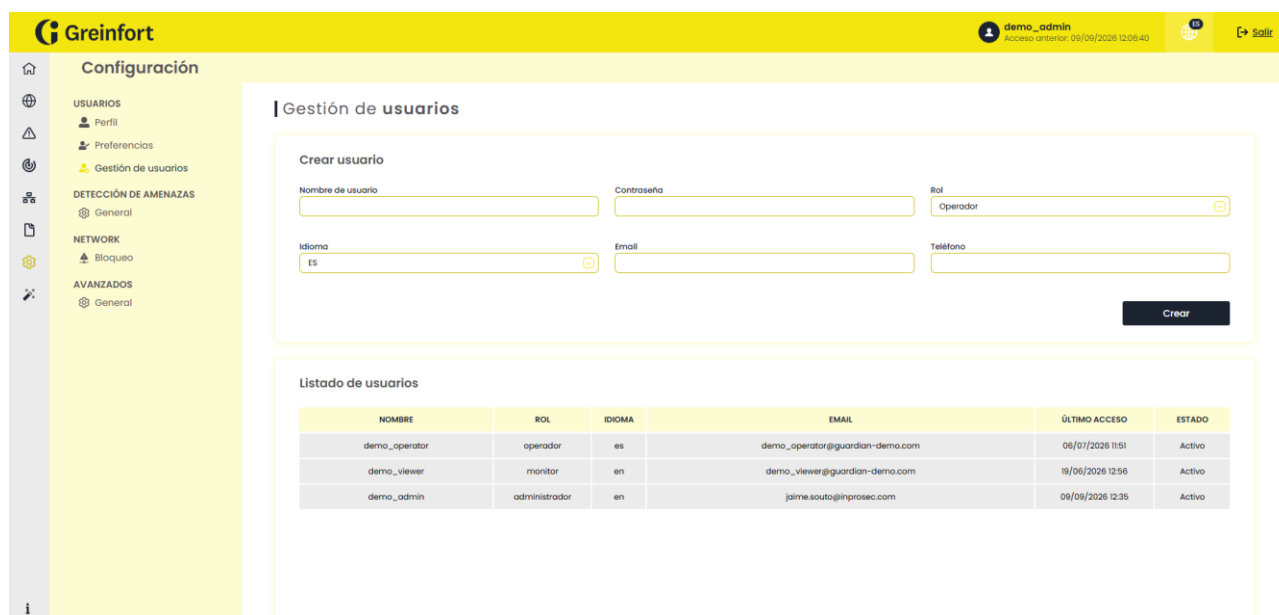
Las notificaciones se enviarán por correo electrónico a la cuenta del usuario.

Importante:

- La notificación de alerta debe estar activada en el backend para permitir al usuario habilitar el envío proactivo.
- En caso de que, con las condiciones establecidas, se generen demasiadas alertas por unidad de tiempo, la funcionalidad se desactivará automáticamente por seguridad (previamente informando por correo electrónico al usuario sobre esta situación), de modo que se puedan seleccionar otras condiciones de envío de notificaciones más exigentes (de menor volumen de eventos).

3.8.4. Gestión de usuarios

En la sección Gestión de Usuarios, un usuario con el rol de administrador puede crear usuarios en su misma fábrica y leer la lista de usuarios correspondiente.



NOMBRE	ROL	IDIOMA	EMAIL	ÚLTIMO ACCESO	ESTADO
demo_operator	operador	es	demo_operator@guardian-demo.com	06/07/2026 11:51	Activo
demo_viewer	monitor	en	demo_viewer@guardian-demo.com	19/06/2026 12:56	Activo
demo_admin	administrador	en	jaime.souto@inprosec.com	09/09/2026 12:35	Activo

Vista de gestión de usuarios

3.8.5. Configuración de bloqueo de tráfico

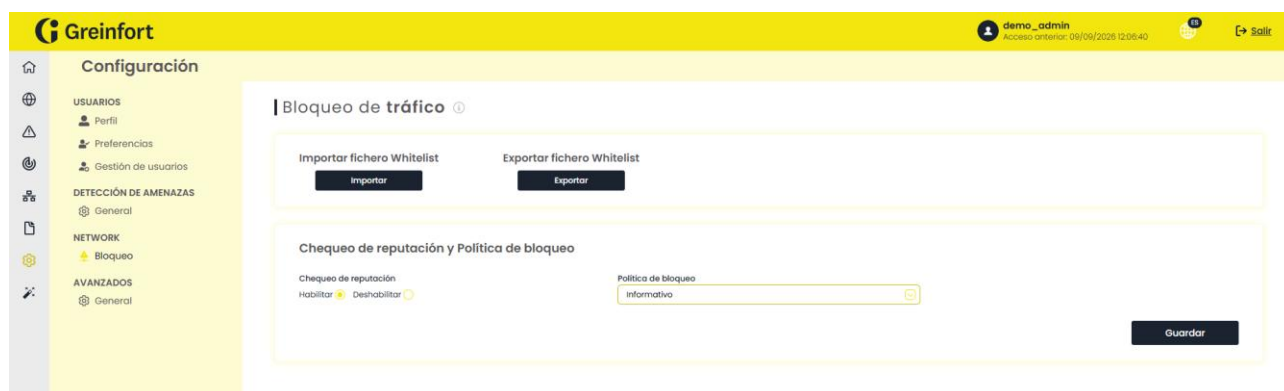
En esta sección se puede habilitar la importación y exportación de una lista blanca de direcciones IP, rangos de IP o direcciones MAC a las que nunca se aplicará el bloqueo.

También se pueden configurar los dos parámetros siguientes:

- Comprobación de reputación: activa o desactiva la consulta de la reputación de direcciones IP públicas en el tráfico entrante o saliente.

- Política de bloqueo: permite seleccionar uno de los cuatro modos de bloqueo de direcciones IP públicas maliciosas:

- **Informativo:** notifica al usuario y sugiere bloquear esa IP.
- **Manual:** proporciona un botón accionable por el usuario en el panel de alertas que envía la IP maliciosa a una lista de bloqueo gestionada por el cortafuegos industrial.
- **Automático:** se comunica con el cortafuegos sin intervención del usuario y añade la dirección IP maliciosa a una lista de bloqueo.
- **Desactivado:** no modifica el panel de alertas ni intenta comunicarse con el cortafuegos industrial.



Vista de bloqueo de tráfico

3.8.6. Información

Sección que permite descargar la última versión del manual de usuario de Greinfort. Apunta a la web de Greinfort, donde se publica la documentación relevante.

También muestra la versión actual de la plataforma y el registro de cambios para el control de versiones.

Para acceder, se debe hacer clic en el icono del menú situado en la esquina inferior izquierda. 

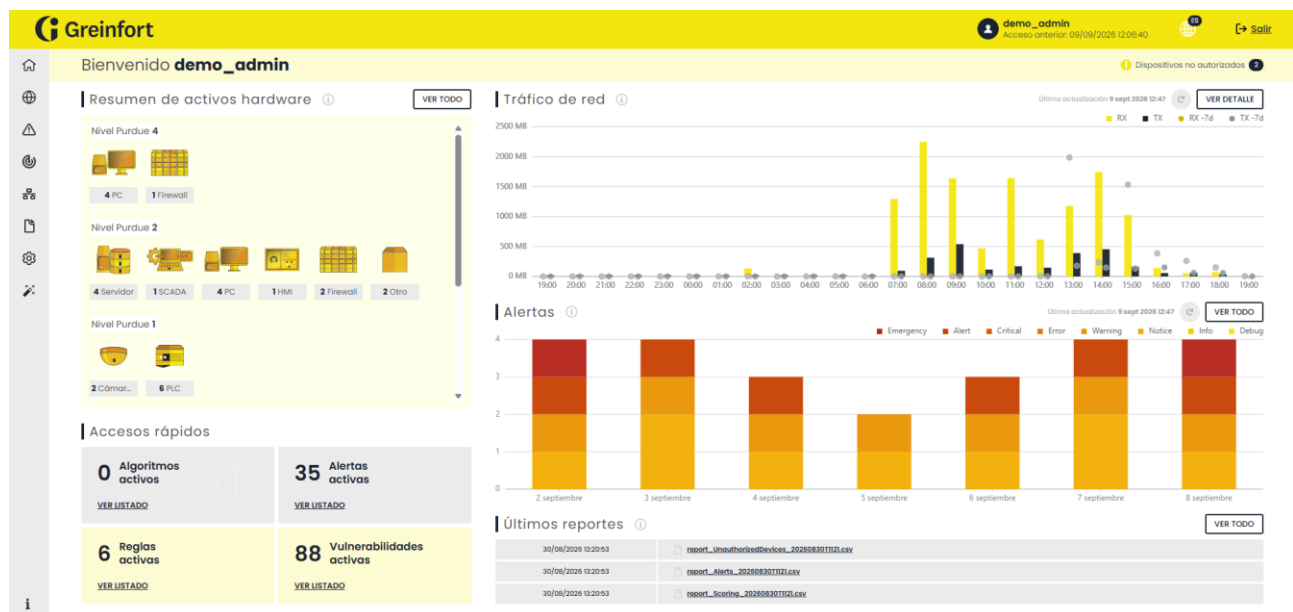


Vista de información

Para cualquier problema técnico, se debe contactar con el servicio de Soporte.

4. Gestión de aplicación

4.1. Panel principal



Panel de inicio

4.1.1. Resumen de activos



Resumen de activos

Se muestra el número de dispositivos conectados a la red, diferenciados por tipo (PLC, RTU, switch, router, robot, PC, SCADA, DCS, HMI, cortafuegos, variador de frecuencia, tarjeta controladora, sensor, cámara V.A., tableta, teléfono, honeypot u otro equipo) y clasificados de acuerdo con el modelo Purdue descrito en el Anexo II (informado manual o automáticamente).

4.1.2. Enlaces rápidos

Accesos rápidos

0 Algoritmos activos

VER LISTADO

35 Alertas activas

VER LISTADO

6 Reglas activas

VER LISTADO

88 Vulnerabilidades activas

VER LISTADO

Enlaces rápidos

a. Algoritmos activos

Al hacer clic en "VER LISTA", se muestra la lista de algoritmos de inteligencia artificial activos para la detección de amenazas en la red de la organización. Esta sección se describe más adelante.

Amenazas basadas en IA/ML

Gestión de algoritmos IA/ML

IDs Sonda

Todos

Búsqueda general

ALGORITMO	ESTADO	ACCIONES		
anagram	Inactivo	Entrenar	Detectar	Parar
deep-payload	Inactivo	Entrenar	Detectar	Parar
ext-iforest	Detectando	Entrenar	Detectar	Parar
Process-Mining	Detectando	Entrenar	Detectar	Parar
isolation-forest	Detectando	Entrenar	Detectar	Parar
autoencoder	Inactivo	Entrenar	Detectar	Parar
UEBA-LSTM	Preparado	Entrenar	Detectar	Parar

Lista de algoritmos

b. Alertas activas

Al hacer clic en "VER LISTA", se muestra la lista completa de alertas activas.

c. Reglas activas

Al hacer clic en "VER LISTA", se muestra la lista de reglas fijas activas para la detección de amenazas en la red de la organización. Esta sección se describe más adelante.

Motor de reglas 6 Reglas

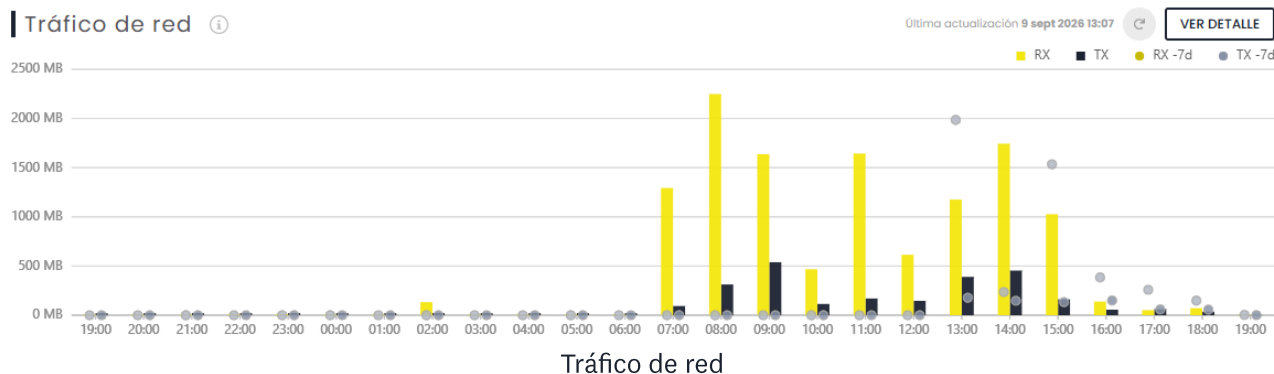
	NOMBRE	ESTADO	UMBRALES	OPCIONES
✓	NewDevice	Production	1 ⓘ	
✓	ARPAAttack	Production	1 ⓘ	
✓	Fingerprinting	Production	5-3-3 ⓘ	
✓	PublicIP	Production	1 ⓘ	
✓	PortAnomaly	Production	1 ⓘ	
✓	NewConnection	Production	1 ⓘ	

Lista de reglas activas

d. Vulnerabilidades activas

Al hacer clic en "VER LISTA", se muestra la lista de vulnerabilidades activas pendientes de gestión.

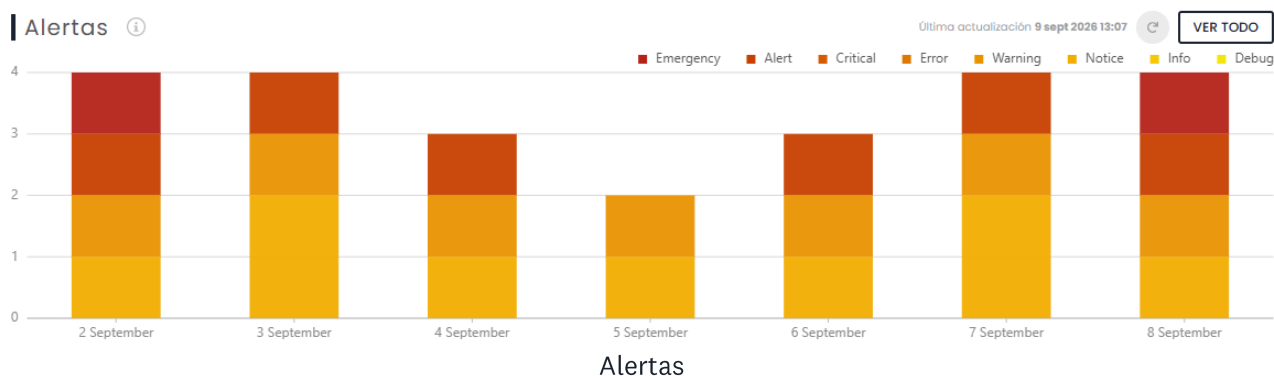
4.1.3. Gráfico de tráfico de red



El panel representa gráficamente el tráfico generado, en bit/s o múltiplos de esta unidad, durante las últimas 24 horas, tanto enviado como recibido. Los datos se actualizan automáticamente y también pueden actualizarse de forma manual. Los puntos circulares de cada barra indican, a modo de comparación, el tráfico registrado siete días antes.

Al hacer clic en "VER DETALLE", se abre la ventana de sesiones de red de Greinfort, descrita más adelante.

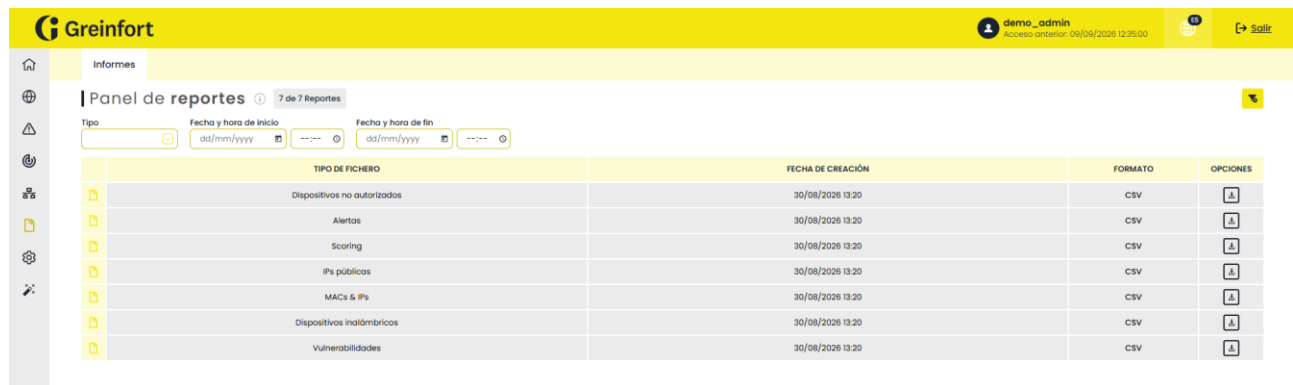
4.1.4. Gráfico de alertas



Se muestra una representación gráfica del número de alertas de los últimos cinco días, diferenciadas por nivel de severidad (véase el Anexo I) y color, así como su tendencia. Los datos se actualizan automáticamente y también pueden actualizarse de forma manual.

Al situar el cursor sobre la barra de un día, se muestra el número exacto de alertas registradas hasta ese momento. Al hacer clic en "VER TODO", se abre la ventana de alertas de Greinfort, descrita más adelante.

4.1.5. Últimos informes



Panel de reportes 7 de 7 Reportes

Tipo: Fecha y hora de inicio: dd/mm/yyyy Fecha y hora de fin: dd/mm/yyyy

TIPO DE FICHERO	FECHA DE CREACIÓN	FORMATO	OPCIONES
Dispositivos no autorizados	30/08/2026 13:20	CSV	[A]
Alertas	30/08/2026 13:20	CSV	[A]
Scoring	30/08/2026 13:20	CSV	[A]
IPs públicas	30/08/2026 13:20	CSV	[A]
MACs & IPs	30/08/2026 13:20	CSV	[A]
Dispositivos inalámbricos	30/08/2026 13:20	CSV	[A]
Vulnerabilidades	30/08/2026 13:20	CSV	[A]

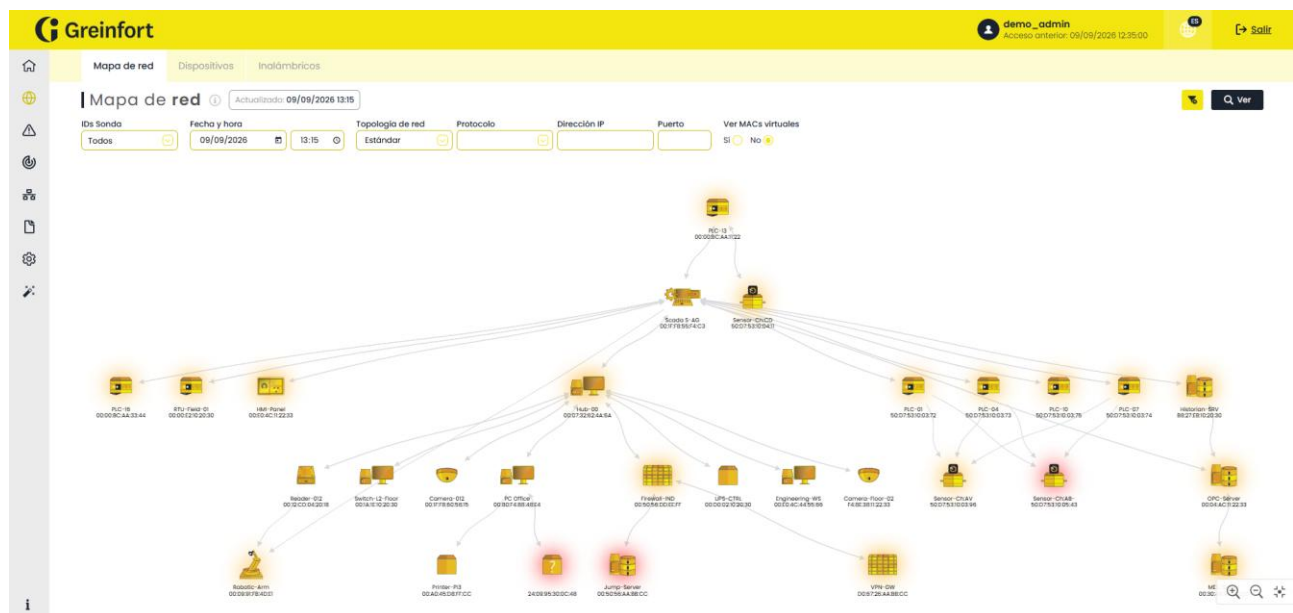
Últimos informes disponibles

Al hacer clic en "VER TODO", se muestra la lista de los informes más recientes, generados automáticamente o a petición del cliente.

4.2. Mapa de red y lista de dispositivos

4.2.1. Mapa de red

Para acceder al mapa de red, el usuario debe hacer clic en el icono  del lado izquierdo de la pantalla y seleccionar la pestaña "Mapa de red".



Mapa de red

En la pestaña "Mapa de red" se muestran en tiempo real todos los dispositivos conectados y sus enlaces de comunicación. Cada dispositivo se representa mediante una imagen y una serie de propiedades, como la dirección MAC o el nombre asignado manualmente. El mapa refleja la topología implementada.

Los iconos representados corresponderán a los descritos en el Anexo II.

Los dispositivos no autorizados se mostrarán en el mapa de red sombreados con un fondo rojo. Los dispositivos fijos y críticos también tendrán su halo correspondiente (véase el Anexo I para definiciones).

Al situar el cursor sobre un dispositivo, se muestra una ventana emergente con su información básica.

Al hacer clic en un dispositivo, se abre la ventana con toda su información.

Al situar el cursor sobre un enlace, se muestra una ventana emergente con la información básica de la comunicación. Al hacer clic en un enlace, se abre la ventana con toda la información de la conexión.

El mapa de red puede simplificarse para mostrar solo los dispositivos de interés usando los diferentes filtros y aceptando el filtrado haciendo clic en el botón "Consultar".



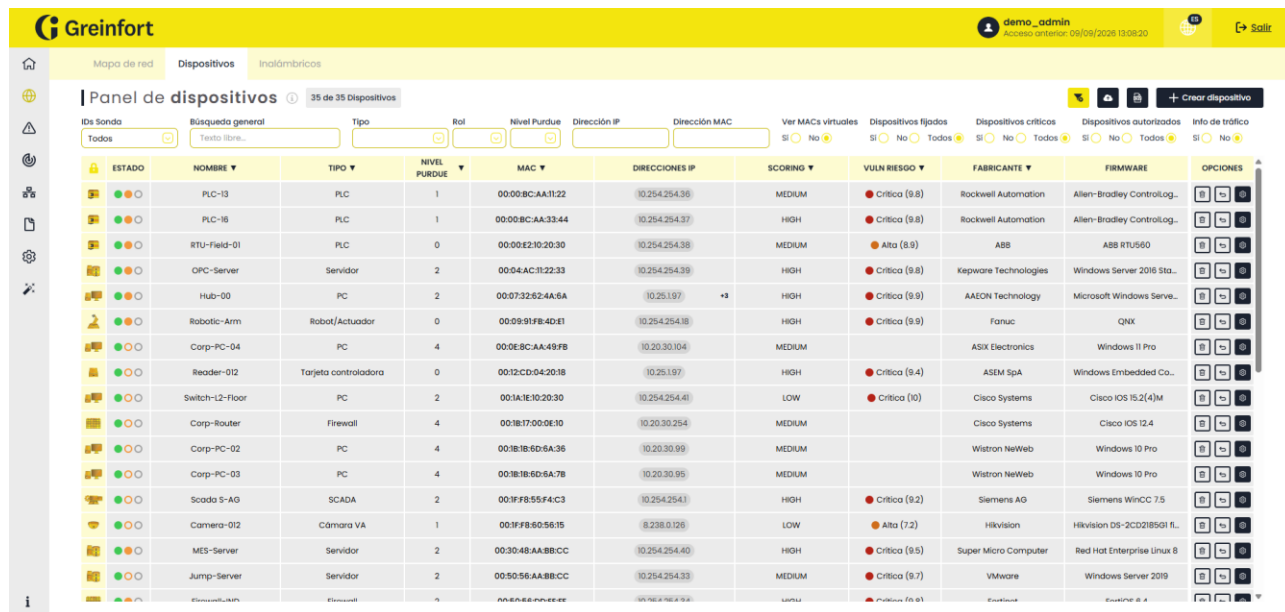
Filtros disponibles en el mapa de red

Los filtros pueden aplicarse de la siguiente manera:

- Fecha y hora: intervalo temporal que se muestra en pantalla.
- Topología de red: modelo de representación de la red de la organización.
- Protocolo: muestra únicamente las conexiones que utilizan el protocolo seleccionado.
- Dirección IP: muestra únicamente los dispositivos y conexiones con la dirección seleccionada.
- Puerto: muestra únicamente las conexiones asociadas al puerto seleccionado.
- Visualización de direcciones MAC virtuales (multicast o broadcast), calculadas automáticamente por el sistema.

4.2.2. Lista de dispositivos

Para acceder a la lista de dispositivos, el usuario debe hacer clic en el icono  del lado izquierdo de la pantalla y seleccionar la pestaña "Lista de dispositivos".



ESTADO	NOMBRE	TIPO	NIVEL PURDUE	MAC	DIRECCIONES IP	SCORING	VULN RIESGO	FABRICANTE	FIRMWARE	OPCIONES
	PLC-13	PLC	1	00:00:8C:AA:11:22	10.254.254.36	MEDIUM	Critica (9.8)	Rockwell Automation	Allen-Bradley ControlLogix...	[Icons]
	PLC-16	PLC	1	00:00:8C:AA:33:44	10.254.254.37	HIGH	Critica (9.8)	Rockwell Automation	Allen-Bradley ControlLogix...	[Icons]
	RTU-Field-01	PLC	0	00:00:22:10:20:30	10.254.254.38	MEDIUM	Alta (8.9)	ABB	ABB RTU560	[Icons]
	OPC-Server	Servidor	2	00:04:AC:11:22:33	10.254.254.39	HIGH	Critica (9.8)	Keypware Technologies	Windows Server 2016 Sta...	[Icons]
	Hub-00	PC	2	00:07:32:62:AA:5A	10.25.197	HIGH	Critica (9.9)	AAEON Technology	Microsoft Windows Serve...	[Icons]
	Robotic-Arm	Robot/Actuador	0	00:09:91:FB:4D:E1	10.254.254.18	HIGH	Critica (9.9)	Fanuc	QNX	[Icons]
	Corp-PC-04	PC	4	00:0E:8C:AA:49:FB	10.20.30.104	MEDIUM		ASIX Electronics	Windows 11 Pro	[Icons]
	Reader-012	Tarjeta controladora	0	00:12:CD:04:20:18	10.25.197	HIGH	Critica (9.4)	ASEM SpA	Windows Embedded Co...	[Icons]
	Switch-12-Floor	PC	2	00:1A:1E:10:20:30	10.254.254.41	LOW	Critica (10)	Cisco Systems	Cisco IOS 15.2(4)M	[Icons]
	Corp-Router	Firewall	4	00:1B:17:00:DE:10	10.20.30.254	MEDIUM		Cisco Systems	Cisco IOS 12.4	[Icons]
	Corp-PC-02	PC	4	00:1B:1B:6D:6A:36	10.20.30.99	MEDIUM		Wistron NetWeb	Windows 10 Pro	[Icons]
	Corp-PC-03	PC	4	00:1B:1B:6D:6A:7B	10.20.30.95	MEDIUM		Wistron NetWeb	Windows 10 Pro	[Icons]
	Scada S-AG	SCADA	2	00:1F:FB:55:F4:C3	10.254.254.1	HIGH	Critica (9.2)	Siemens AG	Siemens WinCC 7.5	[Icons]
	Camara-012	Cámara VA	1	00:1F:FB:60:56:15	8.238.0.126	LOW	Alta (7.2)	Hikvision	Hikvision DS-2CD21850I FL	[Icons]
	MES-Server	Servidor	2	00:30:4B:AA:BB:CC	10.254.254.40	HIGH	Critica (9.5)	Super Micro Computer	Red Hat Enterprise Linux 8	[Icons]
	Jump-Server	Servidor	2	00:50:56:AA:BB:CC	10.254.254.33	MEDIUM	Critica (9.7)	VMware	Windows Server 2019	[Icons]

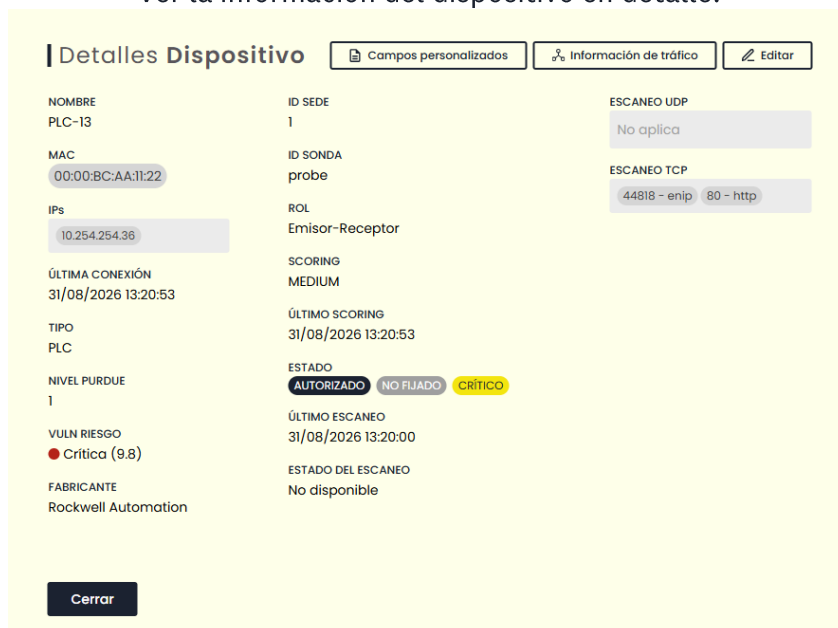
Lista de dispositivos

Se muestra una lista ampliada de todos los dispositivos presentes en la organización y su información:

- **ESTADO:**
 - El primero de los círculos indicará si el dispositivo está autorizado (aprobado por el administrador como conocido), o no.
 - El segundo de los círculos indicará si el dispositivo es crítico o no (si por su relevancia o criticidad no se permite que se realicen sobre él acciones activas).
 - El tercer círculo indica si el dispositivo está fijado o no (si se desea que independientemente de que deje de generar tráfico, siga apareciendo en el mapa de red).
 - **NOMBRE:** Nombre asignado a cada dispositivo.
 - **TIPO:** Diferenciación del tipo de dispositivo (PLC, RTU, SCADA, Honeypot, etc.).
 - **NIVEL PURDUE:** Nivel de clasificación según el modelo de Purdue.
 - **MAC:** Dirección MAC asignada al dispositivo.
 - **DIRECCIONES IP:** direcciones IP asignadas al dispositivo.
 - **PUNTUACIÓN:** importancia o riesgo del dispositivo (bajo, medio o alto) mediante algoritmo propietario que da una medida de su criticidad dentro de la red.
 - **RIESGO VULN.:** nivel de severidad más alto de las vulnerabilidades detectadas en el dispositivo.
 - **PROVEEDOR:** fabricante del dispositivo.
 - **FIRMWARE:** información del firmware integrado en el dispositivo.
 - **CAMPOS PERSONALIZADOS:** Además de los campos existentes, los usuarios pueden crear sus campos personalizados en formato JSON con pares clave-valor. Cada campo personalizable aparecerá en la lista de dispositivos como una nueva columna virtual, permitiendo al usuario catalogar, organizar y filtrar los dispositivos a su conveniencia. Estos campos personalizables también aparecerán en los informes.
- Las columnas creadas como campos personalizables formarán parte de un inventario virtual. El usuario puede aplicar filtros a este inventario según lo desee. Este inventario de campo también es exportable.

- **INFORMACIÓN DE TRÁFICO:** el sistema de inventario pasivo infiere automáticamente variables de interés de cada dispositivo, que se almacenan en este campo con formato clave-valor. El campo también se incluye en el archivo CSV de exportación.
- **ACCIONES:**

Ver la información del dispositivo en detalle.



Detalles del dispositivo



Edición del dispositivo

La pantalla puede filtrarse para mostrar únicamente los dispositivos de interés.



Filtrado de dispositivos

El filtrado puede realizarse según los criterios siguientes:

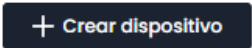
- ID de la sonda, para filtrar por zona de la red industrial y/o sede central.

- Nombre del dispositivo
- Tipo de dispositivo (PLC, RTU, SCADA, Honeypot, FIREWALL, etc.)
- Función del dispositivo (transmisor, receptor o ambos)
- Nivel Purdue, según el Anexo II
- Dirección IP del dispositivo
- Dirección MAC del dispositivo
- Vista de MACs virtuales reservados por difusión (Y/N).
- Dispositivos fijos (Y/N), véase el Anexo I.
- Dispositivos críticos (Y/N), véase el Anexo I.
- Dispositivos autorizados (Y/N), véase el Anexo I.
- Filtro de tráfico (i.e. información agregada de manera pasiva por el motor de Greinform).

El usuario también puede realizar una búsqueda general usando una cadena de texto.

Al pulsar el botón , se restablecen los filtros y Greinform vuelve a mostrar la lista completa de dispositivos.

Mediante el botón correspondiente se exporta a un archivo CSV la lista de dispositivos y su información. 

Puede añadirse manualmente un nuevo dispositivo a la red y a la lista de la organización mediante el botón correspondiente. 

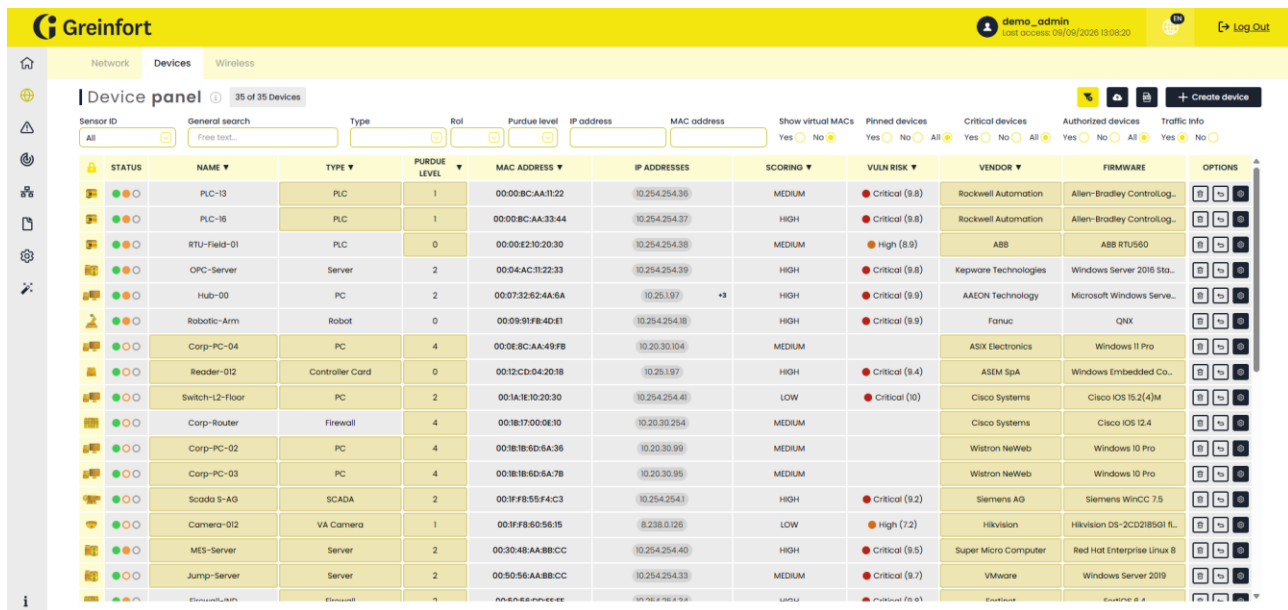
Aparecerá la siguiente ventana emergente:



Campos disponibles para crear un dispositivo

La información del nuevo dispositivo debe introducirse manualmente. Para completar la creación, se debe hacer clic en "Guardar".

El filtro "Info de tráfico" resaltaré aquellos campos que hayan sido inferidos a partir del sistema de inventario pasivo (en vez de editados directamente por el usuario):



STATUS	NAME	TYPE	PURDUE LEVEL	MAC ADDRESS	IP ADDRESSES	SCORING	VULN RISK	VENDOR	FIRMWARE	OPTIONS
	PLC-13	PLC	1	00:00:8C:AA:11:22	10.254.254.36	MEDIUM	Critical (9.8)	Rockwell Automation	Allen-Bradley ControlLogix	[Icons]
	PLC-16	PLC	1	00:00:8C:AA:33:44	10.254.254.37	HIGH	Critical (9.8)	Rockwell Automation	Allen-Bradley ControlLogix	[Icons]
	RTU-Field-01	PLC	0	00:00:23:10:20:30	10.254.254.38	MEDIUM	High (8.9)	ABB	ABB RTU560	[Icons]
	OPC-Server	Server	2	00:04:AC:11:22:33	10.254.254.39	HIGH	Critical (9.8)	Keypower Technologies	Windows Server 2016 Sta...	[Icons]
	Hub-00	PC	2	00:07:32:62-AA:5A	10.25.197	HIGH	Critical (9.9)	AAEON Technology	Microsoft Windows Serve...	[Icons]
	Robotic-Arm	Robot	0	00:09:91:F8:4D:E1	10.254.254.18	HIGH	Critical (9.9)	Fanuc	QNX	[Icons]
	Corp-PC-04	PC	4	00:0E:8C:AA:49:F8	10.20.30.104	MEDIUM		ASIX Electronics	Windows 11 Pro	[Icons]
	Reader-012	Controller Card	0	00:12:CD:04:20:18	10.25.197	HIGH	Critical (9.4)	ASEM SpA	Windows Embedded Ca...	[Icons]
	Switch-L2-floor	PC	2	00:1A:1E:10:20:30	10.254.254.41	LOW	Critical (10)	Cisco Systems	Cisco IOS 15.2(4)M	[Icons]
	Corp-Router	Firewall	4	00:1B:17:00:DE:10	10.20.30.254	MEDIUM		Cisco Systems	Cisco IOS 12.4	[Icons]
	Corp-PC-02	PC	4	00:1B:1B:6D:6A:36	10.20.30.99	MEDIUM		Wistron NetWeb	Windows 10 Pro	[Icons]
	Corp-PC-03	PC	4	00:1B:1B:6D:6A:7B	10.20.30.95	MEDIUM		Wistron NetWeb	Windows 10 Pro	[Icons]
	Scada S-AG	SCADA	2	00:1F:F8:55:F4:C3	10.254.254.1	HIGH	Critical (9.2)	Siemens AG	Siemens WinCC 7.5	[Icons]
	Camera-012	VA Camera	1	00:1F:F8:60:56:15	8.238.0.126	LOW	High (7.2)	Hikvision	Hikvision DS-2CD21850I FL	[Icons]
	MES-Server	Server	2	00:30:4B:AA:BB:CC	10.254.254.40	HIGH	Critical (9.5)	Super Micro Computer	Red Hat Enterprise Linux 8	[Icons]
	Jump-Server	Server	2	00:50:56:AA:BB:CC	10.254.254.33	MEDIUM	Critical (9.7)	VMware	Windows Server 2019	[Icons]

Panel de dispositivos con el filtro "Info de tráfico" activado

a. Importación mediante CSV

El sistema permite la importación/edición masiva de dispositivos, para evitar alertas innecesarias durante la incorporación inicial o cambios importantes en la red industrial.

En la sección "Red", dentro de la pestaña "Lista de dispositivos", aparece el icono de importación. Al hacer clic en él, se abre la ventana emergente siguiente. 

Desde esta ventana se puede seleccionar o arrastrar un archivo CSV con los datos de los dispositivos que se desea añadir o modificar, en el formato indicado a continuación.

Para que el archivo CSV sea válido, debe cumplir con las siguientes características:

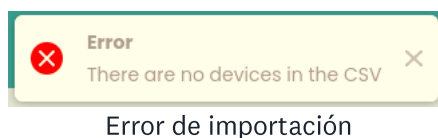
- Un máximo de 250 dispositivos.
- Cabecera con las columnas siguientes (los nombres de las columnas pueden personalizarse):
 - MAC
 - Nombre del dispositivo
 - Autorizado (Y/N)
 - Crítico (Y/N)
 - Fijado (S/N)
 - Tipo de dispositivo (de la lista permitida: virtual, plc, rtu, switch, router, robot, pc, scada, hmi, firewall, adjustable_frequency_drive, controller_card, sensor, va_camera, tablet, voip_phone, servidor, code_bar_scanner, otros)
 - Nivel PURDUE (0 a 4, como se explica en el Anexo II)
 - Campos personalizados.
- El delimitador de campos debe ser ";".
- No debe contener campos vacíos.
- Puede contener nuevos registros de dispositivos o registros ya existentes cuyos atributos deban modificarse. Se requiere una fila por dispositivo, con el formato indicado.
- Los nuevos registros simplemente tendrán todos los campos CSV cubiertos con la información deseada.

- Los registros existentes que se desee modificar deben contener el literal ***CURRENT*** en los campos que deban permanecer sin cambios. En los campos que se vayan a actualizar se debe introducir la información nueva.
 - Los registros que se vayan a modificar deben incluir ***CURRENT*** en alguna de sus propiedades; esto permite distinguirlos de los registros nuevos.
 - El campo MAC no puede contener el literal ***CURRENT***, ya que identifica unívocamente el dispositivo.
 - Los registros nuevos también pueden contener el literal ***CURRENT*** en algunos campos; esto indica que deben conservarse los valores predeterminados. En los campos booleanos el valor será false; los campos de texto, como el nombre, el nivel Purdue y el tipo de dispositivo, permanecerán como NULL y podrán modificarse desde la interfaz web.
 - Existen dos formas posibles de definir un conjunto de campos personalizados, respetando su estructura clave-valor:
 - Formato JSON: {"key1": "value1", "key2": "value2"}
 - Pares: clave1 | valor1 | clave2 | valor2
- Los campos personalizados definidos anteriormente pueden eliminarse sobrescribiendo los datos mediante un nuevo archivo CSV. En el lugar de esos campos se debe incluir el literal ***DELETE***, de forma análoga al uso de ***CURRENT***.
- Es crucial escribir literales entre asteriscos.

Aviso: en caso de duda, se debe consultar con el servicio de Soporte, ya que el uso inadecuado de esta función puede afectar significativamente a la integridad de la información de los dispositivos. Una vez seleccionado el archivo, se debe hacer clic en "Confirmar".

Se trata de una operación de alto impacto, pues permite añadir dispositivos y modificar sus propiedades.

Si el archivo CSV enviado no contiene ningún dispositivo, se muestra el mensaje de error siguiente.



Si hay errores en los datos dentro del archivo ".csv", se mostrará un mensaje con detalles de los errores encontrados, junto con el número de línea donde se encuentra cada error.



Si no se detectan errores, será posible verificar que los dispositivos se han añadido correctamente a la base de datos.

b. Air Watcher (lista de dispositivos inalámbricos)

En la sección de red, la tercera pestaña permite acceder a la lista de dispositivos inalámbricos registrados en la red.

En la parte superior, se puede ver el número total de dispositivos en la base de datos y, si se aplica un filtro, cuántos coinciden con ese filtro en relación con el total.

En el lado derecho, hay un panel de botones para eliminar los filtros aplicados previamente y exportar la lista de dispositivos en formato CSV.

La información proporcionada en esta sección será la siguiente, para todos aquellos dispositivos con capacidad Wi-Fi o Bluetooth detectada en las proximidades de los colectores:

- **Autorizado:** determina si el dispositivo ha sido autorizado por un administrador (verde) o no (rojo).
- **Nombre:** corresponde al nombre del dispositivo.
- **Tipo de conexión:** podría ser Wi-Fi o Bluetooth.
- **Tipo de dispositivo:** los valores pueden variar para dispositivos Bluetooth. Para dispositivos Wi-Fi, puede tomar valores como "Punto de acceso" o "Smartphone o portátil", además de "Desconocido".
- **MAC de origen:** dirección MAC de origen del paquete. Identifica el propio dispositivo en la comunicación capturada.
- **MAC de destino:** dirección MAC de destino del paquete. Identifica el dispositivo receptor del paquete.
- **Actividad:** refleja el estado del dispositivo o el tipo de actividad que ha realizado:

Búsqueda de redes: el dispositivo tiene la antena Wi-Fi activada y está buscando puntos de acceso.

Intento de conexión: el dispositivo ha intentado conectarse a un punto de acceso.

Punto de acceso activo: el dispositivo funciona como punto de acceso.

Transmisión de datos: el dispositivo está enviando información a un punto de acceso.

Dispositivo visible: esto solo se aplica a dispositivos Bluetooth; el dispositivo tiene Bluetooth activado y es visible para otros dispositivos.

- **ID inalámbrico:** nombre o identificador de la red Wi-Fi (podría estar vacío si, por ejemplo, la conexión es Bluetooth).
- **Primera vez detectado:** formato dd/mm/aaaa hh:mm.
- **Última vez detectado:** formato dd/mm/aaaa hh:mm.

Greinfort demo_admin Acceso anterior: 09/09/2026 13:08:20  Salir

Mapa de red Dispositivos **Inalámbricos**

Panel de inalámbricos 30 of 30 Dispositivos inalámbricos  

IDs Sonda: Todos filters.wireless.text filters.wireless.mac Tipo de conexión: Fecha y hora de inicio: dd/mm/yyyy Fecha y hora de fin: dd/mm/yyyy Dispositivos autorizados: Si No Todos

AUTORIZADO	NOMBRE	TIPO CONEXIÓN	TIPO DISPOSITIVO	MAC ORIGEN	MAC DESTINO	ACTIVIDAD	ID WIRELESS	VISTO PRIMERA VEZ	VISTO ÚLTIMA VEZ	OPCIONES
	Samsung Galaxy Buds	Bluetooth	Audio	11:9A:53:10:22:E3		Dispositivo visible		30/08/2026 13:20	31/08/2026 13:20	 
	iPhone-OP02	Bluetooth	Phone	3C:22:F8:AA:8B:CC		Dispositivo visible		30/08/2026 13:20	31/08/2026 13:20	 
	OPPO Find X5 Lite	Bluetooth	Phone	50:D7:53:10:05:55		Dispositivo visible		30/08/2026 13:20	31/08/2026 13:20	 
	Samsung Galaxy S24	Bluetooth	Phone	9B:5A:11:10:05:AB		Dispositivo visible		30/08/2026 13:20	31/08/2026 13:20	 
	iPhone-OP01	Bluetooth	Phone	21:D7:22:10:22:55		Dispositivo visible		30/08/2026 13:20	31/08/2026 13:20	 
	Garmin Forerunner	Bluetooth	Smartwatch	78:A5:04:5D:EE:FF		Dispositivo visible		30/08/2026 13:20	31/08/2026 13:20	 
	Alexa	Bluetooth	Speaker	AA:D7:2C:10:77:87		Dispositivo visible		30/08/2026 13:20	31/08/2026 13:20	 
	Huawei P40 Pro	Bluetooth	Phone	28:31:52:AA:8B:CC		Dispositivo visible		30/08/2026 13:20	31/08/2026 13:20	 
		Wi-Fi	Phone or Laptop	11:11:53:10:05:11	22:D7:AA:10:05:66	Transmitiendo datos	inprosec-wifi	30/08/2026 13:20	31/08/2026 13:20	 
	Cisco AP-Aironet-2	Wi-Fi	Access Point	E8:65:D4:11:22:33	FF:FF:FF:FF:FF:FF	Punto de acceso activo	corp-wifi-AP2	30/08/2026 13:20	31/08/2026 13:20	 
	iPad Pro	Wi-Fi	Tablet	DC:A4:CA:11:22:33		Transmitiendo datos	corp-wifi-API	30/08/2026 13:20	31/08/2026 13:20	 
	MacBook Pro OPS	Wi-Fi	Laptop	8C:85:90:44:55:66		Transmitiendo datos	corp-wifi-API	30/08/2026 13:20	30/08/2026 13:20	 
	Access Point BI	Wi-Fi	Access Point	11:22:53:10:05:22	33:D7:AA:10:05:77	Punto de acceso activo	corp-wifi-API	30/08/2026 13:20	31/08/2026 13:20	 
	Honeywell CT40	Wi-Fi	Tablet	00:01:F0:22:44:66		Transmitiendo datos	corp-wifi-API	30/08/2026 13:20	31/08/2026 13:20	 
	MS Surface Pro 9	Wi-Fi	Laptop	98:D7:E7:11:22:33		Transmitiendo datos	corp-wifi-API	30/08/2026 13:20	31/08/2026 13:20	 
	Hikvision DS-2CD	Wi-Fi	IP Camera	C0:56:E3:33:44:55		Transmitiendo datos	corp-wifi-API	30/08/2026 13:20	31/08/2026 13:20	 

Lista de dispositivos inalámbricos

A continuación, se muestran los filtros disponibles para localizar los dispositivos de interés:

Panel de inalámbricos 30 of 30 Dispositivos inalámbricos  

IDs Sonda: Todos filters.wireless.text filters.wireless.mac Tipo de conexión: Fecha y hora de inicio: dd/mm/yyyy Fecha y hora de fin: dd/mm/yyyy Dispositivos autorizados: Si No Todos

Filtros de dispositivos inalámbricos

Los dispositivos pueden ordenarse alfabéticamente, de forma ascendente o descendente, haciendo clic en cualquiera de las columnas.

Por último, la lista real de activos contiene información y detalles sobre ellos, así como botones para realizar ciertas acciones adicionales (ver más detalles o eliminar).

Detalles Inalámbrico 

NOMBRE	Samsung Galaxy Buds	ID Sonda	probe
TIPO CONEXIÓN	Bluetooth	ID WIRELESS	No aplica
TIPO DISPOSITIVO	Audio	AUTORIZADO	AUTORIZADO
ACTIVIDAD	Dispositivo visible	VISTO PRIMERA VEZ	30/08/2026 13:20:54
MAC ORIGEN	11:9A:53:10:22:E3	VISTO ÚLTIMA VEZ	31/08/2026 13:20:54
MAC DESTINO	No disponible		
CANAL	0		
ID SEDE	1		



Detalles sobre dispositivos inalámbricos

En esta ventana modal se muestran los campos adicionales siguientes:

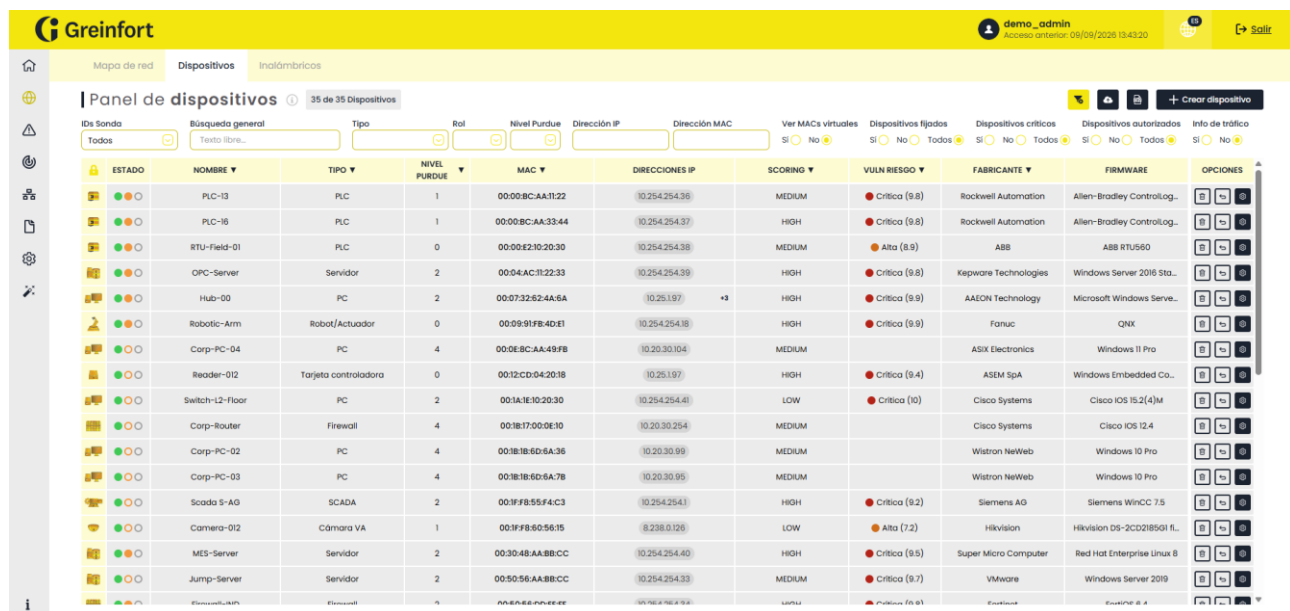
- Canal: identificador de canal de transmisión.
- ID del sitio: representa la fábrica.
- Identificadores de sensores: identifican el sensor.
- Identificación inalámbrica: identificador único del dispositivo.

Al hacer clic en el botón correspondiente, se puede cambiar el nombre del dispositivo y determinar si está autorizado.

c. Smart View (escaneo de dispositivos)

Esta capacidad permite un escaneo activo de los dispositivos en la red OT, para identificar algunas propiedades adicionales de cada nodo mediante una consulta ligera: versión del dispositivo, firmware, puertos abiertos y servicios que se ejecutan en la propia máquina.

Para ello, se escanearán los puertos de los protocolos de red TCP y UDP. Esta información se registrará en la base de datos del sistema y podrá extraerse como atributos adicionales de cada dispositivo, que se actualizarán mediante una consulta periódica en base a lo definido por el sistema por defecto, o la frecuencia establecida en el Asistente.



ESTADO	NOMBRE	TIPO	NIVEL	MAC	DIRECCIONES IP	SCORING	VULN RIESGO	FABRICANTE	FIRMWARE	OPCIONES
	PLC-13	PLC	1	00:00:8C:AA:11:22	10.254.254.36	MEDIUM	Critica (9.8)	Rockwell Automation	Allen-Bradley ControlLog...	[Iconos]
	PLC-16	PLC	1	00:00:8C:AA:33:44	10.254.254.37	HIGH	Critica (9.8)	Rockwell Automation	Allen-Bradley ControlLog...	[Iconos]
	RTU-Field-01	PLC	0	00:00:22:10:20:30	10.254.254.38	MEDIUM	Alta (8.9)	ABB	ABB RTU560	[Iconos]
	OPC-Server	Servidor	2	00:04:AC:11:22:33	10.254.254.39	HIGH	Critica (9.8)	Keypware Technologies	Windows Server 2016 Sta...	[Iconos]
	Hub-00	PC	2	00:07:32:62:4A:5A	10.25.197	HIGH	Critica (9.9)	AAEON Technology	Microsoft Windows Serve...	[Iconos]
	Robotic-Arm	Robot/Actuador	0	00:09:91:F8:4D:E1	10.254.254.18	HIGH	Critica (9.9)	Fanuc	QNX	[Iconos]
	Corp-PC-04	PC	4	00:0E:8C:AA:49:F8	10.20.30.104	MEDIUM		ASIX Electronics	Windows 11 Pro	[Iconos]
	Reader-012	Tarjeta controladora	0	00:12:CD:04:20:18	10.25.197	HIGH	Critica (9.4)	ASEM SPA	Windows Embedded Co...	[Iconos]
	Switch-L2-Floor	PC	2	00:1A:1E:10:20:30	10.254.254.41	LOW	Critica (10)	Cisco Systems	Cisco IOS 15.2(4)M	[Iconos]
	Corp-Router	Firewall	4	00:1B:17:00:0E:10	10.20.30.254	MEDIUM		Cisco Systems	Cisco IOS 12.4	[Iconos]
	Corp-PC-02	PC	4	00:1B:1B:6D:6A:36	10.20.30.99	MEDIUM		Wistron NetWeb	Windows 10 Pro	[Iconos]
	Corp-PC-03	PC	4	00:1B:1B:6D:6A:7B	10.20.30.95	MEDIUM		Wistron NetWeb	Windows 10 Pro	[Iconos]
	Scada 9-A0	SCADA	2	00:1F:F8:55:F4:C3	10.254.254.1	HIGH	Critica (9.2)	Siemens AG	Siemens WinCC 7.5	[Iconos]
	Camera-012	Cámara VA	1	00:1F:F8:6D:56:15	8.238.0.126	LOW	Alta (7.2)	Hikvision	Hikvision DS-2CD21850I FL	[Iconos]
	MES-Server	Servidor	2	00:30:4B:AA:BB:CC	10.254.254.40	HIGH	Critica (9.5)	Super Micro Computer	Red Hat Enterprise Linux 8	[Iconos]
	Jump-Server	Servidor	2	00:50:56:AA:BB:CC	10.254.254.33	MEDIUM	Critica (9.7)	VMware	Windows Server 2019	[Iconos]

Lista de dispositivos

La información del escáner puede consultarse mediante el icono situado a la derecha. La ventana emergente muestra toda la información del dispositivo, además de las secciones "TCP Scan" y "UDP Scan". En ellas se indican los puertos abiertos, la fecha del último escaneo, si este ha finalizado correctamente y los posibles errores.

Detalles Dispositivo

Campos personalizados

Información de tráfico

Editar

NOMBRE PLC-13	ID SEDE 1	ESCANEO UDP No aplica
MAC 00:00:BC:AA:11:22	ID Sonda probe	ESCANEO TCP 44818 - enip 80 - http
IPs 10.254.254.36	ROL Emisor-Receptor	
ÚLTIMA CONEXIÓN 31/08/2026 13:20:53	SCORING MEDIUM	
TIPO PLC	ÚLTIMO SCORING 31/08/2026 13:20:53	
NIVEL PURDUE 1	ESTADO AUTORIZADO NO FIJADO CRÍTICO	
VULN RIESGO ● Crítica (9.8)	ÚLTIMO ESCANEO 31/08/2026 13:20:00	
FABRICANTE Rockwell Automation	ESTADO DEL ESCANEO No disponible	

Cerrar

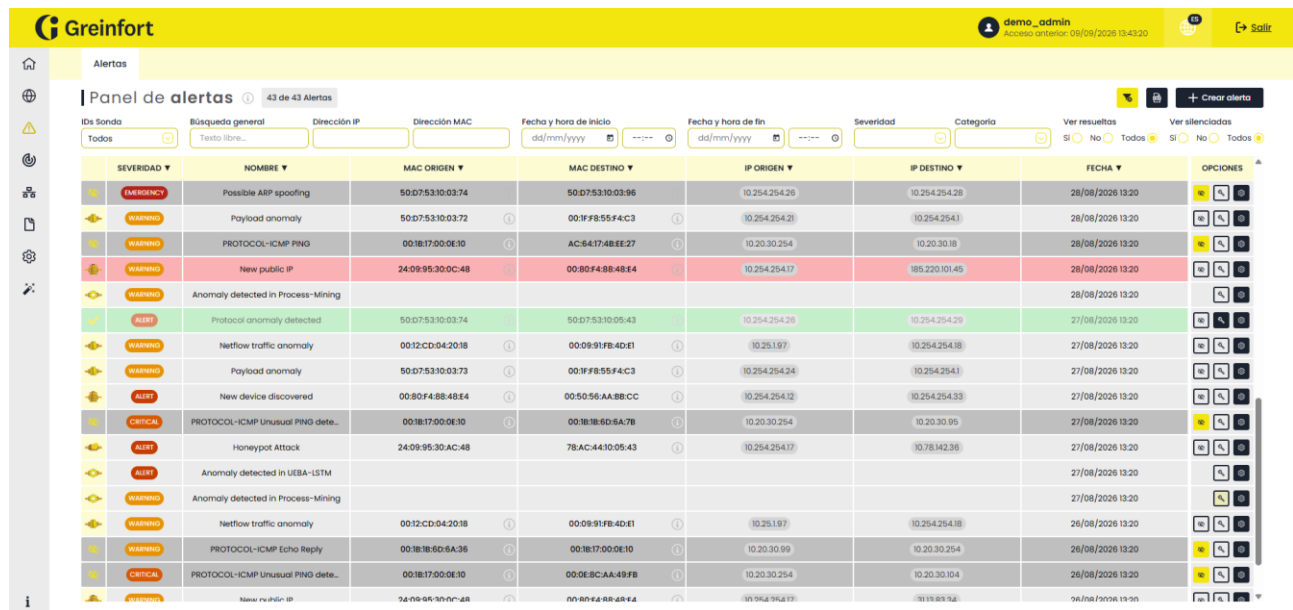
Detalles del dispositivo

AVISO: dada la naturaleza activa de esta operación, no puede descartarse por completo un posible impacto, aunque no se haya observado ninguno. Corresponde al cliente decidir si activa la función. Para excluir determinados dispositivos del análisis, se debe activar la propiedad "Crítico" en el inventario, de forma individual o mediante una actualización masiva.

Además, los dispositivos honeypot etiquetados como tales también están exentos debido a su comportamiento como señuelos con puertos vulnerables. Esto ayuda a prevenir la generación excesiva de falsos positivos.

4.3. Panel de alertas

Para acceder a la lista de alertas, el usuario debe hacer clic en el siguiente icono  en el lado izquierdo de la pantalla.



SEVERIDAD	NOMBRE	MAC ORIGEN	MAC DESTINO	IP ORIGEN	IP DESTINO	FECHA	OPCIONES
EMERGENCY	Possible ARP spoofing	50:D7:53:10:03:74	50:D7:53:10:03:96	10.254.254.25	10.254.254.28	28/08/2026 13:20	[Iconos]
WARNING	Payload anomaly	50:D7:53:10:03:72	00:3F:85:5F:4C:3	10.254.254.21	10.254.254.1	28/08/2026 13:20	[Iconos]
WARNING	PROTOCOL-ICMP PING	00:1B:17:00:0E:10	AC:54:17:ABEE:27	10.20.30.254	10.20.30.18	28/08/2026 13:20	[Iconos]
WARNING	New public IP	24:09:95:30:0C:48	00:80:F4:8B:4B:E4	10.254.254.17	185.220.101.45	28/08/2026 13:20	[Iconos]
WARNING	Anomaly detected in Process-Mining					28/08/2026 13:20	[Iconos]
ALERT	Protocol anomaly detected	50:D7:53:10:03:74	50:D7:53:10:05:43	10.254.254.25	10.254.254.29	27/08/2026 13:20	[Iconos]
WARNING	Netflow traffic anomaly	00:12:CD:04:20:18	00:09:91:F8:4D:E1	10.25.197	10.254.254.18	27/08/2026 13:20	[Iconos]
WARNING	Payload anomaly	50:D7:53:10:03:73	00:3F:85:5F:4C:3	10.254.254.24	10.254.254.1	27/08/2026 13:20	[Iconos]
ALERT	New device discovered	00:80:F4:8B:4B:E4	00:50:56:AA:8B:CC	10.254.254.12	10.254.254.33	27/08/2026 13:20	[Iconos]
CRITICAL	PROTOCOL-ICMP Unusual PING dete...	00:1B:17:00:0E:10	00:1B:1B:6D:5A:7B	10.20.30.254	10.20.30.99	27/08/2026 13:20	[Iconos]
ALERT	Honeypot Attack	24:09:95:30:AC:48	7B:AC:44:10:05:43	10.254.254.17	10.78.142.36	27/08/2026 13:20	[Iconos]
ALERT	Anomaly detected in UEBA-LSTM					27/08/2026 13:20	[Iconos]
WARNING	Anomaly detected in Process-Mining					27/08/2026 13:20	[Iconos]
WARNING	Netflow traffic anomaly	00:12:CD:04:20:18	00:09:91:F8:4D:E1	10.25.197	10.254.254.18	26/08/2026 13:20	[Iconos]
WARNING	PROTOCOL-ICMP Echo Reply	00:1B:1B:6D:5A:36	00:1B:17:00:0E:10	10.20.30.99	10.20.30.254	26/08/2026 13:20	[Iconos]
CRITICAL	PROTOCOL-ICMP Unusual PING dete...	00:1B:17:00:0E:10	00:0E:8C:AA:49:FB	10.20.30.254	10.20.30.104	26/08/2026 13:20	[Iconos]

Lista de alertas

Se mostrará una lista con todas las alertas presentes en la organización e información sobre ellas.

- Gravedad: clasificación de la alerta según su posible impacto en la organización.
- Nombre: nombre asignado a la alerta.
- MAC de origen: dirección MAC del dispositivo que genera la alerta.
- MAC de destino: dirección MAC del dispositivo al que se dirige la acción.
- IP de origen: dirección IP del dispositivo que genera la alerta.
- IP de destino: dirección IP del dispositivo al que se dirige la acción.
- Fecha: fecha y hora en que se genera la alerta.
- Acciones (véase el Anexo I para consultar las definiciones):



: Al situar el cursor encima, se muestra el nombre del dispositivo asignado a esa dirección MAC.



: Botón para cambiar el estado de la alerta a silenciado o no silenciado (véase “Clasificación de alertas” en el Anexo I).



: Botón para cambiar el estado de la alerta (resuelto o no resuelto), según la lógica indicada en el Anexo I.



: Botón para realizar acciones adicionales en la alerta, como ver los detalles o añadir notas.

Detalles alerta			
NOMBRE	FECHA	NOMBRE ORIGEN	CREADOR NOTA
Possible ARP spoofing	28/08/2026 13:20:53	PLC-07	No disponible
CATEGORÍA	MAC ORIGEN	NOMBRE DESTINO	
STATIC	50:D7:53:10:03:74	Sensor-Ch:AV	
PROTOCOLO	MAC DESTINO	VALOR	
No disponible	50:D7:53:10:03:96	50:d7:53:10:03:74	
SEVERIDAD	IP ORIGEN	DESCRIPCIÓN	
EMERGENCY	10.254.254.26	IP 10.254.254.28 MAC change: old -> 50:d7:53:10:05:55, new -> 50:d7:53:10:03:74	
ESTADO	IP DESTINO	NOTA	
SILENCIADA ACTIVA	10.254.254.28	No disponible	
ID SEDE	TIPO ORIGEN	FECHA DE NOTA	
1	1	No disponible	
ID Sonda	TIPO DESTINO		
probe	13		
Cerrar			

Detalles de alerta

Es posible filtrar la pantalla para mostrar solo las alarmas de interés. Este filtrado puede realizarse de la siguiente manera:

- ID de la sonda, para filtrar por zona de la red industrial y/o sede central
- Búsqueda general: introducción de un texto contenido en la alerta, incluidas las notas
- Dirección IP del dispositivo
- Dirección MAC del dispositivo
- Fecha y hora de inicio de la búsqueda de alertas
- Fecha y hora de finalización de la búsqueda de alertas
- Gravedad, según el Anexo I
- Alarmas resueltas o no resueltas, según el Anexo I
- Alarmas silenciadas o no, según el Anexo I

Al pulsar el botón, se restablecen los filtros y se vuelve a mostrar la lista completa de alarmas.



Mediante el botón correspondiente se exporta a un archivo CSV la lista de alarmas y su información.



Puede crearse manualmente una alarma específica en la red de la organización mediante el botón correspondiente. Aparecerá la siguiente ventana emergente:

Create alert

Title*	Protocol
Source IP	Description*
Destination IP	Severity*
Source MAC	Date
	dd/mm/yyyy
Destination MAC	Value

* Required fields

Cancel **Save**

Creación de alertas

La información de la nueva alarma debe introducirse manualmente. Para completar la creación, se debe hacer clic en "Guardar".

4.3.1. IP pública

Esta alerta está conectada a un servicio de ciberinteligencia que permite obtener información adicional sobre el extremo de comunicación situado fuera de la red de confianza, con el fin de determinar si puede ser malicioso.

Detalles alerta

[Datos de IP pública](#)

NOMBRE New public IP	FECHA 28/08/2026 13:20:53	NOMBRE ORIGEN Unknown-Dev-01	CREADOR NOTA No disponible
CATEGORÍA STATIC	MAC ORIGEN 24:09:95:30:0C:48	NOMBRE DESTINO PC Office	
PROTOCOLO TCP	MAC DESTINO 00:80:F4:88:48:E4	VALOR 185.220.101.45	
SEVERIDAD WARNING	IP ORIGEN 10.254.254.17	DESCRIPCIÓN Connection with public IP (destination IP: 185.220.101.45)	
ESTADO ACTIVA	IP DESTINO 185.220.101.45	NOTA No disponible	
ID SEDE 1	TIPO ORIGEN No aplica	FECHA DE NOTA No disponible	
ID Sonda probe	TIPO DESTINO No aplica		

Cerrar

Detalles de alerta

Para acceder a los detalles de la alerta, se debe hacer clic en el icono de engranaje situado a la derecha del panel y seleccionar "Ver detalles". A continuación, se muestra esta información:

En la parte superior de esta pestaña se encuentra el botón "Datos IP públicos". Al hacer clic en él, se muestra información adicional sobre la dirección IP, como la ciudad y región de origen, la zona horaria, el continente, el país, las coordenadas, la organización y el código postal.

Detalles IPs Públicas

[< Ir a detalles](#)

Nombre del país  Germany	Ubicación geográfica 50.1155,8.6842
Ciudad Frankfurt am Main	Organización AS205100 F3 Netze e.V.
Región Hesse	Código postal 60306
Zona horaria Europe/Berlin	Reputación Bad IP
Continente Europe	Fuente de reputación AbuseIPDB
Nombre de host tor-exit-45.relay.quintex.org	
IP 185.220.101.45	

Cerrar

Detalles de la IP pública

4.3.2. Política de reputación de IP y bloqueo

Cuando el sistema detecta una nueva alerta asociada a una conexión con una dirección IP pública, Greinfo consulta varias listas públicas en las que se notifican actividades consideradas abusivas (spam, hacking, etc.). Esta información enriquece la alerta con datos reputacionales y, si la dirección IP pública se considera sospechosa, modifica la gravedad y la descripción, y la resalta en rojo.

Alertas

Panel de alertas 43 de 43 alertas

IdS Sonda

Todos

Búsqueda general

Texto libre...

Dirección IP

Dirección MAC

Fecha y hora de inicio

dd/mm/yyyy

Fecha y hora de fin

dd/mm/yyyy

Severidad

Categoría

Ver resultados

Si No Todos

Ver silenciadas

Si No Todos

+ Crear alerta

SEVERIDAD	NOMBRE	MAC ORIGEN	MAC DESTINO	IP ORIGEN	IP DESTINO	FECHA	OPCIONES
EMERGENCY	Possible ARP spoofing	50:D7:53:10:03:74	50:D7:53:10:03:98	10.254.254.28	10.254.254.28	28/08/2028 13:20	
WARNING	Payload anomaly	50:D7:53:10:03:72	00:3F:85:5F:4C:3	10.254.254.21	10.254.254.1	28/08/2028 13:20	
WARNING	PROTOCOL-ICMP PING	00:18:17:00:0E:10	AC:54:17:ABEE:27	10.20.30.254	10.20.30.18	28/08/2028 13:20	
WARNING	New public IP	24:09:95:30:0C:48	00:80:F4:88:48:E4	10.254.254.17	185.220.101.45	28/08/2028 13:20	
WARNING	Anomaly detected in Process-Mining					28/08/2028 13:20	
ALERT	Protocol anomaly detected	50:D7:53:10:03:74	50:D7:53:10:05:43	10.254.254.28	10.254.254.29	27/08/2028 13:20	
WARNING	Netflow traffic anomaly	00:12:CD:04:20:18	00:08:91:F8:4D:E1	10.25.1.97	10.254.254.18	27/08/2028 13:20	
WARNING	Payload anomaly	50:D7:53:10:03:73	00:3F:85:5F:4C:3	10.254.254.24	10.254.254.1	27/08/2028 13:20	
ALERT	New device discovered	00:80:F4:88:48:E4	00:50:56:AA:8B:CC	10.254.254.12	10.254.254.33	27/08/2028 13:20	
CRITICAL	PROTOCOL-ICMP Unusual PING dete...	00:18:17:00:0E:10	00:18:18:6D:6A:78	10.20.30.254	10.20.30.95	27/08/2028 13:20	
ALERT	Honeypot Attack	24:09:95:30:AC:48	78:AC:44:10:05:43	10.254.254.17	10.78.142.36	27/08/2028 13:20	
ALERT	Anomaly detected in UEBA-ISTM					27/08/2028 13:20	
WARNING	Anomaly detected in Process-Mining					27/08/2028 13:20	
WARNING	Netflow traffic anomaly	00:12:CD:04:20:18	00:08:91:F8:4D:E1	10.25.1.97	10.254.254.18	26/08/2028 13:20	
WARNING	PROTOCOL-ICMP Echo Reply	00:18:18:6D:6A:36	00:18:17:00:0E:10	10.20.30.99	10.20.30.254	26/08/2028 13:20	
CRITICAL	PROTOCOL-ICMP Unusual PING dete...	00:18:17:00:0E:10	00:0E:8C:AA:49:F8	10.20.30.254	10.20.30.104	26/08/2028 13:20	

Dirección IP pública maliciosa resaltada en rojo

Detalles IPs Públicas

< Ir a detalles

Nombre del país

 Germany

Ciudad

Frankfurt am Main

Región

Hesse

Zona horaria

Europe/Berlin

Continente

Europe

Nombre de host

tor-exit-45.relay.quintex.org

IP

185.220.101.45

Ubicación geográfica

50.1155.8.6842

Organización

AS205100 F3 Netze e.V.

Código postal

60306

Reputación

Bad IP

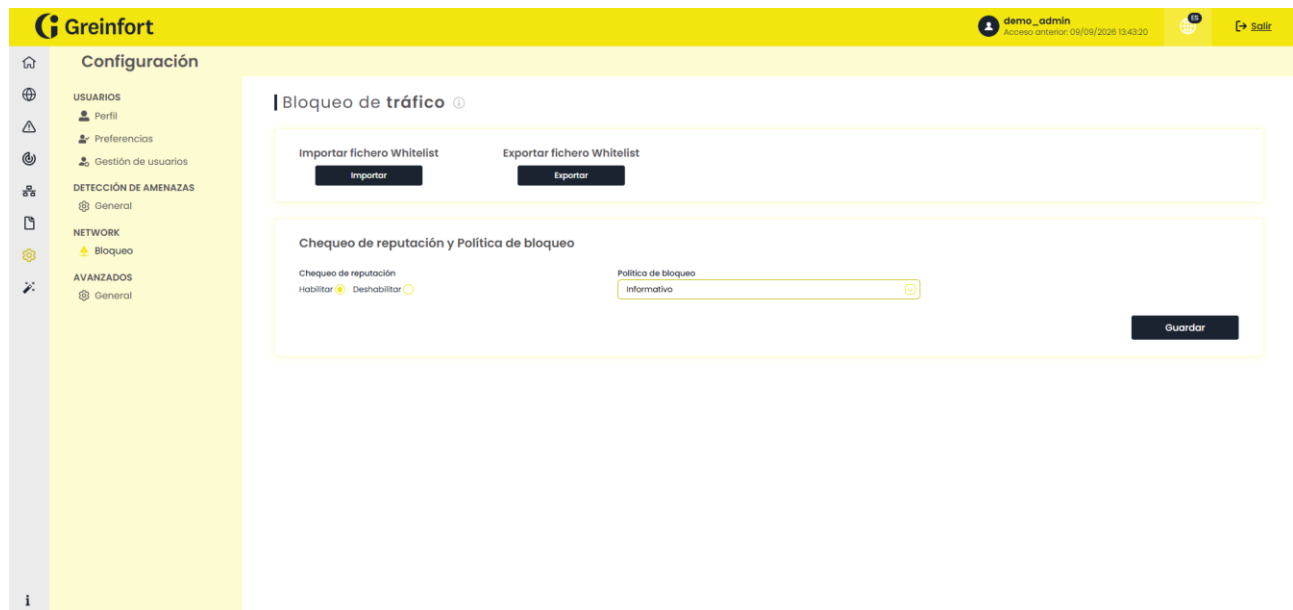
Fuente de reputación

AbuseIPDB

Cerrar

Detalles de una dirección IP pública con información reputacional

La comprobación de reputación puede activarse y desactivarse en el menú de configuración en la sección de Bloqueo de Tráfico. Esta opción afecta a las alertas entrantes, es decir, habilitar la reputación no afectará retroactivamente a las alertas públicas de IP que llegaron mientras la reputación estaba desactivada.



Configuración de reputación y bloqueo

Cuando el sistema recibe una alerta asociada a una dirección IP pública considerada maliciosa, Greinfort responde aplicando una de las tres políticas de bloqueo disponibles:¹

- Informativa: se notifica la situación y se recomienda revisar y bloquear el tráfico desde o hacia esa dirección;
- Manual o semiautomática: se habilita un botón para bloquear o desbloquear la dirección IP mediante una instrucción al cortafuegos;
- Automática: Greinfort envía la instrucción al cortafuegos sin intervención humana.

La Política de Bloqueo también puede desactivarse. En este caso, toda la información sobre la reputación IP en las alertas será deshabilitada, así como las reglas de bloqueo (enviando un comando al cortafuegos para eliminar la regla de bloqueo de direcciones). Esta información no se elimina y se volverá a aplicar si la Política de Bloqueo se vuelve a seleccionar como valor activo. En el mismo menú se puede encontrar un selector desplegable para la Política de Bloqueo. Las alertas públicas de IP que llegan al sistema mientras la Política de Bloqueo está desactivada no cambian retroactivamente cuando se vuelve a activar la Política de Bloqueo.

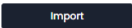
4.3.3. Lista blanca de IP

Puede proporcionarse una lista de direcciones IP o rangos en formato CIDR que siempre estarán permitidos (lista blanca). Su reputación no se evalúa, aunque la comprobación esté activada al recibirse una alerta relacionada. En el menú de datos de IP pública, el campo de reputación las identifica como incluidas en la lista blanca.

El archivo de carga debe estar en formato CSV y contener una única columna por fila, con una dirección IP (192.168.0.1) o un rango CIDR (192.168.1.0/24). La carga es atómica: un solo dato con formato incorrecto o no válido invalida toda la operación. Las redundancias de direcciones y rangos

¹ La disponibilidad de las opciones no informativas dependerá del contexto del cliente, en particular del fabricante/modelo del cortafuegos con el que Greinfort debe comunicarse. En caso de dudas adicionales, debe contactarse con el equipo de Soporte.

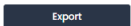
(direcciones repetidas, direcciones incluidas en rangos CIDR o rangos superpuestos) no se consideran errores.

La importación se realiza desde las opciones de bloqueo mediante el botón situado bajo "Importar archivo de lista blanca". En la ventana emergente se puede arrastrar el archivo al área verde o seleccionarlo desde el árbol de archivos. 

Las importaciones posteriores sustituyen por completo la lista blanca anterior. Para no aplicar ninguna lista blanca, se debe cargar un archivo vacío.

Subir una nueva lista blanca influye en las alertas IP públicas que ya están en la base de datos:

- Las alertas cuyas direcciones IP ya se hayan procesado y estén incluidas en la nueva lista blanca vuelven a su estado original y se marcan como "incluidas en la lista blanca".
- Las alertas cuyas direcciones IP estaban incluidas en la lista blanca anterior pero no en la nueva se someten al cálculo de reputación y su descripción se modifica en consecuencia.

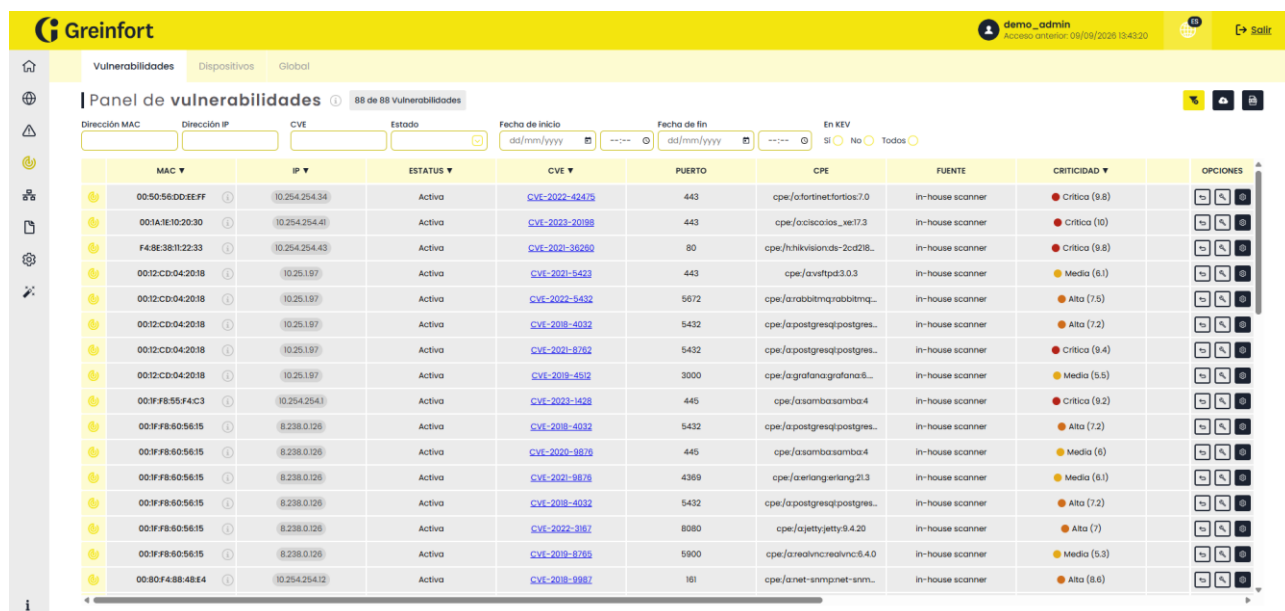
La lista blanca cargada puede descargarse para su revisión mediante el botón correspondiente, que genera un archivo CSV con los datos guardados. 

4.4. Análisis de vulnerabilidades

4.4.1. Panel de vulnerabilidades

Para acceder al panel de vulnerabilidades, el usuario debe hacer clic en el icono  que aparece en el lado izquierdo de la pantalla y seleccionar la pestaña "Panel de vulnerabilidades".

En la pestaña "Panel de vulnerabilidades" se muestra una lista de todas las vulnerabilidades presentes en la red. Se localizan en los servicios asociados a los puertos abiertos detectados por Smart View y se comparan con la National Vulnerability Database (NVD) del NIST y con el catálogo de CISA.



The screenshot shows the 'Panel de vulnerabilidades' interface in the Greinfort application. The interface has a yellow header with the Greinfort logo, user 'demo_admin', and a 'Salir' button. Below the header, there are tabs for 'Vulnerabilidades', 'Dispositivos', and 'Global'. The 'Vulnerabilidades' tab is active, showing a table of vulnerabilities. The table has columns for MAC, IP, ESTATUS, CVE, PUERTO, CPE, FUENTE, CRITICIDAD, and OPCIONES. The table contains 18 rows of data, each representing a vulnerability found on a specific IP address. The 'OPCIONES' column contains icons for each row, likely for actions like 'Ver', 'Editar', and 'Eliminar'.

MAC	IP	ESTATUS	CVE	PUERTO	CPE	FUENTE	CRITICIDAD	OPCIONES
00:50:56:00:EEFF	10.254.254.34	Activa	CVE-2022-42475	443	cpe:/a:fortinet:fortios:7.0	in-house scanner	Critica (9.8)	
00:1A:1E:10:20:30	10.254.254.41	Activa	CVE-2023-20398	443	cpe:/a:cisco:ios_xe:17.3	in-house scanner	Critica (10)	
F4:8E:38:1F:22:33	10.254.254.43	Activa	CVE-2022-36260	80	cpe:/h:hikvision:ds-2cd28...	in-house scanner	Critica (9.8)	
00:12:CD:04:20:18	10.25.197	Activa	CVE-2021-5423	443	cpe:/a:avast:avast3.0.3	in-house scanner	Media (6.1)	
00:12:CD:04:20:18	10.25.197	Activa	CVE-2022-5432	5672	cpe:/a:arabimq:rabbitmq...	in-house scanner	Alta (7.5)	
00:12:CD:04:20:18	10.25.197	Activa	CVE-2018-4032	5432	cpe:/a:postgresql:postgres...	in-house scanner	Alta (7.2)	
00:12:CD:04:20:18	10.25.197	Activa	CVE-2021-8762	5432	cpe:/a:postgresql:postgres...	in-house scanner	Critica (9.4)	
00:12:CD:04:20:18	10.25.197	Activa	CVE-2018-4592	3000	cpe:/a:grafana:grafana5...	in-house scanner	Media (5.5)	
00:1F:F8:55:F4:C3	10.254.254.1	Activa	CVE-2023-1428	445	cpe:/a:samba:samba:4	in-house scanner	Critica (9.2)	
00:1F:F8:60:56:15	8.238.0.126	Activa	CVE-2018-4032	5432	cpe:/a:postgresql:postgres...	in-house scanner	Alta (7.2)	
00:1F:F8:60:56:15	8.238.0.126	Activa	CVE-2020-9876	445	cpe:/a:samba:samba:4	in-house scanner	Media (6)	
00:1F:F8:60:56:15	8.238.0.126	Activa	CVE-2021-9876	4369	cpe:/a:erlang:erlang:21.3	in-house scanner	Media (6.1)	
00:1F:F8:60:56:15	8.238.0.126	Activa	CVE-2018-4032	5432	cpe:/a:postgresql:postgres...	in-house scanner	Alta (7.2)	
00:1F:F8:60:56:15	8.238.0.126	Activa	CVE-2022-3167	8080	cpe:/a:jetty:jetty:9.4.20	in-house scanner	Alta (7)	
00:1F:F8:60:56:15	8.238.0.126	Activa	CVE-2018-8765	5900	cpe:/a:realvnc:realvnc:6.4.0	in-house scanner	Media (5.3)	
00:80:F4:8B:4B:E4	10.254.254.12	Activa	CVE-2018-8887	181	cpe:/a:net-snmp:net-snmp...	in-house scanner	Alta (8.6)	

Panel de vulnerabilidades

 demo_admin Acceso anterior: 08/08/2026 13:43:20										
Vulnerabilidades Dispositivos Global										
Panel de vulnerabilidades 88 de 88 Vulnerabilidades										
Dirección MAC	Dirección IP	CVE	Estado	Fecha de inicio	Fecha de fin	En KEV				
				dd/mm/yyyy	dd/mm/yyyy	SI No Todos				
CPE	FUENTE	CRITICIDAD	CWE	FECHA DESCUBRIMIENTO	FECHA PUBLICACIÓN	VISTO ÚLTIMA VEZ	KEV AÑADIDA	KEV VENCIMIENTO	OPCIONES	
cpe:/a:fortinet:fortios:7.0	in-house scanner	Critica (9.8)	CWE-787	31/08/2026	19/06/2026	31/08/2026	13/12/2022	03/01/2023		
cpe:/o:ciocaios:_se17.3	in-house scanner	Critica (10)	CWE-289	31/08/2026	19/06/2026	31/08/2026	16/10/2023	20/10/2023		
cpe:/h:hikvision:ds-2cd288...	in-house scanner	Critica (9.8)	CWE-78	31/08/2026	19/06/2026	31/08/2026	10/01/2022	24/01/2022		
cpe:/a:vsftpd:3.0.3	in-house scanner	Media (6.1)	CWE-364	31/08/2026	19/06/2026	31/08/2026				
cpe:/a:rabbitmq:rabbitmq...	in-house scanner	Alta (7.5)	CWE-390	31/08/2026	19/06/2026	31/08/2026				
cpe:/a:postgres:postgres...	in-house scanner	Alta (7.2)	CWE-287	31/08/2026	19/06/2026	31/08/2026				
cpe:/a:postgres:postgres...	in-house scanner	Critica (9.4)	CWE-352	31/08/2026	19/06/2026	31/08/2026				
cpe:/a:grafana:grafana:8...	in-house scanner	Media (5.5)	CWE-838	31/08/2026	19/06/2026	31/08/2026				
cpe:/a:samba:samba:4	in-house scanner	Critica (9.2)	CWE-352	31/08/2026	19/06/2026	31/08/2026				
cpe:/a:postgres:postgres...	in-house scanner	Alta (7.2)	CWE-287	31/08/2026	19/06/2026	31/08/2026				
cpe:/a:samba:samba:4	in-house scanner	Media (6)	CWE-475	31/08/2026	19/06/2026	31/08/2026				
cpe:/a:erlang:erlang:21.3	in-house scanner	Media (6.1)	CWE-475	31/08/2026	19/06/2026	31/08/2026				
cpe:/a:postgres:postgres...	in-house scanner	Alta (7.2)	CWE-287	31/08/2026	19/06/2026	31/08/2026				
cpe:/o:jetty:jetty:9.4.20	in-house scanner	Alta (7)	CWE-475	31/08/2026	19/06/2026	31/08/2026				
cpe:/a:realvnc:realvnc:6.4.0	in-house scanner	Media (5.3)	CWE-200	31/08/2026	19/06/2026	31/08/2026				
cpe:/a:net-snmp:net-snmp...	in-house scanner	Alta (8.6)	CWE-339	31/08/2026	19/06/2026	31/08/2026				

Detalle del panel de vulnerabilidades

La información que se muestra en cada fila es la siguiente:

- Dirección MAC: la dirección MAC del dispositivo donde se ha detectado la vulnerabilidad.
- Estado: indica si la vulnerabilidad está activa, resuelta, silenciada o es un falso positivo.
- CVE: "Vulnerabilidades y exposiciones comunes". Identificador según el glosario de clasificación de vulnerabilidades.
- Puerto: puerto del dispositivo.
- CPE: "Enumeración común de plataformas." Identificador del producto o sistema afectado por la vulnerabilidad en cuestión.
- Fuente: sistema o dispositivo que encontró la vulnerabilidad.
- Criticidad: puntuación de 0 a 10, asignada según el nivel de severidad de la vulnerabilidad.
- CWE: "Enumeración común de debilidades." Identificador de la debilidad común asociada a la vulnerabilidad encontrada.
- Fecha de descubrimiento: fecha en la que se detectó la vulnerabilidad.
- Fecha de publicación: fecha en la que la vulnerabilidad referenciada mediante el CVE se publicó en la base de datos NVD.
- "Última vez visto": marca temporal en la que se vio la vulnerabilidad por última vez.
- KEV AÑADIDA: KEV corresponde a "Vulnerabilidades Explotadas Conocidas". Es el catálogo de CISA de CVE explotados activamente en entornos reales; se muestra la fecha de inclusión y un  cuando el CVE está vinculado a campañas de ransomware.
- KEV VENCIMIENTO: fecha límite propuesta por CISA para la resolución del CVE correspondiente.
- Opciones (Acciones):



Ir a: permite ver las alertas generadas por esta vulnerabilidad o los dispositivos en los que está presente.



Cambiar estado (activo, resuelto, silenciado o falso positivo).



Otras acciones: permite ver los detalles de una vulnerabilidad y añadir una nota.

Detalles Vulnerabilidad

ID SEDE 1	CWE CWE-787	DESCRIPCIÓN Heap-based buffer overflow in FortiOS SSL-VPN allows
MAC 00:50:56:DD:EE:FF	ESTADO Activa	FECHA DE INCLUSIÓN KEV 13/12/2022
IP 10.254.254.34	NOTA No disponible	FECHA LÍMITE KEV 03/01/2023
CVE CVE-2022-42475	CREADOR NOTA No disponible	<i>Esta vulnerabilidad ha sido vinculada a campañas de ransomware</i>
PUERTO 443	FECHA DE NOTA No disponible	
CPE cpe:/o:fortinet:fo	FECHA DESCUBRIMIENTO 31/08/2026 13:20:54	
ORIGEN in-house scanner	FECHA PUBLICACIÓN 19/06/2026 12:36:57	
CRITICIDAD ● Crítica (9.8)	VISTO ÚLTIMA VEZ 31/08/2026 13:20:54	

Cerrar

Detalles de una vulnerabilidad

Junto al encabezado se muestra el número de vulnerabilidades visibles y el recuento total.

Panel de vulnerabilidades ⓘ 88 de 88 Vulnerabilidades

Dirección MAC	Dirección IP	CVE	Estado	Fecha de inicio	Fecha de fin	En KEV
						☐ Sí ☐ No ☐ Todos

Número de vulnerabilidades y filtros

En la captura de pantalla superior se observa que pueden aplicarse filtros para mostrar únicamente las vulnerabilidades de interés. El filtrado se realiza mediante:

- Dirección MAC
- CVE
- Estado
- Fecha y hora de inicio
- Fecha y hora de finalización
- Presencia en el catálogo KEV



Al pulsar el botón , los valores del filtro se restablecerán y la lista completa con todas las vulnerabilidades se mostrará de nuevo.

Mediante el botón correspondiente se puede importar un archivo CSV con las vulnerabilidades que se desea añadir. El archivo debe contener los campos siguientes y mantener las fechas en el formato YYYY-MM-DDTHH:MM:SS.000GMT+XX:XX:

- ID de proveedor
- Dirección MAC
- CVE

- Puerto
- CPE (Opcional)
- Fuente
- Criticidad
- CWE (Opcional)
- Estado
- URL
- Nota (Opcional)
- Nota del creador (opcional)
- Marca de tiempo descubierta
- Marca de tiempo publicada
- Última vez que se vio con marca de tiempo

Mediante el botón correspondiente se puede exportar un archivo CSV con la lista de vulnerabilidades y su información. 

4.4.2. Estadísticas del dispositivo

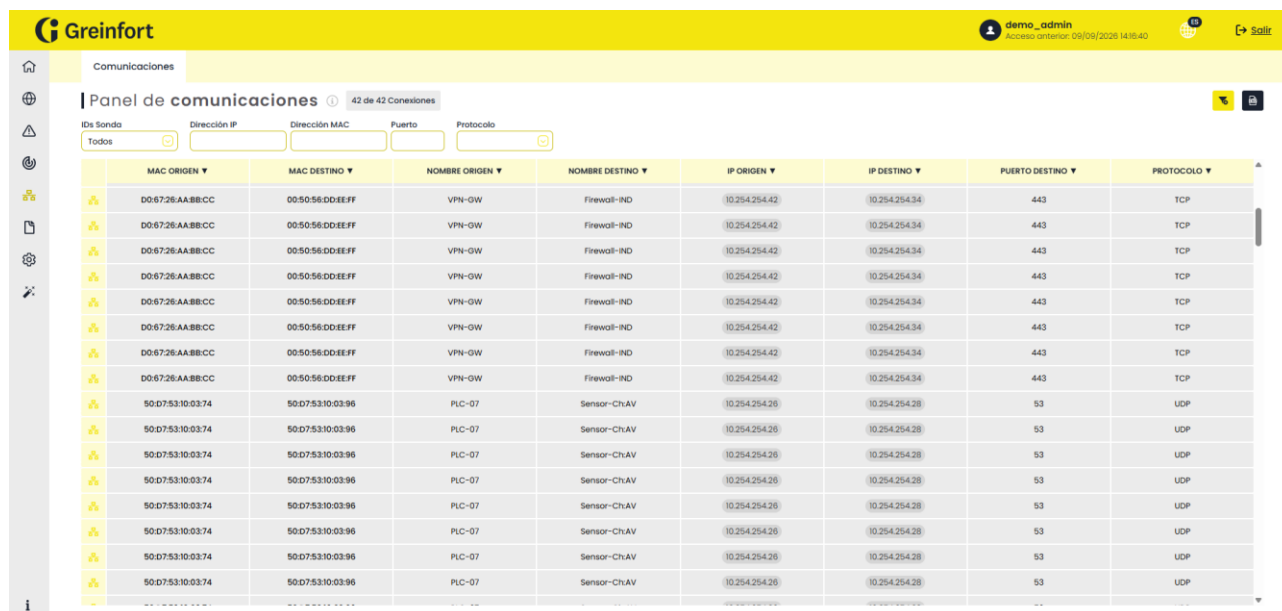
Muestra las vulnerabilidades encontradas en la red, clasificadas por dispositivo.

4.4.3. Estadísticas globales

Proporciona estadísticas globales de la red a partir de sus vulnerabilidades.

4.5. Comunicaciones

Para acceder a la lista de comunicaciones, el usuario debe hacer clic en el icono  que aparece en el lado izquierdo de la pantalla.



MAC ORIGEN ▼	MAC DESTINO ▼	NOMBRE ORIGIN ▼	NOMBRE DESTINO ▼	IP ORIGEN ▼	IP DESTINO ▼	PUERTO DESTINO ▼	PROTOCOLO ▼
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP

Lista de comunicaciones

Se muestra una lista de todas las comunicaciones realizadas entre los dispositivos de OT de la red de la organización, así como información sobre estas.

Una comunicación se entiende como el agrupamiento de conexiones entre MAC, IP y puerto de origen, y lo mismo para el destino. Se considera una comunicación nueva si hay un cambio de protocolo.

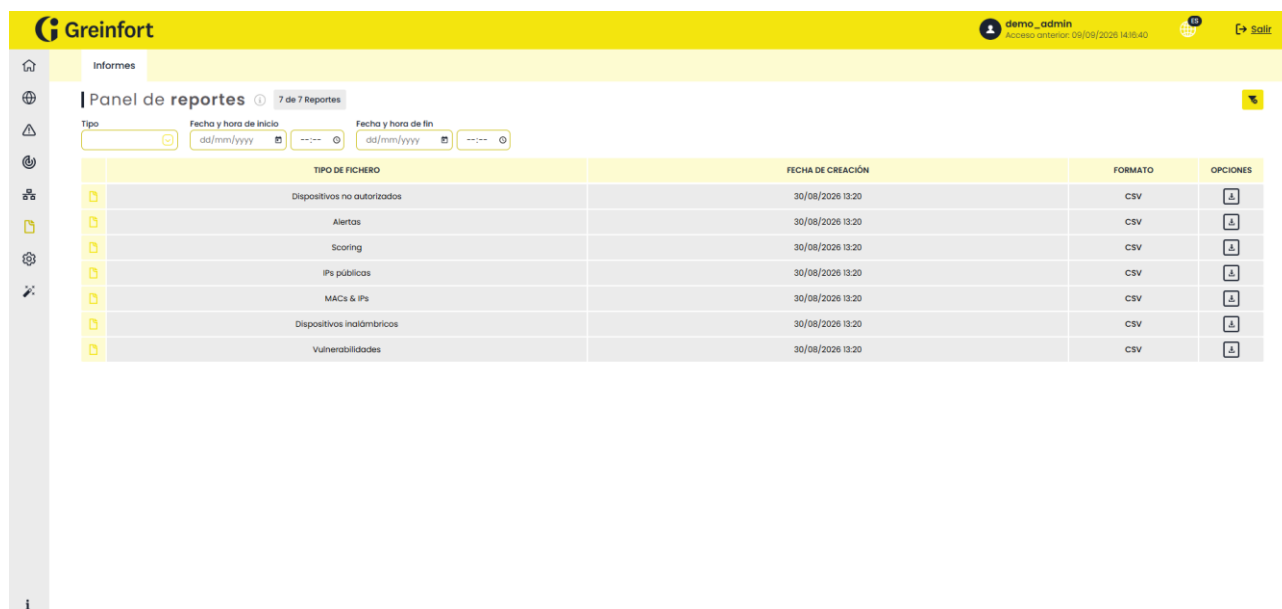
Panel de comunicaciones ⓘ 42 de 42 Conexiones

IDs Sonda: Dirección IP: Dirección MAC: Puerto: Protocolo:

Filtros de comunicaciones disponibles

4.6. Informes

Para acceder a la lista de informes, el usuario debe hacer clic en el icono  que aparece en el lado izquierdo de la pantalla.



TIPO DE FICHERO	FECHA DE CREACIÓN	FORMATO	OPCIONES
Dispositivos no autorizados	30/08/2026 13:20	CSV	
Alertas	30/08/2026 13:20	CSV	
Scoring	30/08/2026 13:20	CSV	
IPs públicas	30/08/2026 13:20	CSV	
MACs & IPs	30/08/2026 13:20	CSV	
Dispositivos inalámbricos	30/08/2026 13:20	CSV	
Vulnerabilidades	30/08/2026 13:20	CSV	

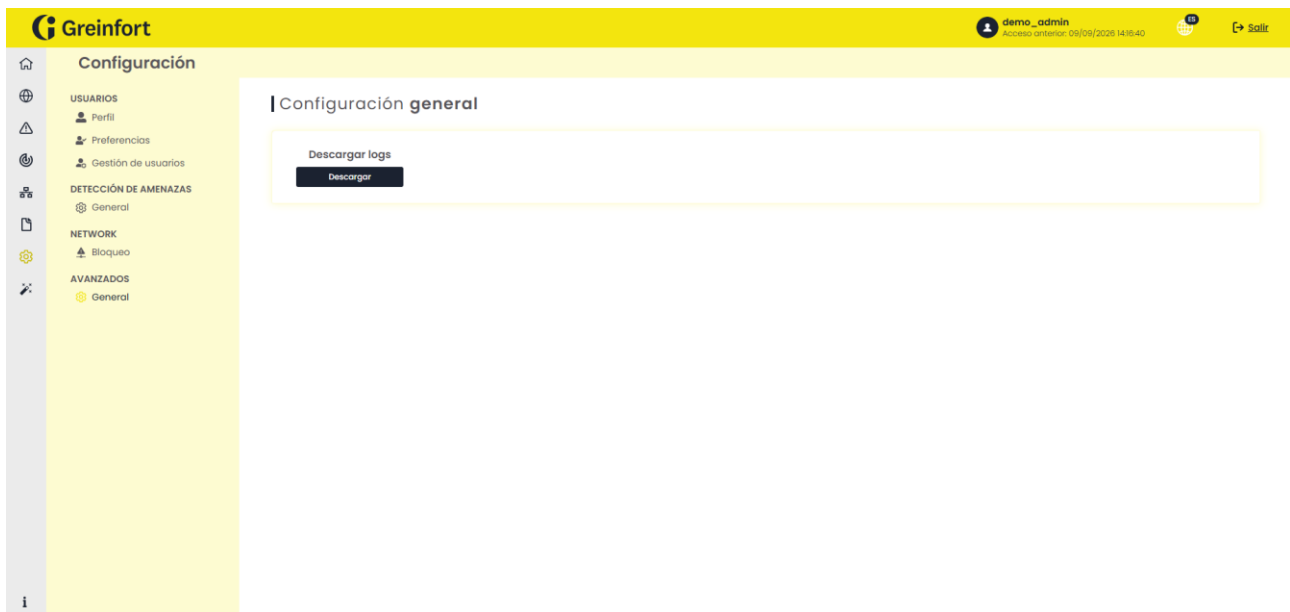
Últimos informes disponibles

La pantalla muestra una lista de los informes generados manual o automáticamente con una periodicidad determinada. Los informes están disponibles para su descarga.

4.7. Otros escenarios

En la configuración, se pueden personalizar diferentes parámetros del Servicio.

En la sección General Avanzado, el usuario puede descargar los registros del sistema.



Sección de registros de exportación

En la Detección de Amenazas, el estado general de las diferentes estrategias de detección de anomalías se presenta inicialmente en modo semáforo:



Pantalla de configuración del algoritmo

Amenazas basadas en reglas

- Rojo: todas las reglas están en modo entrenamiento, inactivas o no cubiertas por su campo de estado.
- Naranja: algunas reglas están en modo de producción, pero no todas.
- Verde: todas las reglas están en modo producción.
- Gris: no existen reglas.

Amenazas basadas en IA/ML

- Rojo: todas las reglas están en modo entrenamiento, inactivas o no cubiertas por su campo de estado.
- Naranja: algunos algoritmos están en modo de producción, pero no todos.
- Verde: todos los algoritmos están en modo producción.
- Gris: no existen algoritmos.

Amenazas basadas en firmas

- Rojo: todos los elementos están en modo de entrenamiento o inactivos, o su campo de estado no está cubierto.
- Naranja: algunos de los elementos tienen un valor distinto a activo, pero no todos.
- Verde: todos los elementos tienen un estado igual a activo y el campo signature_timestamp tiene menos de siete días.
- Gris: no existen elementos.

5. ANEXO I: Clasificación de dispositivos y alertas

5.1. Clasificación de dispositivos

5.1.1. Según el Estado

- **Autorizado/No autorizado:** los dispositivos autorizados son aquellos que el cliente ha reconocido explícitamente como legítimos.
- **Crítico/No crítico:** Greinfort no interactúa activamente con los dispositivos marcados como críticos, por ejemplo, equipos antiguos, sin soporte de mantenimiento o sin repuestos.
- **Fijos/No fijos:** Los dispositivos fijos aparecerán en la aplicación Greinfort aunque no hayan establecido ninguna comunicación en la red de la organización. Por ejemplo, dispositivos temporalmente aislados de la red para mantenimiento.

5.2. Clasificación de alertas

5.2.1. Según el Estado

- **Resuelto/No resuelto:** las alarmas resueltas ya han sido gestionadas, pero se desea conservar su aparición ante situaciones futuras idénticas (misma tipología, direcciones MAC, direcciones IP y puertos implicados). Las alarmas no resueltas están pendientes de gestión.
- **Silenciado/No silenciado:** las alarmas silenciadas no vuelven a generarse en el mismo contexto de red. Por ejemplo, puede silenciarse la comunicación de un dispositivo con una dirección IP pública conocida y controlada por la organización.

Cabe mencionar que las alarmas silenciadas, aunque no se muestren al usuario, se almacenan en una base de datos para su posterior consulta por parte del personal de Greinfort a petición del cliente, si es necesario.

5.2.2. Según la gravedad

Los niveles de gravedad utilizados para las alertas se basan en el RFC 5424, aunque no son equivalentes, ya que los eventos se han catalogado de acuerdo con la experiencia del personal técnico.

De mayor a menor gravedad, las alertas se clasifican de la siguiente manera:

- Emergencia
- Alerta
- Crítica
- Error
- Advertencia
- Aviso

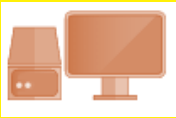
- Informativo
- Depuración

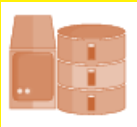
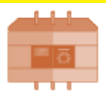
6. ANEXO II: Iconos de Activos y Nivel Purdue

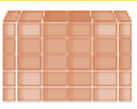
El modelo de Purdue define los siguientes niveles para los dispositivos existentes:

- Nivel 0: Dispositivos de campo, como sensores o actuadores.
- Nivel 1: Controladores básicos, PLCs, dispositivos de E/S y la primera capa de seguridad.
- Nivel 2: Dispositivos de monitorización, supervisión y representación (sistemas SCADA y HMI, interfaces o servidores de datos históricos).
- Nivel 3: Dispositivos de gestión de operaciones y sistemas, como servidores de bases de datos y MES. Planificación en tiempo real y control de producción.
- Nivel 4: Dispositivos de gestión empresarial, como ERP, CRM o sistemas SCM.

Ciertos dispositivos pueden cambiar su nivel Purdue dependiendo de su función y ubicación.

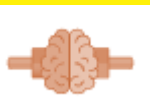
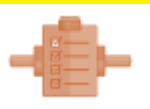
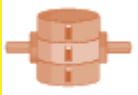
Icono	Descripción	Nivel PURDUE
	PC	2
	SCADA	2
	DCS	2
	Virtual	2
	HMI	2
	TABLETA	2
	TELÉFONO VOIP	2

	SERVIDOR	2
	TELÉFONO	2
	RTU	1
	VS-CAM	1
	LECTOR DE CÓDIGOS DE BARRAS	1
	PLC	1
	ROBOT	0
	VARIADOR DE FRECUENCIA	0
	TARJETA CONTROLADOR	0
	SENSOR	0
	AFD	0
	SWITCH	Varios

	ENRUTADOR	Varios
	CORTAFUEGOS	Varios
	OTROS	Varios
	HONEYPOT	Varios

Iconos representativos de dispositivos

7. ANEXO III: Iconos de alertas

Icono	Descripción
	Alerta manual
	Alerta de aprendizaje automático
	Alerta de regla estática
	Alerta IDS
	Alerta de honeypot

Iconos representativos de alertas



Greinform Solutions S.L

Maria Berdiales 20, 4º.
36203 | Vigo | Spain

(+34) 886 251 058

info@greinform.com

sales@greinform.com