InprOTech

Smart security for your industry

Manual de usuario

InprOTech Guardian

Fecha: 07/2023

Referencia documento: IN-Manual de usuario InprOTech Guardian

Versión: 0.11

INDICE

1 Introducción

InprOTech Guardian es una herramienta de descubrimientos de activos y monitorización y detección de anomalías, capaz de identificar amenazas de ciberseguridad en entornos industriales. Analiza el tráfico de red, identifica los activos en la misma, genera informes comprensibles, y eleva alertas mediante el uso de reglas estáticas, firmas de IDS e inteligencia artificial con el fin de mitigar amenazas en la red industrial.

La interfaz de InprOTech Guardian es altamente interactiva, fácil de entender y manejable. Además, se encuentra tanto en español como en inglés.

Esta interfaz está desarrollada utilizando el framework Angular siguiendo las mejores prácticas y metodologías de seguridad para garantizar una navegación segura de la información.

Mediante la aplicación InprOTech Guardian el usuario tendrá una visión y un conocimiento completo de los siguientes aspectos:

- **Dashboard continuo**: Panel con autorrefresco para monitorizar los aspectos principales de activos, amenazas y reporting 24x7 en un centro de operaciones.
- **Resumen de activos:** Visualización del número de dispositivos conectados a la red, clasificados según el modelo PURDUE.
- **Accesos rápidos:** A alertas, vulnerabilidades, algoritmos y reglas activas.
- **Gráfica de tráfico de red:** Gráfico del tráfico generado, tanto emitido como recibido, en las últimas 24 horas y comparado con el mismo periodo de tiempo de 7 días antes.
- **Gráfico de alertas:** Gráfico de las alertas recibidas de los últimos 7 días, diferenciadas por colores según su nivel de severidad y la tendencia que éstas siguen a lo largo del tiempo.
- **Mapeo de la red:** Visualización de todos los dispositivos de la red, cómo están conectados y cómo está estructurada la red de la organización. También se visualizarán todos aquellos dispositivos conectados y que no han sido considerados como legítimos.
- **Gestor de dispositivos:** Listado de activos para su identificación y administración. Desde la identificación y el etiquetado de dispositivos, hasta la inclusión de dispositivos en la lista negra según su nivel crítico…
- **Gestor de alertas:** Listado de eventos y alertas en la red OT de la organización, clasificadas según su nivel de severidad. Están codificadas por colores y detalladas con información dinámica. Serán clasificadas según su estado (resueltas y silenciadas), y se generan en base a heurísticos, firmas de IDS e inteligencia artificial/machine learning.
- **Integración con terceros sistemas (SIEM**): Guardian provee la capacidad de enviar las alertas activas generadas a un tercer sistema como puede ser un SIEM (Security Information and Event Management), para su ingesta y correlación con otras fuentes de logs. Para ello, hace uso del protocolo syslog.
- **Gestor de vulnerabilidades**: Posibilidad de realizar escáneres de vulnerabilidades bajo petición del cliente y únicamente a los dispositivos seleccionados (en desarrollo).

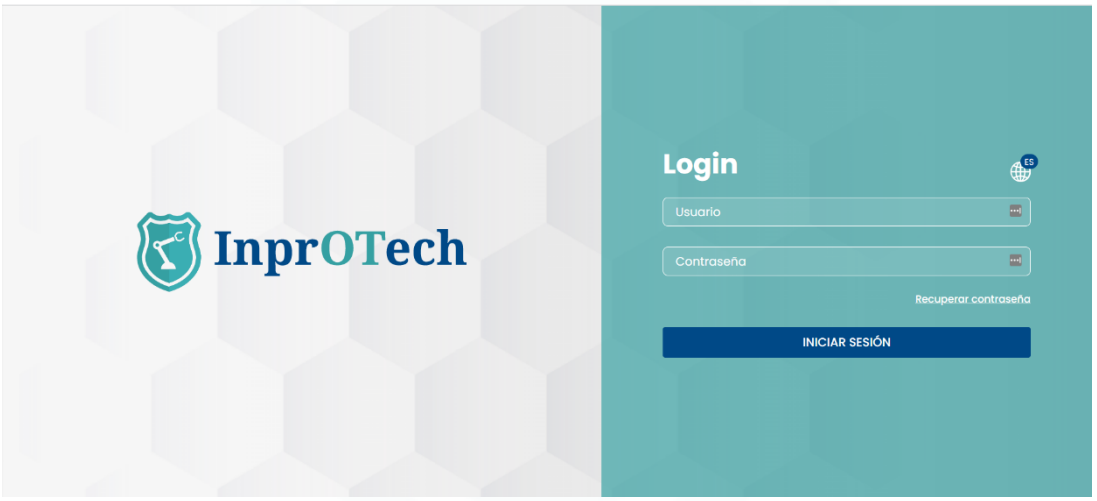
- **Lista de comunicaciones:** Listado con todas las comunicaciones que se han realizado entre los dispositivos OT de la red de la organización, e información acerca de ellas.
- **Generación de reportes:** Recopilación de información acerca de la red, dispositivos, indicadores, etc., para futuros análisis y verificaciones tanto a nivel técnico como de negocio.

Es importante destacar que además del propio uso del aplicativo, el servicio implica una serie de preparativos para el onboarding, que pasan por una adecuada toma de datos, despliegue, instalación, y fine-tuning de la solución para sacarle el máximo partido, en base a acciones como las que se indican en la siguiente sección.

2 Primeros pasos

2.1 Acceso a la consola web

Primeramente, se ha de acceder al navegador e introducir la dirección http://[IP]:9000, en donde IP es la dirección asignada a la interfaz de gestión.



Pantalla de acceso a InprOTech Guardian

En todo momento, podrá seleccionar el idioma de su elección en el icono del mapamundi (inglés o español).

El usuario deberá autenticarse, introduciendo el nombre de usuario y contraseña que se le ha asignado. En caso de tener el segundo factor de autenticación activado, deberá introducir adicionalmente el token de un solo uso recibido vía email en su cuenta de correo de usuario del servicio.

El usuario podrá ser:

- **Admin Inprotech:** Tendrá acceso a toda la información presentada por la aplicación y podrá realizar las configuraciones que considere oportunas de algoritmos, Ids de fábrica, modos de producción, etc.

- **Admin Fábrica:** Acceso similar a el caso anterior, excepto a la parte especifica de configuración mencionada.

- **Operador Guardian:** Usuario exclusivo de lectura. Contará con acceso a la descarga de manuales, reportes y, exportación de resultados de búsquedas y determinados listados (Dispositivos, Alertas, Vulnerabilidades, Comunicaciones, Análisis del tráfico, etc.).

En el caso de que el usuario haya olvidado o bloqueado su contraseña, tendrá la opción de recuperarla, pulsando sobre la opción de "Olvidé mi contraseña".

Pantalla de recuperación de contraseña

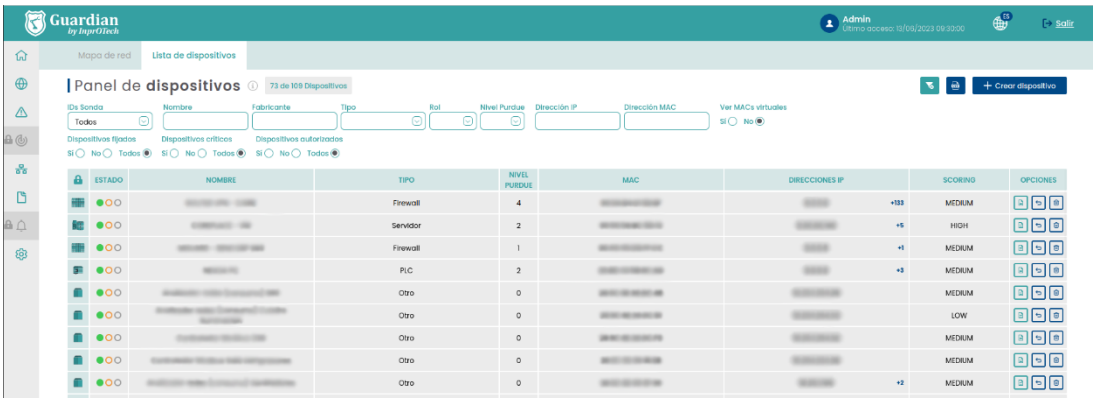
Al Introducir el correo electrónico, en caso de ser válido, se le enviará un enlace a dicho correo para poder restablecer la contraseña de acceso mediante un token de un solo uso.

**Esta funcionalidad, así como otras necesarias para las actualizaciones de software de Guardian o acceso remoto, requieren que exista conectividad entre el sistema y ciertos servicios de inprosec o internet, por lo que se facilitará la lista de reglas a aplicar en el cortafuegos.*

2.2 Organización de lista de dispositivos

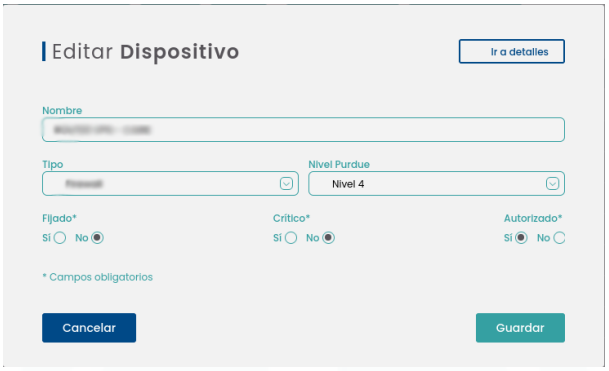
Se ha de organizar el listado de dispositivos mediante la declaración del nombre de cada dispositivo, así como, su nivel PURDUE y su estado (Ver Anexo I). Mediante esta declaración, el usuario contará con una mayor facilidad para la identificación de cada dispositivo en las distintas ventanas de la aplicación, y así poder realizar las gestiones en cada dispositivo con mayor agilidad, así como extraer más valor del servicio.

El usuario deberá dirigirse a la lista de dispositivos, pulsando en el icono  de la parte de la izquierda de la pantalla y seleccionando la pestaña "Lista de dispositivos".



Pantalla de listado de dispositivos

Posteriormente deberá pulsar el botón  de cada uno de los dispositivos de la lista



Pantalla de editado de dispositivos

Y rellenar manualmente los campos de nombre de dispositivo, nivel PURDUE al que pertenece el equipo y, seleccionar su estado indicando si el dispositivo se encuentra fijado, crítico y/o autorizado (ver definiciones en Anexo I).

Para hacer cambios masivos de manera más ágil, esta configuración anterior puede realizarse directamente en la lista de activos pulsando el icono del candado  , y aceptando en el pop-up de confirmación.

Una vez realizado lo anterior, se pulsará el botón “Guardar” para hacer efectivos los cambios en el sistema.

2.3 Configuración de reglas

El sistema Guardian realiza la detección de amenazas en base a múltiples criterios basados en comportamiento, como son:

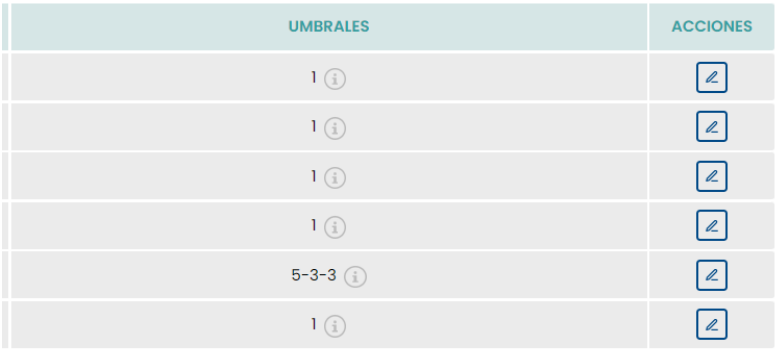
- Amenazas basadas en reglas predefinidas parametrizables
- Amenazas basadas en firmas de IDS
- Amenazas basadas en algoritmos de IA/ML

El usuario deberá configurar qué reglas desea que sean operativas para el análisis de la red de su organización, así como los rangos de tiempos para obviar cada una de las alarmas si lo considera oportuno. Esto se haría de mutuo acuerdo con InprOTech en el onboarding; a priori el usuario sólo verá las reglas y umbrales, pero no podrá editarlas.

El rango de tiempo para obviar una regla significa que podemos establecer un umbral o periodo de tiempo en el que las reglas establecidas no generarán una alerta en un escenario idéntico, y de esta forma evitar avisos y alertas innecesarias de las que ya somos conscientes.

Adicionalmente, podrán configurarse otros parámetros. Se detallará más adelante. Para la configuración de estos rangos de tiempo, pulsaremos el botón del menú izquierdo de la pantalla y pincharemos en Detección de Amenazas > General > Amenazas basadas en reglas, VER ESTADO.

En la columna de umbrales, podremos ver rápidamente los configurados por cada regla.



En la columna de acciones podremos editar estos parámetros.

Adicionalmente, en esta sección se incluirá una vez esté disponible, la configuración de la mensajería asociada a notificaciones de alertas que se deseen recibir, y de los reportes.

2.4 Ajustes

En el apartado Ajustes de la sección Guía rápida, se puede consultar la parametrización básica acerca de los datos de perfil de usuario, la configuración de seguridad, y las preferencias de notificaciones de alertas. Se recomienda su revisión y adaptación a las necesidades.

2.5 Configuración de reportes

Por el momento, los reportes se generan de forma automática con periodicidad semanal.

2.6 Dashboard continuo (opcional)

Si le interesa poder consultar de forma permanente el estado de Guardian y los principales indicadores asociados (dispositivos no autorizados, tráfico de red, alertas, etc.), puede disponer del dashboard principal de Guardian en un monitor en su sala de operaciones con autorrefresco cada 5 minutos.

Para ello, contacte con su Soporte de Guardian y solicite la creación de un usuario de Monitorización.

2.7 Exportación de alertas (opcional)

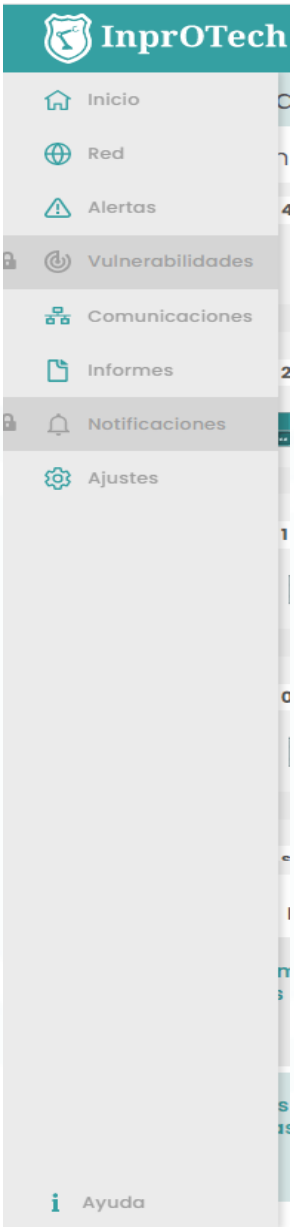
Si el cliente lo desea, puede contactar con su Soporte de Guardian para que habiliten el envío automático de las alertas generadas a un servidor syslog de un SIEM o similar, para su ingesta y correlación* con otras fuentes de logs.

Lo único que debe proporcionar, es la IP y puerto a la que desee que se envíen los mensajes.

* A estos efectos es importante señalar que todas las fechas que devuelve la aplicación web se muestran en hora UTC.

3 Guía rápida

3.1 Ventana de accesos



Detalle de ventana de accesos

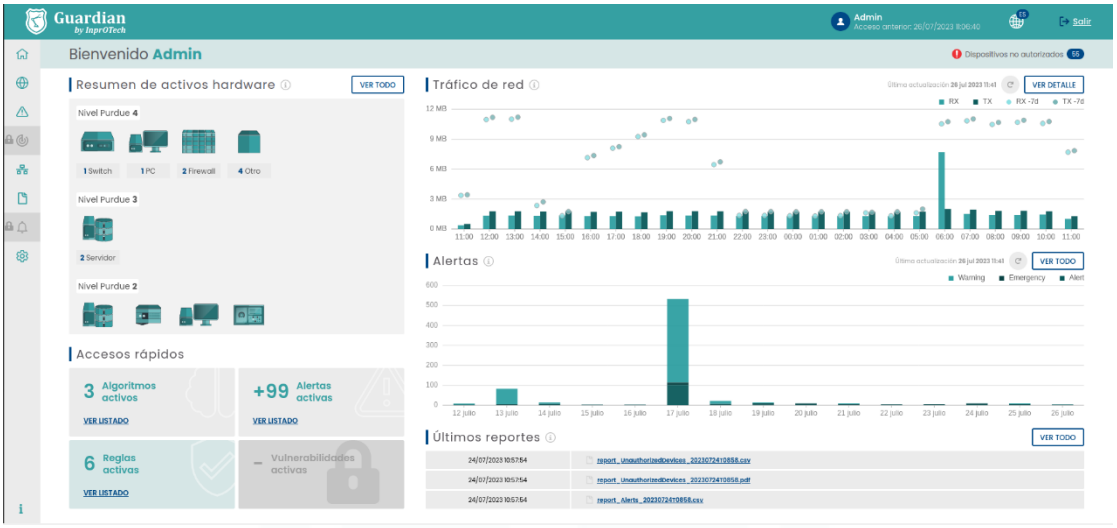
- 1: Inicio: Dashboard principal
- 2: Red: Mapa de red y lista de dispositivos
- 3: Alertas: Lista de alertas
- 4: Vulnerabilidades: Lista de vulnerabilidades (en construcción)
- 5: Sesiones de tráfico: Lista de comunicaciones entre dispositivos
- 6: Informes: Lista de informes automáticos

- 7: Notificaciones: Menú de notificaciones del servicio (en construcción)

- 8: Ajustes: Ventana de ajuste de parámetros

- 9: Documentación de ayuda

3.2 Dashboard principal



Ventana explicativa del dashboard principal

Barra superior:

Tipo de sesión y fecha del anterior acceso

Cambio de idioma de la aplicación

Salir de la sesión iniciada

Contador de dispositivos no autorizados

Widget superior izquierdo:

Número de activos de la organización clasificados por modelo Purdue

Widget superior derecho:

Representación gráfica del tráfico de red emitido y recibido en bits/seg las últimas 24 horas, y comparación con respecto a la misma magnitud justo 7 días antes

Widget inferior izquierdo:

Accesos rápidos a listados

Vulnerabilidades activas (en construcción)

Widgets inferiores derechos:

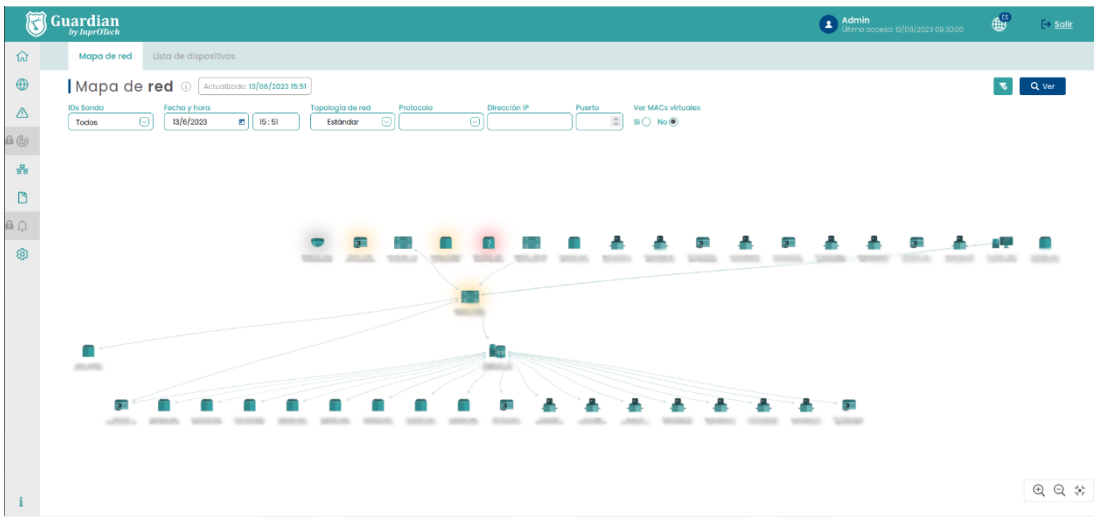
Representación gráfica de número de alertas según su severidad

Acceso a lista de reportes generados

3.3 Mapa de red

El mapa de red presenta dos vistas de topología: clásica de red, o por niveles PURDUE.

En el primer caso, tenemos lo siguiente:



Ventana de mapa de red en vista clásica

Tenemos en la parte superior la pestaña para seleccionar la visión del mapa de red, la fecha de última actualización de la representación gráfica de la topología, así como un botón para hacer efectivos los filtros introducidos

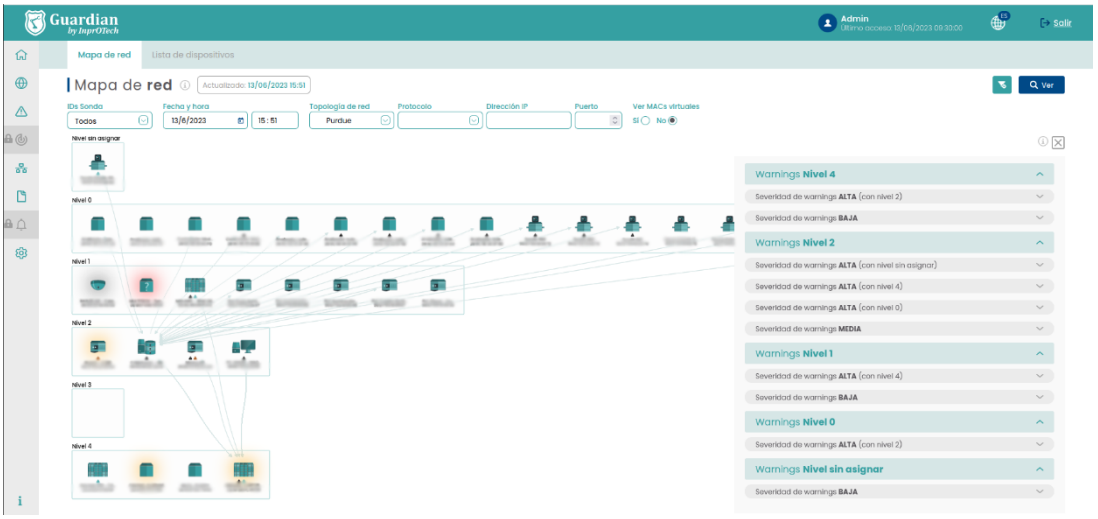
En la siguiente fila, se muestran los filtros posibles para ver por pantalla los dispositivos de nuestro interés.

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

Destacar que:

- Haciendo hover con el ratón se pueden ver las propiedades de un nodo o un enlace.
- Clicándolos, se puede ir a la vista detalle y edición de propiedades del dispositivo, o a la sección de comunicaciones filtradas para ese origen de enlace, respectivamente.

En la vista PURDUE de la topología, se analiza el cumplimiento normativo de las comunicaciones en base al estándar ISA/IEC 62443. Los warnings se califican en severidad alta (de tipo comunicaciones, señalando la existencia de las mismas entre niveles no adyacentes), severidad media (de asignación de nivel PURDUE a tipologías de dispositivo que nos parezcan cuestionables) o severidad baja (no asignación de nivel y/o recomendación de revisión manual para ciertas tipologías de dispositivo).



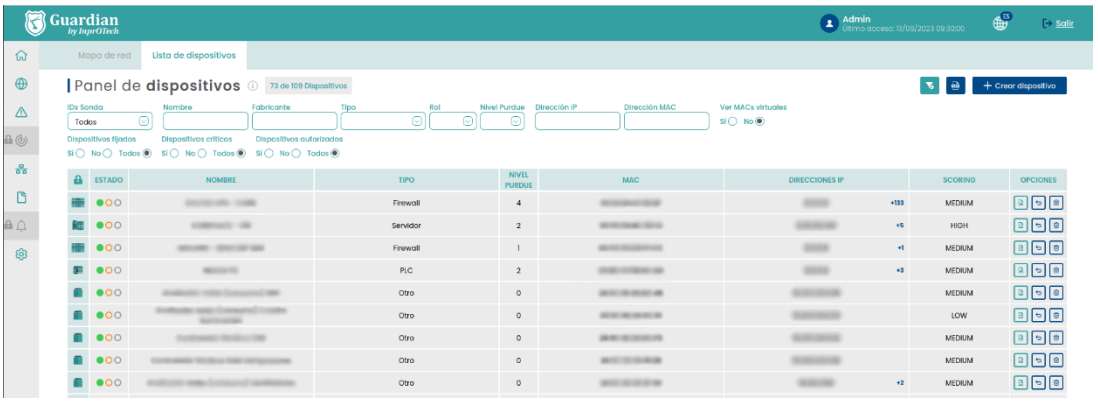
Mapa de red en vista PURDUE

Comentar que en la versión gráfica (zona izquierda de la ventana):

- Se muestran solamente las comunicaciones entre niveles diferentes, no las existentes entre dispositivos de un mismo nivel.
- Se indica con iconos triangulares bajo la imagen del dispositivo, si está afectado por algún warning de cumplimiento normativo. Los colores son negro, naranja y cerceta, y representan los warning de severidad alta, media y baja, respectivamente.
- Los dispositivos se pueden clicar para poder filtrar los warning de la parte derecha que aplican al nodo en cuestión. En caso de desmarcar el filtro, se muestran todos los detectados, por orden descendente de niveles y severidades.

El resto de las capacidades de filtrado son las mismas que en la vista clásica, y en la zona derecha de la ventana, como se mencionaba, se listan los warnings globales o asociados a un dispositivo seleccionado.

3.4 Lista de dispositivos



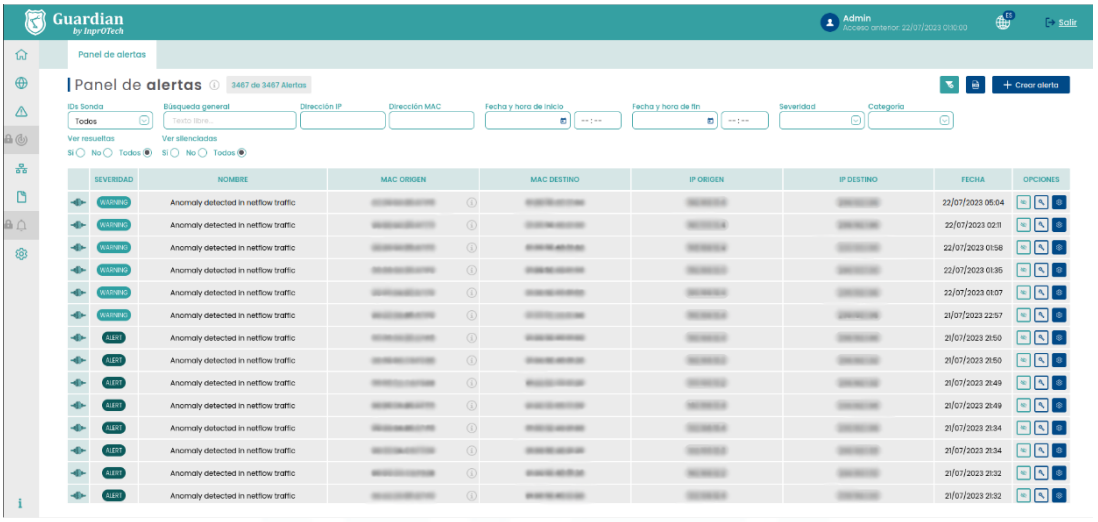
Ventana de listado de dispositivos

En la pestaña para seleccionar la vista del listado de dispositivos registrados en la red, se muestra junto al título del panel el número de dispositivos con el filtro actual aplicado frente al total de dispositivos en la base de datos. En la zona derecha, la botonera 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 quedarnos con los dispositivos de nuestro interés.

Por último, el listado en sí de los activos con información sobre ellos, y botones para realizar ciertas acciones (ver detalles, editarlos, suprimirlos, o acceder a alertas, comunicaciones o vulnerabilidades presentes, esto último en construcción). Es posible ordenar los dispositivos alfabéticamente de forma directa o inversa haciendo click en cualquiera de las columnas.

3.5 Panel de alertas



Ventana explicativa de listado de alertas

Junto al título de la sección, se muestra el número de alertas en la red de la organización (filtrado vs el total). En la parte derecha, está la botonera para eliminar los filtros establecidos, exportar la lista de alertas en formato CSV o crear manualmente una alerta en la aplicación.

En la siguiente fila, se incluyen los filtros posibles para ver por pantalla las alertas de nuestro interés. Destacar que el campo de búsqueda general es de tipo CONTIENE, y también permite efectuar búsquedas sobre el campo de notas interno de la alerta, visible en Detalles.

Por último, tenemos el listado de alertas con información asociada y botones para realizar acciones sobre las mismas (actualizaciones de estado*, acceso a detalle y adición de notas).

Como podéis ver en la imagen si un dispositivo tiene asignado un nombre, al lado de la MAC podemos ver un signo de exclamación que si ponemos el cursor encima nos mostrara el nombre asignado a esa dirección MAC.

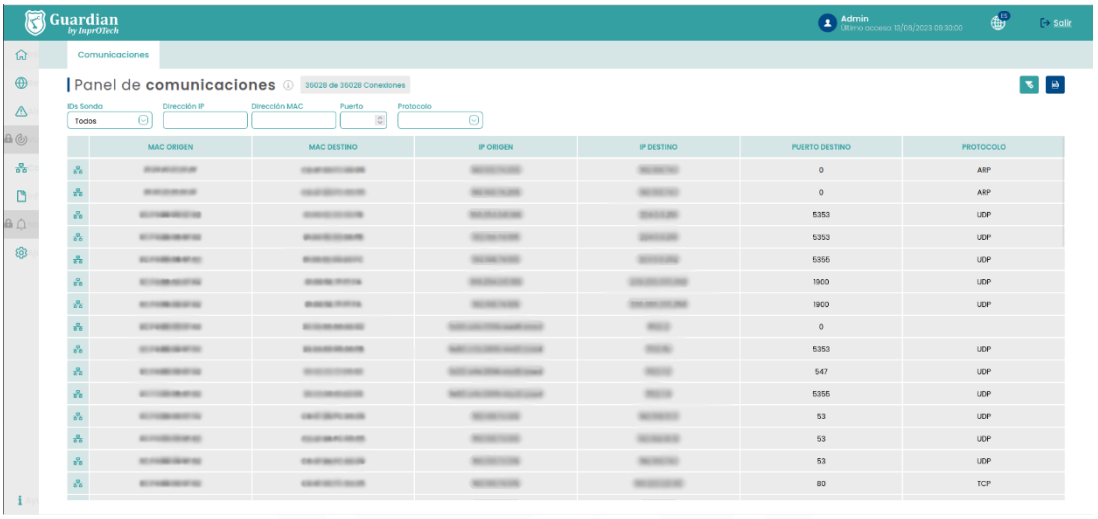
*Para consultar las opciones de cambio de estado, ver definiciones en Anexo I.

3.6 Lista de vulnerabilidades

(En construcción.

3.7 Lista de comunicaciones

Comunicaciones, entendidas como agrupación de conexiones entre MAC, IP y puerto origen, e ídem en destino. Desagregadas si hay cambio de protocolo.



Ventana de listado de comunicaciones

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

En la siguiente fila, se ubican los filtros posibles para ver por pantalla las conexiones de nuestro interés.

Por último, el listado de conexiones con información sobre ellas. Es posible ordenar las comunicaciones alfabéticamente de manera directa o inversa, haciendo click en cualquiera de las columnas.

3.8 Lista de informes

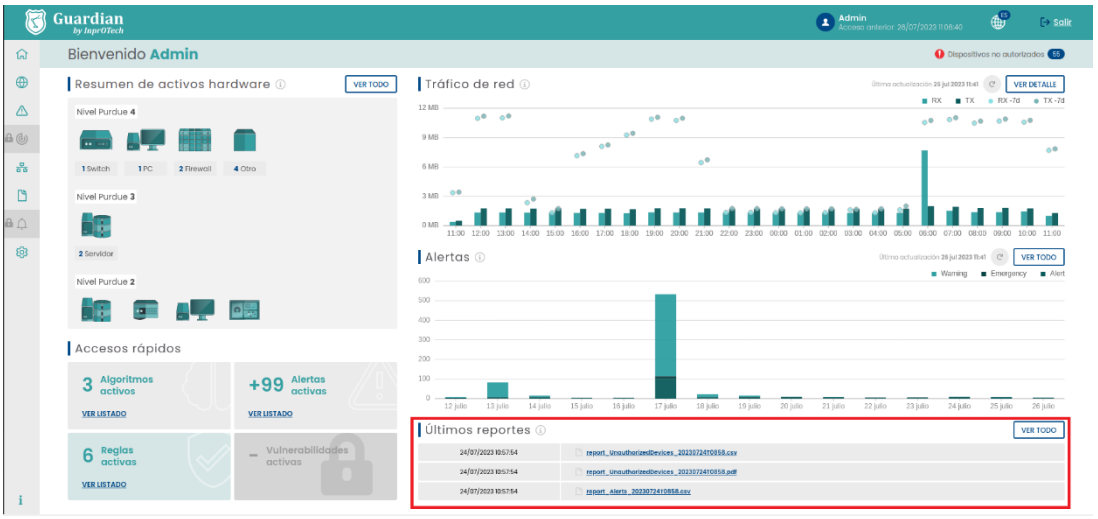
Esta sección permitirá la descarga de reportes de diferente tipología, generados automáticamente por el sistema. A día de hoy, se generan reportes semanales la madrugada de los lunes, con ficheros descargables tanto en formato PDF como CSV, con la siguiente información:

- Informe de dispositivos detectados “desconocidos”:
  - Nombre
  - MAC
  - Fabricante
  - Rol
  - Fecha de descubrimiento
- Informe de alertas detectadas:
  - Título informativo de la alerta

    - Categoría
    - Severidad
    - Silenciada
    - Resuelta
    - Valor
    - IP origen
    - MAC origen
    - IP destino
    - MAC destino
    - Protocolo
    - Fecha
- Relación MAC-IP
    - MAC
    - Fabricante
    - IP
    - Pública
    - Fecha de descubrimiento
- Lista de IPs públicas contactadas (máquinas que están expuestas a Internet):
    - IP
    - MAC
    - Fecha de descubrimiento
- Informe de puntuaciones de riesgo (scoring):
    - Nombre
    - MAC
    - Fabricante
    - Puntuación individual
    - Fecha de puntuación
    - Puntuación global de fabrica
    - Puntuación global de cloud
- KPIs:
    - Número de nuevas IPs detectadas
    - Número de intentos de intrusión
    - Porcentaje de tráfico OT e IT sobre tráfico el total
    - Dispositivos indisponibles/desactivados.
    - Número medio de alertas generadas al día
    - Número medio de alertas por dispositivo
    - Número de sesiones de tráfico.
    - Top 5 puertos usados (%)
    - Top 5 IPs (%)
    - Top 5 de protocolos (%)

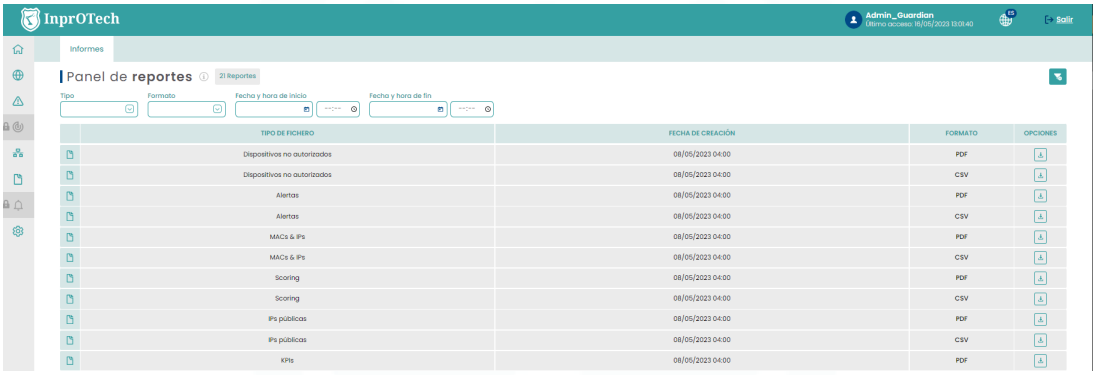
El campo MAC en el informe de alertas, en caso de que el dispositivo tenga la etiqueta Nombre informada, será sustituido por dicho valor en estos reportes. En cambio, en las descargas manuales de búsquedas del usuario desde el panel de alertas o la lista de dispositivos, ambos campos se mostrarán de manera independiente.

Los últimos informes generados, se pueden descargar desde el acceso rápido del Dashboard principal.



Últimos reportes en Dahsboard principal

Adicionalmente, Guardian tiene su propia sección dedicada a Informes, donde se podrá hacer uso del buscador, para filtrar y descargar el reporte que sea de interés:



Vista del listado de reportes

Junto al título se muestran los reportes totales generados, y a la derecha el botón de reinicio de los filtros.

En la siguiente fila, tenemos los diferentes filtros de búsqueda.

Finalmente, se encuentra el grid con los reportes disponibles en PDF y CSV para su descarga.

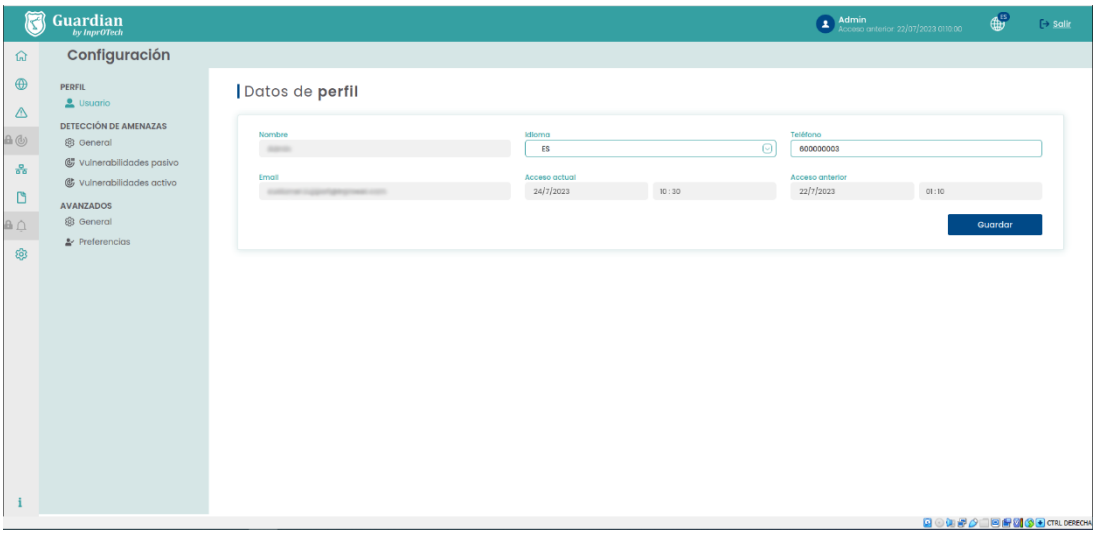
3.9 Ajustes

En este apartado podremos hacer ajustes en nuestro perfil o el servicio, modificar algunos parámetros relacionados con la detección de amenazas, o distintas configuraciones de alertas, amenazas y gestión de usuarios.

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

3.9.1 Datos de perfil

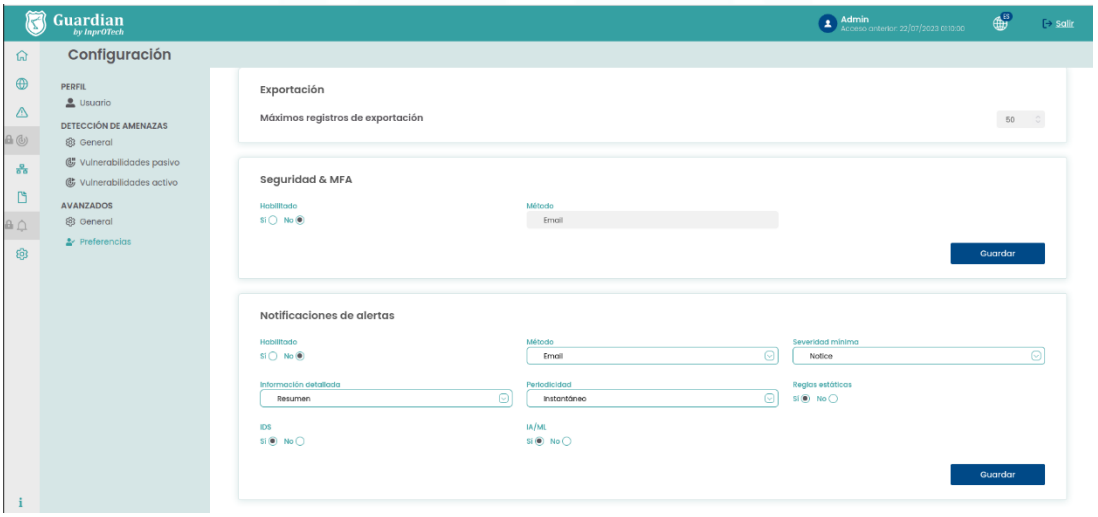
En esta sección se visualiza información básica como el nombre de usuario, email asociado, fecha y hora de la última conexión y de la conexión actual, la preferencia de idioma (EN/ES), y el teléfono de contacto. Los dos últimos son editables por el propio usuario.



Vista de datos del perfil de usuario

3.9.2 Seguridad

En el apartado 'Seguridad & MFA', podremos indicar si queremos activar o no el segundo factor de autenticación como mecanismo de seguridad (recomendado) adicional para evitar suplantaciones de identidad. En ese caso, tras la identificación con usuario y contraseña, se nos invitará a introducir un token de un solo uso que habremos recibido (inicialmente, por email).



Vista de datos de sección Seguridad & MFA

Recordar a su vez, que como método de control de acceso se ha implantado un mecanismo basado en roles, mediante el cual hay grupos de permisos asociados a tres niveles de usuario:

- Administrador InprOTech
- Administrador de planta
- Operador de planta

La asignación de roles a usuarios no puede ser gestionado directamente por su organización, sino que se define con InprOTech en tiempo de despliegue de la solución. Contacte con nosotros para más información.

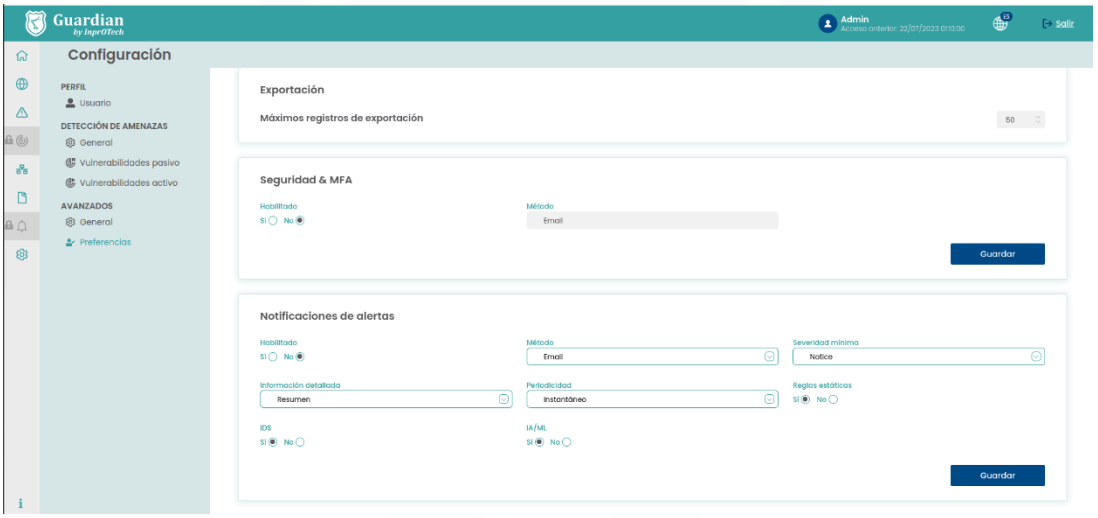
3.9.3 Notificaciones

En caso de que se considere adecuado, se pueden configurar avisos proactivos de generación de alertas en el sistema. Las alertas y avisos, se generan en base a la detección de anomalías según las diferentes estrategias implementadas en Guardian (heurísticos, IA/ML, IDS, manuales…).

Esto permite que Guardian avise de potenciales incidentes, en lugar de tener que estar acudiendo periódicamente a la interfaz web a revisar si se han generado eventos.

El usuario por tanto podrá:

- Decidir si quiere recibir notificaciones de alertas de seguridad
- En caso afirmativo, a partir de qué umbral de severidad se le enviarán
- De qué tipología de alertas (heurísticos, IA/ML, IDS, todas…)
- Con qué formato
    - Individuales: una notificación por alerta
    - Agregadas: una notificación diaria con el resumen de todas las alertas, pudiendo seleccionar de lunes a viernes, o de lunes a domingo
- En caso de haber seleccionado individuales, si desea un formato resumido o verboso



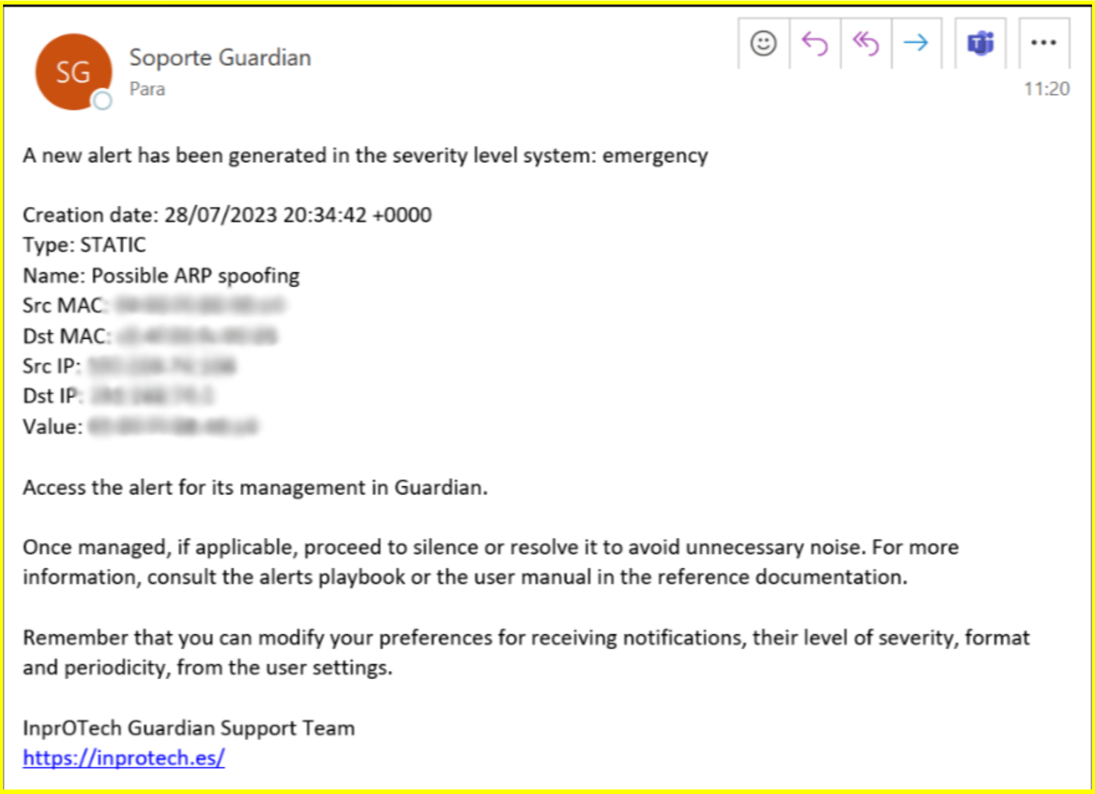
Vista de datos de sección Notificaciones de alertas

Por el momento, las notificaciones se enviarán vía email a la cuenta del usuario.

Importante:

- La notificación de alertas debe estar activada en el backend para permitir al usuario habilitar los envíos proactivos.
- En caso de que con las condiciones establecidas se generen demasiados avisos por unidad de tiempo, la funcionalidad se autodesactivará por seguridad (informado vía email previamente al usuario sobre esta circunstancia), para que puedan seleccionarse otras condiciones de envío más exigentes (de inferior volumen de eventos).

A continuación, se muestran un par de ejemplos de notificaciones de alertas con diferente formato:



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: [illegible]
Dst MAC: [illegible]
Src IP: [illegible]
Dst IP: [illegible]
Value: [illegible]

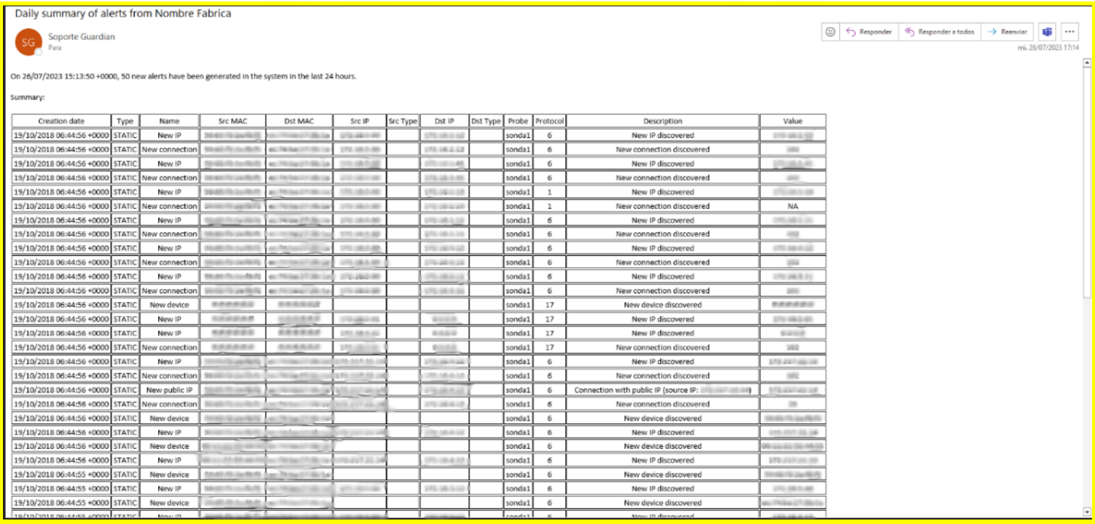
Access the alert for its management in Guardian.

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/

Formato de alerta individual resumida



Daily summary of alerts from Nombre Fabrica

Soporte Guardian
Para

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

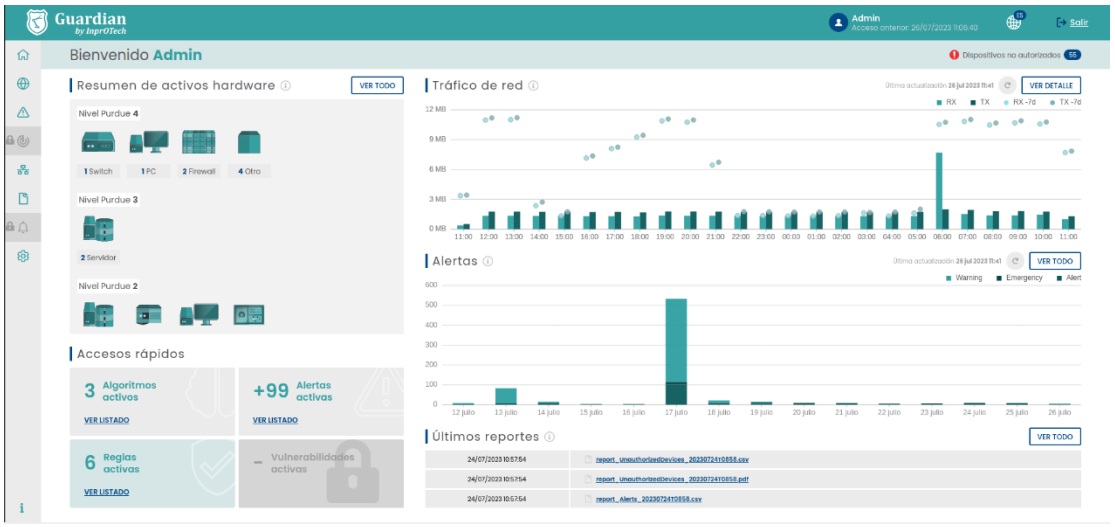
Summary:

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	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New IP discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New connection	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New connection discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New IP	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New IP discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New connection	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New connection discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New IP	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	1	New IP discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New connection	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	1	New connection discovered	NA
19/10/2018 06:44:56 +0000	STATIC	New IP	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New IP discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New connection	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New connection discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New IP	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New IP discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New connection	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New connection discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New IP	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New IP discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New connection	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New connection discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New device	[illegible]	[illegible]					sonda1	17	New device discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New IP	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	17	New IP discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New IP	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	17	New IP discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New connection	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	17	New connection discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New IP	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New IP discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New connection	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New connection discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New public IP	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	Connection with public IP (source IP: [illegible])	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New connection	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New connection discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New device	[illegible]	[illegible]					sonda1	6	New device discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New IP	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New IP discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New device	[illegible]	[illegible]					sonda1	6	New device discovered	[illegible]
19/10/2018 06:44:56 +0000	STATIC	New IP	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New IP discovered	[illegible]
19/10/2018 06:44:55 +0000	STATIC	New device	[illegible]	[illegible]					sonda1	6	New device discovered	[illegible]
19/10/2018 06:44:55 +0000	STATIC	New IP	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New IP discovered	[illegible]
19/10/2018 06:44:55 +0000	STATIC	New device	[illegible]	[illegible]					sonda1	6	New device discovered	[illegible]
19/10/2018 06:44:55 +0000	STATIC	New IP	[illegible]	[illegible]	[illegible]		[illegible]		sonda1	6	New IP discovered	[illegible]

Formato de resumen diario de alertas

3.10 Ayuda

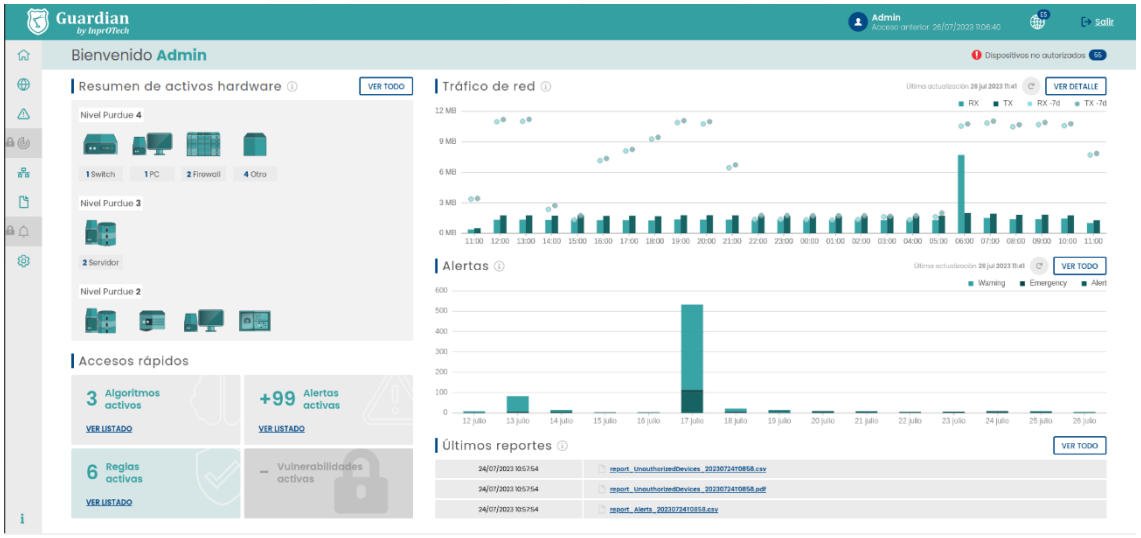
Sección que habilita la descarga de la última versión en vigor del manual de usuario de InprOTech Guardian. Conduce a la web de InprOTech, donde se cuelga la documentación relevante.



El acceso a la documentación se encuentra en la esquina inferior izquierda. Para cualquier problema técnico, contactar con customer.support@inprosec.com.

4 Manejo de aplicación web

4.1 Dashboard principal



Dashboard principal

4.1.1 Resumen de activos

Resumen de activos

El usuario podrá visualizar el número de dispositivos conectados a la red, diferenciados por su tipo (PLCs, RTU, Switch, Router, Robot, PC, SCADA, DCS, HMI, Firewall, variador de frecuencia, Tarjetas controladoras, sensores, Cámaras de V.A., tablets, Teléfonos, otros equipos), y clasificados según el modelo de Purdue tal y como indica el Anexo II (siempre que se haya informado tal y como se indica en la sección 4.4).

4.1.2 Accesos rápidos

Accesos rápidos

4.1.2.1 Algoritmos Activos

Al pulsar sobre el link "VER LISTADO", el usuario podrá visualizar el listado con los algoritmos de inteligencia artificial que están activos para la detección de amenazas dentro de la red de la organización (Apartado que se verá posteriormente en el presente manual).

4.1.2.2 Alertas Activas

Al pulsar sobre el link "VER LISTADO", el usuario podrá visualizar un listado con las alertas activas totales.

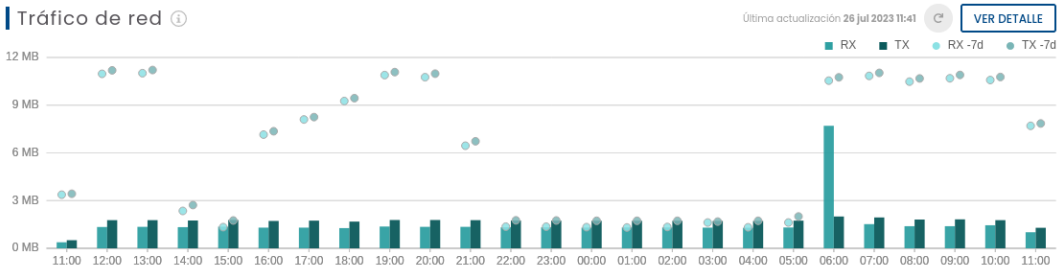
4.1.2.3 Reglas Activas

Al pulsar sobre el link "VER LISTADO", el usuario podrá visualizar el listado con las reglas fijas que están activas para la detección de amenazas dentro de la red de la organización (Apartado que se verá posteriormente en el presente manual).

4.1.2.4 Vulnerabilidades Activas

Al pulsar sobre el link "VER LISTADO", el usuario podrá visualizar un listado con las vulnerabilidades activas totales no gestionadas (en construcción).

4.1.3 Gráfico de tráfico de red

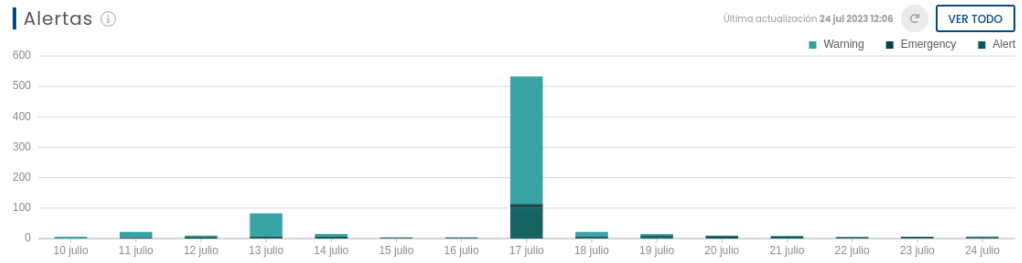


Tráfico de red

El usuario podrá visualizar gráficamente el tráfico generado (en bit/s, o múltiplo de dicha unidad) en las últimas 24 horas, tanto emitido (naranja) como recibido (verde). También contará con un refresco automático en ese intervalo de tiempo y con un botón para un refresco de forma manual por el operario. Los puntos circulares dispuestos en cada una de las barras indicarán el tráfico ocurrido 7 días antes, a modo de comparativa.

Al pulsar sobre el botón "VER DETALLE" el usuario visualizará por pantalla la ventana de sesiones de red del aplicativo InprOTech Guardian (Apartado que se verá posteriormente en el presente manual).

4.1.4 Gráfico de alertas



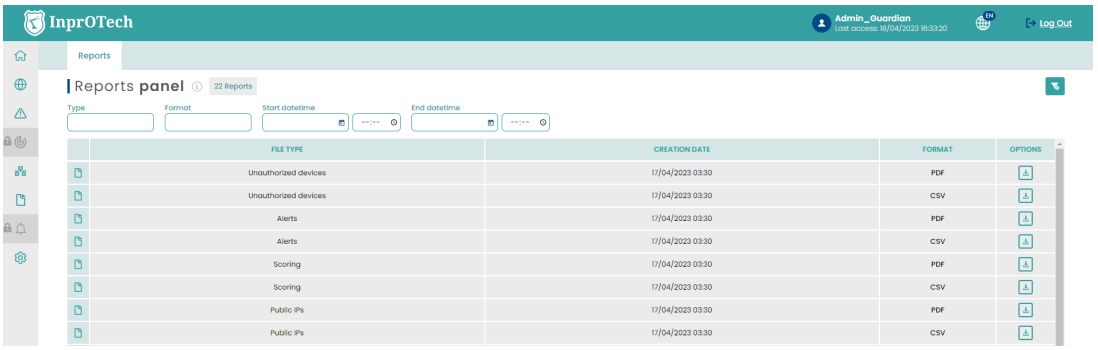
Alertas

El usuario tendrá una representación gráfica del número de alertas diferenciadas, según su nivel de severidad (Ver anexo I) y colores, por día de los últimos cinco días, y la tendencia que han seguido éstas. También contará con un refresco automático en ese intervalo de tiempo y con un botón para un refresco de forma manual por el operario.

Si el usuario sitúa el cursor sobre la barra gráfica de uno de los días, podrá visualizar el número exacto de alertas y emergencias captadas hasta el momento.

Al pulsar sobre el botón “VER TODO” el usuario visualizará por pantalla la ventana de alertas del aplicativo InprOTech Guardian (Apartado que se verá posteriormente en el presente manual).

4.1.5 Últimos reportes



Acceso a últimos reportes disponibles

Al pulsar en el botón “VER TODO”, el usuario podrá visualizar un listado con los últimos reportes generados de forma automática o a petición del cliente.

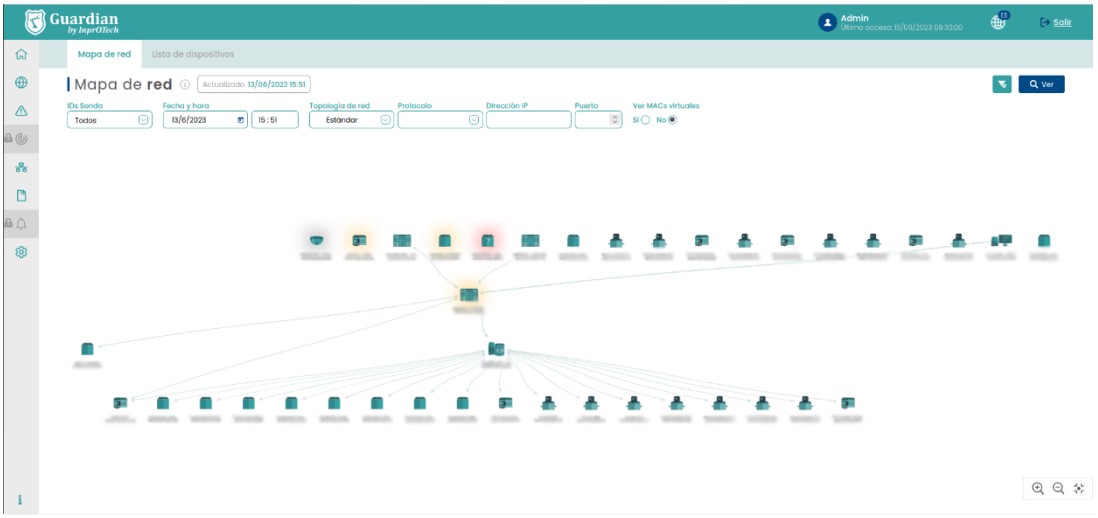
Actualmente, los reportes generados con periodicidad semanal, son:

- Listado de últimas alertas detectadas
- Listado de dispositivos no autorizados conectados a la red
- Relación MAC-IP vistas en la red
- Puntuaciones de scoring de la red
- Informe de indicadores técnicos de servicio (KPIs)

4.2 Mapa de red y lista de dispositivos

4.2.1 Mapa de red

Para acceder al mapa de red, el usuario deberá pulsar sobre el icono  que aparece en la parte izquierda de la pantalla y seleccionar la pestaña de “Mapa de red”.



Ventana de mapa de red

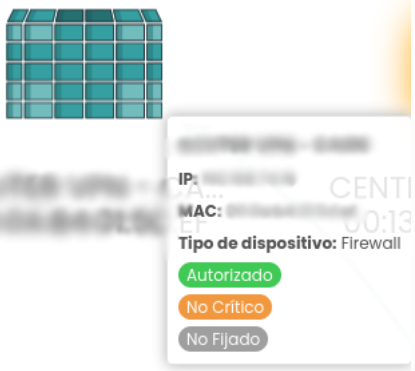
En la pestaña de mapa de red el usuario podrá visualizar todos los dispositivos conectados a la red en tiempo real, así como los enlaces para la comunicación existentes entre ellos. Cada dispositivo vendrá referenciado con una imagen representativa y una serie de propiedades como su dirección MAC o nombre en caso de haber sido informado manualmente. El mapa de red dará a conocer la topología implantada.

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

Aquellos dispositivos no autorizados se visualizarán en el mapa de red sombreados con un fondo de color rojo. Los fijados y críticos, también tendrán su halo correspondiente (ver anexo I para definiciones).

Dispositivo no autorizado

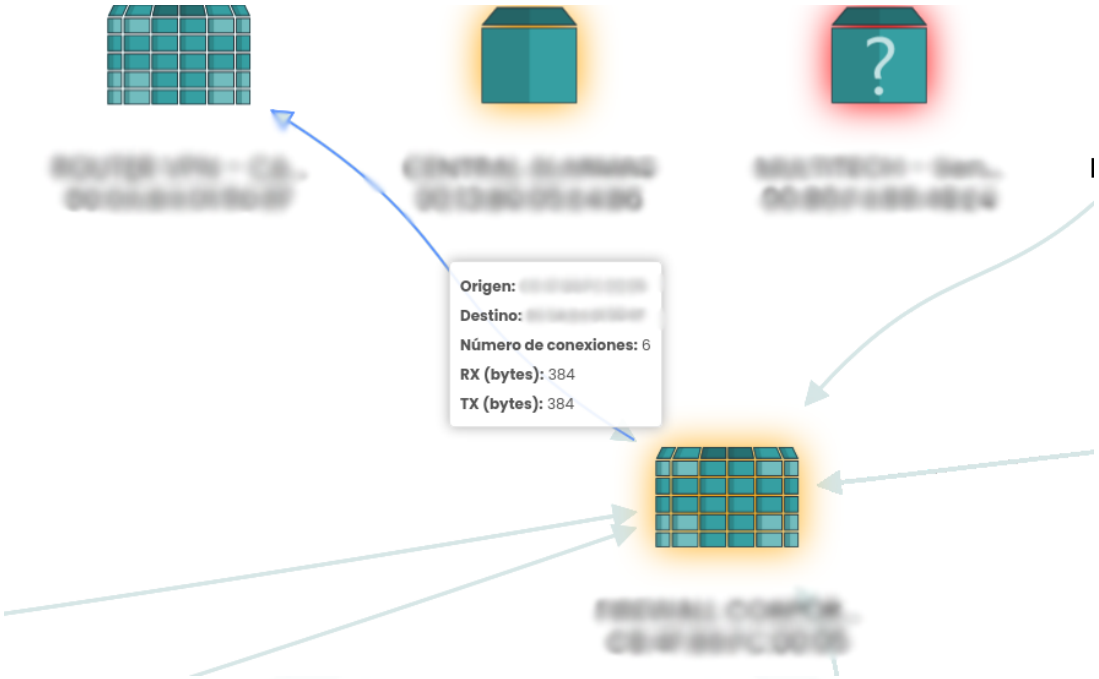
Si situamos el cursor sobre un dispositivo, obtendremos una ventana emergente en donde nos aparecerá la información básica del dispositivo.



Información básica de dispositivo

Si pulsamos sobre el dispositivo se nos mostrará la ventana con toda la información del dispositivo.

Si situamos el cursor sobre uno de los enlaces se nos mostrará una ventana emergente con la información básica de esa comunicación.



Información básica de enlace

Si pulsamos sobre el enlace se nos mostrará la ventana con toda la información de la conexión.

El mapa de red se puede simplificar para visualizar únicamente los dispositivos de nuestro interés mediante el uso de los distintos filtros y, aceptando ese filtrado mediante la pulsación del botón “Consultar”

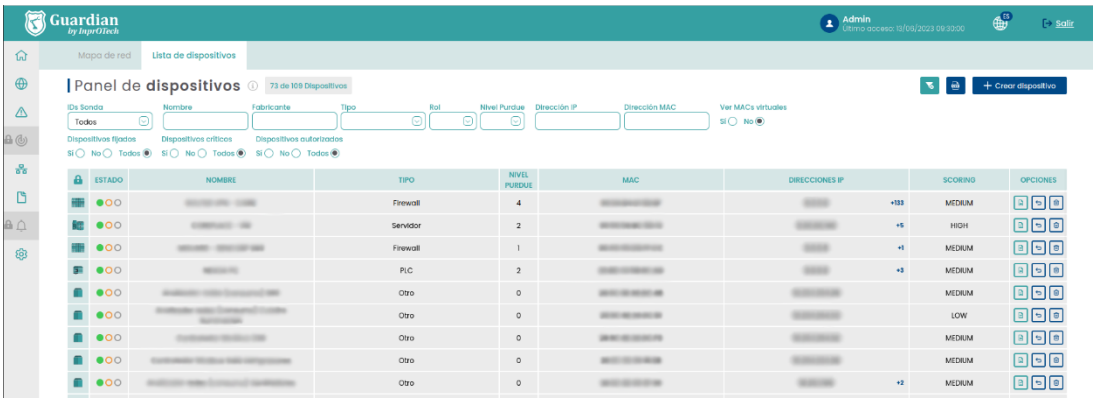
Filtros disponibles en mapa de red

Los filtros se pueden aplicar según:

- Fecha y hora: Espacio de tiempo que se quiere visualizar por pantalla.
- Topología de la red: Modelo de muestreo de la red de la organización por pantalla.
- Protocolo: Muestreo por pantalla de únicamente conexiones que utilizan el protocolo seleccionado.
- Dirección IP: Muestreo únicamente de dispositivo y conexiones con la IP seleccionada.
- Puerto: Muestreo por pantalla de conexiones al puerto seleccionado.
- Visión o no de MACs virtuales (multicast/broadcast), calculadas automáticamente por el sistema

4.2.2 Lista de dispositivos

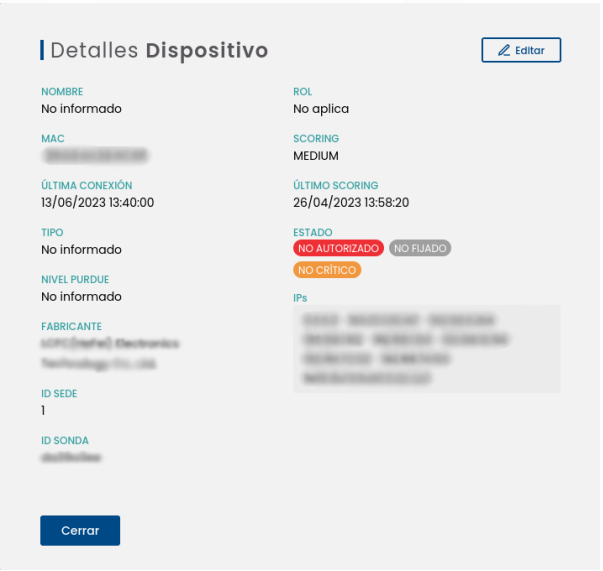
Para acceder a la lista de dispositivos, el usuario deberá pulsar sobre el icono  que aparece en la parte izquierda de la pantalla y seleccionar la pestaña de “Lista de dispositivos”.



Ventana de lista de dispositivos

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

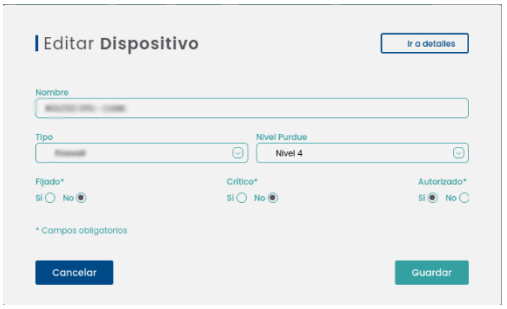
- ESTADO
  - El primero de los círculos indicará si el dispositivo está autorizado (color verde) o no autorizado (color rojo).
  - El segundo de los círculos indicará si el dispositivo es crítico (color naranja con relleno) o no crítico (color naranja sin relleno).
  - El tercero de los círculos indicará si el dispositivo se encuentra fijado (color gris con relleno) o no fijado (color gris sin relleno).
- NOMBRE: Nombre que se le ha asignado a cada dispositivo.
- TIPO: Diferenciación del tipo de dispositivo (PLC, RTU, SCADA, etc..).
- NIVEL PURDUE: Nivel de clasificación según el modelo de Purdue.
- MAC: Dirección MAC asignada del dispositivo.
- DIRECCIONES IP: Dirección IP asignada del dispositivo.
- ACCIONES:
  -  : Botón para ver en detalle la información del dispositivo.



Ventana de información ampliada de dispositivo

- o 

: Botón para modificar parámetros del dispositivo.



Ventana de parámetros de dispositivo

- o 
: Botón para realizar otras acciones en el dispositivo, como acceso con vista prefiltrada a la lista de alertas, vulnerabilidades (en desarrollo), así como eliminación del nodo.

Existe la posibilidad de realizar un filtrado para que la pantalla muestre únicamente los dispositivos de nuestro interés.

Filtros disponibles en listado de dispositivos

Éste filtrado se puede realizar según:

- ID de sonda, para filtrar por zona de la red industrial y/o sede
- Nombre de dispositivo
- Fabricante del dispositivo
- Tipo de dispositivo (PLC, RTU, SCADA, FIREWALL, etc.)
- Rol del dispositivo (Emisor, receptor o ambos)
- Nivel de Purdue, según anexo II
- Dirección IP del dispositivo
- Dirección MAC del dispositivo
- Visión de MACs virtuales reservadas de broadcast
- Dispositivos fijados, ver anexo I
- Dispositivos críticos, ver anexo I
- Dispositivos autorizados, ver anexo I

Al pulsar el botón  se realizará un reinicio de los valores de filtrado y se mostrará nuevamente la lista completa con todos los dispositivos.

Mediante el botón  se realizará una exportación de un archivo en formato CSV del listado de dispositivos con su información.

Es posible añadir manualmente un dispositivo nuevo a la red de la organización y listado, mediante el botón 

.

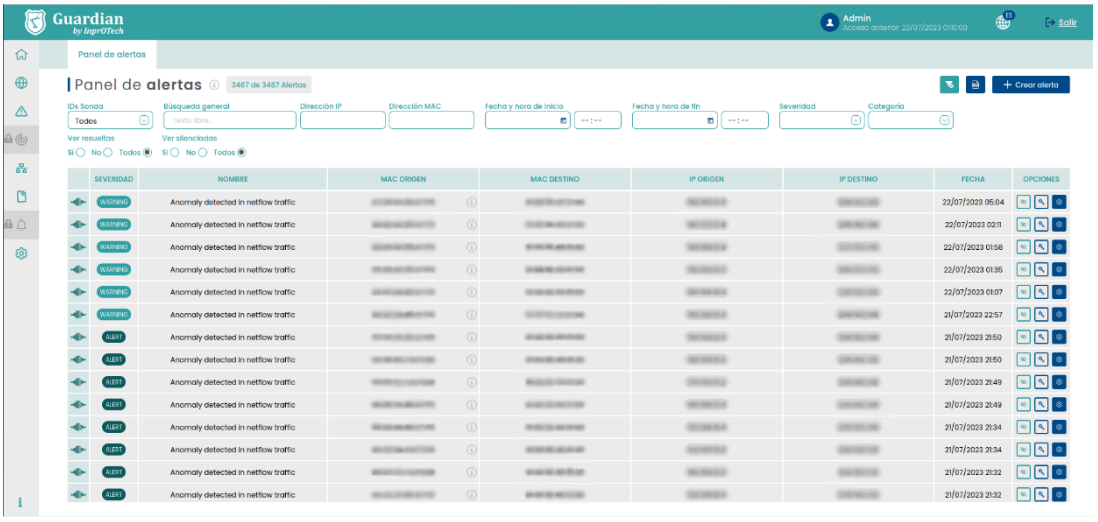
Aparecerá la siguiente ventana emergente:

Filtros disponibles en listado de dispositivos

Se ha de introducir manualmente la información solicitada sobre el dispositivo a añadir y para hacer efectiva esa creación se ha de pulsar en el botón de “Guardar”.

4.3 Panel de alertas

Para acceder al listado de alertas, el usuario deberá pulsar sobre el icono  que aparece en la parte izquierda de la pantalla.

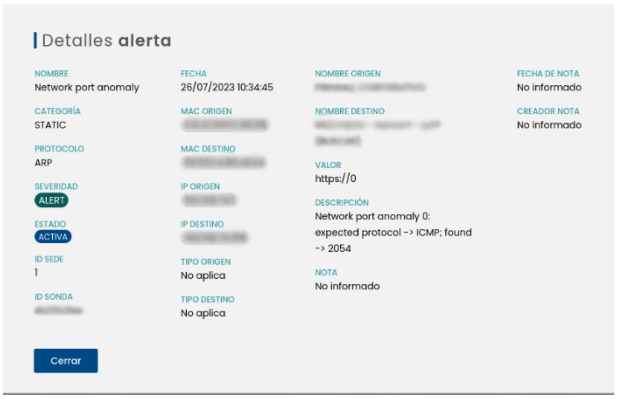


Ventana de listado de alertas

Se mostrará un listado con todas las alertas presentes en la organización e información acerca de ellas.

- Severidad: Clasificación de la alerta en función del impacto que podría tener sobre la organización.
- Nombre: Nombre definido de la alerta.
- MAC de origen: MAC de dispositivo generador de la alerta.
- MAC de destino: MAC de dispositivo al que iba dirigida la acción.
- IP de origen: IP de dispositivo generador de la alerta.
- IP de destino: IP de dispositivo al que iba dirigida la acción.
- Fecha: Fecha y hora de aparición de la alerta.
- Acciones (ver anexo I para definiciones):

-  : Si ponemos el cursor encima podremos saber el nombre del dispositivo asignado a esa dirección MAC.
-  : Botón para cambiar el estado de alerta a silenciada o no silenciada (ver sección 6.2 en Anexo I).
-  : Botón para modificar el estado de la alerta (resuelta o no resuelta), según lógica indicada en anexo I.
-  : Botón para realizar más acciones sobre la alerta, como ver los detalles o añadir notas.



Ventana de información ampliada de alerta

Existe la posibilidad de realizar un filtrado para que la pantalla muestre únicamente las alarmas de nuestro interés.

Filtros disponibles en listado de alertas

Este filtrado se puede realizar según:

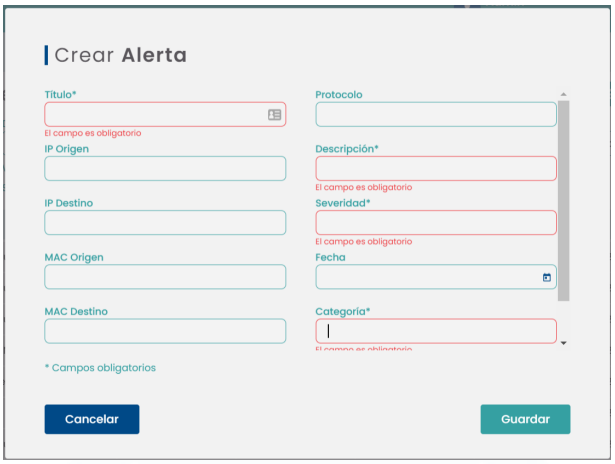
- ID de sonda, para filtrar por zona de la red industrial y/o sede
- Búsqueda general: Búsqueda a través de la introducción de un texto que contenga la alarma (incluso en sus notas)
- Dirección IP del dispositivo
- Dirección MAC del dispositivo
- Fecha y hora de inicio de búsqueda de alertas
- Fecha y hora de fin de búsqueda de alertas
- Severidad, según anexo I
- Alarmas resueltas o no resueltas, según anexo I
- Alarmas silenciadas o no silenciadas, según anexo I

Al pulsar el botón  se realizará un reinicio de los valores de filtrado y se mostrará nuevamente la lista completa con todas las alarmas.

Mediante el botón  se realizará una exportación de un archivo en formato CSV del listado de alarmas con su información.

Es posible crear manualmente una alarma especifica en la red de la organización, mediante el botón + CREAR ALERTA .

Aparecerá la siguiente ventana emergente:



Ventana de creación de alertas

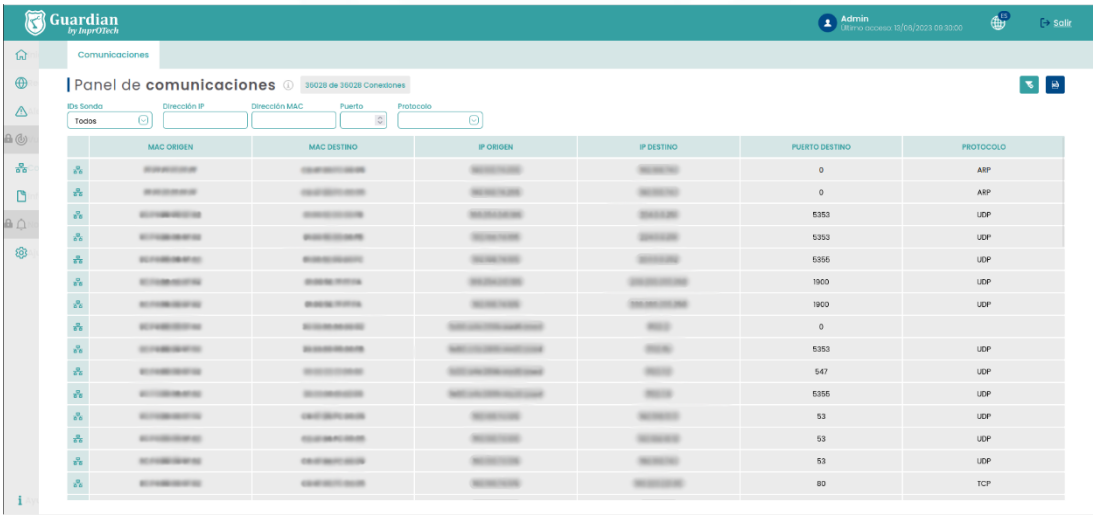
Se ha de introducir manualmente la información solicitada sobre la nueva alarma creada y para hacer efectiva esa creación se ha de pulsar en el botón de "Guardar".

4.4 Vulnerabilidades

Para acceder al listado de vulnerabilidades, el usuario deberá pulsar sobre el icono que aparece en la parte izquierda de la pantalla. En construcción.

4.5 Comunicaciones

Para acceder al listado de comunicaciones, el usuario deberá pulsar sobre el icono que aparece en la parte izquierda de la pantalla.



Ventana de listado de comunicaciones

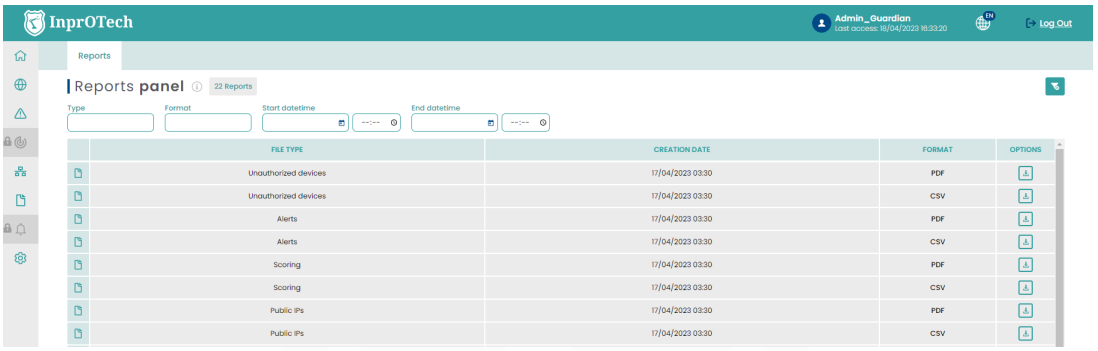
Se mostrará un listado con todas las comunicaciones que se han realizado entre los dispositivos OT de la red de la organización, e información acerca de ellas.

Se entiende por comunicación la agrupación de conexiones entre MAC, IP y puerto origen, e ídem en destino. Se considera nueva comunicación si hay cambio de protocolo.

Filtros disponibles en listado de comunicaciones

4.6 Informes

Para acceder al listado de informes, el usuario deberá pulsar sobre el icono que aparece en la parte izquierda de la pantalla.



Acceso a últimos reportes disponibles

Se mostrará por pantalla un listado con los reportes generados tanto de forma manual como de forma automática con una periodicidad determinada, disponibles para su descarga.

4.7 Ajustes

Ver sección homónima en el apartado Guía rápida.

5 ANEXO I: Clasificación de dispositivos y alarmas

5.1 Clasificación de dispositivos

5.1.1 Según su estado

- **Autorizado/No autorizado**: Los dispositivos autorizados, son aquellos que explícitamente el cliente ha reconocido como legítimos.
- **Crítico/No crítico**: El sistema Guardian no va a interactuar activamente con aquellos dispositivos marcados como críticos. P.ej. dispositivos muy antiguos, sin personal para su mantenimiento, sin repuestos, etc.

- **Fijado/No fijado**: Los dispositivos fijados aparecerán en el aplicativo de Guardian aunque éstos no hayan establecido ninguna comunicación en la red de la organización. P.ej. dispositivos aislados de la red temporalmente para su mantenimiento.

5.2 Clasificación de alarmas

5.2.1 Según su estado

- **Resueltas/No resueltas**: Las alarmas marcadas como resueltas son aquellas que han sido tratadas, pero se quiere mantener la aparición de la alarma en futuras situaciones idénticas (misma tipología, MACs, IPs y puertos involucrados). Las no resueltas, están pendientes de gestión.
- **Silenciadas/No silenciadas:** Las alarmas declaradas como silenciadas no volverán a surgir en el mismo contexto de red*. P.ej. un dispositivo que se comunica con una IP pública conocida y controlada por la organización, y no se desea que se generen alarmas para esta situación.
  * Cabe mencionar que las alarmas silenciadas, a pesar de no mostrarse al usuario, se almacenan igualmente en base de datos para consulta posterior por el personal de InprOTech a petición del cliente, si fuese necesario.

5.2.2 Según su severidad

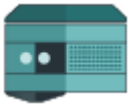
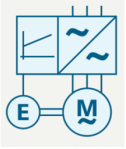
Los niveles de severidad del aplicativo en cuanto a la generación de alertas se toman del RFC 5424, aunque no son equivalentes, dado que la gravedad de los eventos se ha catalogado en base a la experiencia de nuestros técnicos.

De mayor a menor gravedad, las alertas se clasifican en:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debug

6 ANEXO II: Iconos representativos de dispositivos

Icono	Descripción	Nivel PURDUE
	PC	2
	SCADA	2
	DCS	2
	Virtual	2
	HMI	2
	TABLET	2
	TELÉFONO VOIP	2
	SERVIDOR	2
	TELÉFONO MÓVIL	2

	RTU	1
	CÁMARA V.A.	1
	LECTOR CODIGO BARRAS	1
	PLC	1
	ROBOT	0
	VARIADOR DE FRECUENCIA	0
	TARJETA CONTROLADORA	0
	SENSOR	0
	AFD	0
	SWITCH	Según ubicación
	ROUTER	Según ubicación

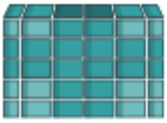
	FIREWALL	Según ubicación
	OTHER	Según ubicación

Tabla 1: Iconos representativos de dispositivos

7 ANEXO III: Iconos representativos de tipos de alertas

Icono	Descripción
	Alerta manual
	Alerta algoritmo de Machine Learning
	Alerta en base a regla estática
	Alerta del IDS (sistema de detección de intrusiones)