InprOTech

Smart security for your industry

Manual de usuario

InprOTech Guardian

Fecha: 06/2026

Referencia del documento: IN-User Manual InprOTech Guardian

Versión: 0.18

ÍNDICE

1 Introducción

InprOTech Guardian es una herramienta de detección de activos y monitorización y detección de anomalías capaz de identificar amenazas de ciberseguridad en entornos industriales. Analiza el tráfico de red, identifica activos en la red, genera informes completos y genera alertas utilizando reglas estáticas, firmas IDS e inteligencia artificial para mitigar amenazas en la red industrial.

La interfaz de InprOTech Guardian es altamente interactiva, fácil de entender y manejable. Además, está disponible en inglés, español, catalán, vasco y gallego.

Esta interfaz se desarrolla utilizando el marco Angular siguiendo las mejores prácticas y metodologías de seguridad para garantizar una navegación segura de la información.

A través de la aplicación InprOTech Guardian, el usuario tendrá una visión completa y conocimiento 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.
- **Resumen del** activo: Visualización del número de dispositivos conectados a la red, clasificados según el modelo PURDUE.
- **Acceso rápido**: a alertas, vulnerabilidades, algoritmos y reglas activas.
- **Gráfico de tráfico de red**: Gráfico del tráfico generado, tanto enviado como recibido, en las últimas 24 horas y en comparación con el mismo periodo 7 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.
- **Mapeo de red**: Visualización de todos los dispositivos de red, cómo están conectados y cómo está estructurada la red de la organización. También visualizará todos esos dispositivos conectados y que no se han considerado legítimos.
- **Gestor de dispositivos**: Lista de activos, cableados o inalámbricos, para identificación y gestión. Incluyendo la identificación y etiquetado de dispositivos, o la inclusión de dispositivos en la lista negra según su nivel de criticidad. Además, el usuario puede definir campos personalizables para clasificar y filtrar los dispositivos de red, con un inventario virtual de los campos creados que puede organizarse, filtrarse y exportarse.
- **Responsable de** alertas: Lista de eventos y alertas en la red de TO de la organización, clasificados según su nivel de gravedad. Están codificados por colores y detallados con información dinámica. Se clasificarán según su estado (resueltos y silenciados), y se generarán en base a heurísticas, firmas IDS e inteligencia artificial/aprendizaje automático.
- **Integración con sistemas de terceros (SIEM):** Guardian 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.

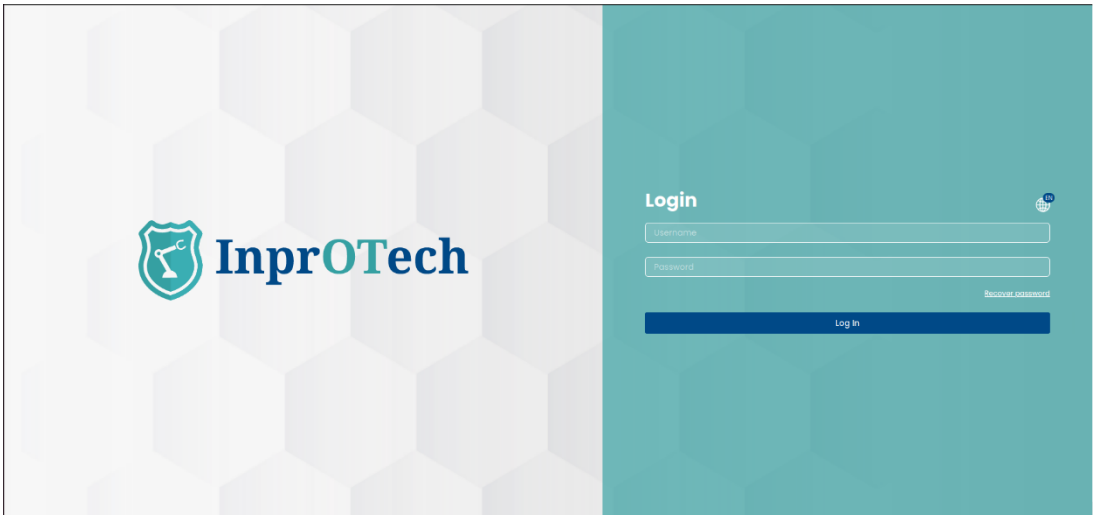
- **Reputación de la IP pública:** En caso de conexiones a direcciones IP públicas, su reputación será analizada automáticamente, destacando visualmente aquellas para las que se recomienda una acción activa de mitigación. El usuario tendrá la posibilidad de subir una lista de IPs que siempre estarán permitidas.
- **Lista de** comunicaciones: Lista con todas las comunicaciones realizadas entre dispositivos de TO en la red de la organización e información sobre ellos.
- **Generación de informes**: Compilación de información sobre la red, dispositivos, indicadores, etc., para su análisis y verificación futura tanto a nivel técnico como empresarial.

Es importante señalar que, además del uso de la propia aplicación, el servicio implica una serie de preparativos para la incorporación, que incluyen la recogida adecuada de datos, despliegue, instalación y ajuste fino de la solución para sacarle el máximo partido, basándose en acciones como las indicadas en la siguiente sección.

2 Primeros pasos

2.1 Acceso a consolas web

Primero, accede al navegador e introduce la dirección http://[IP]:9000, donde IP es la dirección asignada a la interfaz de gestión.



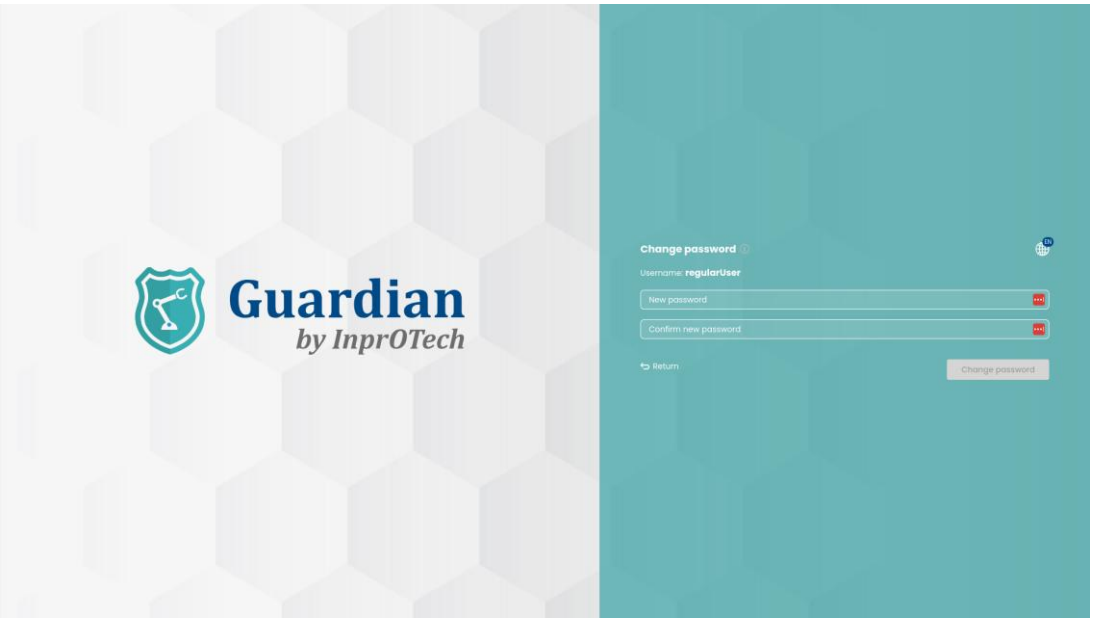
Pantalla de inicio de sesión de InprOTech Guardian

En cualquier momento, puedes seleccionar el idioma que prefieras en el icono del mapa mundial (inglés, español, catalán, vasco, gallego).

El usuario debe autenticarse introduciendo el nombre de usuario y la contraseña que se le asignan. En caso de que se active el segundo factor de autenticación, deben introducir además el token de un solo uso recibido por correo electrónico en su cuenta de correo de usuario del 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:

1. Introduce la nueva contraseña en el primer campo.
2. Confirma la nueva contraseña en el segundo campo.
3. Haz 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.

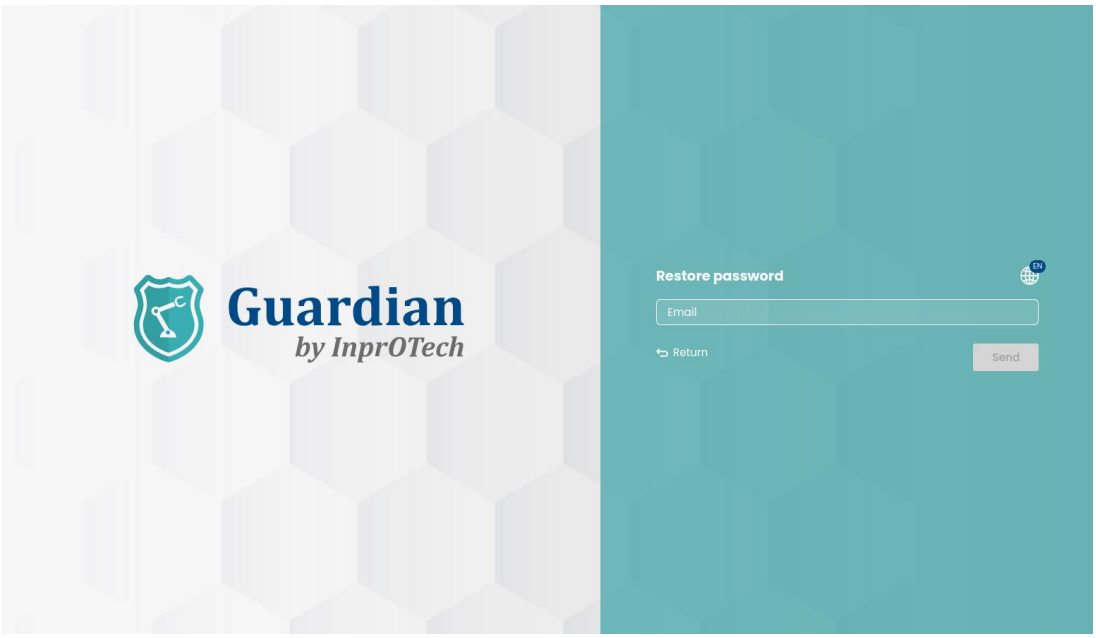
El usuario puede ser:

- **Administrador**: Tendrá acceso a toda la información presentada por la aplicación y podrá hacer las configuraciones que considere apropiadas para algoritmos, identificadores de fábrica, modos de producción, etc.

- **Operador**: Acceso como en el caso anterior, excepto por la parte de configuración específica mencionada anteriormente.

- **Monitor:** Usuario con permisos exclusivos de lectura. Tendrán acceso a descargar manuales, informes y exportar resultados de búsqueda y ciertas 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".

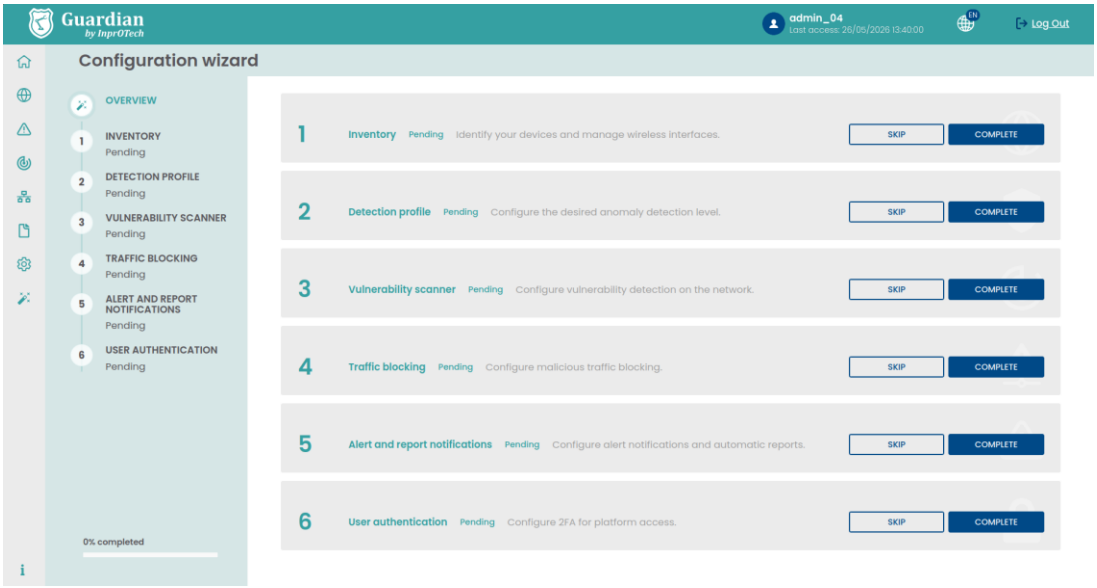


Pantalla de recuperación de contraseñas

Al introducir la dirección de correo electrónico, si es válida, se enviará un enlace a la dirección de correo electrónico para restablecer la contraseña de acceso mediante un token de uso único.

**Esta funcionalidad, así como otras necesarias para actualizaciones de software de Guardian o acceso remoto, requieren conectividad entre el sistema y ciertos servicios InprOTech o de internet, por lo que se proporcionará la lista de reglas que se aplicarán en el cortafuegos.*

Cuando inicies sesión por primera vez, se abrirá el asistente de configuración de Guardian. Aquí, el usuario será guiado a través de la configuración inicial de la solución. Se dividirá en seis etapas, cada una de las cuales debe completarse (o, alternativamente, saltarse).

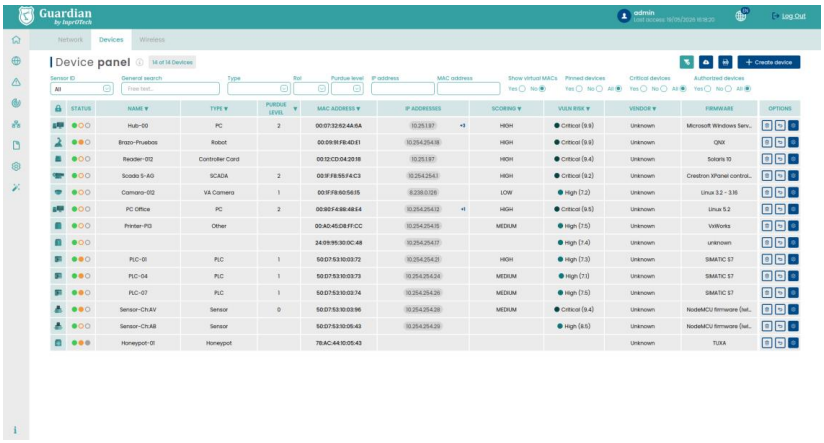


2.2 Organización de la lista de dispositivos

La lista de dispositivos debe organizarse declarando el nombre de cada dispositivo, así como su nivel PURDUE 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.

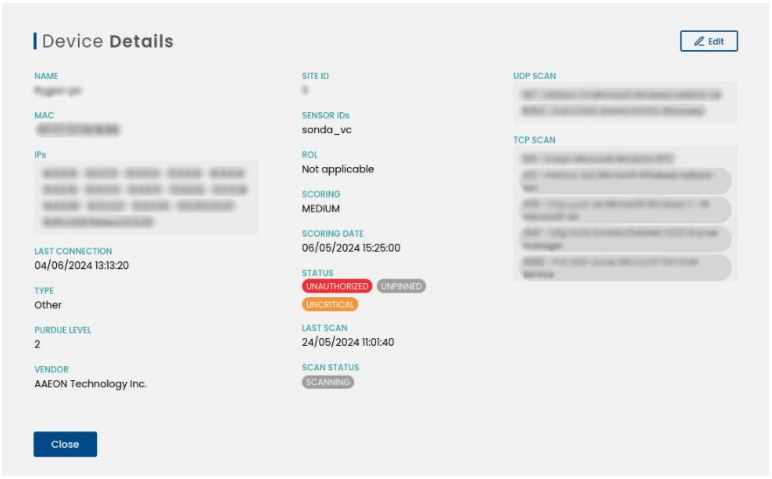
En la primera fase del asistente, se muestra un panel que resume el número de dispositivos no identificados actualmente presentes.

El usuario debe acceder a la lista de dispositivos haciendo clic en los contadores del asistente. Esto les llevará a la lista de dispositivos ya filtrada para mostrar esos dispositivos pendientes de identificación. Alternativamente, haciendo clic en el  icono y seleccionando la pestaña "Lista de dispositivos", también se puede acceder a él.



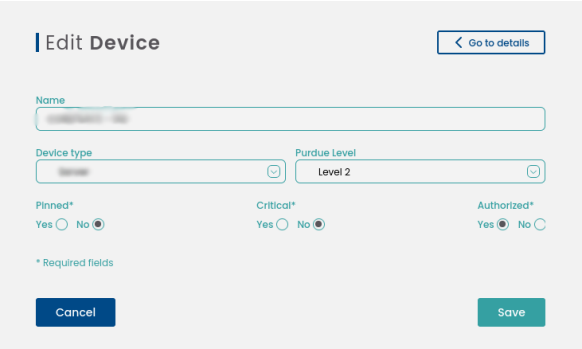
Pantalla de lista de dispositivos

Para poder modificar un dispositivo, tendremos que hacer clic en el botón  y se abrirá la siguiente pestaña.



Ventana emergente de detalles del dispositivo

Luego haz clic en el botón  para modificar el dispositivo seleccionado.



Editar pantalla de dispositivos.

Y rellenar manualmente el nombre del dispositivo, el nivel PURDUE al que pertenece el dispositivo y seleccionar su estado indicando si es fijo, crítico y/o autorizado (véanse definiciones en el 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.

2.3 Análisis de dispositivos inalámbricos

Si se desea, y si las sondas de recolección de tráfico cuentan con el hardware adecuado, el usuario puede configurar el escaneo inalámbrico de dispositivos desde esta primera etapa. Para ello, deben configurar las interfaces que se van a utilizar, y la sonda escaneará en busca de dispositivos inalámbricos en su zona.

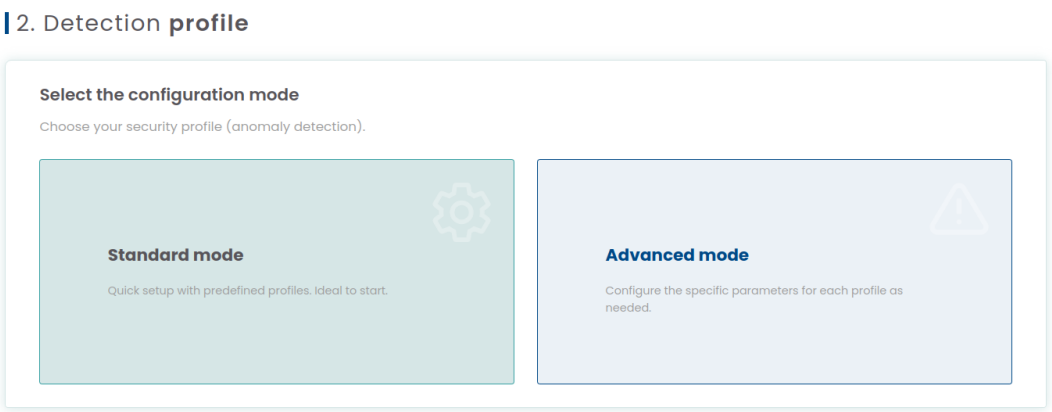
Consulte la sección de la Lista de Dispositivos Inalámbricos dentro de la Gestión de Aplicaciones para más detalles.

2.4 Configuración de reglas

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

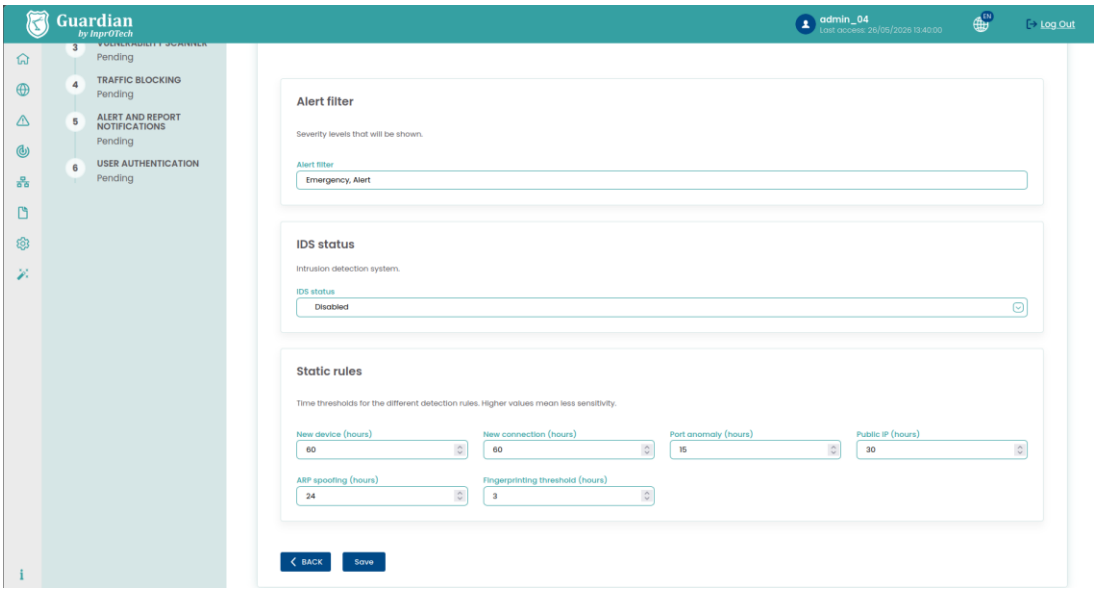
- Amenazas basadas en reglas parametrizables predefinidas
- Amenazas basadas en firmas IDS
- Amenazas basadas en algoritmos de IA/ML
- Amenazas de honeypot

A partir de la segunda etapa del asistente de configuración, el usuario podrá abstraer toda su configuración y elegir uno de los tres perfiles de seguridad predefinidos (modo básico), o editar manualmente las reglas, parámetros y filtros basándose en uno de ellos (modo avanzado).



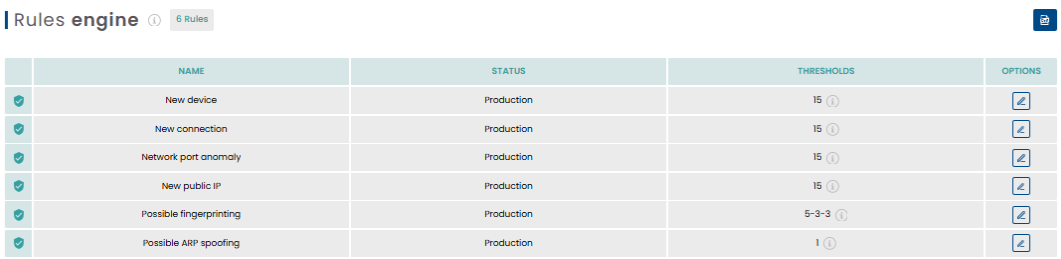
Para la edición manual, el usuario debe configurar qué reglas quiere que estén activas para analizar la red de su organización, así como los intervalos de tiempo para suprimir cada una de las alertas si se considera oportuno. También pueden establecer un filtro para determinar el nivel de gravedad al que se envían las alertas al portal web.

El intervalo de tiempo para saltarse una regla significa que podemos establecer un umbral o tiempo en el que las reglas establecidas no generarán una alerta en un escenario idéntico y, por tanto, evitar advertencias innecesarias y alertas de las que ya somos conscientes.



Además, se pueden configurar otros parámetros. Estos detalles se detallarán más adelante. Para configurar estos intervalos de tiempo, haga clic en el botón izquierdo del menú  en pantalla y en Detección de amenazas > General > Amenazas basadas en reglas, VER ESTADO.

Mecanismo de detección de pantalla de estado



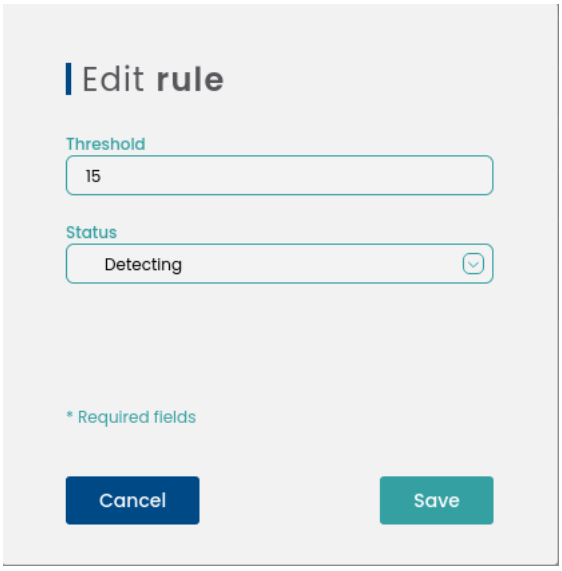
Pantalla del motor de reglas

En la columna de umbrales, podemos ver rápidamente los umbrales configurados para cada regla.

THRESHOLDS	OPTIONS
15	
15	
15	
15	
5-3-3	
1	

Pantalla umbral

En la columna de acciones podemos editar estos parámetros.



Pantalla de edición de reglas.

Además, esta sección incluirá, una vez disponible, la configuración de los mensajes asociados a notificaciones de alertas que desea recibir e informes.

2.5 Escenarios

Los ajustes básicos para datos de perfil de usuario, ajustes de seguridad y preferencias de notificaciones de alertas se pueden encontrar en la sección de Configuración de la Guía Rápida. Se recomienda revisarlas y adaptarlas a las necesidades del entorno.

2.6 Escáner activo de dispositivos (opcional)

Si el cliente lo desea, en la tercera etapa del asistente puede activar el motor de consultas activo para dispositivos, así como configurar la frecuencia de escaneo, para obtener propiedades adicionales de los nodos (como versión de firmware, puertos abiertos y servicios en ejecución, entre otros). Es importante señalar que se trata de un escaneo activo y puede interferir potencialmente con algunos dispositivos.

Consulta la sección "Escáner de dispositivos" en la sección de Gestión de Aplicaciones Web para más detalles.

2.7 Configuración de respuesta activa

En la cuarta etapa del asistente, podemos configurar el sistema de comprobación de reputación y el bloqueo de tráfico. El cliente puede decidir si habilitar estas funcionalidades y elegir el modo de operación. También pueden configurar la integración con su cortafuegos aquí para aprovechar el bloqueo de tráfico. Los modos y configuraciones de estas funcionalidades se detallarán más adelante.

2.8 Configuración de los informes

En la siguiente etapa, se puede configurar la generación de informes de Guardian. El cliente puede decidir si habilitar o desactivar esta funcionalidad, así como establecer la frecuencia con la que se generan los informes.

2.9 Exportación de alertas (opcional)

Si el cliente lo desea, en esta misma quinta etapa del asistente, tiene la opción de habilitar el envío automático de alertas generadas a un servidor syslog de un SIEM o sistema similar, para la ingestión y correlación* con otras fuentes de registro.

La única información que necesitan proporcionar es la dirección IP y el puerto al que quieren enviar los mensajes, así como el protocolo que se va a usar (syslog cifrado o no).

* 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)

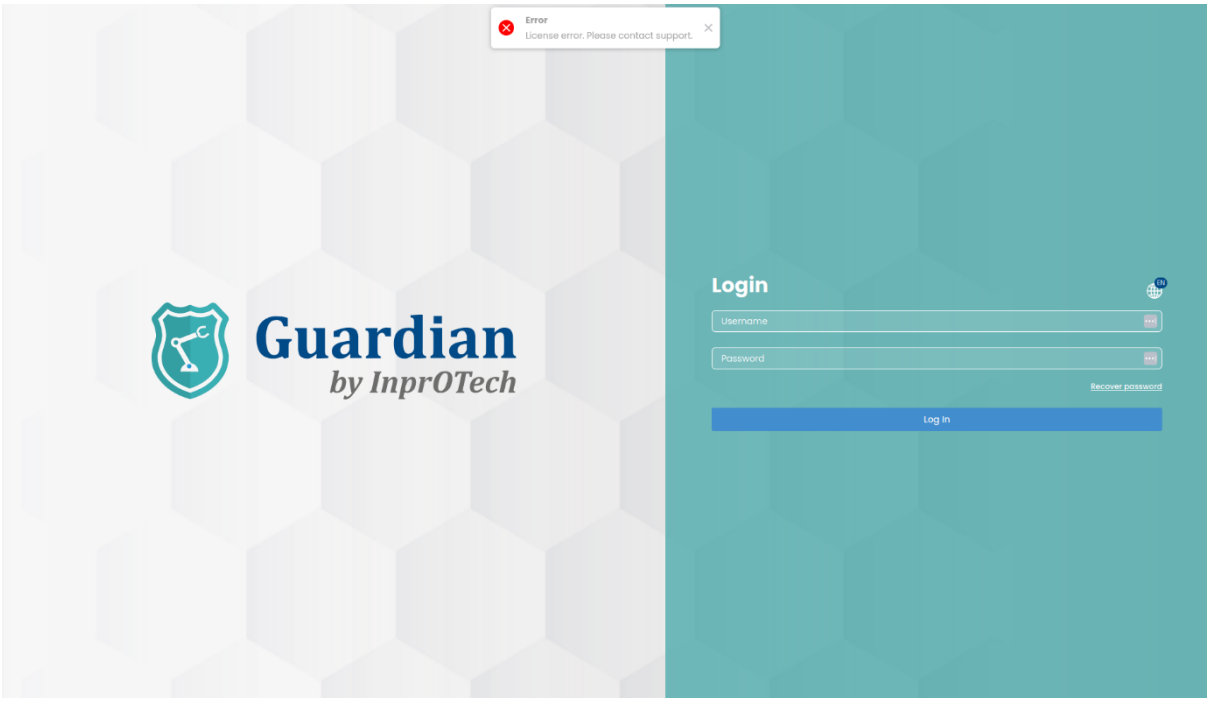
Si te interesa poder consultar permanentemente el estado de Guardian y los principales indicadores asociados (dispositivos no autorizados, tráfico de red, alertas, etc.), puedes tener el panel principal de Guardian en un monitor de tu sala de operaciones con refresco automático cada 5 minutos.

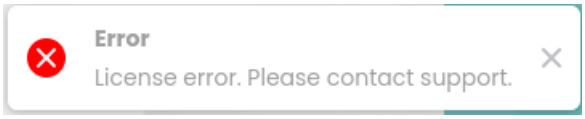
Para ello, contacta con el Soporte de tu Guardian y solicita la creación de un usuario de Monitorización.

2.11 Licencias

Esto permitirá proporcionar el Servicio Guardian solo de forma temporal, para que pueda ser proporcionado para fines de prueba limitando la ventana de uso.

Si ves el mensaje **"Error de licencia. Contacta con soporte."**, significa que los archivos de licencia faltan o que la licencia ha caducado.





2.12 Control de acceso y funciones

Esta función permite controlar el acceso del usuario y las acciones realizadas en el sistema. La implementación de este sistema proporciona una capa adicional de seguridad y privacidad en el manejo de la información y los recursos del sistema.

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

- **Roles y permisos predefinidos:** se pueden establecer diferentes roles y permisos predefinidos en el sistema, que se concederán para determinar sus niveles de acceso y control en el 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:** los grupos de usuarios deben establecerse para permitir la asignación de permisos a varios usuarios al mismo tiempo, lo que facilitará la gestión de permisos.
- **Control de acceso a recursos:** el sistema permitirá controlar el acceso a diferentes recursos Guardianes asignando permisos específicos.

Los roles a implementar serán los siguientes:

- **Administrador:** Se concede acceso completo a la configuración, operaciones de servicio, registros, etc., incluyendo la capacidad de transitar entre entornos

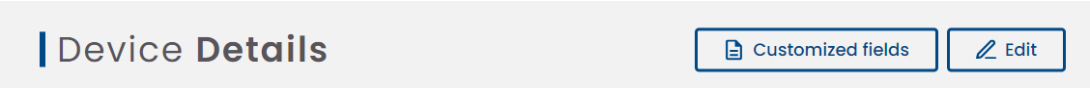
de entrenamiento y producción, y modificar conjuntos de algoritmos de IA según sea necesario.
- **Operador:** Modo de usuario privilegiado de la fábrica, se pueden hacer cambios en los datos visibles del frontend, como los datos del dispositivo, y las alertas pueden marcarse como resueltas o silenciadas.
- **Monitor:** modo de usuario estándar de fábrica, los permisos son más restringidos. Los usuarios solo pueden ver datos y descargar informes o CSVs.

2.13 Campos personalizados

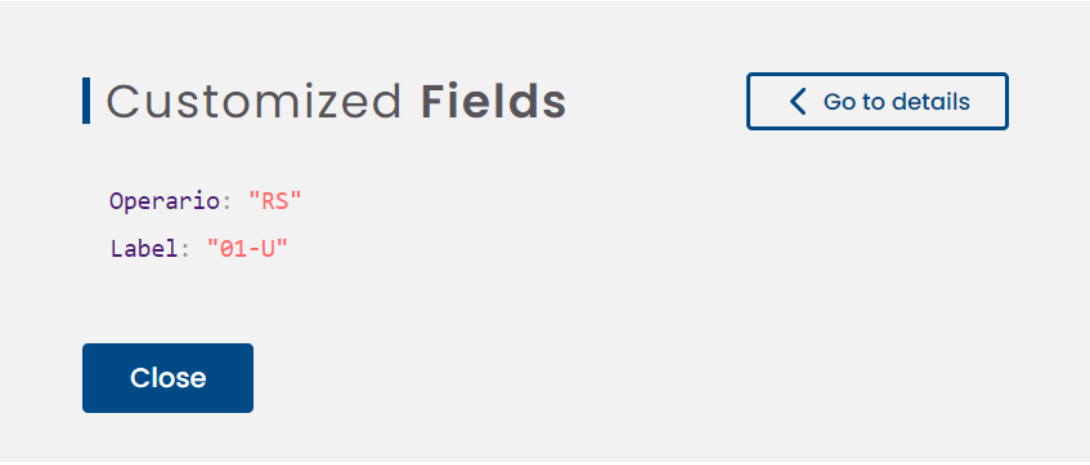
Si el usuario cree que se pueden añadir nuevos campos a la lista de dispositivos para permitir una mejor categorización, puede definirlos en un formato clave-valor usando un archivo ".csv".

Solo hay que añadir un archivo nuevo desde el botón del panel de dispositivos, incluyendo los dispositivos que queremos en las filas junto con los nuevos campos personalizables en cualquiera de los formatos explicados en la sección 4.2.2.1.

El usuario puede consultar los campos cargados desde el panel de dispositivos haciendo clic en el enlace 'Mostrar campos' en los dispositivos con cualquier campo configurado o en 'Detalles del dispositivo' y continuar haciendo clic en el botón 'Campos personalizados'.

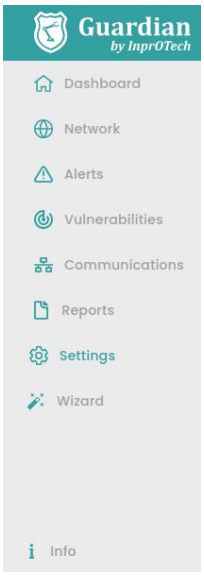


Esta acción abrirá un nuevo modal que permitirá al usuario verlos.



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

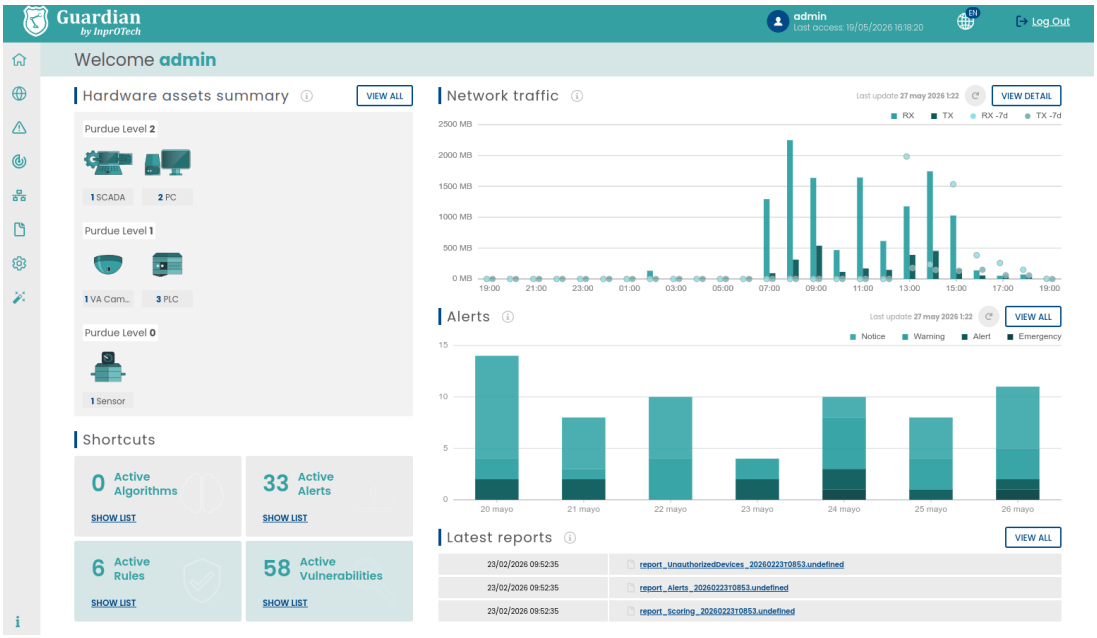
- 6: Informes: Lista de informes automáticos

- 7: Configuración: Ventana de configuración de parámetros

- 8: Asistente: Guía asistida para configurar 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 de acceso anterior

Cambia el lenguaje de la aplicación.

Cerrar sesión desde la sesión iniciada.

Dispositivos no autorizados que se contrarrestan.

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 bits/seg en las últimas 24 horas, y comparación respecto a la misma magnitud apenas 7 días antes.

Widget inferior izquierdo:

Atajos a los listados

Vulnerabilidades activas (en construcción)

Widgets en la parte inferior derecha:

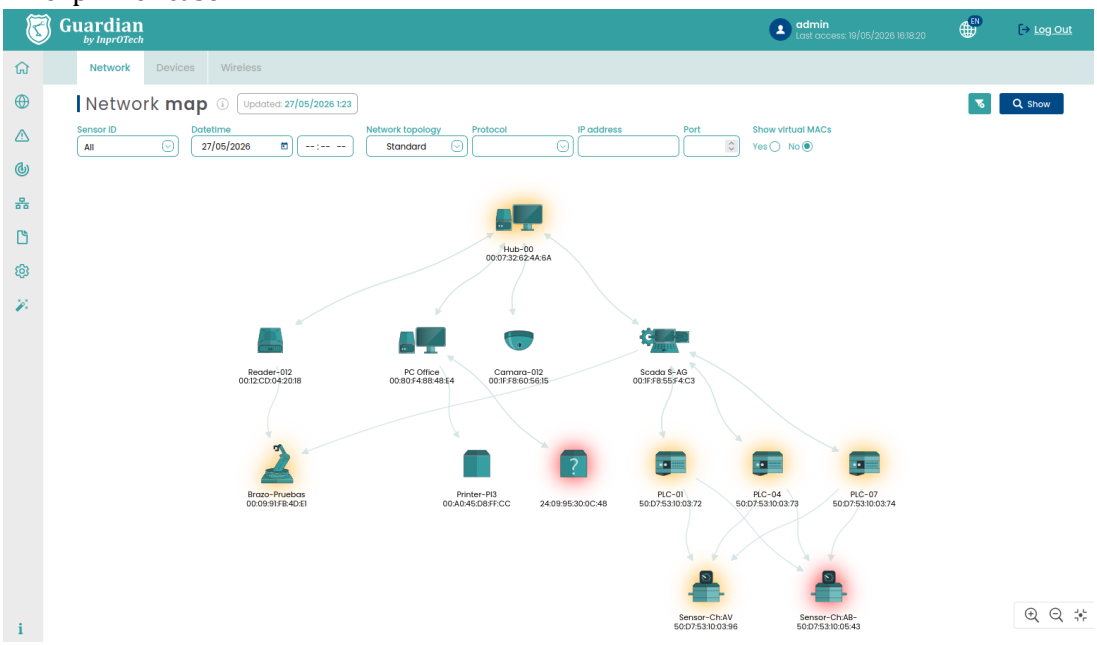
Representación gráfica del número de alertas según su gravedad.

Acceso a la lista de informes generados

3.3 Mapa de la 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.

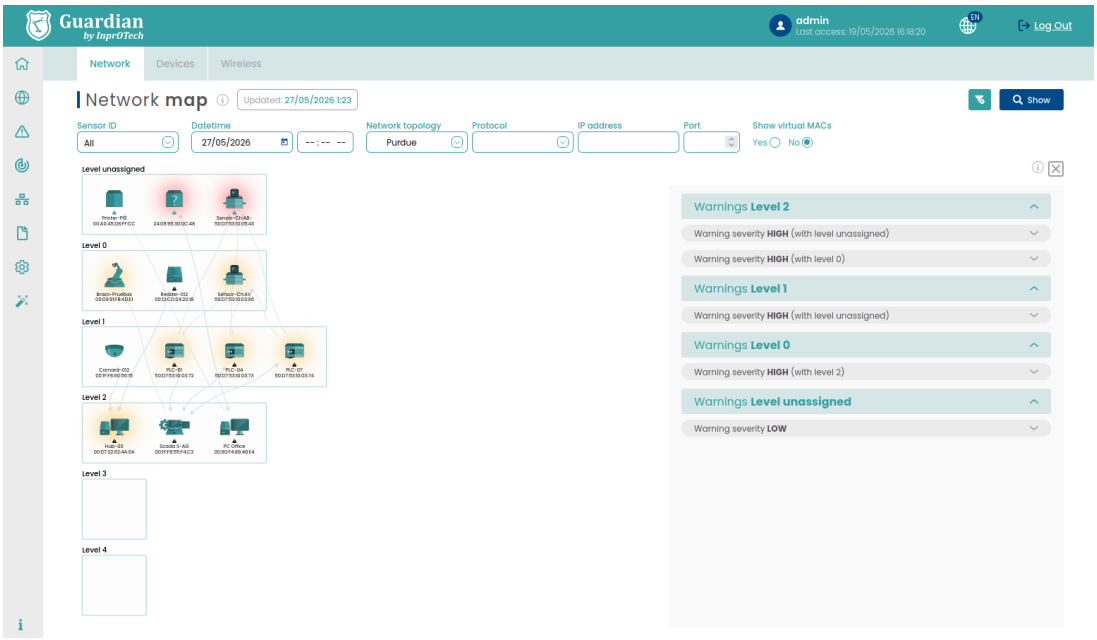
A continuación, ya tenemos el mapa y la topología de los dispositivos de red de la organización.

Ten en cuenta que:

- Al pasar el cursor con el ratón, puedes ver las propiedades de un nodo o enlace.

- Al hacer clic en ellos, puedes ir a la vista de detalle y editar las propiedades del dispositivo, o a la sección de comunicaciones filtradas para esa fuente de enlace, respectivamente.

En la visión de PURDUE sobre la topología, el cumplimiento de comunicaciones se analiza basándose en la norma ISA/IEC 62443. Las advertencias se clasifican en **alta severidad** (tipo de comunicación, que indica la existencia de comunicaciones entre niveles no adyacentes), **de gravedad media** (asignación de niveles PURDUE a tipos de dispositivos que parecen cuestionables) o **baja severidad** (sin asignación de niveles y/o recomendación de revisión manual para ciertos tipos de dispositivos).



Mapa de red en vista PURDUE.

Fíjate en que en la versión gráfica (lado izquierdo de la ventana):

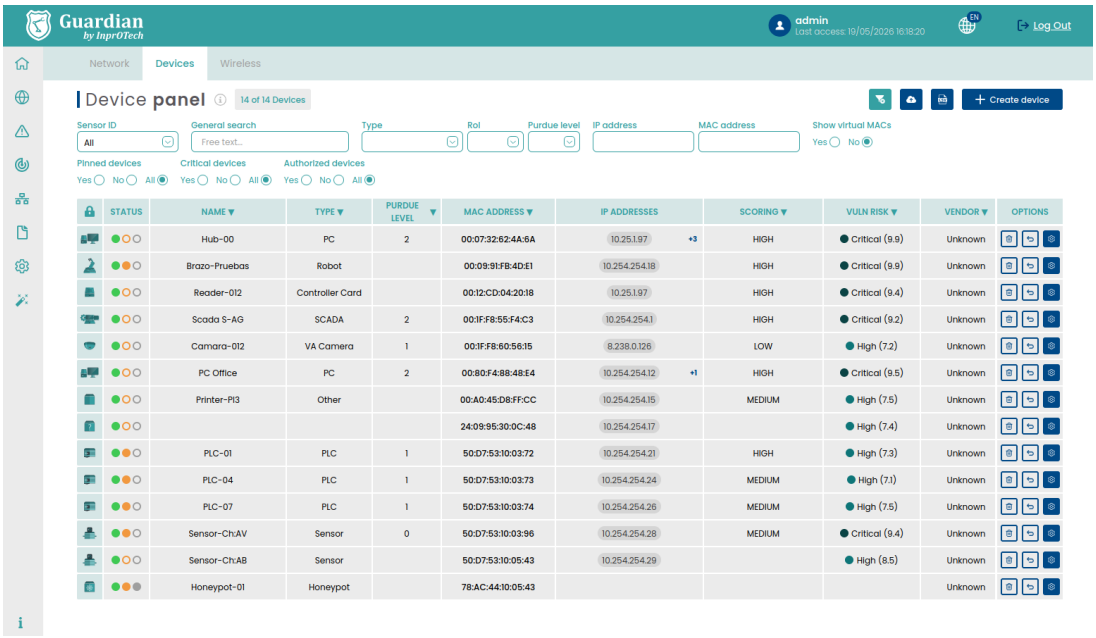
- Solo se muestran comunicaciones entre niveles distintos, no aquellas entre dispositivos del mismo nivel.

- Se indica con iconos triangulares bajo la imagen del dispositivo, si está afectado por alguna advertencia de cumplimiento normativo. Los colores son rojo, naranja y azul verdoso, y representan advertencias de gravedad alta, media y baja, respectivamente.

- 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 capacidades de filtrado son las mismas que en la vista clásica, y en el lado derecho de la ventana, como se mencionó antes, se listan las advertencias globales o las asociadas a un dispositivo seleccionado.

3.4 Lista de dispositivos



Ventana de lista de dispositivos

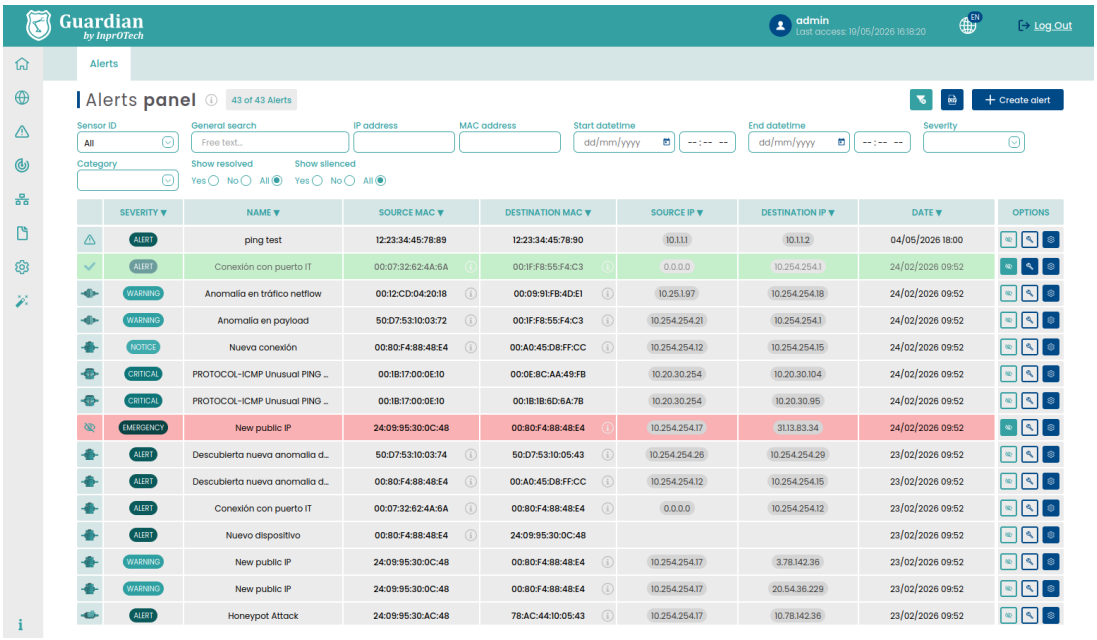
En la pestaña para seleccionar la vista de la lista de dispositivos registrados en la red, se muestra el número de dispositivos con el filtro actual aplicado frente al número total de dispositivos en la base de datos junto al título del panel. En el lado derecho, el panel de botones para eliminar los filtros previamente aplicados, exportar la lista de dispositivos en formato CSV y registrar manualmente un dispositivo en la aplicación.

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

La lista de activos con información sobre ellos y botones para realizar ciertas acciones (ver detalles, editarlos, eliminarlos o acceder a alertas, comunicaciones o vulnerabilidades presentes, estos últimos pendientes de desarrollo). 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 por el personal de soporte de Guardian).

3.5 Panel de alertas.



Las alertas indican la ventana explicativa.

Junto al título de la sección, se muestra el número de alertas en la red de la organización (filtradas frente a total). En el lado derecho, hay un panel de botones para eliminar los filtros establecidos, exportar la lista de alertas en formato CSV o crear manualmente una alerta en la aplicación.

La siguiente fila incluye los posibles filtros para ver las alertas de interés en la pantalla. Tenga en cuenta que el campo de búsqueda general es del tipo CONTAINS y permite realizar búsquedas en el campo de notas internas de la alerta, visible en Detalles.

Por último, tenemos la lista de alertas con información asociada y botones para realizar acciones sobre ellas (actualizaciones de estado*, acceso a detalles y adición de notas).

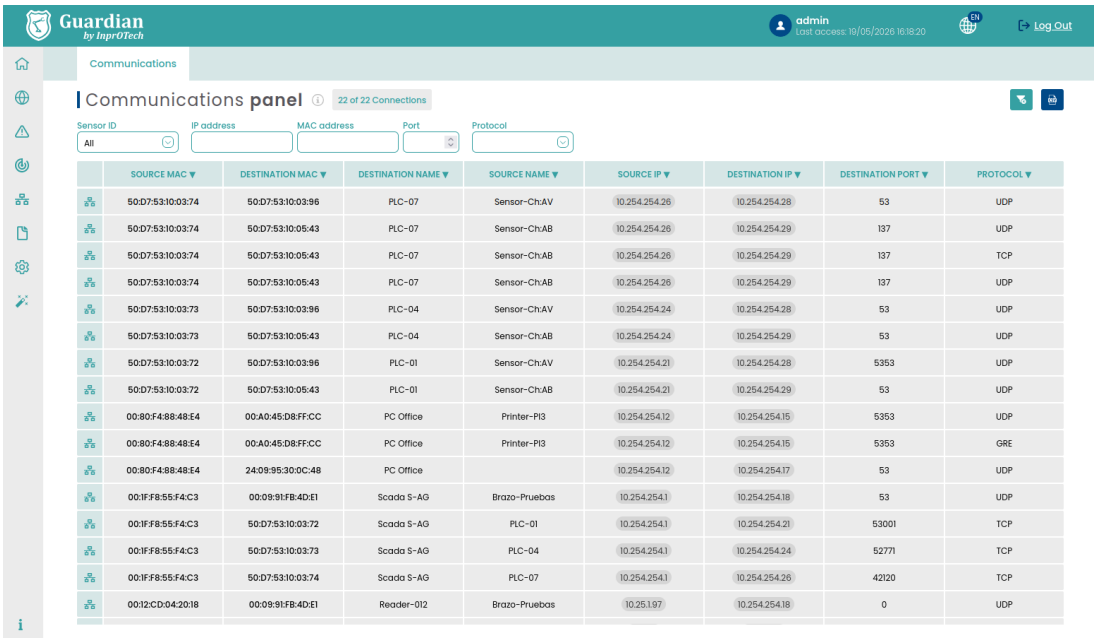
Como puedes ver en la imagen, si un dispositivo tiene un nombre asignado, junto a la MAC podemos ver un signo de exclamación que, si colocamos el cursor encima, nos mostrará el nombre asignado a esa dirección MAC.

Si la Política de Bloqueo está activa de cualquier manera (informativa, manual o automática), las alertas públicas de IP cuya IP haya sido clasificada como maliciosa se marcarán con un rojo llamativo, que se suavizará si esa dirección aparece en la lista de bloqueo del firewall industrial.

*Para comprobar las opciones de cambio de estado, consulte las definiciones en el Anexo I.

3.6 Lista de comunicaciones

Las comunicaciones, entendidas como un agrupamiento de conexiones entre MAC, IP y puerto de origen, y lo mismo en el destino. Desagregado si hay un cambio de protocolo.



SOURCE MAC	DESTINATION MAC	DESTINATION NAME	SOURCE NAME	SOURCE IP	DESTINATION IP	DESTINATION PORT	PROTOCOL
50:D7:53:10:03:74	50:D7:53:10:03:96	PLC-07	Sensor-Ch:AV	10.254.254.26	10.254.254.28	53	UDP
50:D7:53:10:03:74	50:D7:53:10:05:43	PLC-07	Sensor-Ch:AB	10.254.254.26	10.254.254.29	137	UDP
50:D7:53:10:03:74	50:D7:53:10:05:43	PLC-07	Sensor-Ch:AB	10.254.254.26	10.254.254.29	137	TCP
50:D7:53:10:03:74	50:D7:53:10:05:43	PLC-07	Sensor-Ch:AB	10.254.254.26	10.254.254.29	137	UDP
50:D7:53:10:03:73	50:D7:53:10:03:96	PLC-04	Sensor-Ch:AV	10.254.254.24	10.254.254.28	53	UDP
50:D7:53:10:03:73	50:D7:53:10:05:43	PLC-04	Sensor-Ch:AB	10.254.254.24	10.254.254.29	53	UDP
50:D7:53:10:03:72	50:D7:53:10:03:96	PLC-01	Sensor-Ch:AV	10.254.254.21	10.254.254.28	5353	UDP
50:D7:53:10:03:72	50:D7:53:10:05:43	PLC-01	Sensor-Ch:AB	10.254.254.21	10.254.254.29	53	UDP
00:80:F4:88:48:E4	00:A0:45:D8:FF:CC	PC Office	Printer-PI3	10.254.254.12	10.254.254.15	5353	UDP
00:80:F4:88:48:E4	00:A0:45:D8:FF:CC	PC Office	Printer-PI3	10.254.254.12	10.254.254.15	5353	GRE
00:80:F4:88:48:E4	24:09:95:30:0C:48	PC Office		10.254.254.12	10.254.254.17	53	UDP
00:1F:F8:55:F4:C3	00:09:91:FB:4D:E1	Scada S-AG	Brazo-Pruebas	10.254.254.1	10.254.254.18	53	UDP
00:1F:F8:55:F4:C3	50:D7:53:10:03:72	Scada S-AG	PLC-01	10.254.254.1	10.254.254.21	53001	TCP
00:1F:F8:55:F4:C3	50:D7:53:10:03:73	Scada S-AG	PLC-04	10.254.254.1	10.254.254.24	52771	TCP
00:1F:F8:55:F4:C3	50:D7:53:10:03:74	Scada S-AG	PLC-07	10.254.254.1	10.254.254.26	42120	TCP
00:12:CD:04:20:18	00:09:91:FB:4D:E1	Reader-012	Brazo-Pruebas	10.25.1.97	10.254.254.18	0	UDP

Ventana de lista de comunicaciones.

En esta sección, el número de dispositivos con el filtro actual aplicado se muestra junto al título, en comparación con el número total de dispositivos en la base de datos. En el lado derecho, los botones para eliminar los filtros y para exportar la lista de conexiones en formato CSV, respectivamente.

En la siguiente fila, hay los posibles filtros para ver las conexiones de interés en la pantalla.

Por último, la lista de conexiones con información sobre ellos. Es posible ordenar las comunicaciones alfabéticamente, ya sea directamente o inversamente, haciendo clic en cualquiera de las columnas.

3.7 Informes

Esta sección permitirá descargar informes de varios tipos, generados automáticamente por el sistema. A día de hoy, Guardian genera informes semanales los lunes por la mañana, con archivos descargables en formato CSV, con la siguiente información:

- Dispositivos conectados no autorizados:
    - Nombre: Nombre del dispositivo
    - MAC del dispositivo
    - Vendedor: Fabricante
    - Rol: Rol
    - Fecha de descubrimiento: Fecha de descubrimiento
    - Ips
    - Nivel Purdue

- Fijado (S/N)
- Crítico (Y/N)
- Tipo de dispositivo
- Puntuación y marca de tiempo.
- Estado del escaneo y último escaneo.
- Número de riesgo de vulnerabilidad
- Etiqueta de riesgo de vulnerabilidad
- OS
- Bloqueado (Permitido/No permitido).
- Campo personalizado

- Últimas alertas detectadas:
  - ID
  - Título
  - Categoría
  - Gravedad
  - Silenciado
  - Resuelto
  - Valor
  - IP de origen
  - ID de fuente
  - IP de destino
  - ID de destino
  - Protocolo
  - Fecha de creación
  - Ubicación (Ciudad / Continente / País / Latitud / Longitud...)
  - Nombre de anfitrión
  - IP
  - Dispositivo fuente (nombre / tipo)
  - Dispositivo del destino (nombre / tipo)
  - Creador

- Asociaciones MAC-IP:
  - MAC
  - IP asociada
  - Vendedor: Fabricante
  - IP pública: Sea pública o no.
  - Fecha de descubrimiento: Fecha y hora del descubrimiento

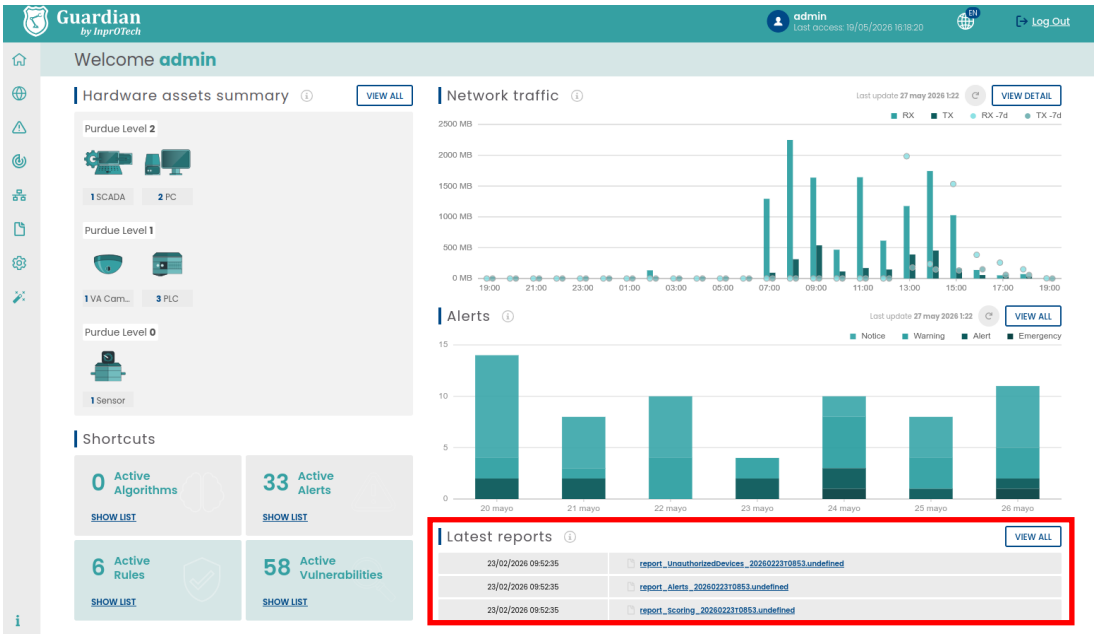
- IPs públicas (IPs externas conectadas):
  - IP (origen/destino)
  - MAC (origen/destino)
  - Fecha de descubrimiento

- Informe de Puntuación de Riesgo (puntuación)
  - Nombre
  - MAC
  - Fabricante
  - Puntuación individual
  - Fecha de la puntuación

    - Puntuación general de fábrica
    - Puntuación global de nubes
- Dispositivos inalámbricos
    - IP
    - MAC
    - Tipo de conexión
    - Autorizado (Y/N)
    - Tipo de dispositivo
    - Canal
    - Potencia de señal
    - Modo AP
    - Banda de frecuencia
- Vulnerabilidades
    - MAC
    - IP
    - CVE
    - Estado
    - Fuente
    - Fecha de descubrimiento
    - Última vez que se vio
    - Puerto
    - CPE
    - Criticidad
    - Descripción
    - Hora publicada.
    - CWE
    - URL

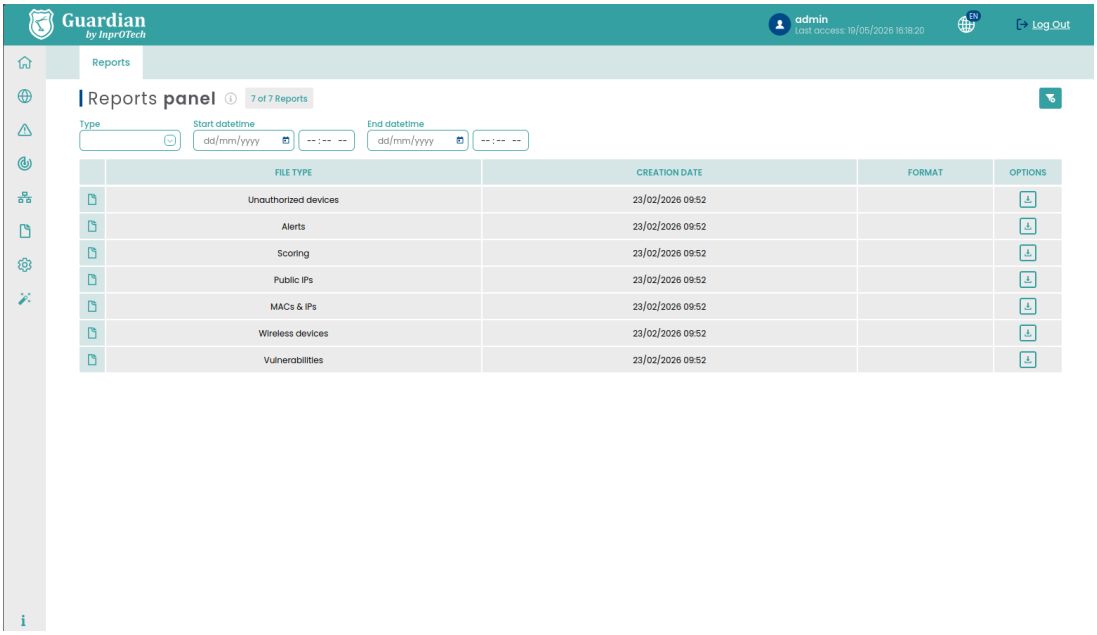
Si el dispositivo tiene el nombre de la etiqueta informado, reemplazará el campo MAC en los informes de la alerta. Por otro lado, en las descargas manuales de búsquedas de usuarios desde el panel de alertas o la lista de dispositivos, la sección "Últimos informes" mostrará ambos campos de forma independiente.

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



Últimos informes sobre el Panel principal

Además, Guardian tiene su propia sección dedicada a los Informes, donde puedes usar el motor de búsqueda para filtrar y descargar el informe de interés:



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 siguiente fila, tenemos los diferentes filtros de búsqueda.

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

3.8 Escenarios

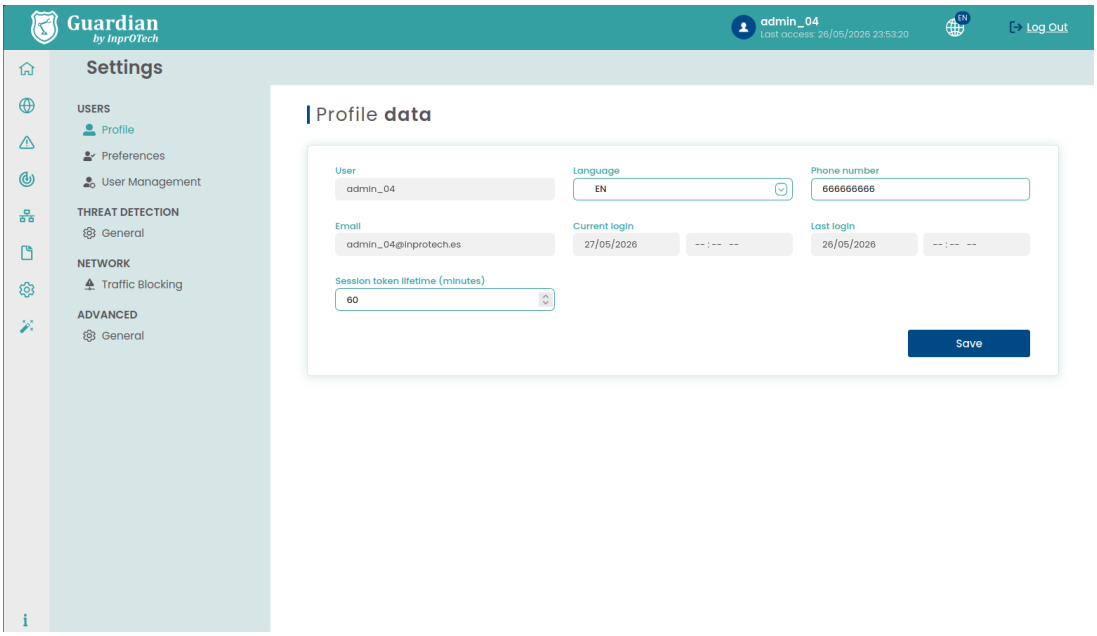
En esta sección podemos ajustar nuestro perfil o el servicio, modificar algunos parámetros relacionados con la detección de amenazas o diferentes configuraciones de alertas, amenazas y gestión de usuarios.

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

3.8.1 Perfil de usuario

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

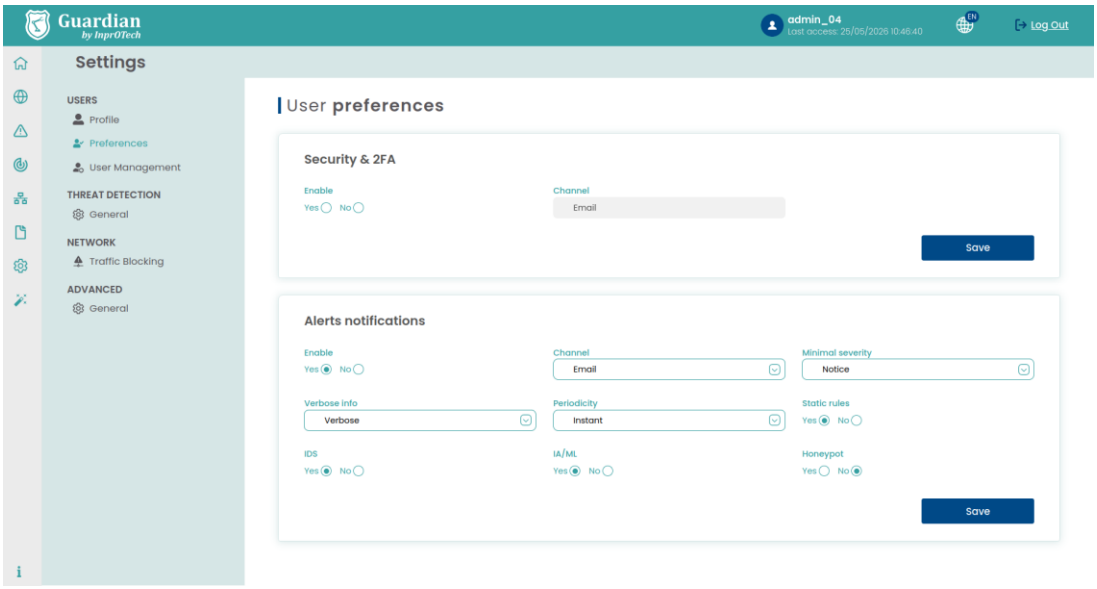
El usuario puede acceder a ella desde  "Configuración" en el menú lateral izquierdo.



Vista de datos del perfil de usuario

3.8.2 Preferencias de los usuarios

En Preferencias de > Avanzadas, en la sección 'Seguridad y MFA', podemos indicar si queremos activar el segundo factor de autenticación como mecanismo de seguridad adicional (recomendado) para prevenir el robo de identidad. En este caso, tras identificarnos con nombre de usuario y contraseña, se nos invitará a introducir un token de un solo uso que hayamos recibido (inicialmente por correo electrónico).



Vista de preferencias del usuario

Recuerda que, como método de control de acceso, se ha implementado un mecanismo basado en roles, mediante el cual existen grupos de permisos asociados a tres niveles de usuario:

- Administrador
- Operador
- Monitor

La asignación de roles a los usuarios no puede ser gestionada directamente por tu organización, pero está definida con InprOTech en el momento del despliegue de la solución. Contáctanos para más información.

3.8.3 Notificación de alertas

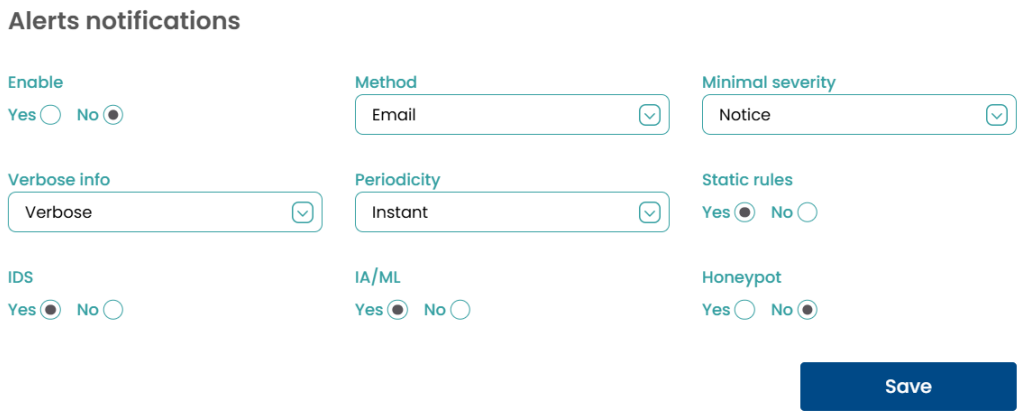
Si se considera apropiado, se pueden configurar alertas de toma de iniciativa para generar alertas en el sistema. Las alertas y advertencias se generan en función de la detección de anomalías según las diferentes estrategias implementadas en Guardian (heurísticas, IA/ML, IDS, Honeypot, manuales...).

Esto permite a Guardian advertir de posibles incidentes, en lugar de tener que ir periódicamente a la interfaz web para comprobar si se han generado eventos.

Por tanto, el usuario podrá hacerlo:

- Decide si quieren recibir notificaciones de alertas de seguridad.
- Si es así, ¿desde qué umbral de gravedad se enviarán al usuario?
- ¿Qué tipo de alertas (heurísticas, IA/ML, IDS, Honeypot, todas...)
- En qué formato
    - 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 es individual, se desea formato resumen o extenso.



Vista de notificaciones de alertas

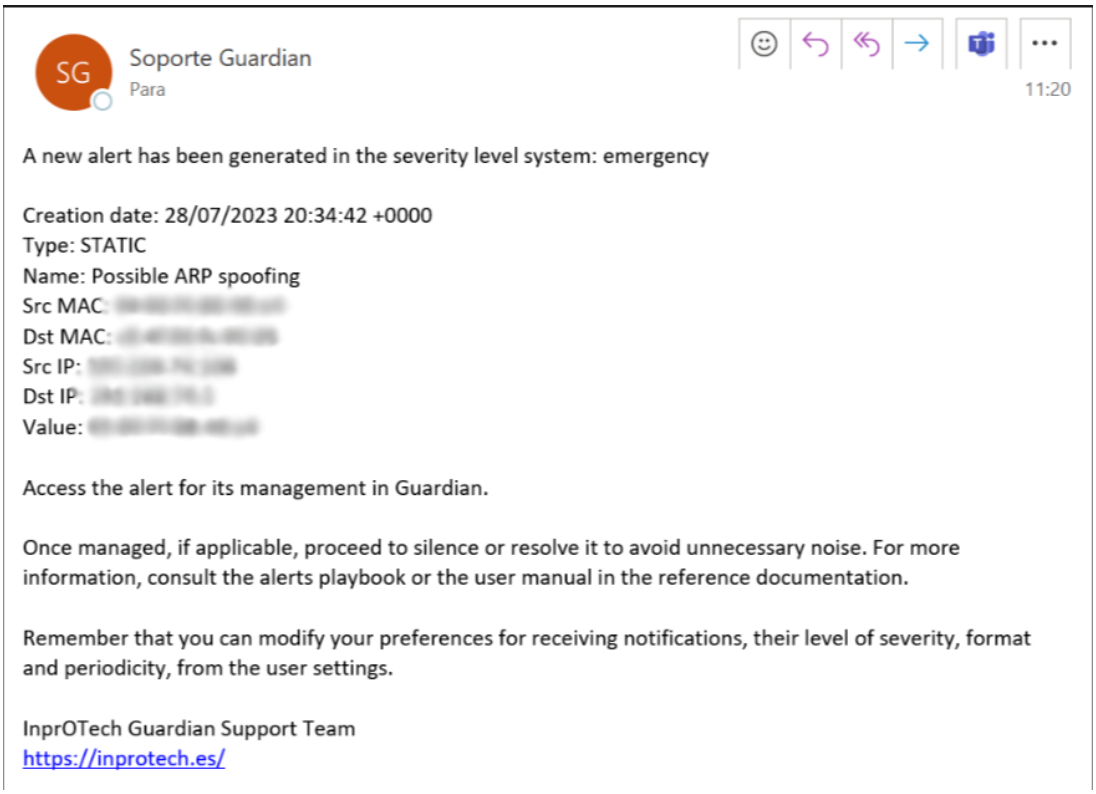
Por el momento, las notificaciones se enviarán por correo electrónico a la cuenta del usuario.

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).

A continuación se muestran un par de ejemplos de notificaciones de alertas con diferentes formatos:



Soporte Guardian
Para
11:20

A new alert has been generated in the severity level system: emergency

Creation date: 28/07/2023 20:34:42 +0000
Type: STATIC
Name: Possible ARP spoofing
Src MAC:
Dst MAC:
Src IP:
Dst IP:
Value:

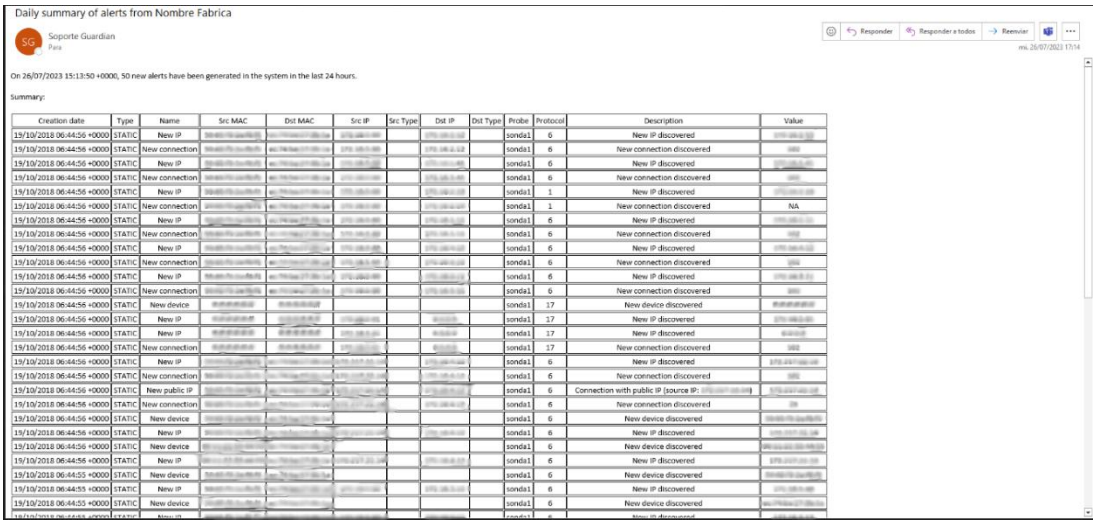
Access the alert for its management in Guardian.

Once managed, if applicable, proceed to silence or resolve it to avoid unnecessary noise. For more information, consult the alerts playbook or the user manual in the reference documentation.

Remember that you can modify your preferences for receiving notifications, their level of severity, format and periodicity, from the user settings.

InprOTech Guardian Support Team
https://inprotech.es/

Ejemplo resumido de notificación individual de alerta.



Daily summary of alerts from Nombre Fabrica

Soporte Guardian

On 26/07/2023 15:13:50 +0000, 50 new alerts have been generated in the system in the last 24 hours.

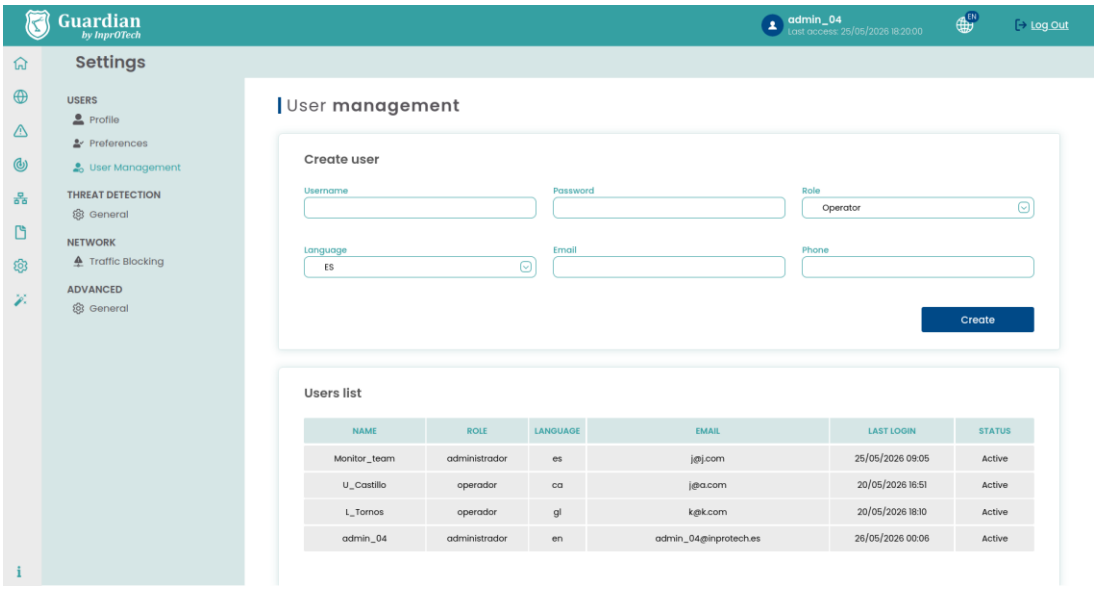
Summary:

Creation date	Type	Name	Src MAC	Dst MAC	Src IP	Src Type	Dst IP	Dst Type	Probe	Protocol	Description	Value
19/10/2018 06:44:56 +0000	STATIC	New IP							sonda1	6	New IP discovered	
19/10/2018 06:44:56 +0000	STATIC	New connection							sonda1	6	New connection discovered	
19/10/2018 06:44:56 +0000	STATIC	New IP							sonda1	6	New IP discovered	
19/10/2018 06:44:56 +0000	STATIC	New connection							sonda1	6	New connection discovered	
19/10/2018 06:44:56 +0000	STATIC	New IP							sonda1	1	New IP discovered	
19/10/2018 06:44:56 +0000	STATIC	New connection							sonda1	1	New connection discovered	NA
19/10/2018 06:44:56 +0000	STATIC	New IP							sonda1	6	New IP discovered	
19/10/2018 06:44:56 +0000	STATIC	New connection							sonda1	6	New connection discovered	
19/10/2018 06:44:56 +0000	STATIC	New IP							sonda1	6	New IP discovered	
19/10/2018 06:44:56 +0000	STATIC	New connection							sonda1	6	New connection discovered	
19/10/2018 06:44:56 +0000	STATIC	New IP							sonda1	6	New IP discovered	
19/10/2018 06:44:56 +0000	STATIC	New connection							sonda1	6	New connection discovered	
19/10/2018 06:44:56 +0000	STATIC	New device							sonda1	17	New device discovered	
19/10/2018 06:44:56 +0000	STATIC	New IP							sonda1	17	New IP discovered	
19/10/2018 06:44:56 +0000	STATIC	New IP							sonda1	17	New IP discovered	
19/10/2018 06:44:56 +0000	STATIC	New connection							sonda1	17	New connection discovered	
19/10/2018 06:44:56 +0000	STATIC	New IP							sonda1	6	New IP discovered	
19/10/2018 06:44:56 +0000	STATIC	New connection							sonda1	6	New connection discovered	
19/10/2018 06:44:56 +0000	STATIC	New public IP							sonda1	6	Connection with public IP (source IP:	
19/10/2018 06:44:56 +0000	STATIC	New connection							sonda1	6	New connection discovered	
19/10/2018 06:44:56 +0000	STATIC	New device							sonda1	6	New device discovered	
19/10/2018 06:44:56 +0000	STATIC	New IP							sonda1	6	New IP discovered	
19/10/2018 06:44:56 +0000	STATIC	New device							sonda1	6	New device discovered	
19/10/2018 06:44:56 +0000	STATIC	New IP							sonda1	6	New IP discovered	
19/10/2018 06:44:55 +0000	STATIC	New device							sonda1	6	New device discovered	
19/10/2018 06:44:55 +0000	STATIC	New IP							sonda1	6	New IP discovered	
19/10/2018 06:44:55 +0000	STATIC	New device							sonda1	6	New device discovered	

Ejemplo de notificación diaria agrupada.

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.



Vista de gestión de usuarios

3.8.5 Configuración de bloqueo de tráfico

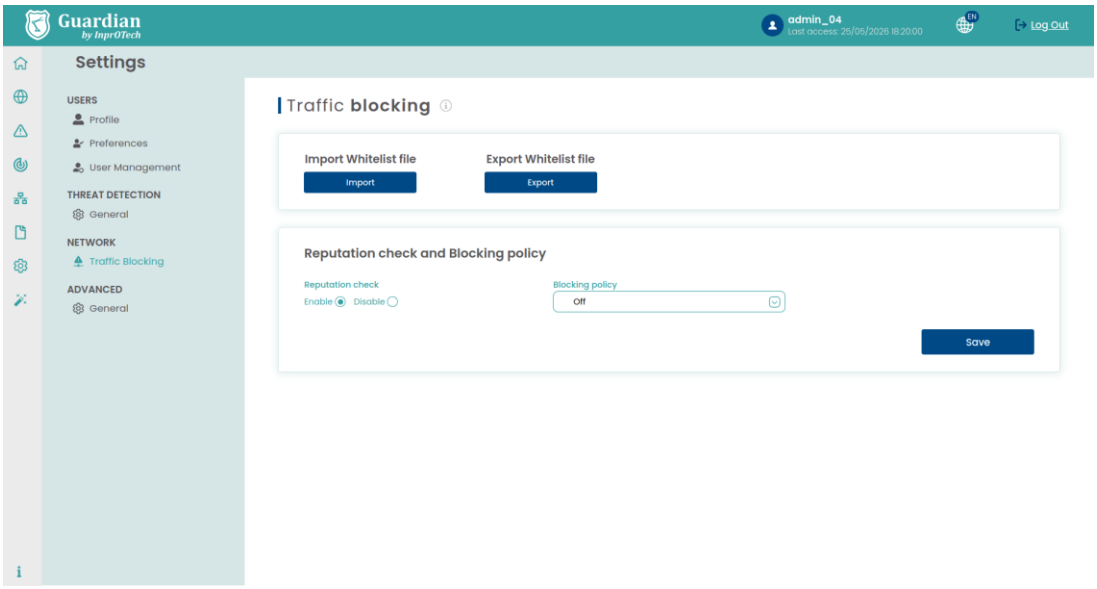
En esta sección, puedes habilitar la importación de una lista blanca de direcciones IP, rangos de IP o direcciones MAC (direcciones a las que este bloque nunca se aplicará), así como exportarla a un archivo CSV.

Además, puedes configurar los dos parámetros de esta sección:

-Comprobación de reputación: permite o desactiva la búsqueda de la reputación de IPs públicas en el tráfico entrante o saliente.

-Política de bloqueo: selecciona el modo para bloquear IPs públicas maliciosas entre cuatro modos:

- **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, añadiendo la IP maliciosa a una lista de bloqueo.
- **Apagado**: No hace cambios en el panel de alertas y no intenta comunicarse con el cortafuegos industrial. Traductor de inglés español



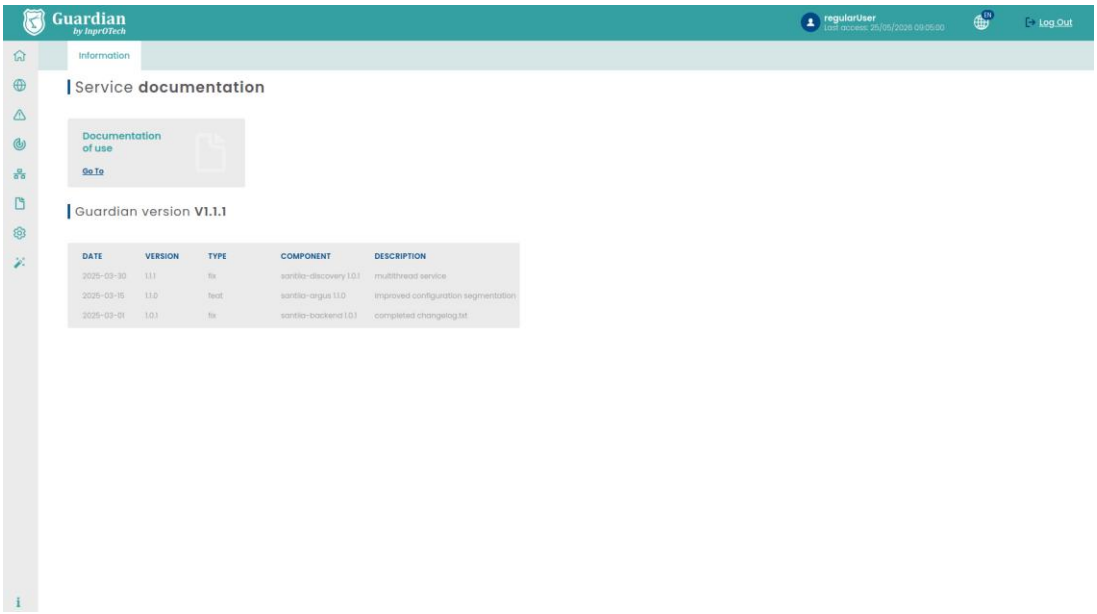
Vista de bloqueo de tráfico

3.9 Información

Sección que permite descargar la última versión del manual de usuario de InprOTech Guardian. Lleva a la web de InprOTech, 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, haz clic en el icono del menú  en la esquina inferior izquierda.

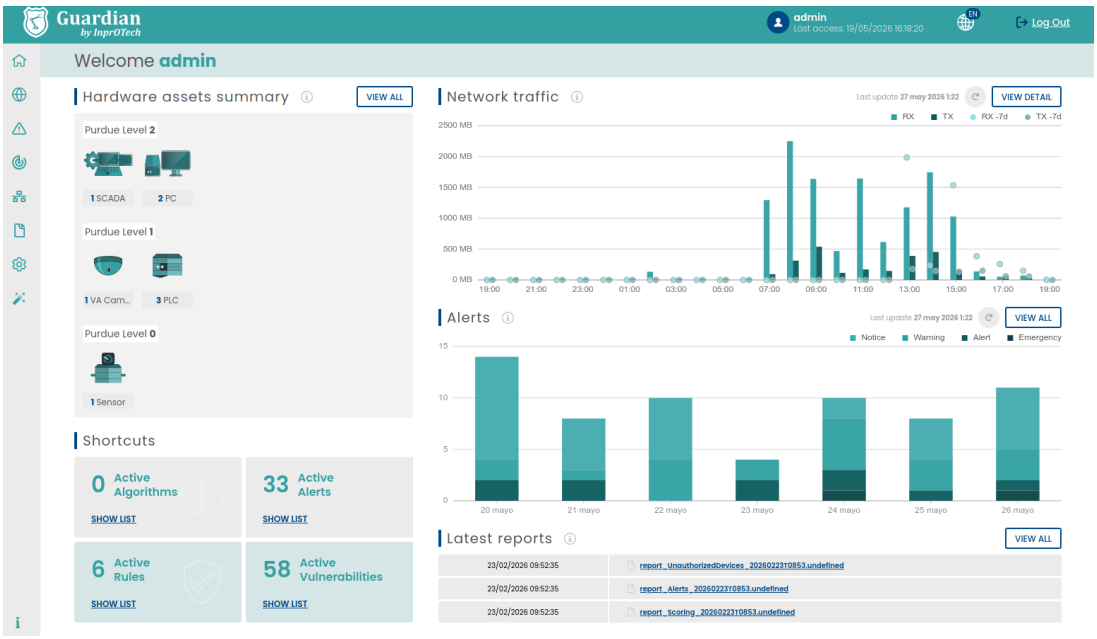


Vista de información

El acceso a la documentación está en la esquina inferior izquierda. Para cualquier problema técnico, por favor contacta con customer.support@inprosec.com.

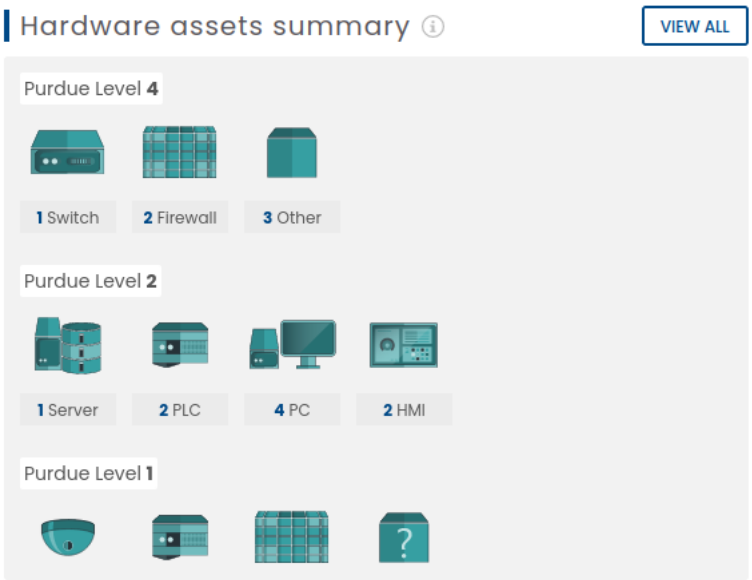
4 Gestión de aplicaciones

4.1 Panel principal



Principio del panel

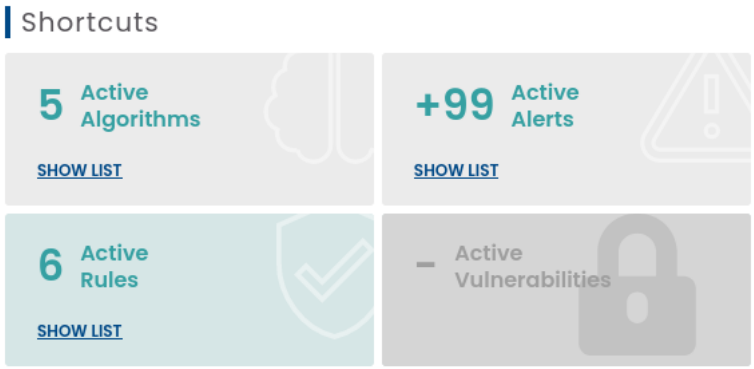
4.1.1 Resumen de activos



Resumen de activos

El usuario puede visualizar el número de dispositivos conectados a la red, diferenciados por tipo (PLC, RTU, Switch, Router, Robot, PC, SCADA, DCS, HMI, Cortafuegos, inversor de frecuencia, tarjetas controladoras, sensores, cámaras V.A., tabletas, teléfonos, honeypots, otros equipos), y clasificados según el modelo de Purdue según el Anexo II (siempre que se haya reportado según la sección 4.4).

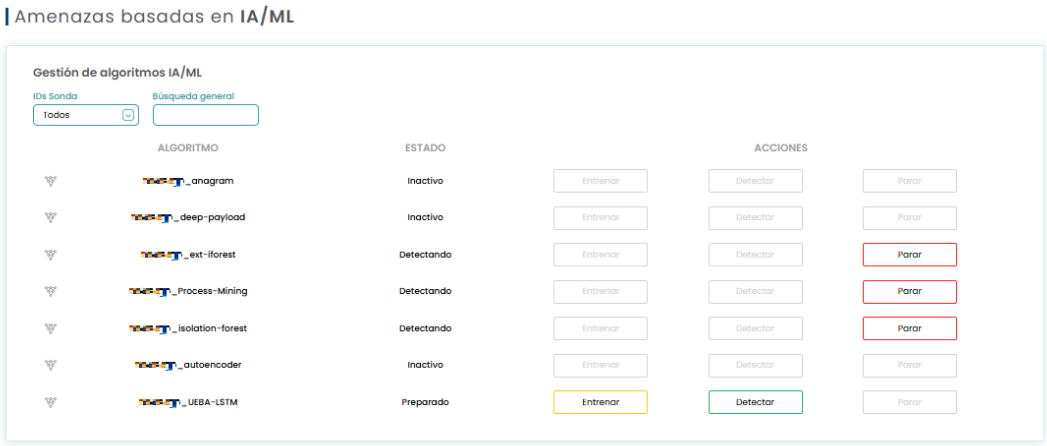
4.1.2 Enlaces rápidos



Enlaces rápidos

4.1.2.1 Algoritmos activos

Al hacer clic en el enlace "VER LISTA", el usuario podrá ver la lista de algoritmos de inteligencia artificial activos para la detección de amenazas dentro de la red de la organización (esta sección se discutirá más adelante en este manual).



Lista de algoritmos

4.1.2.2 Alertas activas

Al hacer clic en el enlace "VER LISTA", el usuario podrá ver una lista de las alertas activas totales.

4.1.2.3 Reglas activas

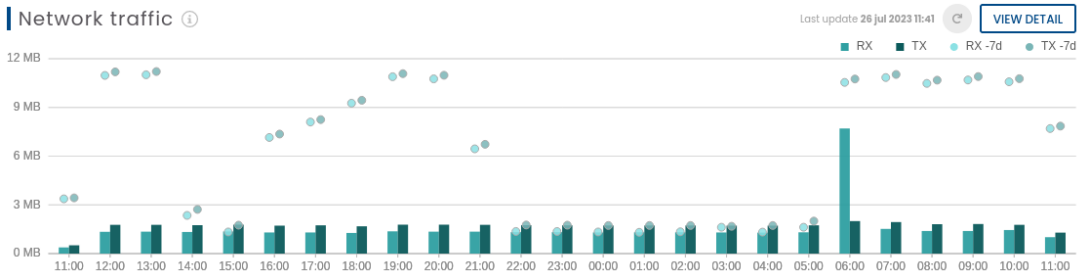
Al hacer clic en el enlace "VER LISTA", el usuario podrá ver una lista de las reglas fijas activas para la detección de amenazas dentro de la red de la organización (esta sección se discutirá más adelante en este manual).

Lista de reglas activas

4.1.2.4 Vulnerabilidades activas

Al hacer clic en el enlace "VER LISTA", el usuario puede ver una lista de las vulnerabilidades activas totales que no se gestionan. Pendiente de desarrollo.

4.1.3 Gráfico de tráfico de red.

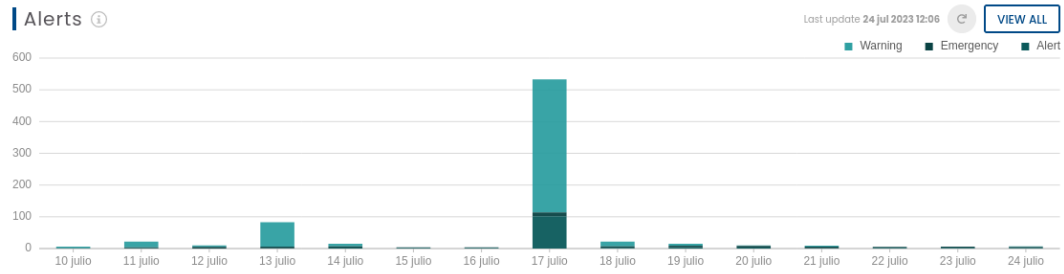


Tráfico de red

El usuario puede mostrar gráficamente el tráfico generado (en bit/s, o en múltiples de esa unidad) en las últimas 24 horas, tanto enviado (verde oscuro) como recibido (verde más claro). También tendrá una actualización automática en ese intervalo de tiempo y un botón para una actualización manual por parte del operador. Los puntos circulados en cada una de las barras indicarán el tráfico que ocurrió 7 días antes, como comparación.

Al hacer clic en el botón "VER DETALLE", el usuario verá en pantalla la ventana de sesiones de red de la aplicación InprOTech Guardian (sección que se tratará más adelante en este manual).

4.1.4 Alertas gráficas.



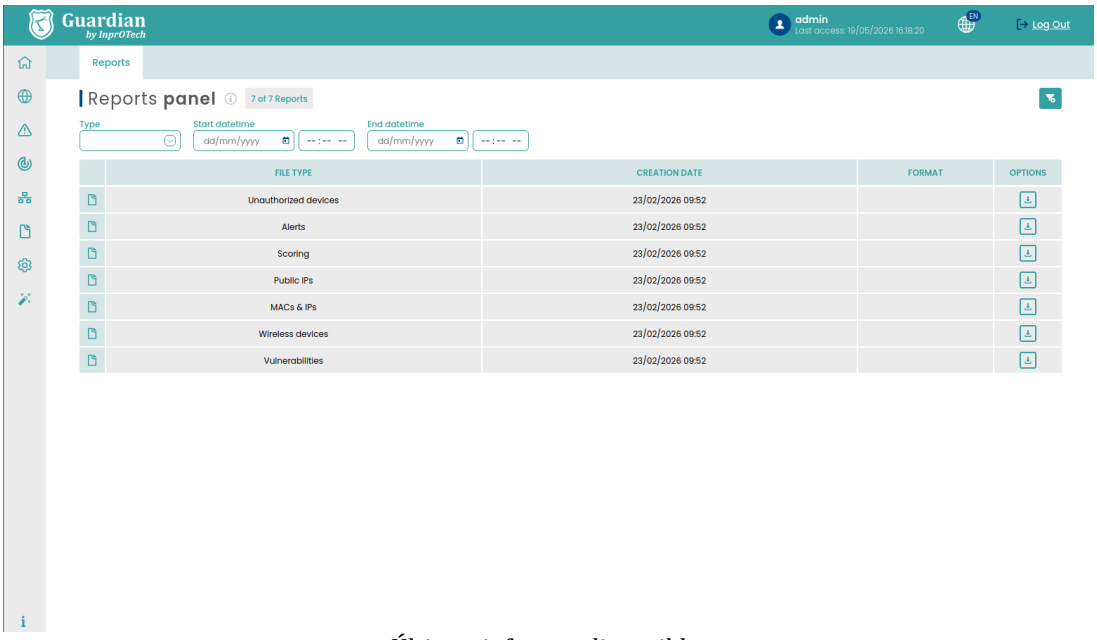
Alertas

El usuario tendrá una representación gráfica del número de alertas diferenciadas según su nivel de gravedad (véase Anexo I) y colores, por día de los últimos cinco días, y la tendencia que ha seguido. También tendrá una actualización automática en ese intervalo de tiempo y un botón para una actualización manual por parte del operador.

Si el usuario coloca el cursor sobre la barra gráfica de uno de los días, se puede mostrar el número exacto de alertas y emergencias capturadas hasta ese momento.

Al hacer clic en el botón "VER TODO", el usuario verá en pantalla la ventana de alertas de la aplicación InprOTech Guardian (sección que se tratará más adelante en este manual).

4.1.5 Últimos informes



Últimos informes disponibles

Al hacer clic en el botón "VER TODO", el usuario puede ver automáticamente una lista de los informes más recientes generados o a petición del cliente.

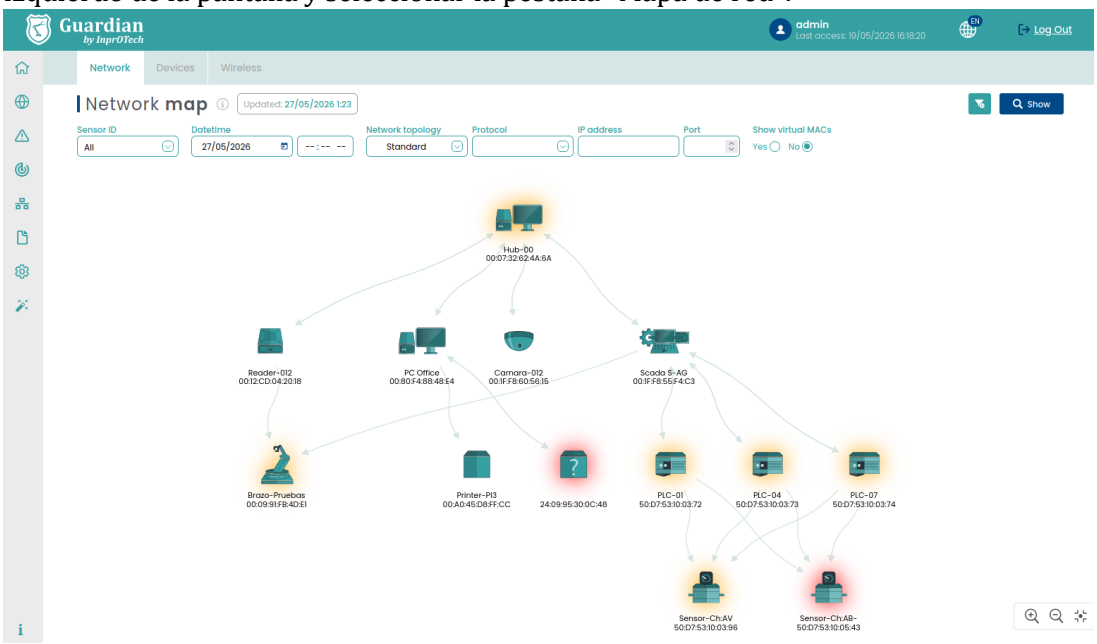
Actualmente, los informes generados semanalmente son:

- Lista de las últimas alertas detectadas.
- Lista de dispositivos no autorizados conectados a la red.
- Relación MAC-IP vista en la red.
- Puntuaciones de puntuación en cadena.
- Informe de indicadores técnicos de servicio (KPI)

4.2 Mapa de red y lista de dispositivos.

4.2.1 Mapa de la 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 la red

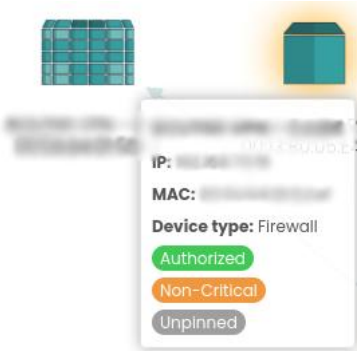
En la pestaña de mapa de red, el usuario podrá visualizar todos los dispositivos conectados a la red en tiempo real, así como los enlaces de comunicación entre ellos. Cada dispositivo será referenciado con una imagen representativa y una serie de propiedades como su dirección MAC o nombre en caso de que haya sido informado manualmente. El mapa de la red mostrará 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).

Dispositivo no autorizado

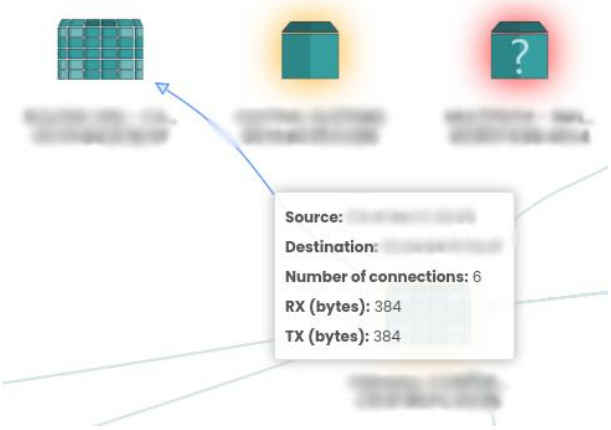
Si colocamos el cursor sobre un dispositivo, aparecerá una ventana emergente donde veremos la información básica del dispositivo.



Información básica del dispositivo

Si hacemos clic en el dispositivo, se mostrará la ventana con toda la información del dispositivo.

Si colocamos el cursor sobre uno de los enlaces, veremos una ventana emergente con



la información básica de esa comunicación.

Enlace información básica.

Si hacemos clic en el enlace, se mostrará la ventana con toda la información de 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: Marco temporal que se mostrará por pantalla.

- Topología de red: Modelo de muestreo de la red de la organización por pantalla.

- Protocolo: muestreo mediante filtrado solo de conexiones usando el protocolo seleccionado.

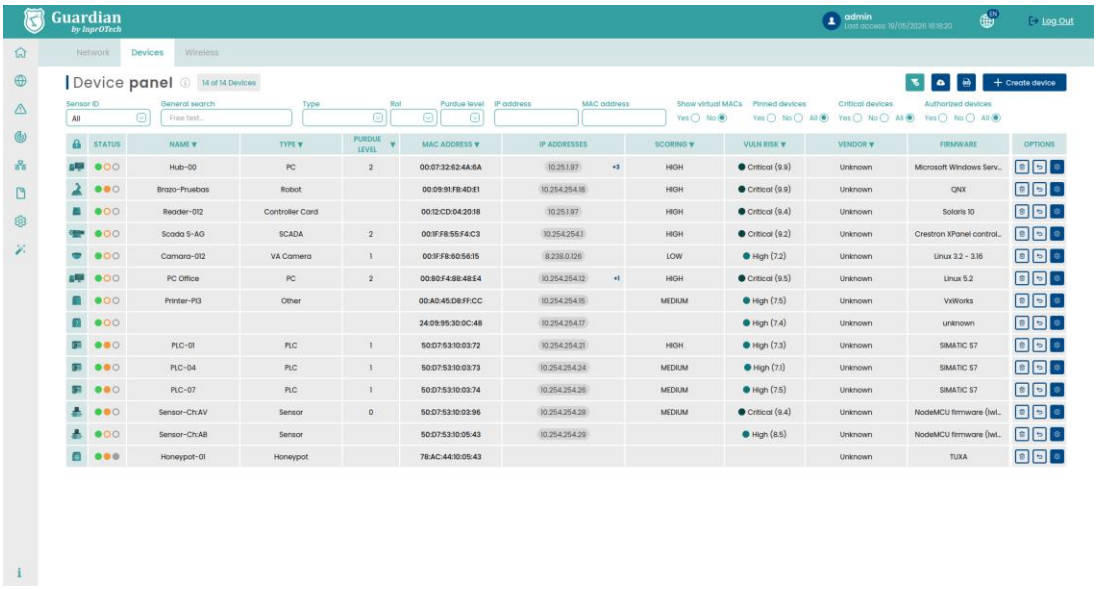
- Dirección IP: muestreo solo de dispositivos y conexiones con la IP seleccionada.

- Puerto: Muestreo mediante pantalla de conexiones al puerto seleccionado.

- Visualización o no de MACs virtuales (multicast/broadcast), calculados 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".



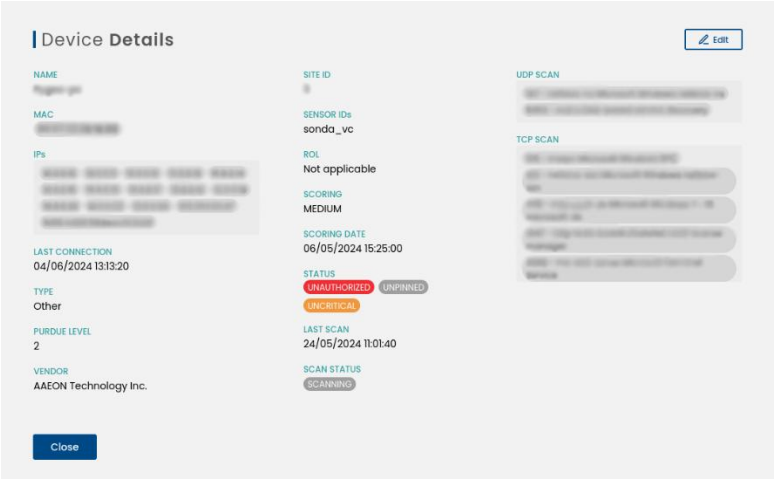
Lista de dispositivos

Se mostrará una lista de todos los dispositivos presentes en la organización junto con su información en una forma más ampliada:

- SITUACIÓN
  - El primero de los círculos indicará si el dispositivo está autorizado (color verde) o no autorizado (color rojo).
  - El segundo de los círculos indicará si el dispositivo es crítico (color naranja con relleno) o no crítico (color naranja sin relleno).
  - El tercer círculo indica si el dispositivo es fijo (color gris con relleno) o no fijo (color gris sin relleno).
- 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: Dirección IP asignada al dispositivo.
- PUNTUACIÓN: importancia/riesgo del dispositivo (bajo, medio o alto).
- RIESGO VULN: nivel de criticidad más alto para todas las vulnerabilidades del dispositivo.

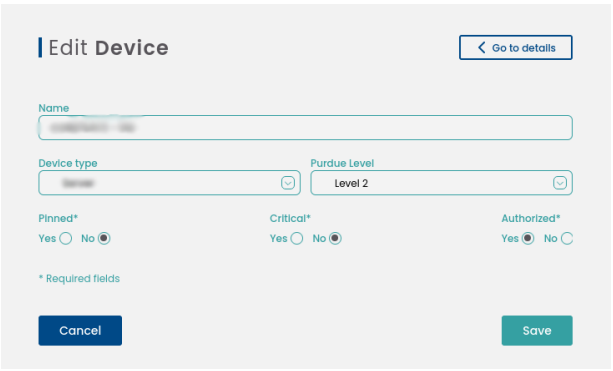
- PROVEEDOR: fabricante del dispositivo, identificado por los tres primeros campos de su dirección MAC.
- FIRMWARE: dispositivo de firmware integrado.
- CAMPOS PERSONALIZADOS: Además de los campos existentes, los usuarios pueden crear sus campos personalizados en formato clave-valor. Cada campo personalizable aparecerá en la lista de dispositivos como una nueva columna virtual, permitiendo al usuario catalogar, organizar y filtrar los dispositivos. 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.
- ACCIONES:

 : Botón para ver la información del dispositivo en detalle.



Detalles del dispositivo

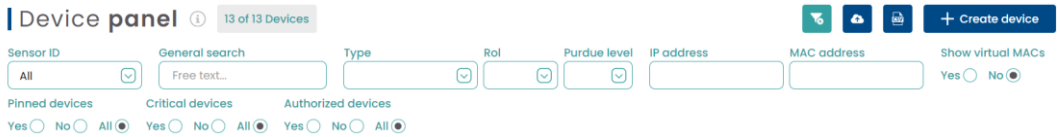
 : Botón para modificar los parámetros del dispositivo.



Parámetros de dados

 : Botón para realizar otras acciones en el dispositivo, como acceder con vista pre-filtrada a la lista de alertas, vulnerabilidades (en desarrollo), así como eliminación de nodos.

Existe la posibilidad de filtrar para que la pantalla muestre solo los dispositivos que nos interesan.



Filtrado de dispositivos

El usuario puede realizar este filtrado según a:

- 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.

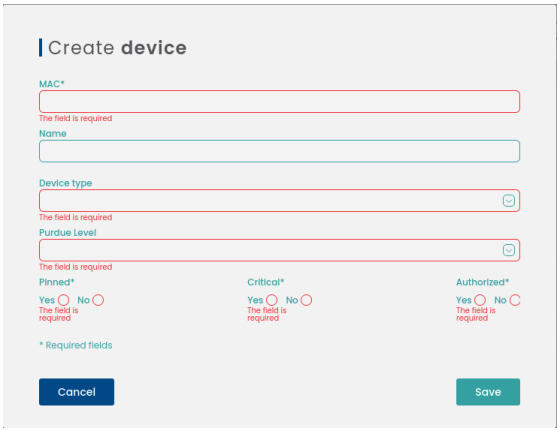
El usuario también puede realizar una búsqueda general usando una cadena de texto.

Pulsar el botón  se reinician los valores de filtrado y Guardian mostrará de nuevo la lista completa con todos los dispositivos.

Mediante el botón,  nuestro producto realizará una exportación de archivo CSV de la lista de dispositivos con su información.

Es posible añadir manualmente un nuevo dispositivo a la red y la lista de la organización haciendo clic en el botón  .

Aparecerá la siguiente ventana emergente:



Campos disponibles para crear un dispositivo.

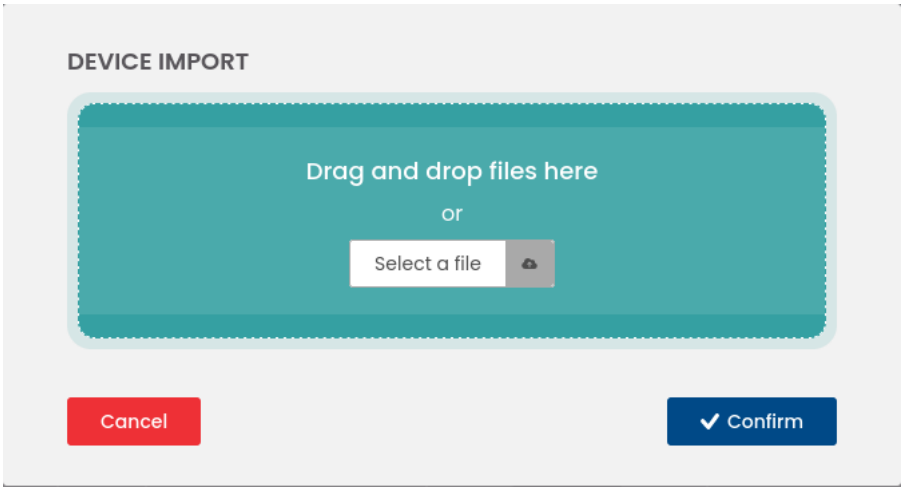
La información solicitada sobre el dispositivo a añadir debe introducirse manualmente y, para que la creación sea efectiva, haz clic en el botón "Guardar".

4.2.2.1 CSV de importación

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 de red y en la pestaña "Lista de dispositivos", verás el siguiente icono: . Al hacer clic en este icono se abrirá la siguiente ventana emergente.

Desde esta ventana, puedes seleccionar o arrastrar un archivo con la extensión ".csv" que contenga los datos de los dispositivos que deseas añadir o modificar, en el formato indicado a continuación.



Importar ventana emergente de CSV.

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

- Un máximo de 250 discos.

- Cabecera con las siguientes columnas (podemos nombrar las columnas como queramos):

  - 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 ";".

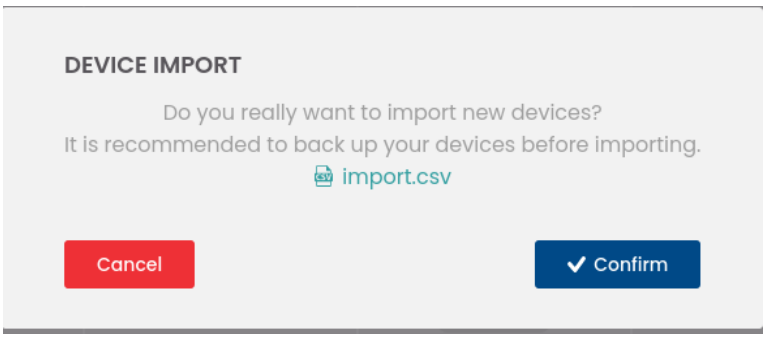
- No debe contener campos vacíos.
- Puede contener nuevos registros de dispositivos, o dispositivos existentes en la base de datos a los que quieras cambiar uno o más de los atributos mencionados en el punto anterior. Se requiere una fila por dispositivo, en el formato indicado.
- Los nuevos registros simplemente tendrán todos los campos CSV cubiertos con la información deseada.
- Los registros existentes que queremos modificar contendrán el literal *CURRENT* en todos esos campos que deben permanecer fijos. En los campos a actualizar, simplemente pondremos la información más reciente basada en lo establecido previamente.
- Los que queremos modificar deben tener *CURRENT* en algunas de sus propiedades; Esto nos permite distinguir estos registros de los nuevos.
- El campo mac no puede contener el literal *CURRENT* ya que identifica univocamente el dispositivo.
- Los nuevos registros también pueden contener el literal *CURRENT* en algunos de sus campos; Esto significa dejar esos campos con valores por defecto. En el caso de datos booleanos, será falso, y los campos de texto, como nombre, Purdue y tipo de dispositivo, permanecerán como NULL, y el usuario podrá modificarlos a través de la interfaz web.
- Existen dos formas posibles de definir un conjunto de campos personalizados, respetando su estructura clave-valor:
    - .json formato: {"key1": "value1", "key2": "value2"}
    - Compases: llave 1 | value1 | clave2 | value2

  Podrías eliminar campos personalizables previamente definidos sobrscribiendo los datos con un nuevo documento CSV. Este documento debería contener el literal *DELETE* en lugar de esos campos, como el uso del literal "CURRENT".

- Es crucial escribir literales entre asteriscos.

Aviso: Por favor, consulte con Soporte si tiene alguna duda, ya que el uso inadecuado de esta funcionalidad puede afectar significativamente a la integridad de la información del nodo.

Una vez seleccionado el archivo, haz clic en "Confirmar", ya que es una operación de alto impacto (permite tanto añadir como modificar propiedades del dispositivo):



Desplegable de "Importación de dispositivo".

Si el archivo ".csv" que hemos enviado no contiene ningún dispositivo, se mostrará el siguiente mensaje de error.

Error de importación.

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.

Error de importación.

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

4.2.2.2 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.

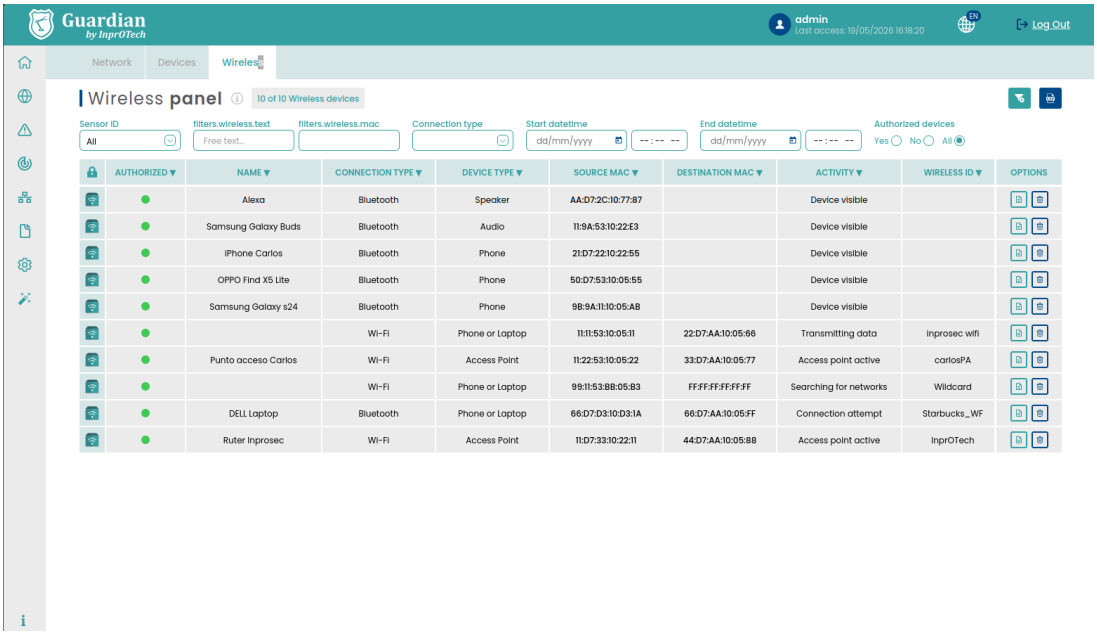
En el lado derecho, hay un panel de botones para eliminar los filtros aplicados previamente y exportar la lista de dispositivos en formato CSV.

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** visto: formato dd/mm/yyyy hh:mm.
- **Última vez:** formato dd/mm/yyyy hh:mm.

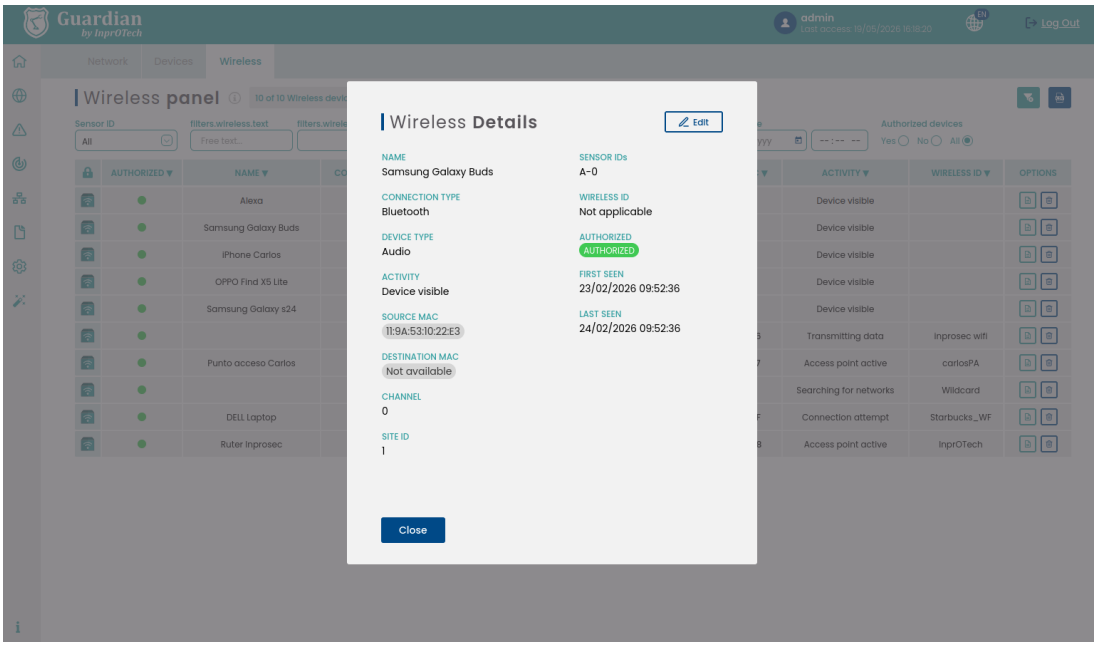


Lista de dispositivos inalámbricos

A continuación se muestran los posibles filtros que se pueden aplicar para mantener los dispositivos que nos interesan:

Recuerda que es posible ordenar los dispositivos alfabéticamente, ya sea directamente o inversamente, 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).



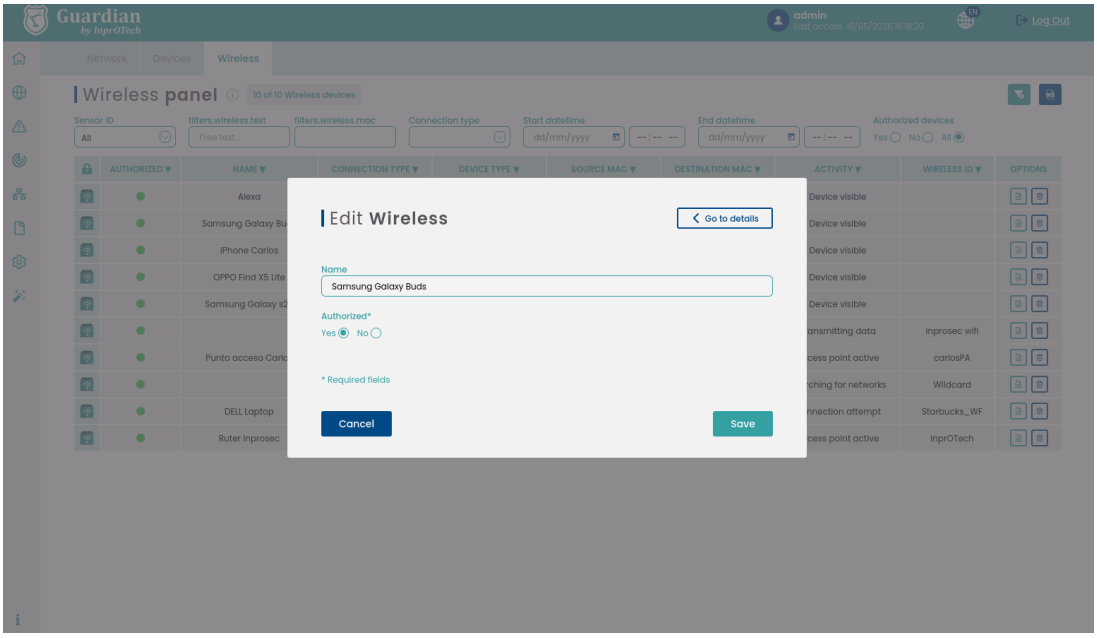
Detalles sobre dispositivos inalámbricos

También podremos ver algunos campos adicionales en esta nueva ventana modal:

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

Si hacemos clic en el 

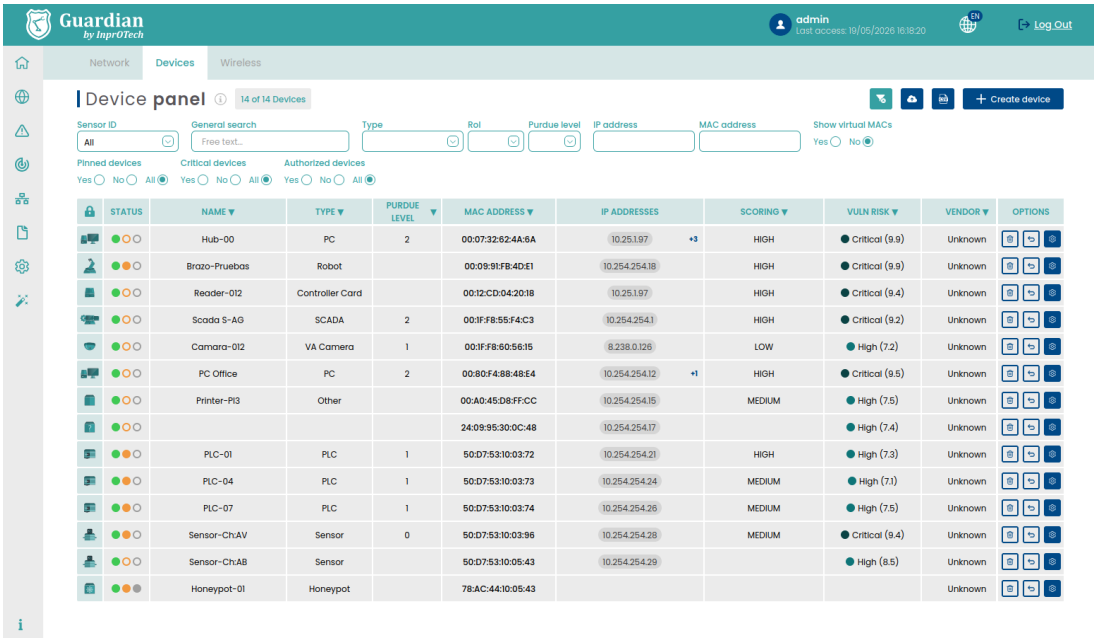
botón, podemos renombrar el dispositivo y determinar si está autorizado o no.



4.2.2.3 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 huella dactilar ligera: versión del dispositivo, firmware, puertos abiertos y servicios que se ejecutan en la propia máquina.

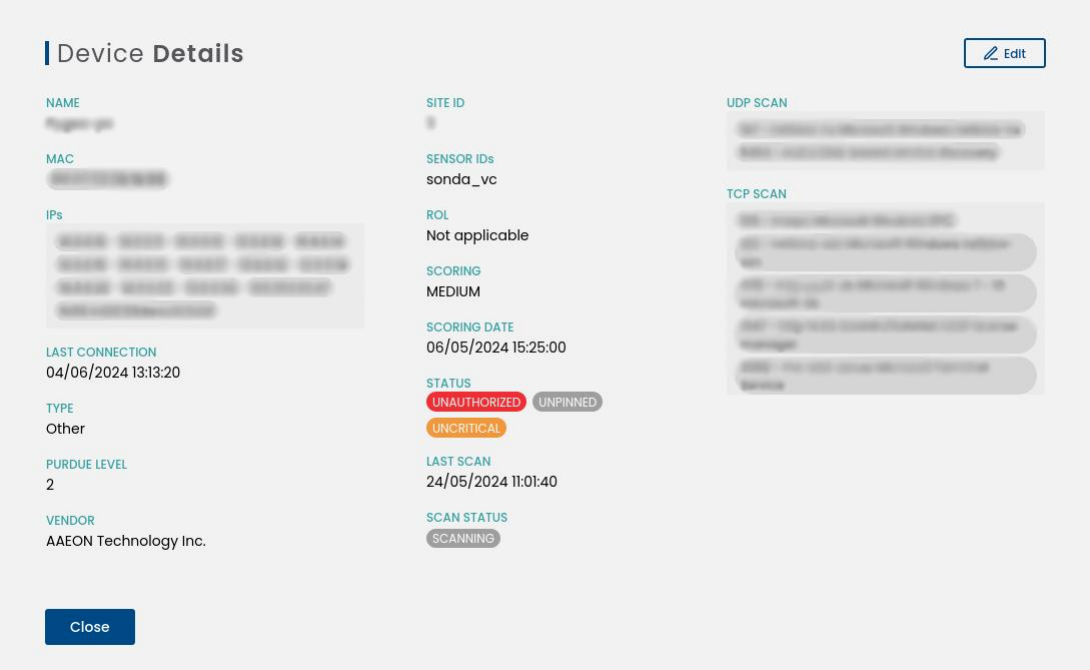
Para ello, se utilizará la herramienta nmap y se escanearán los puertos de los protocolos de red TCP y UDP. Esta información se registrará en la base de datos del sistema y podrá extraerse como atributos adicionales de cada dispositivo, que se actualizarán mediante un agrupamiento periódico.



Lista de dispositivos

Como se puede ver, una vez que el escáner ha sido ejecutado, la información asociada al firmware de algunos dispositivos aparece en la lista.

El resto de la información del escáner puede consultarse haciendo clic en el icono de la derecha  . En la ventana emergente aparecerá toda la información del dispositivo en cuestión, y dos secciones llamadas 'TCP Scan' y 'UDP Scan'. Allí se mostrarán todos los puertos abiertos encontrados para un dispositivo determinado, así como la fecha del último escaneo y si ha terminado correctamente o si ha habido algún tipo de error.



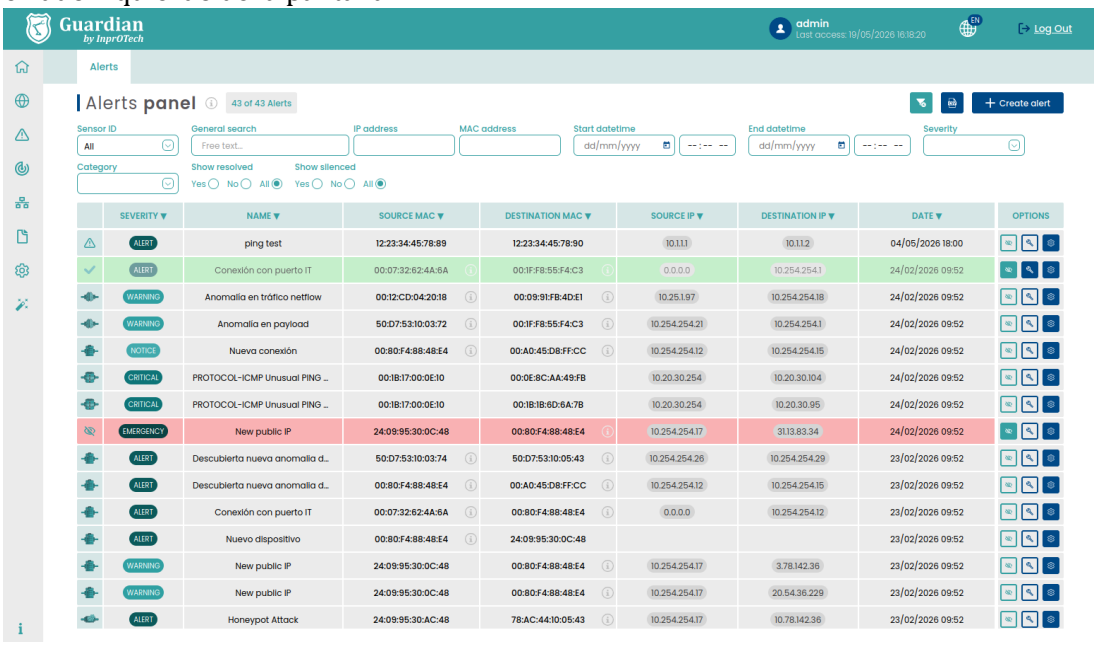
Detalles del dispositivo

AVISO: Dada la naturaleza activa de esta operación, aunque no se ha observado ningún impacto operativo, no puede descartarse por completo. Por tanto, corresponde al cliente decidir si activa esta funcionalidad (para lo cual se debe consultar el soporte de InprOTech). Si quieres activarlo en tu instancia pero dejar algún subconjunto de dispositivos excluido de la lista de nodos para analizar, simplemente etiquétalos con la propiedad 'Crítico' activada en el inventario de dispositivos (individualmente 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.



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 el impacto que pueda tener en la organización.

- Nombre: Nombre definido de la alerta.

- MAC de origen: MAC del dispositivo generador de alertas.

- MAC de destino: MAC del dispositivo al que se dirigía la acción.

- IP de origen: IP del dispositivo que genera la alerta.

- IP de destino: IP del dispositivo al que se dirigía la acción.

- Fecha: Fecha y hora de la aparición de la alerta.

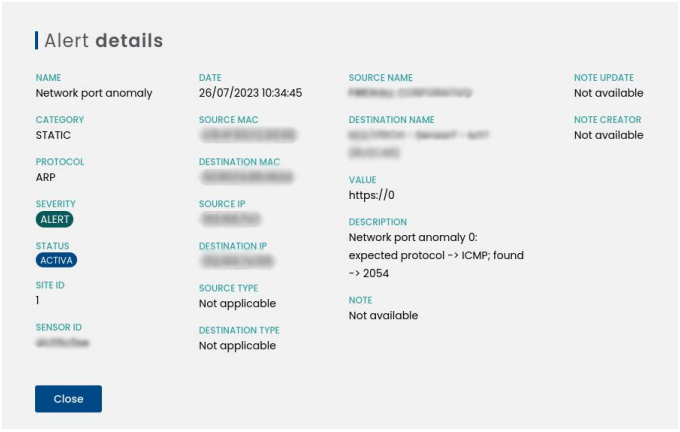
- Acciones (véase el anexo I para definiciones):

: Si colocamos el cursor encima, podremos saber el nombre del dispositivo asignado a esa dirección MAC.

: Botón para cambiar el estado de la alerta a silenciado o no silenciado (véase la sección 6.2 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 de alerta

Es posible filtrar la pantalla para mostrar solo las alarmas de interés.

Filtros de alerta disponibles

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: Búsqueda introduciendo un texto que contiene la alarma (incluido en tus notas).

- Dirección IP del dispositivo

- Dirección MAC del dispositivo

- Fecha y hora de inicio de la búsqueda de alertas

- Fecha y hora de la búsqueda de alerta, fecha y hora de fin

- Gravedad, según el Anexo I

- Alarmas resueltas o no resueltas, según el Anexo I

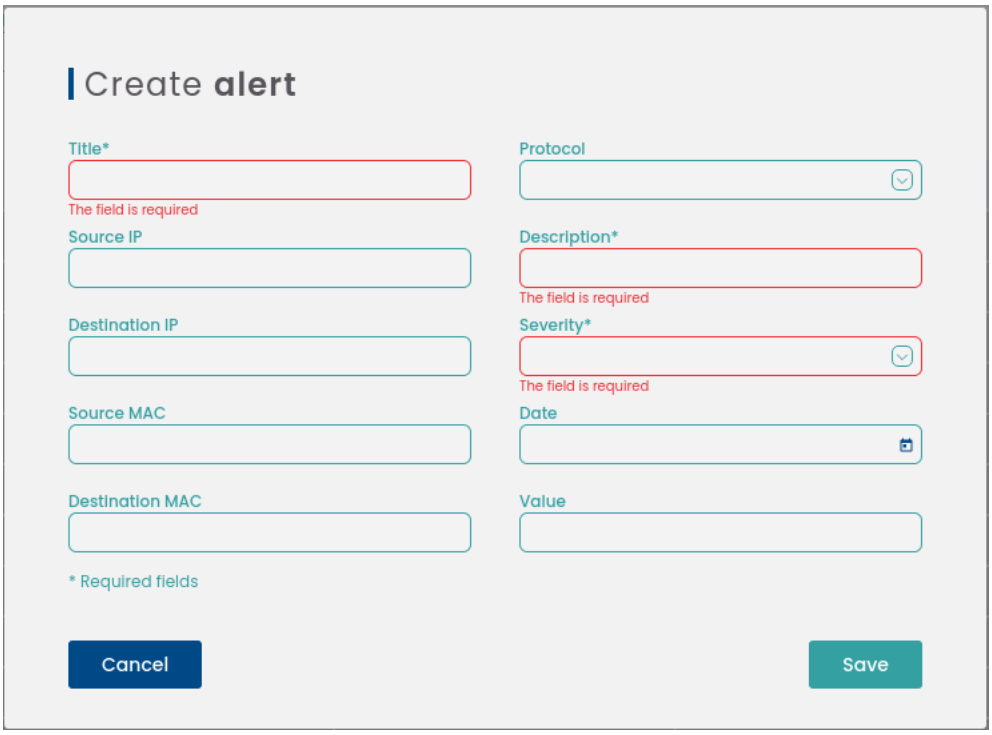
- Alarmas silenciadas o no, según el anexo I

Pulsar el botón se reinician los valores de filtrado y se mostrará de nuevo la lista completa con todas las alarmas.

Mediante el botón se realizará una exportación de archivo CSV con la lista de alarmas con su información.

Es posible crear manualmente una alarma específica en la red de la organización haciendo clic en el botón + Create alert.

Aparecerá la siguiente ventana emergente:



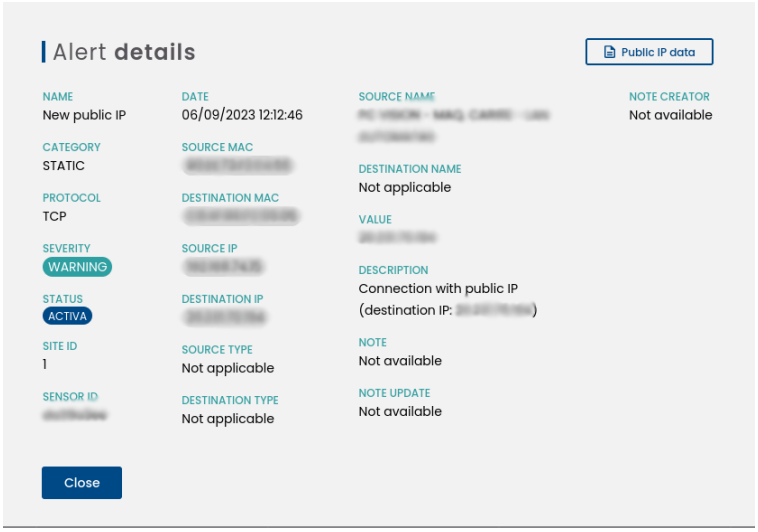
Creación de alertas

La información solicitada sobre la nueva alarma creada debe introducirse manualmente y, para que la creación sea efectiva, haz clic en el botón "Guardar".

4.3.1 IP pública

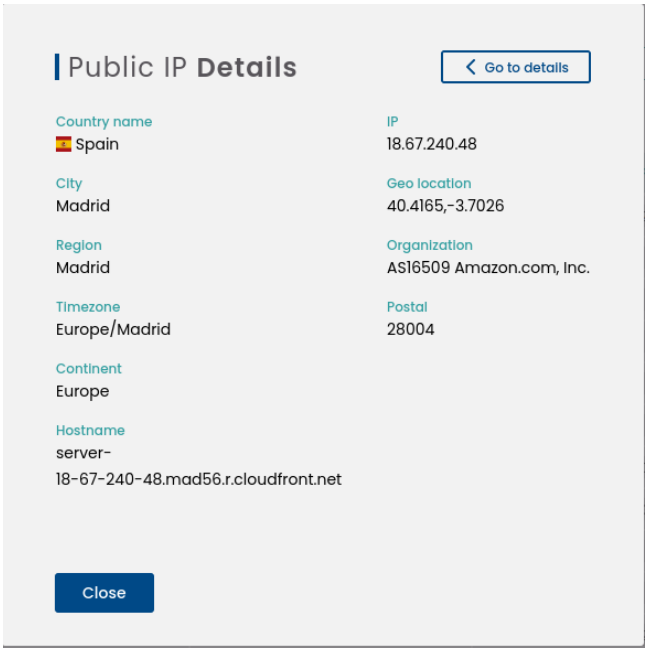
Esta alerta está conectada a un servicio de ciberinteligencia que nos permite obtener más información sobre el punto final de comunicación fuera de la red confiable, para intentar determinar si puede ser malicioso.

Para acceder a los detalles de la alerta, haz clic en el icono de engranaje, que se puede ver en el lado derecho del panel. Luego, haciendo clic en "Ver detalles", puedes acceder a esta información:



Pantalla con detalles de alerta.

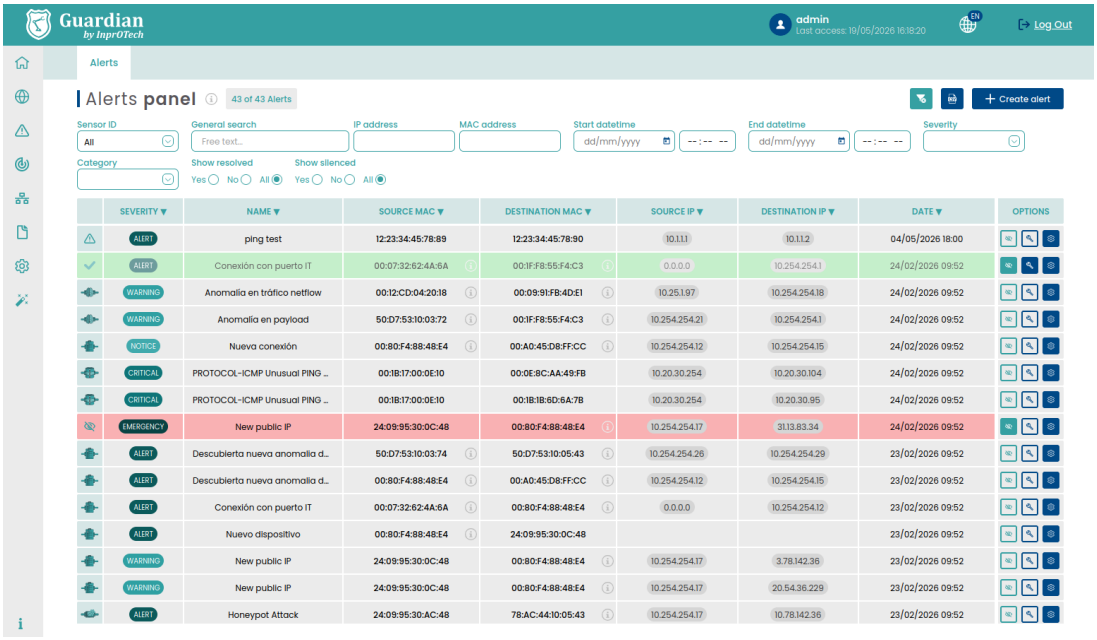
En la parte superior de esta pestaña hay un botón llamado 'Datos IP Públicos'. Al hacer clic en este botón accederás a información adicional sobre la IP, que puede incluir detalles como ciudad de origen, región, zona horaria, continente, nombre del país, dirección IP pública, coordenadas, organización y código postal.



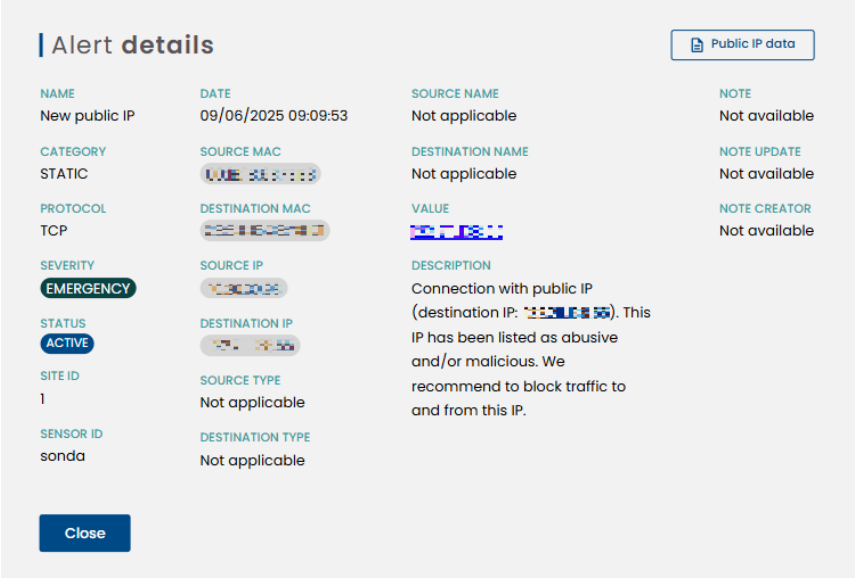
Detalles de la IP pública

4.3.2 Política de Reputación de IP y Bloqueo

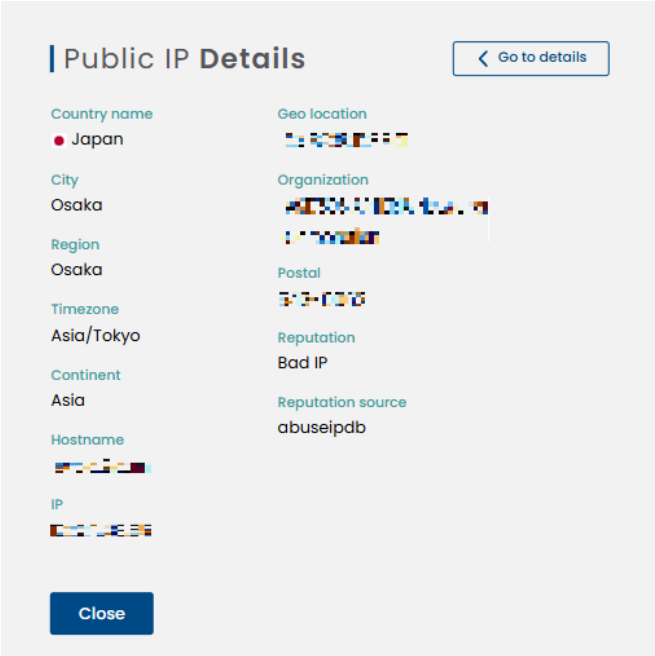
Cuando el sistema detecta una *nueva alerta pública de conexión IP* , Guardian se conecta a una serie de listados públicos donde se reportan actividades consideradas abusivas (spam, hacking, etc.). Esta información enriquece la alerta con más detalles reputacionales y, en caso de que detecte que el discurso público es sospechoso, cambia la gravedad, la descripción y la marca en rojo.



Alerta pública maliciosa de IP resaltada en rojo

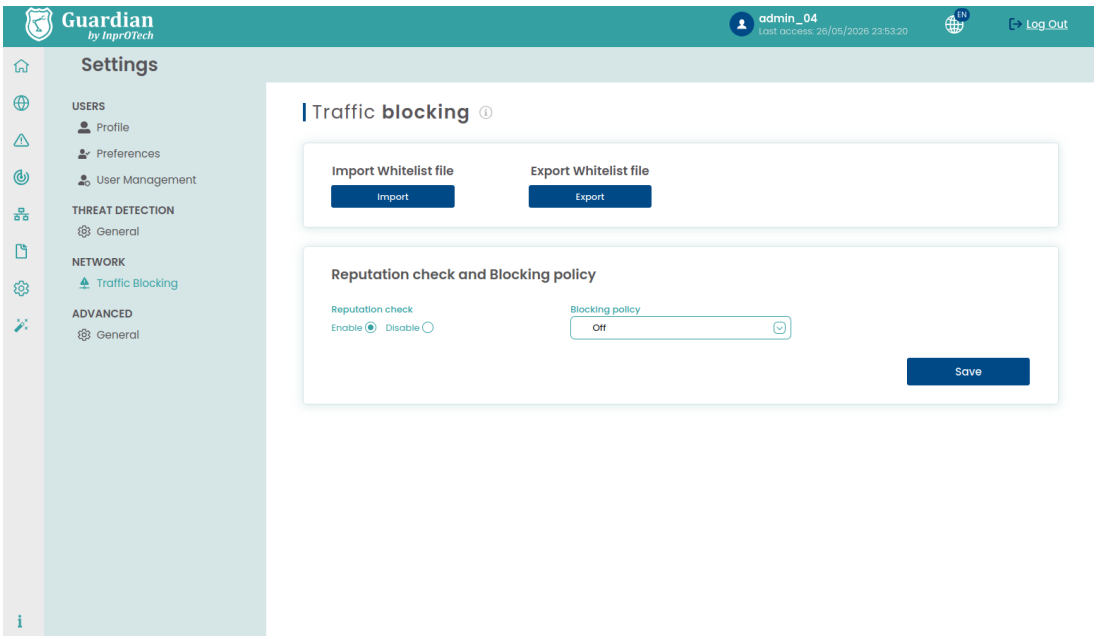


Detalles de alerta con información enriquecida



Detalles públicos de la propiedad intelectual con información reputacional

La comprobación de reputación puede activarse y desactivarse en el menú de configuración, sección Red/Bloqueo. 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.



Cuando el sistema recibe una alerta IP pública considerada maliciosa, Guardian responderá aplicando una de las tres Políticas de Bloqueo disponibles*:

* La disponibilidad de las opciones no informativas dependerá del contexto del cliente, en particular del fabricante/modelo del cortafuegos con el que Guardian debe comunicarse. Por si tienes dudas o si necesitas más
Información, por favor contacte con el equipo de soporte.

-Informativo, donde se informa y se recomienda al usuario revisar y bloquear el tráfico desde/hacia esa dirección.
-Manual o semi-desatendido, donde se habilita un botón para bloquear o desbloquear la IP maliciosa enviando al firewall una instrucción para incluir esa dirección en un filtro. -Automático, donde Guardian envía esta instrucción al firewall sin intervención humana.

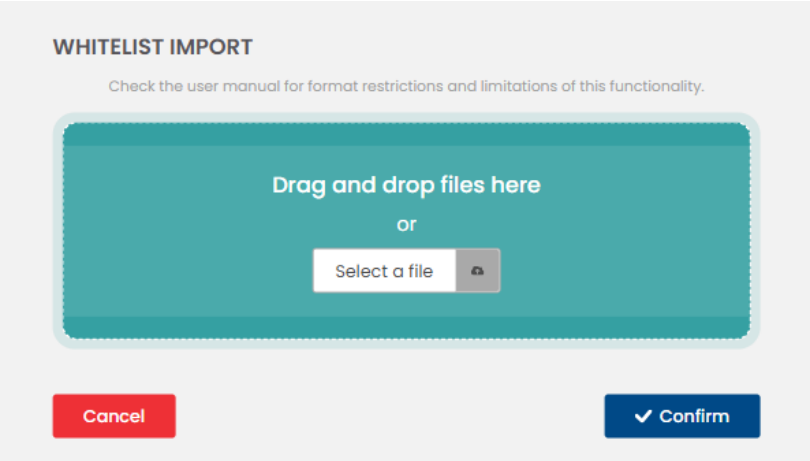
La Política de Bloqueo también puede desactivarse. En este caso, toda la información sobre la reputación IP en las alertas será deshabilitada, así como las reglas de bloqueo (enviando un comando al cortafuegos para eliminar la regla de bloqueo de direcciones). Esta información no se elimina y se volverá 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.

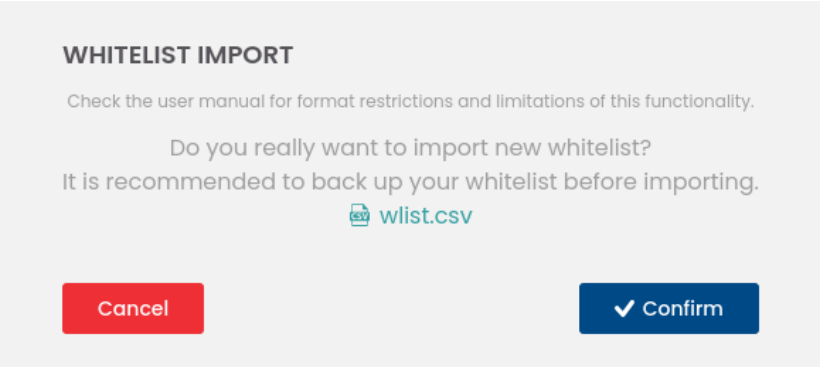
4.3.3 Lista blanca de IP

El usuario puede proporcionar una lista de direcciones IP siempre permitidas, o también rangos de direcciones en formato CIDR (lista blanca). Estas direcciones nunca tendrán su reputación calculada, incluso si la comprobación se activa cuando se recibe una alerta relacionada. Esto solo se reflejará en el menú público de datos IP en su campo de reputación como *lista blanca*.

El archivo de subida debe estar en *formato csv*, con solo una columna por fila, que debe contener una dirección IP (192.168.0.1) o un rango CIDR (192.168.1.0/24). La carga se realiza de forma atómica: un solo dato mal formateado o inválido invalida toda la operación. Las posibles redundancias en la lista de direcciones y rangos (IPs repetidas, IPs contenidas en rangos CIDR, rangos CIDR superpuestos) no se consideran errores.

La importación se realizará en las opciones de bloqueo, a través de la pantalla que se muestra tras pulsar el botón Import bajo la opción "*Importar archivo de lista blanca*", que mostrará la siguiente ventana emergente donde puedes arrastrar el archivo a la caja verde o encontrarlo en el árbol de archivos del usuario.





Las siguientes importaciones reemplazarán completamente la lista blanca anterior. Por tanto, si no quieres implementar ninguna lista blanca, simplemente carga un archivo vacío.

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

- aquellas alertas con IPs que ya tienen la reputación procesada antes y que están incluidas en la nueva lista blanca, se devuelven al estado original con el estado '*reputación: Wlisted*'.

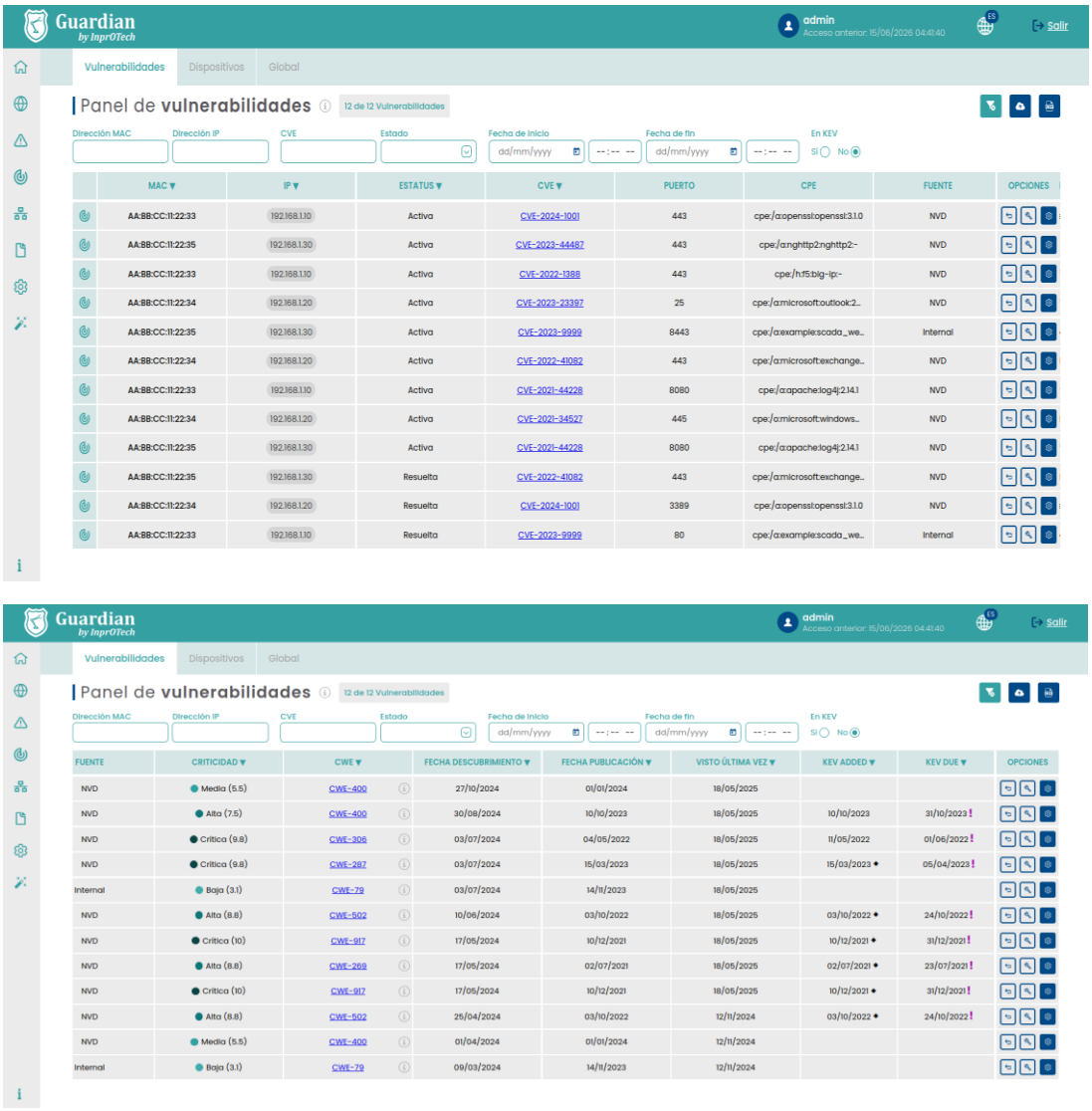
- Aquellas alertas con IPs dentro de la lista blanca anterior, pero que están fuera de la nueva lista blanca, tienen su reputación calculada y la descripción de la alerta modificada en consecuencia.

La lista blanca cargada puede descargarse para su examen haciendo clic en el botón Export, que descargará 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".



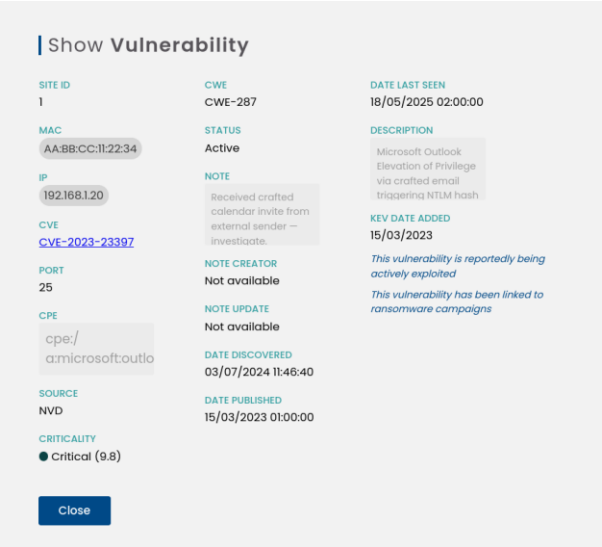
Vista del Panel de Vulnerabilidades

En la pestaña del panel de vulnerabilidades, el usuario puede ver una lista de todas las vulnerabilidades presentes en la red. Estos se encuentran en los servicios detectados tras los puertos abiertos descubiertos por Smart View y comparados con la base de datos de vulnerabilidades del NIST, la National Vulnerability Database (NVD) y el catálogo CISA.

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 f 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 criticidad 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 ha detectado la vulnerabilidad.
- Fecha de publicación: la fecha de documentación en la que se reportó la vulnerabilidad con el CVE referenciado en la base de datos de vulnerabilidades NVD.
- "Última vez visto": marca temporal en la que se vio la vulnerabilidad por última vez.
- KEV AÑADIDA: KEV, siglas en inglés de "Vulnerabilidades Explotadas Conocidas". Catálogo CISA de CVE activamente explotados en el estado real, con la fecha de inclusión y un ◆ cuando el CVE se vincula a campañas de ransomware.
- KEV VENCIMIENTO: Fecha límite propuesta por la administración CISA para incentivar 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 de una vulnerabilidad.

Junto al encabezado, podemos ver el número de vulnerabilidades mostradas, junto con el recuento total.

Número de vulnerabilidades y filtros.

En la captura de pantalla superior, también podemos ver que es posible aplicar filtros, por lo que la pantalla solo muestra las vulnerabilidades deseadas. Este 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.

Usando el botón, puedes importar un archivo con una extensión ".csv" que contenga las vulnerabilidades que quieres añadir. Deben contener los siguientes campos, manteniendo 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

Por otro lado, usando el  botón, es posible exportar un archivo CSV que contenga la lista de dispositivos y su información.

4.4.2 Estadísticas del dispositivo

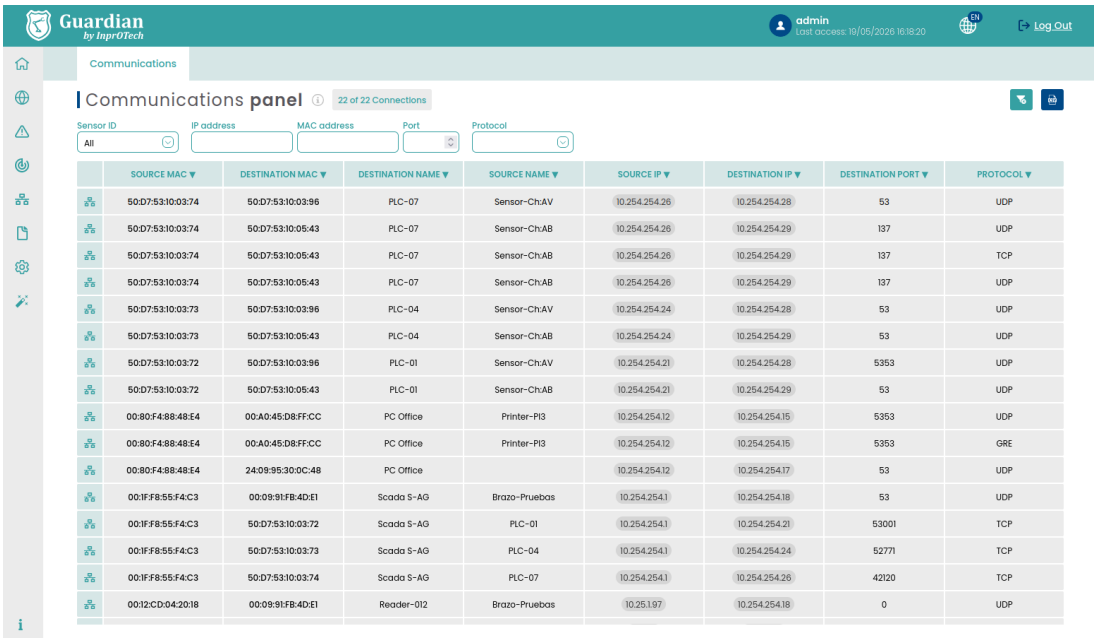
Ofrece las vulnerabilidades encontradas en la red, ordenadas por los dispositivos disponibles.

4.4.3 Estadísticas globales

Ofrece estadísticas globales de la red dadas 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.



Lista de comunicaciones.

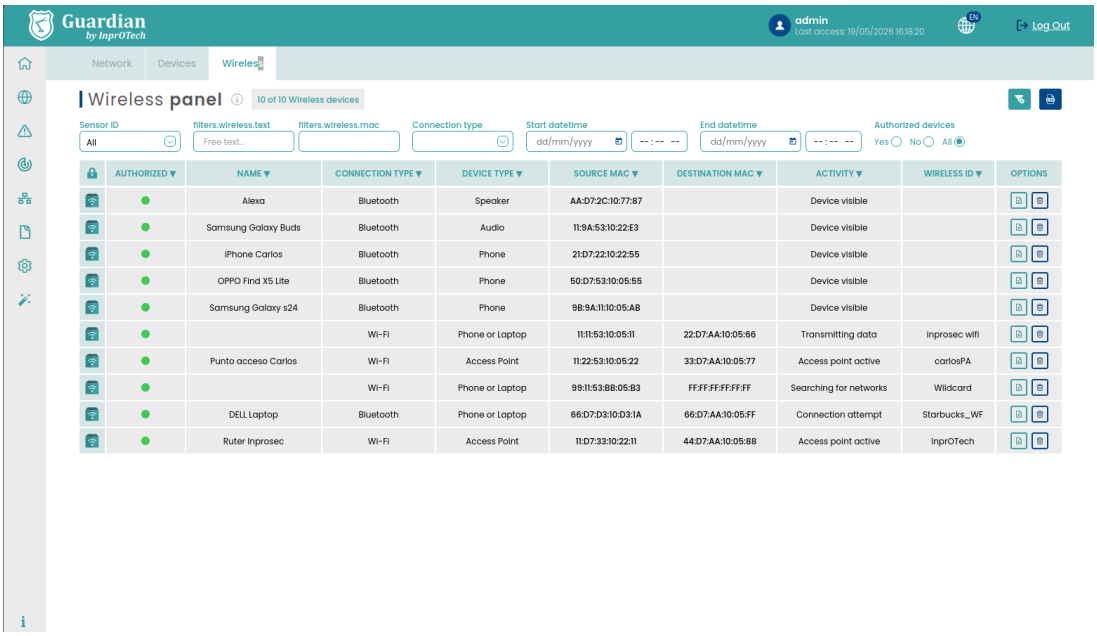
Se mostrará una lista de todas las comunicaciones realizadas entre los dispositivos OT de la red de la organización, así como la información sobre ellos.

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.

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.



Últimos informes disponibles

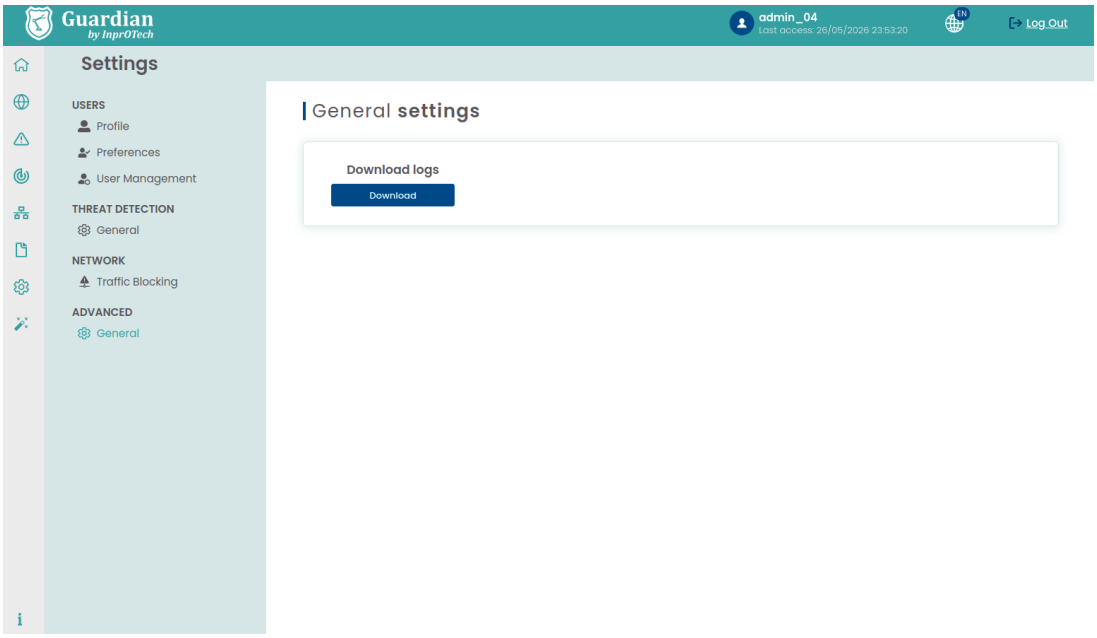
En la pantalla se mostrará una lista de los informes generados tanto manual como automáticamente con una periodicidad determinada, disponible para descargar.

4.7 Otros escenarios

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

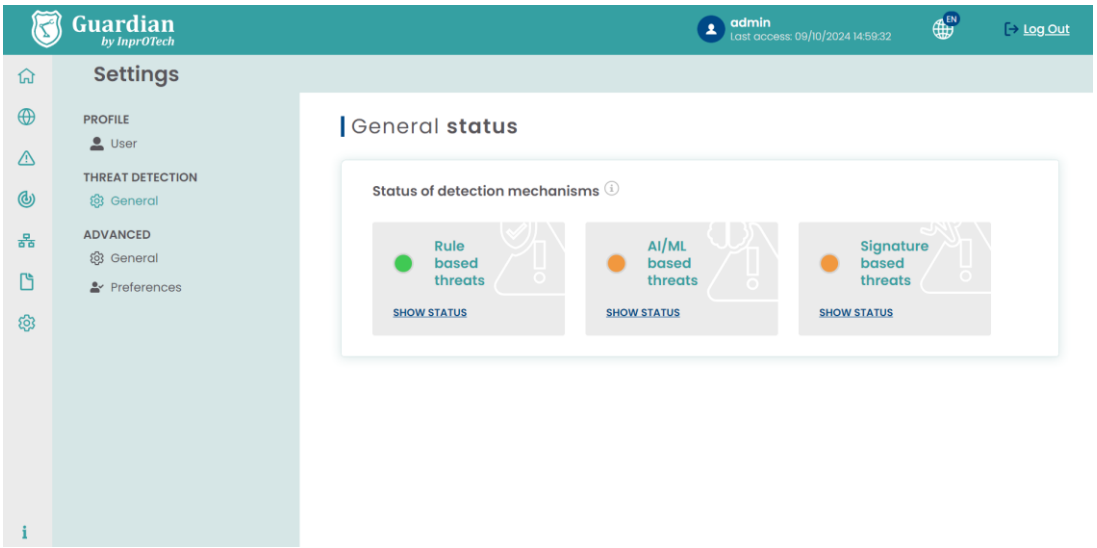
En la sección General Avanzado, el usuario puede descargar los registros del sistema en un archivo en su carpeta de descargas. El formato de registro es una pequeña variación respecto al estándar de registro de Python:

```
[2026/05/26 23:42:33] DEBUG loggingguardian >> → GET /alert
[2026/05/26 23:42:33] DEBUG loggingguardian >> Params: {"count": "100", "offset": "0", "order_type": "desc",
"order_property": "timestamp", "silenced": "false", "resolved": "false"}
[2026/05/26 23:42:33] DEBUG loggingguardian >> Respuesta | HTTP 200 | {"elementos": [{"id": 1, "título": "aparici\u00f3n
fantasmal", "timestamp": 1779832800.0, "severity": "emergency", "silenciado": falso, "resuelto": falso, "bloqueado": falso,
"id_fabrica": 1, "id_sonda": null, "categoría": null, "description": "Prepara los dados de la muerte", "value": null,
"src_ip": "127.1.1.2", "src_mac": "aa:bb:cc:11:22:33", "src_device_type": null, "src_device_name": "jarl", "dst_ip":
"192.121.1.2", "dst_mac": "11:22:11:22:11:22", "dst_device_type": nulo, "dst_device_name": nulo, "protocolo": "17",
"nota": nulo, "creador": nulo, "timestamp_note": nulo, "otros": nulo}], "has_more_elements": falso, "desplazamiento": 0}

[2026/05/26 23:42:33] DEBUG loggingguardian >> → GET /alert/module
[2026/05/26 23:42:33] DEBUG loggingguardian >> 192.168.1.64 [f001|u000] GET /alert HTTP/1.1 ::200::

[2026/05/26 23:42:33] DEBUG loggingguardian >> Páramos: {"order_property": "id", "order_type": "asc"}
[2026/05/26 23:42:33] DEBUG loggingguardian >> → GET /vulnerabilities/count
[2026/05/26 23:42:33] DEBUG loggingguardian >> Respuesta | HTTP 200 | []
[2026/05/26 23:42:33] DEBUG loggingguardian >> Params: {"status": "active"}
[2026/05/26 23:42:33] DEBUG loggingguardian >> 192.168.1.64 [f001|u000] GET /alert/module HTTP/1.1 ::200::


[2026/05/26 23:42:33] DEBUG loggingguardian >> Respuesta | HTTP 200 | {"contar": 18}
[2026/05/26 23:42:33] DEBUG loggingguardian >> 192.168.1.64 [f001|u000] GET /vulnerabilities/count HTTP/1.1 ::200::

[2026/05/26 23:42:33] DEBUG loggingguardian >> → GET /algorithm/
status[2026/05/26 23:42:33] DEBUG loggingguardian >> Params: {}
[2026/05/26 23:42:33] DEBUG loggingguardian >> Respuesta | HTTP 200 | [{"id": 5, "id_fabrica": 1, "status": "Inactivo",
"algoritmo": "inprotech_anagram", "timestamp": 1779667846.648889}]
[2026/05/26 23:42:33] DEBUG loggingguardian >> 192.168.1.64 [f001|u000] GET /algorithm/status HTTP/1.1 ::200::
```



Sectón 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 (rojo, naranja, verde):



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 tienen estatus 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 de los algoritmos están en modo producción, pero no todos.
- Verde: todos los algoritmos están en modo producción.
- Grey: No existen algoritmos

Amenazas basadas en la firma

- Rojo: todos los elementos tienen un valor de entrenamiento, inactivo o algunos no cubiertos en su campo de estado.
- 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**: El sistema Guardian no interactuará activamente con aquellos dispositivos marcados como críticos. Por ejemplo, dispositivos antiguos, sin tripulación para mantenimiento, sin repuestos, etc.
- **Fijos/No fijos**: Los dispositivos fijos aparecerán en la aplicación Guardian 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 marcadas como resueltas son aquellas que ya han sido gestionadas, pero quieres mantener la ocurrencia de la alarma en futuras situaciones idénticas (misma tipología, MACs, IPs y puertos implicados). Los que no se resuelven están pendientes de gestión.
- **Silenciado/No silenciado**: Las alarmas declaradas como silenciadas no volverán a ocurrir en el mismo contexto de red*. Por ejemplo, un dispositivo que se comunique con una IP pública conocida y controlada por la organización, y no quieres que se generen alarmas para esta situación.

* 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 InprOTech a petición del cliente, si es necesario.

5.2.2 Según la gravedad

Los niveles de gravedad de la solicitud en términos de generación de alertas se toman del RFC 5424, aunque no son equivalentes ya que la gravedad de los eventos se ha catalogado en función de la experiencia de nuestros técnicos.

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

-Emergencia

- Alerta

- Crítica

- Error

- Advertencia

- Advertencia

- 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

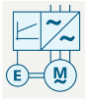
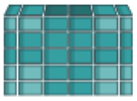
	TELÉFONO	2
	RTU	1
	VS-CAM	1
	LECTOR DE CÓDIGOS DE BARRAS	1
	PLC	1
	ROBOT	0
	VARIADOR DE FRECUENCIA	0
	TARJETA CONTROLADOR	0
	SENSOR	0
	AFD	0
	SWITCH	Varios
	ENRUTADOR	Varios
	CORTAFUEGOS	Varios
	OTROS	Varios
	HONEYPOT	Varios

Tabla 1: Iconos representativos de dispositivos

7 ANEXO III: Alert icons.

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