InprOTech

Smart security for your industry

Manual de usuario

InprOTech Guardian

Fecha: 12/2024

Referencia documento: IN-Manual de usuario InprOTech Guardian

Versión: 0.15

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, ya sea por cable o inalámbricos, 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. El usuario, además, podrá definir campos personalizables para clasificar y filtrar los dispositivos de la red, teniendo a su disposición un inventario virtual de los campos que ha creado y que podrá organizar, filtrar y exportar.
- **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.

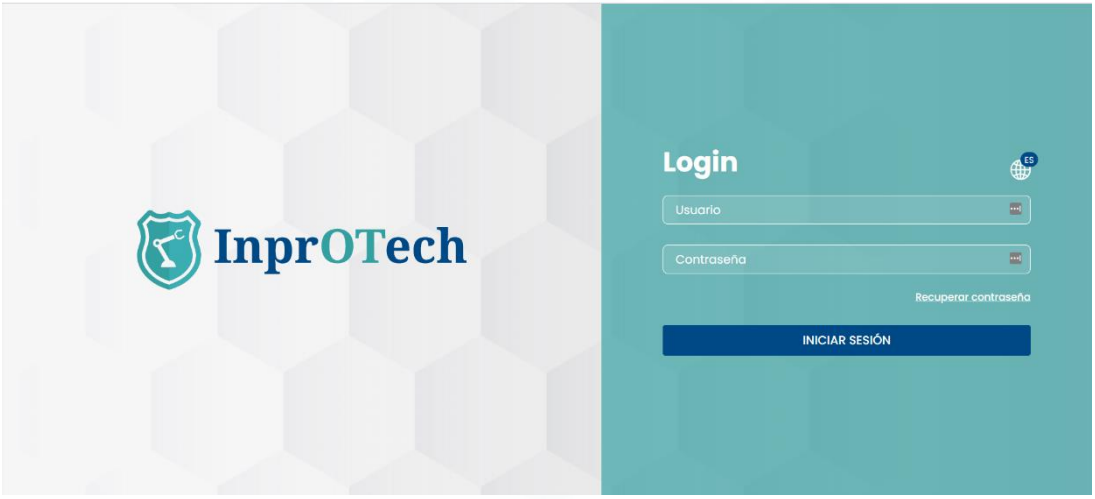
- **Gestor de vulnerabilidades**: Posibilidad de realizar escáneres de vulnerabilidades bajo petición del cliente y únicamente a los dispositivos seleccionados (en desarrollo).
- **Lista de comunicaciones:** Listado con todas las comunicaciones que se han realizado entre los dispositivos OT de la red 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

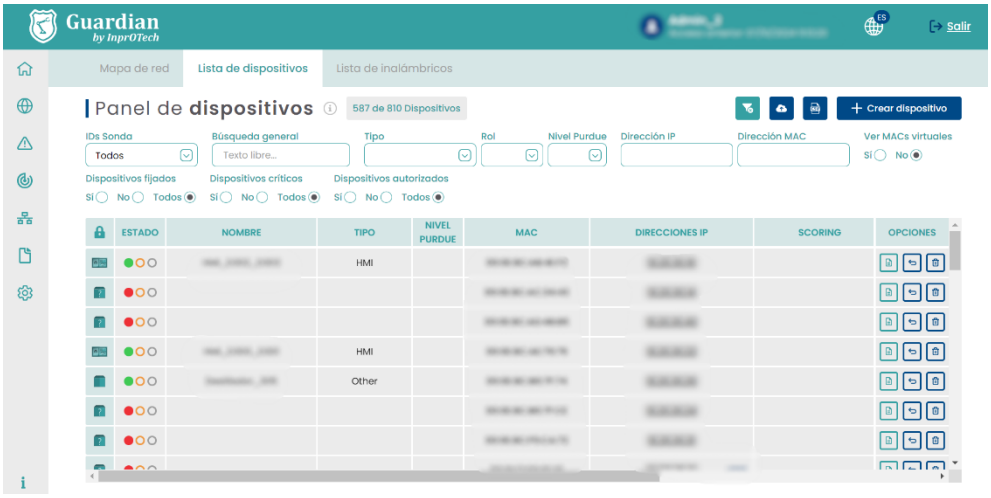
Al Introducir el correo electrónico, en caso de ser válido, se le enviará un enlace a dicho correo para poder restablecer la contraseña de acceso mediante un token de un solo uso.

**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

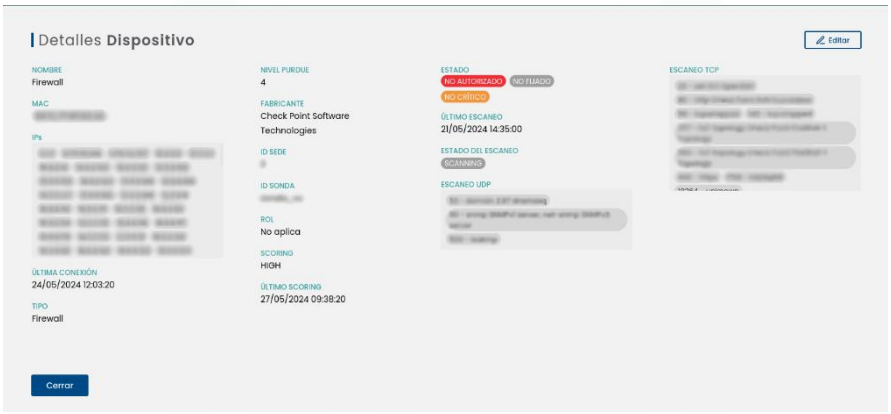
Se ha de organizar el listado de dispositivos mediante la declaración del nombre de cada dispositivo, así como, su nivel PURDUE y su estado (Ver Anexo I). Mediante esta declaración, el usuario contará con una mayor facilidad para la identificación de cada dispositivo en las distintas ventanas de la aplicación,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



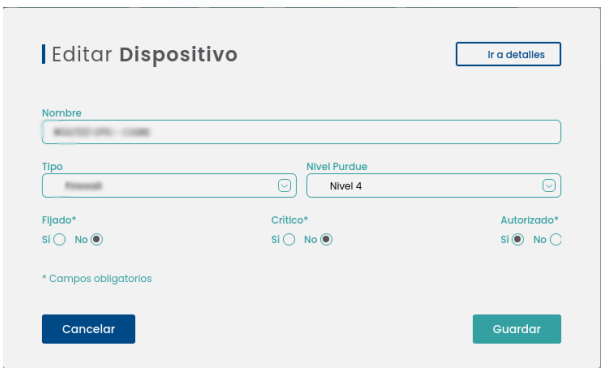
Pantalla de listado de dispositivos

Para poder modificar un dispositivo, tendremos que pulsar sobre el botón  y se abrirá la siguiente pestaña.



Desplegable de detalles de dispositivo

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

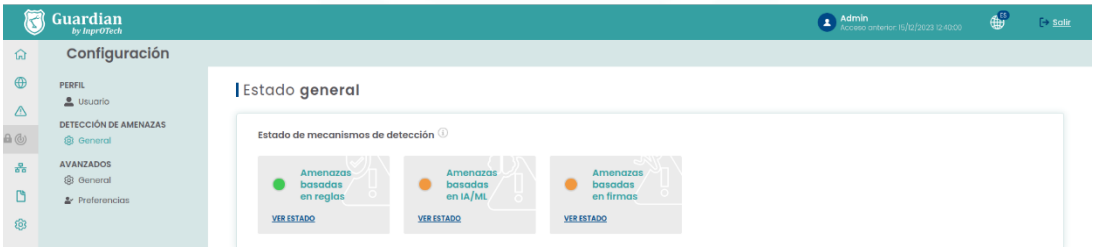
El sistema Guardian realiza la detección de amenazas en base a múltiples criterios basados en comportamiento, como son:

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

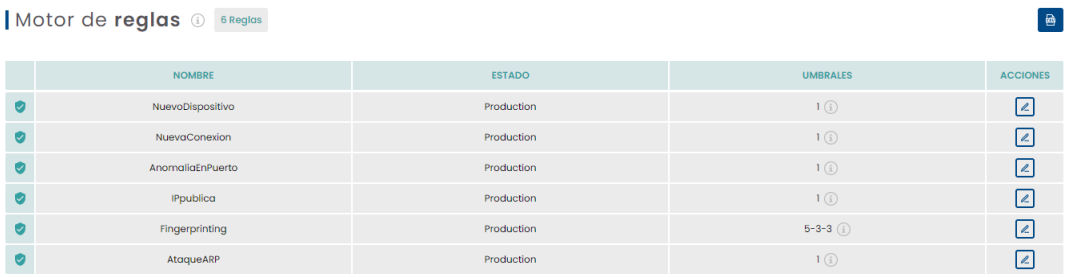
El usuario deberá configurar qué reglas desea que sean operativas para el análisis de la red de su organización, así como los rangos de tiempos para obviar cada una de las alarmas si lo considera oportuno. Esto se haría de mutuo acuerdo con InprOTech en el onboarding; a priori el usuario sólo verá las 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.



Pantalla de estados mecanismos de detección



Pantalla motor de reglas

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

UMBRALES	ACCIONES
1	
1	
1	
1	
5-3-3	
1	

Pantalla de umbrales

En la columna de acciones podremos editar estos parámetros.

Pantalla de edición de regla

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

La configuración básica de los datos del perfil de usuario, la configuración de seguridad y las preferencias de notificación de alertas se encuentran en la sección Configuración de la Guía rápida. Se recomienda revisarlos y adaptarlos a las necesidades del entorno.

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.

2.8 Escáner activo de dispositivos (opcional)

Si el cliente lo requiere, puede contactar con su Soporte de Guardian para habilitar el motor de consultas activas a los dispositivos, para obtener propiedades adicionales de los nodos (versión de firmware, puestos abiertos y servicios en ejecución en los mismos, entre otros).

Consulte la sección Escáner de Dispositivos dentro de Manejo de aplicación web para más detalle.

2.9 Análisis de dispositivos inalámbricos (opcional)

Si se desea, y las sondas recolectoras de tráfico tienen el hardware adecuado para ello, puede contactar con su Soporte de Guardian para habilitar el escaneo de dispositivos inalámbricos en las inmediaciones de las sondas.

Consulte la sección Lista de dispositivos inalámbricos dentro de Manejo de aplicación web para más detalle.

2.10 Licencias

Esta capacidad permitirá proveer el servicio de Guardian a un cliente o proveedor únicamente de manera temporal, generalmente con propósitos de testing o validación.

2.11 Control de acceso y roles

Esta funcionalidad permitirá controlar el acceso y las acciones de los usuarios en el sistema. Esta implementación proporciona una capa adicional de seguridad y privacidad en el manejo de la información y los recursos del sistema.

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

- **Roles y permisos predefinidos:** Se podrán establecer diferentes roles y permisos predefinidos en el sistema, los cuales se otorgarán para determinar sus niveles de acceso y control en el sistema.
- **Asignación de permisos a usuarios y grupos:** El sistema permite asignar permisos a los usuarios y grupos en función a sus roles y responsabilidades en la organización.
- **Gestión de grupos de usuarios:** Deben establecerse grupos de usuarios para permitir la asignación de permisos a múltiples usuarios al mismo tiempo, lo que facilitará la gestión de los permisos.
- **Control de acceso a recursos:** El sistema permitirá el control de acceso a los diferentes recursos de Guardian mediante la asignación de permisos específicos.

Los roles que se implementarán serán los siguientes:

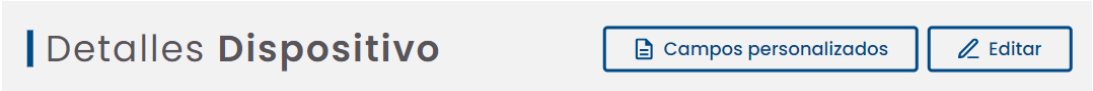
- **INPROTECH:** Acceso total a la configuración, operación del servicio, logs, etc., incluyendo la capacidad de pasar de training a producción o modificar el set de algoritmos de IA cuando aplique.
- **ADMINISTRADOR:** Modo privilegiado de usuario fábrica, podrá hacer cambios en los datos que puede ver en el front, como por ejemplo los datos de los dispositivos listados, o poder marcar las alertas como resueltas o silenciarlas.
- **OPERADOR:** Modo estándar de usuario fábrica, con permisos más restringidos. Solo podrá ver los datos y descargar los reportes o los CSV.

2.12 Campos personalizables

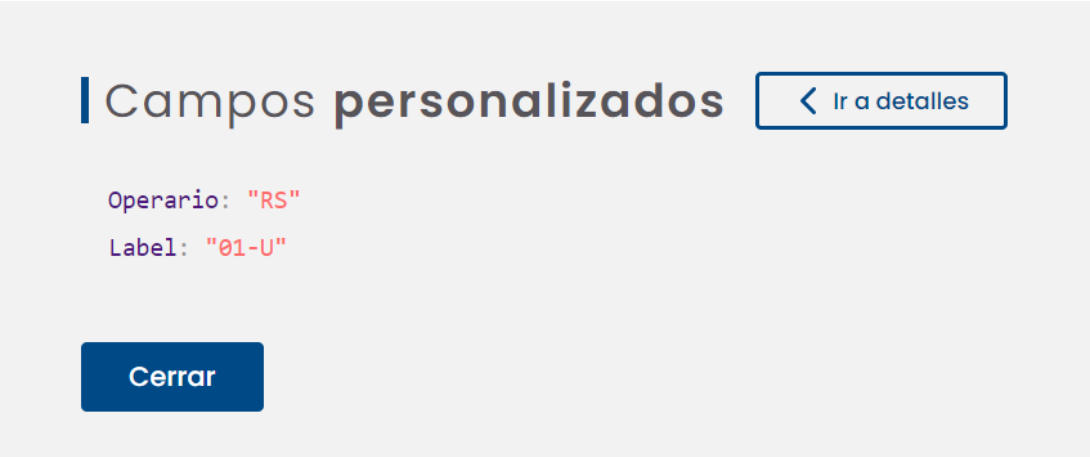
Si el usuario considera que en la lista de dispositivos se pueden añadir nuevos campos que permitan una mejor catalogación, pueden definirlos en formato clave-valor por medio de importaciones a partir de un archivo ".csv".

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

Al cargar los campos, se podrán comprobar desde el panel de dispositivos, bien pulsando sobre el enlace "Mostrar campos" de los dispositivos que los tengan configurados o pulsando sobre  "Detalles Dispositivo" para continuar haciendo clic sobre el botón "Campos personalizados".



Esto abrirá un nuevo modal que permitirá consultarlos.



3 Guía rápida

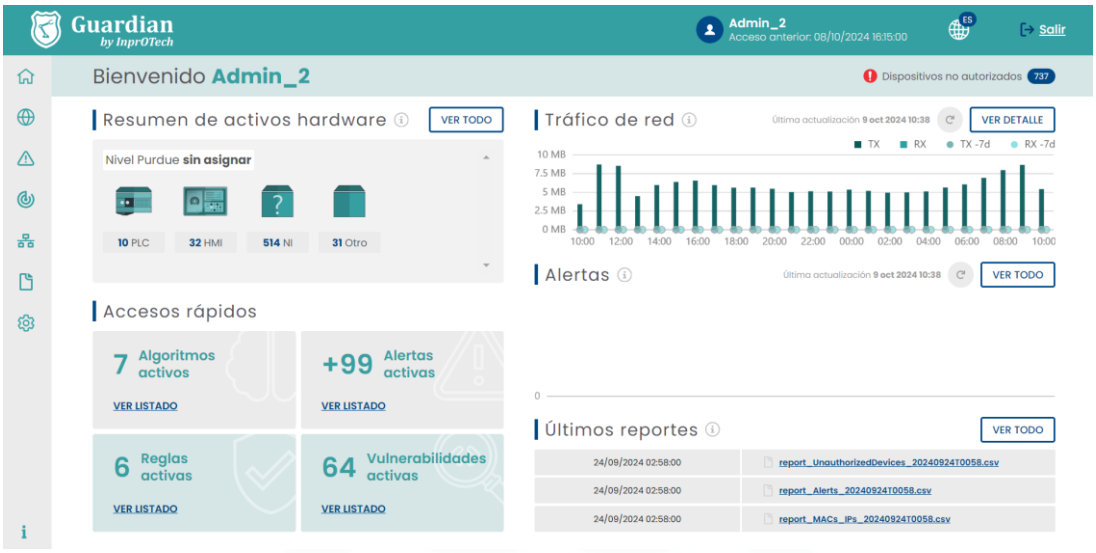
3.1 Ventana de accesos

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
- 5: Sesiones de tráfico: Lista de comunicaciones entre dispositivos
- 6: Informes: Lista de informes automáticos
- 7: Ajustes: Ventana de ajuste de parámetros
- 8: 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:

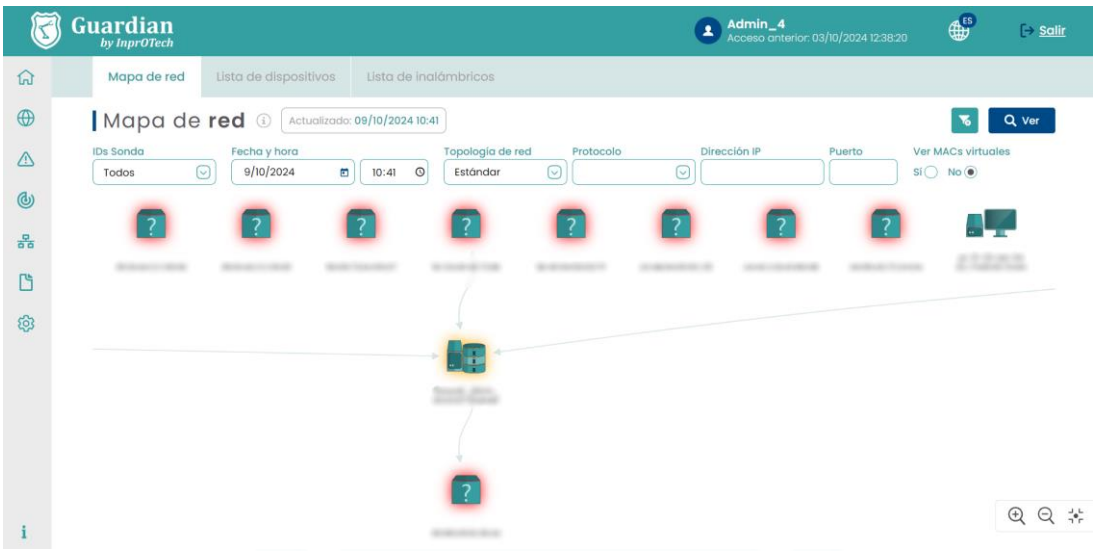
Representación gráfica de número de alertas según su severidad

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

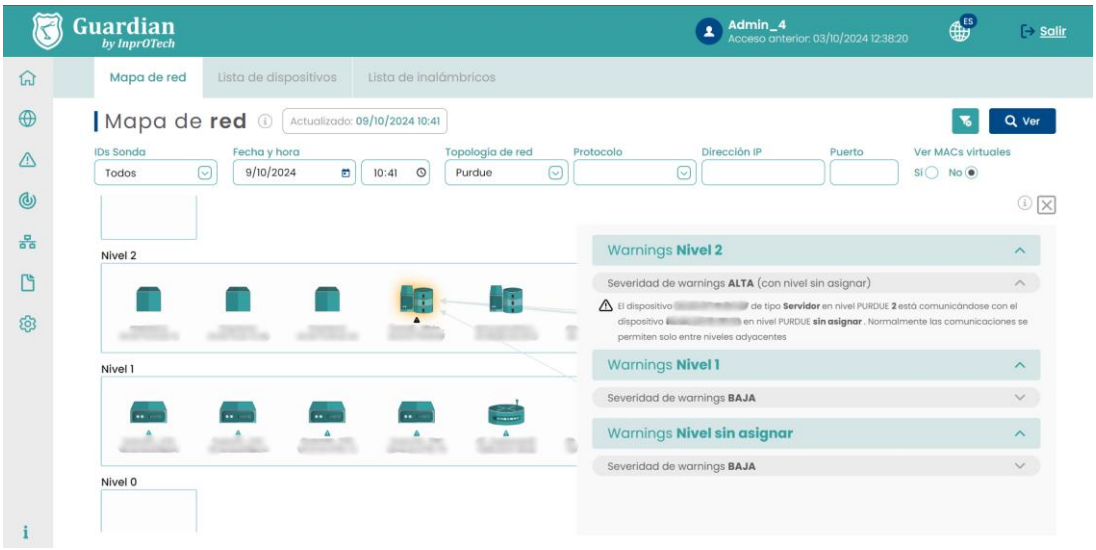
En la siguiente fila, se muestran los filtros posibles para ver por pantalla los dispositivos de nuestro interés.

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

Hay que 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 warning se califican en **severidad alta** (de tipo comunicaciones, señalando la existencia de estas 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).



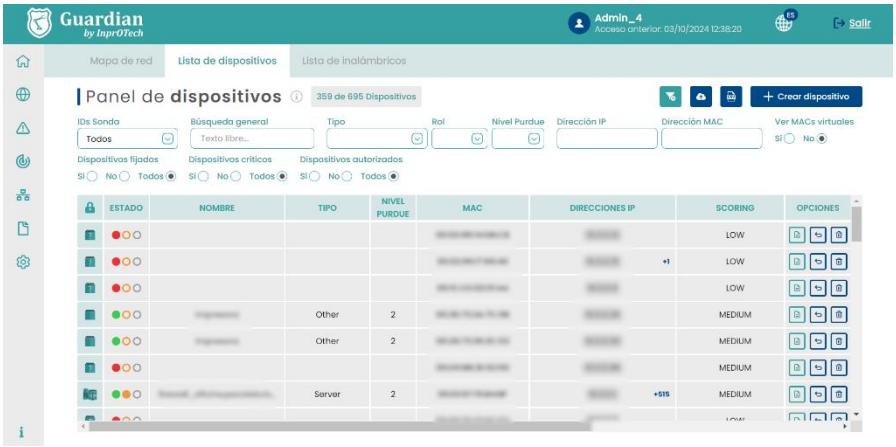
Mapa de red en vista PURDUE

Hay que 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 warning globales o asociados a un dispositivo seleccionado.

3.4 Lista de dispositivos



Ventana de listado de dispositivos

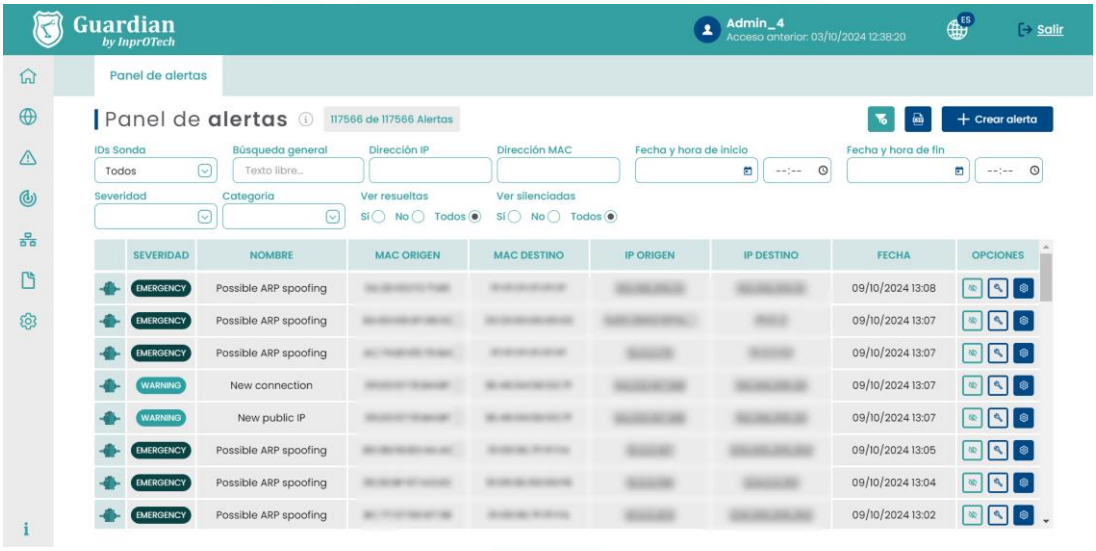
En la pestaña para seleccionar la vista del listado de dispositivos registrados en la red, se muestra junto al título del panel el número de dispositivos con el filtro actual aplicado frente al total de dispositivos en la base de datos. En la zona derecha, la botonera para eliminar los filtros previamente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

El listado en sí de los activos contiene 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 clic en cualquiera de las columnas.

La tercera pestaña, contiene el inventario de dispositivos inalámbricos detectados en la inmediación de las sondas (en caso de disponer de hardware compatible y estar la funcionalidad habilitada por personal de Soporte de Guardian).

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. Hay que 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 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 clic en cualquiera de las columnas.

3.7 Lista de informes

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

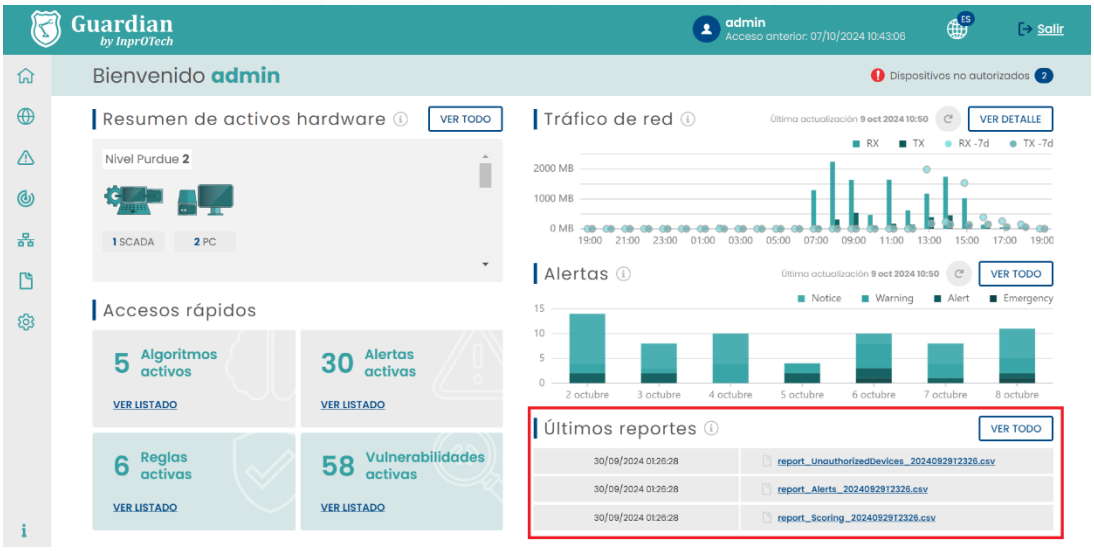
- Informe de dispositivos detectados “desconocidos”:
  - Nombre
  - MAC
  - Fabricante

    - Rol
    - Fecha de descubrimiento
    - IPs
    - Nivel Purdue
    - Solucionado (S/N)
    - Crítico (S/N)
    - Tipo de dispositivo
    - Puntuación y su registro de tiempo
    - Scan status y último escaneo
    - N.º de riesgo de vulnerabilidad
    - Etiqueta de riesgo de vulnerabilidad
    - SO
    - Bloqueado (Permitido / No permitido)
    - Campo personalizable (desglosando cada campo en columnas)
- Informe de alertas detectadas:
    - Título informativo de la alerta
    - Categoría
    - Severidad
    - Silenciada
    - Resuelta
    - Valor
    - IP origen
    - MAC origen
    - IP destino
    - MAC destino
    - Protocolo
    - Fecha
    - Ubicación (Ciudad / Continente / País / Latitud / Longitud…)
    - Nombre del anfitrión
    - IP
    - Dispositivo origen (nombre/tipo)
    - Dispositivo destino (nombre/tipo)
    - Creador
- Relación MAC-IP
    - MAC
    - Fabricante
    - IP
    - Pública
    - Fecha de descubrimiento
- Lista de IPs públicas contactadas (máquinas que están expuestas a Internet):
    - IP (origen/destino)
    - MAC (origen/destino)
    - 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
- Dispositivos inalámbricos
    - IP
    - MAC

  - Tipo de conexión
  - Autorizado (S/N)
  - Tipo de dispositivo
  - Canal
  - Potencia de señal
  - Modo PA
  - Banda de frecuencia
- Vulnerabilidades
  - MAC
  - IP
  - CVE
  - Estado
  - Origen
  - Fecha de descubrimiento
  - Última vez vista
  - Puerto
  - CPE
  - Criticidad
  - Descripción
  - Marca de tiempo de su publicación
  - CWE
  - URL

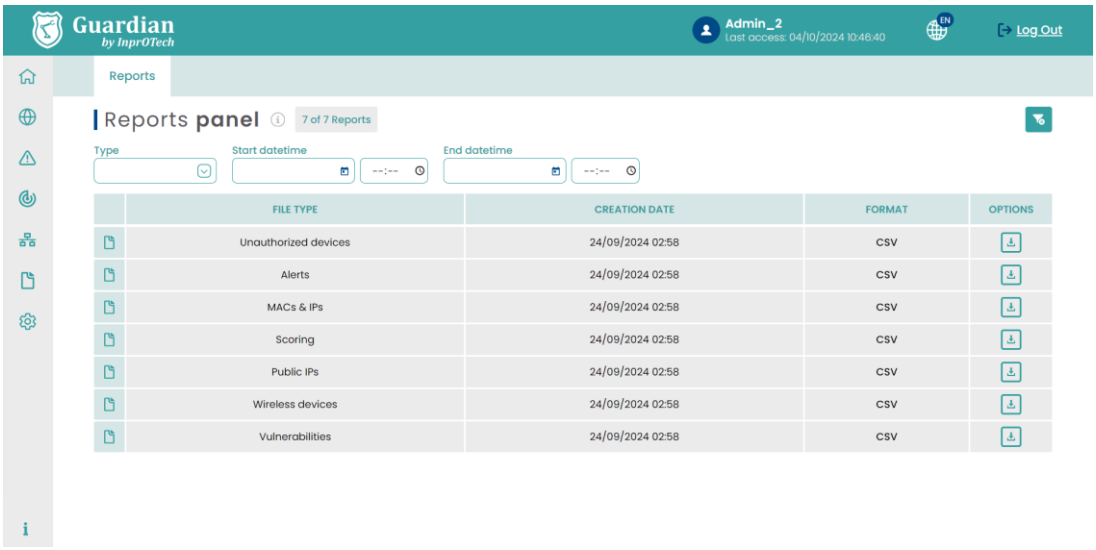
El campo MAC en el informe de alertas, en caso de que el dispositivo tenga la etiqueta Nombre informada, será sustituido por dicho valor en estos reportes. En cambio, en las descargas manuales de búsquedas del usuario desde el panel de alertas o la lista de dispositivos, ambos campos se mostrarán de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

3.8 Ventana de ajuste de parámetros

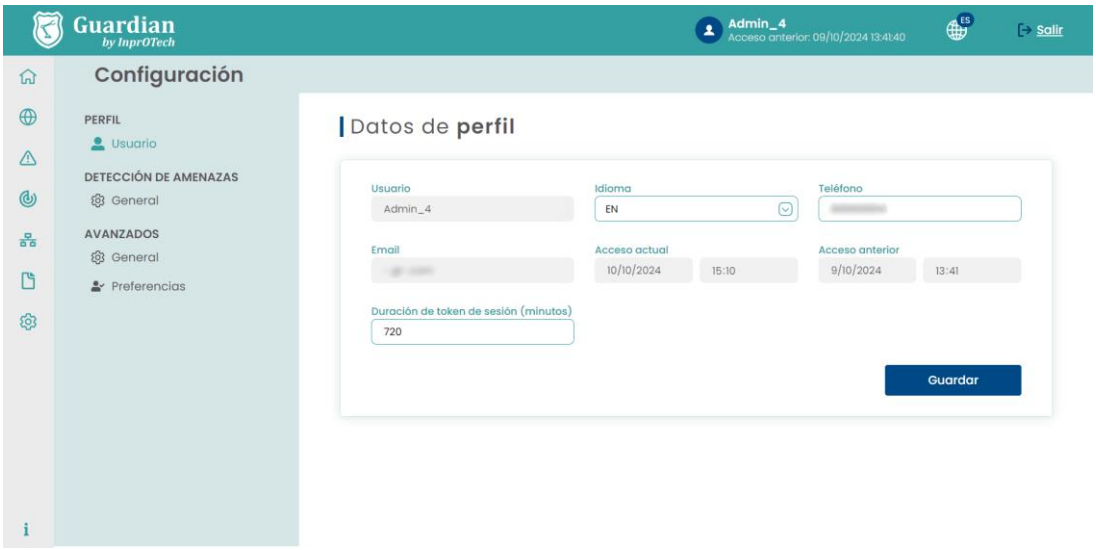
En este apartado podremos hacer ajustes en nuestro perfil o perfil del empleado autorizado, ajustar algunos parámetros relacionados con la detección de amenazas o distintas configuraciones de alertas, amenazas y gestión de usuarios.

En desarrollo, sujeto a cambios.

3.8.1 Perfil de usuario

Esta sección muestra información básica como el nombre de usuario, el correo electrónico asociado, la fecha y hora de la última y actual conexión, el idioma preferido (EN/ES) y el número de teléfono de contacto. Los dos últimos son editables por el usuario.

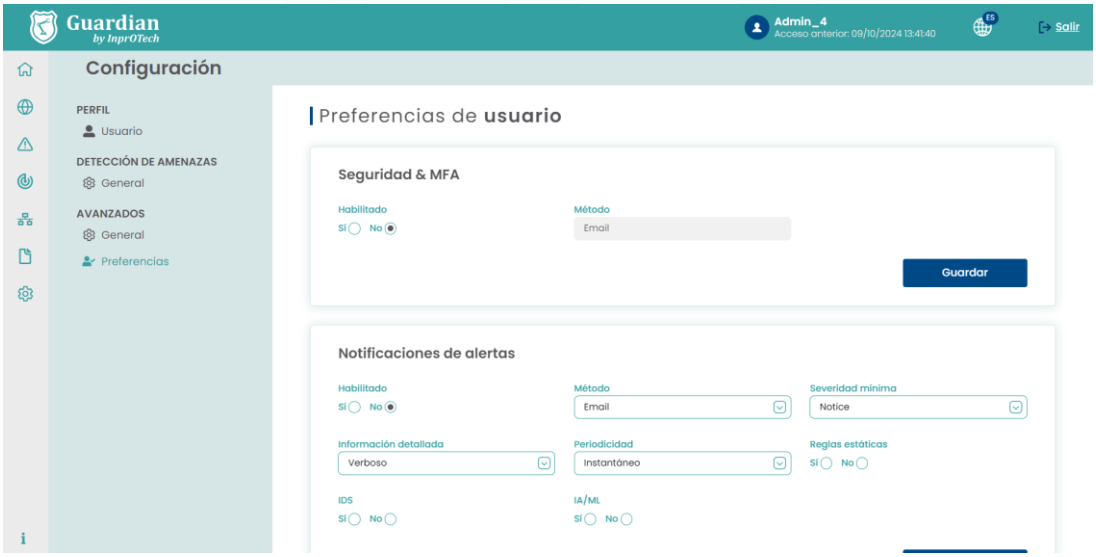
Se puede llegar a ella desde  “Ajustes” desde el Menú lateral izquierdo.



Pestaña perfil de usuario

3.8.2 Seguridad

En Avanzados > Preferencias, en el apartado 'Seguridad y MFA', podemos indicar si queremos activar o no el segundo factor de autenticación como mecanismo de seguridad adicional (recomendado) para evitar la suplantación 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 habremos recibido (inicialmente por correo electrónico).



Pestaña de seguridad & MFA

Recuerde 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 InprOTech
- Administrador de planta
- Operador de planta

La asignación de roles a los usuarios no puede ser gestionada directamente por su organización, sino que se define con InprOTech en el momento de la implantación de la solución. Contacte con nosotros para más información.

3.8.3 Notificaciones de alertas

En caso de que se considere oportuno, se pueden configurar alertas proactivas para generar avisos en el sistema. Las alertas y avisos se generan en base a la detección de anomalías según las diferentes estrategias implementadas en Guardian (heurística, IA/ML, IDS, Honeypot, manuales...).

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

El usuario podrá, por tanto:

- Decidir si quiere recibir notificaciones de alertas de seguridad.

- En caso afirmativo, a partir de qué umbral de gravedad se enviarán al usuario.

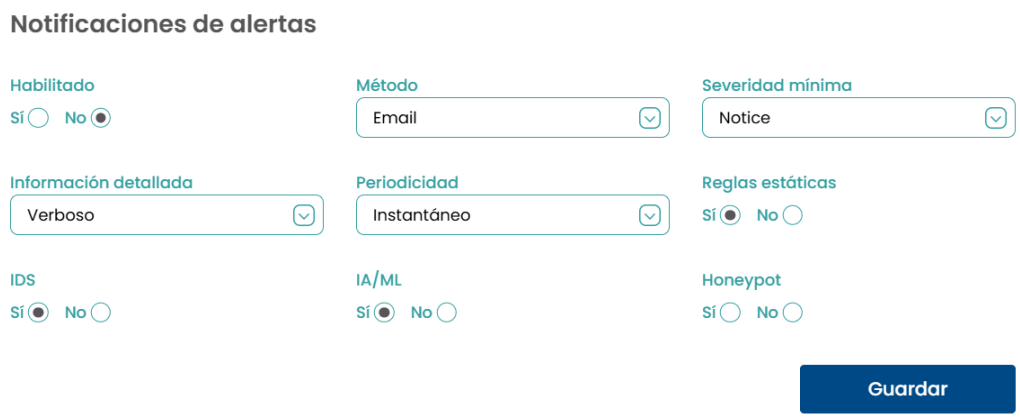
- Qué tipo de alertas (heurísticas, IA/ML, IDS, Honeypot, todas...)

- En qué formato

    o Individual: una notificación por alerta

    o Agrupada: una notificación diaria con el resumen de todas las alertas, seleccionable de lunes a viernes o de lunes a domingo.

- Si es individual, si se desea formato resumido o verboso.



Notificaciones de alertas

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

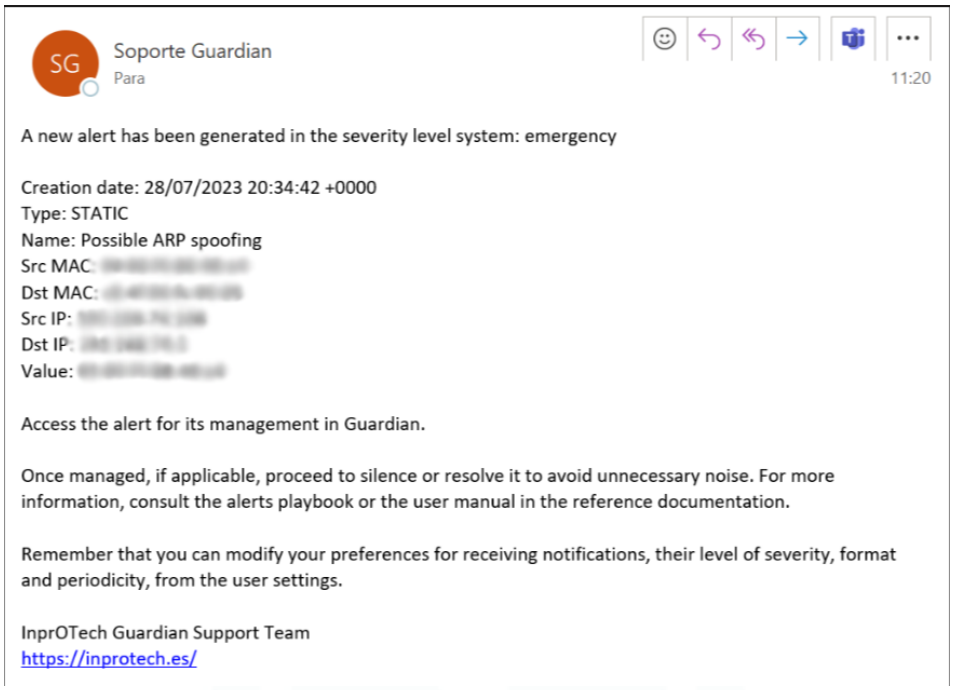
Importante:

- La notificación de alertas debe estar habilitada en el backend para que el usuario pueda habilitar los envíos proactivos.

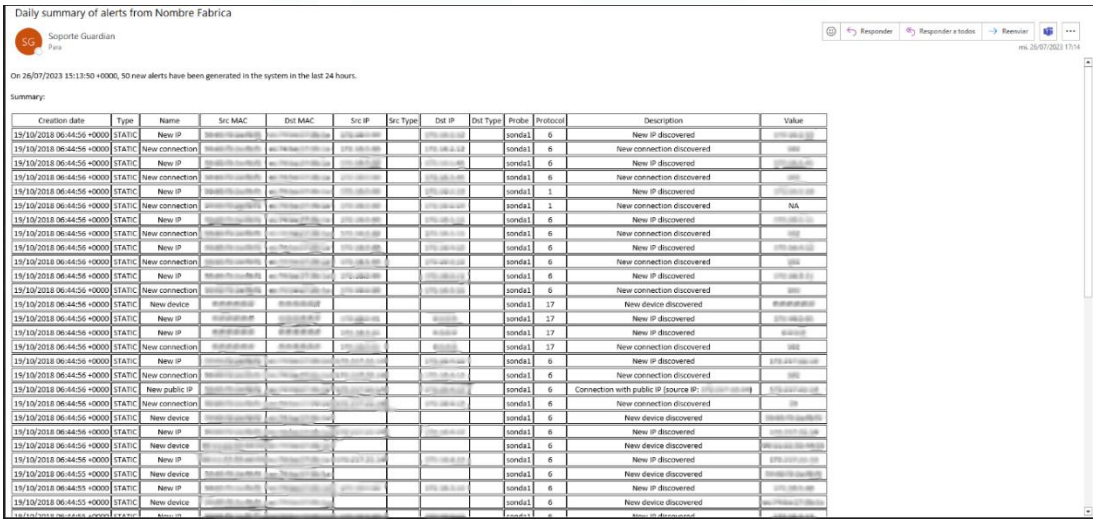
- En caso de que con las condiciones establecidas se generen demasiadas alertas por unidad de tiempo, la funcionalidad se auto deshabilitará por seguridad (informando previamente vía email al usuario de esta circunstancia), para que se puedan seleccionar

otras condiciones de envío de notificaciones más exigentes (de menor volumen de eventos).

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



Ejemplo de notificación de alerta individual resumida

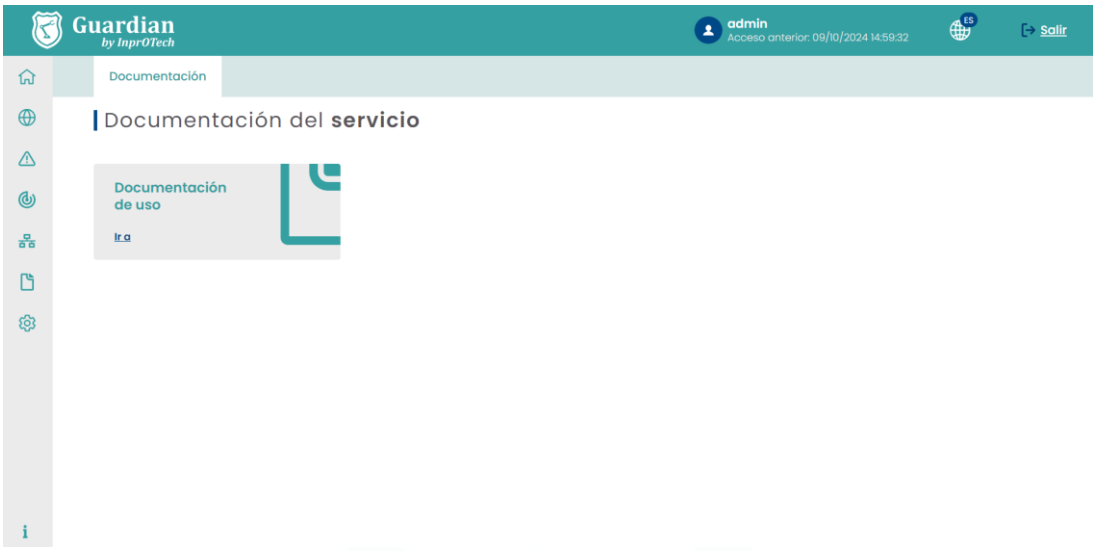


Ejemplo de notificación de alerta diaria agrupada

3.9 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.

Para acceder a ella, haz clic en el icono del Menú  , en la esquina inferior izquierda.

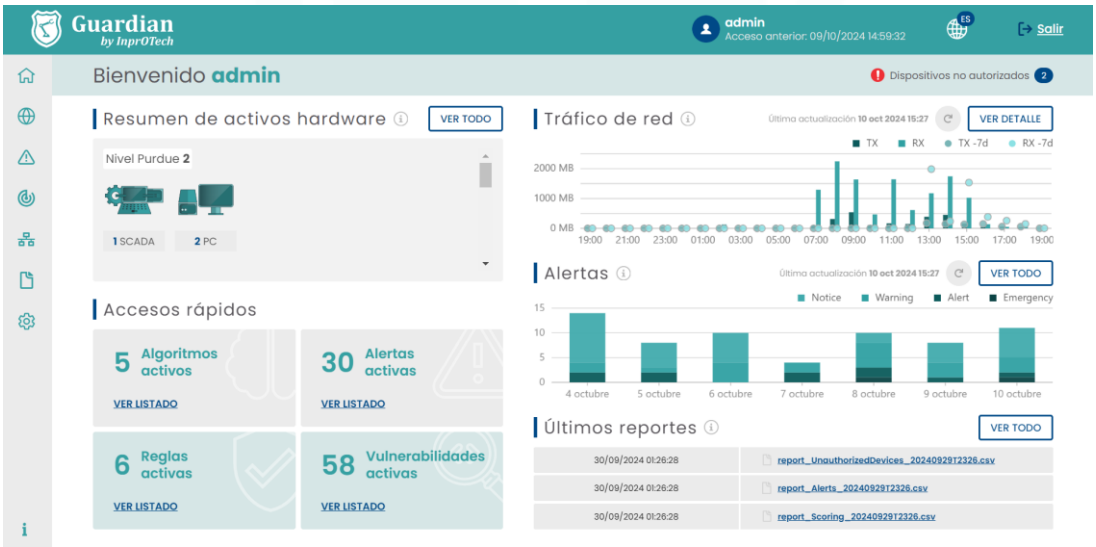


Pantalla principal

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



Pantalla 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, Rúter, Robot, PC, SCADA, DCS, HMI, Firewall, variador de frecuencia, Tarjetas controladoras, sensores, Cámaras de V.A., tabletas, Teléfonos, Honeypot, 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 enlace “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).

Lista de algoritmos

4.1.2.2 Alertas Activas

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

4.1.2.3 Reglas Activas

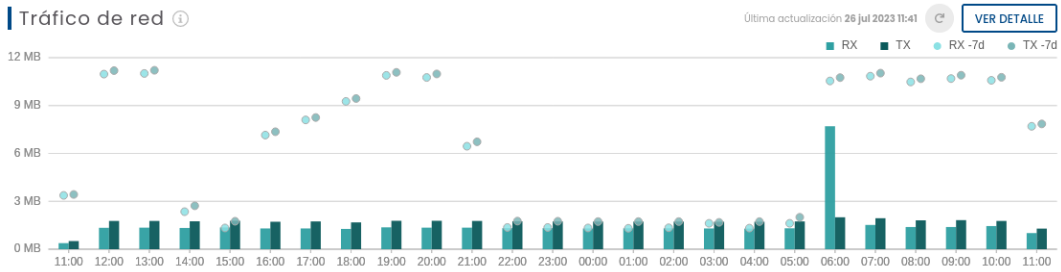
Al pulsar sobre el enlace "VER LISTADO", el usuario podrá visualizar el listado con las reglas fijas que están activas para la detección de amenazas dentro de la red de la organización (Apartado que se verá posteriormente en el presente manual).

Lista de reglas activas

4.1.2.4 Vulnerabilidades Activas

Al pulsar sobre el enlace "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

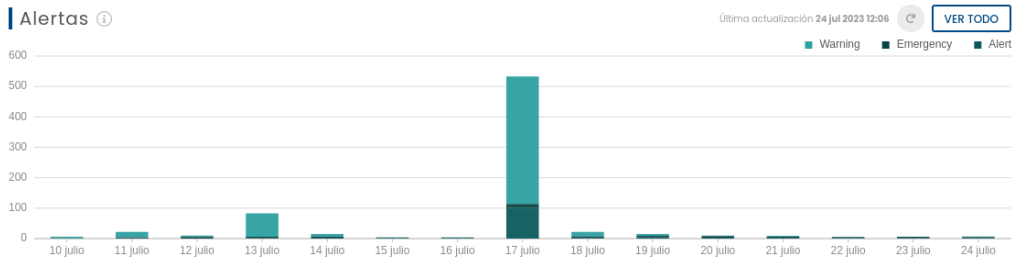


Tráfico de red

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



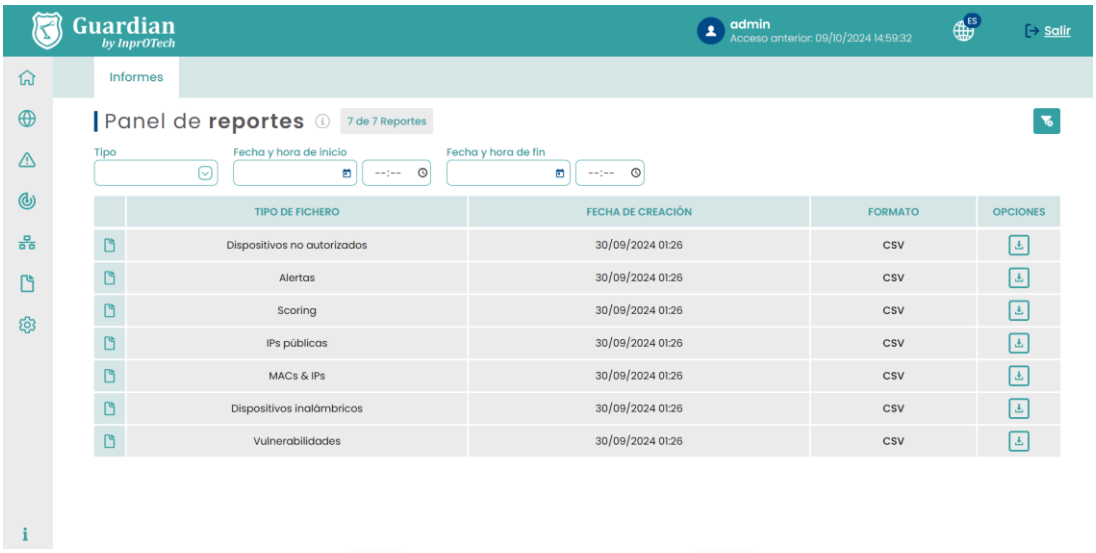
Alertas

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.

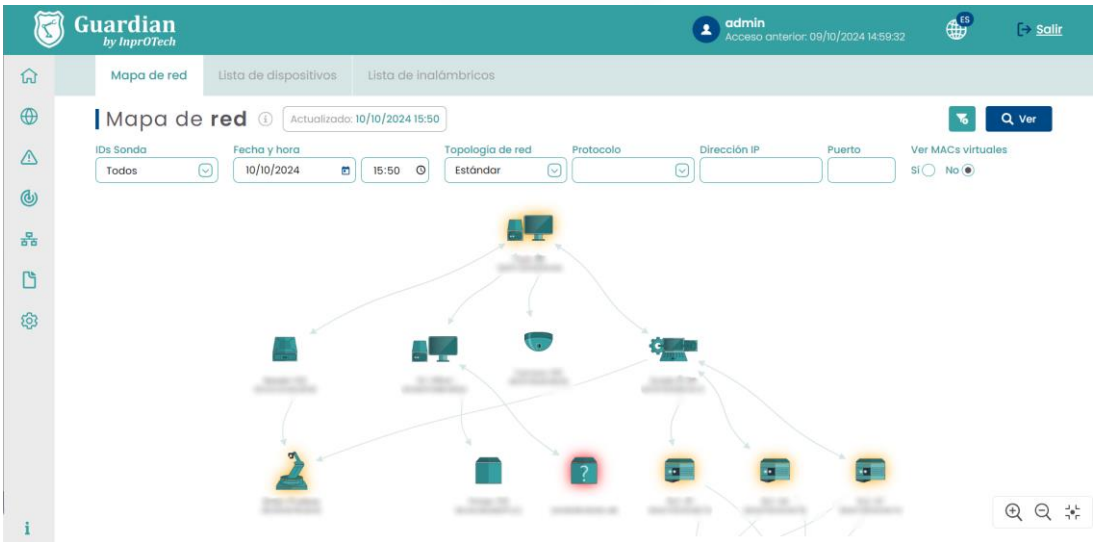
Actualmente, los reportes generados con periodicidad semanal son:

- 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).

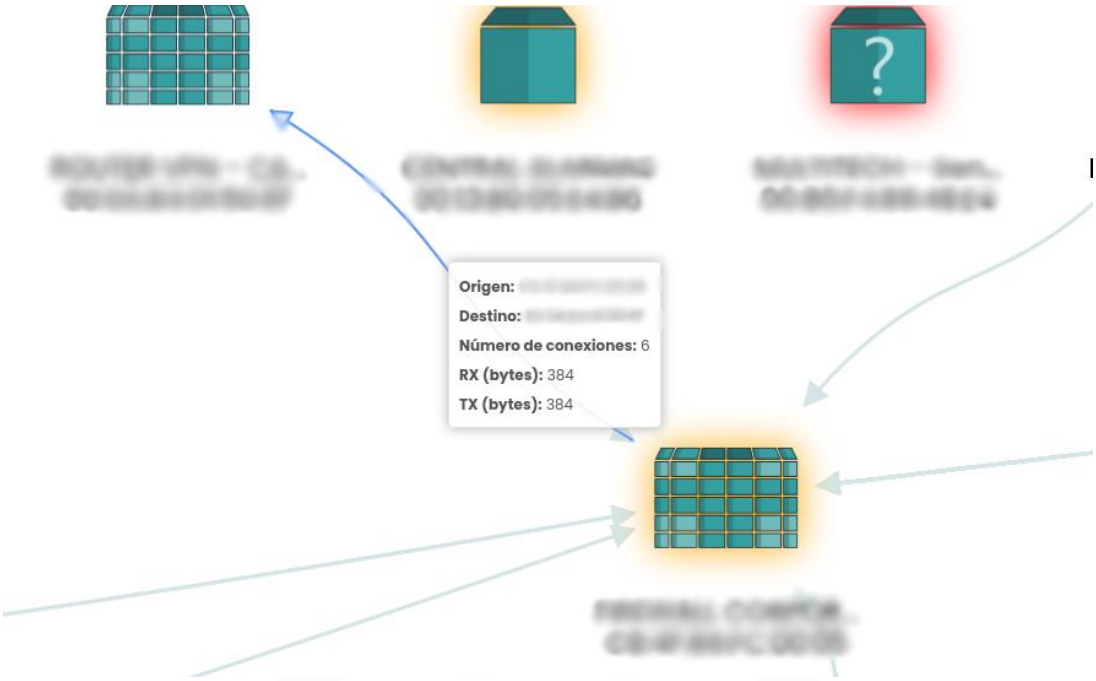
Dispositivo no autorizado

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”

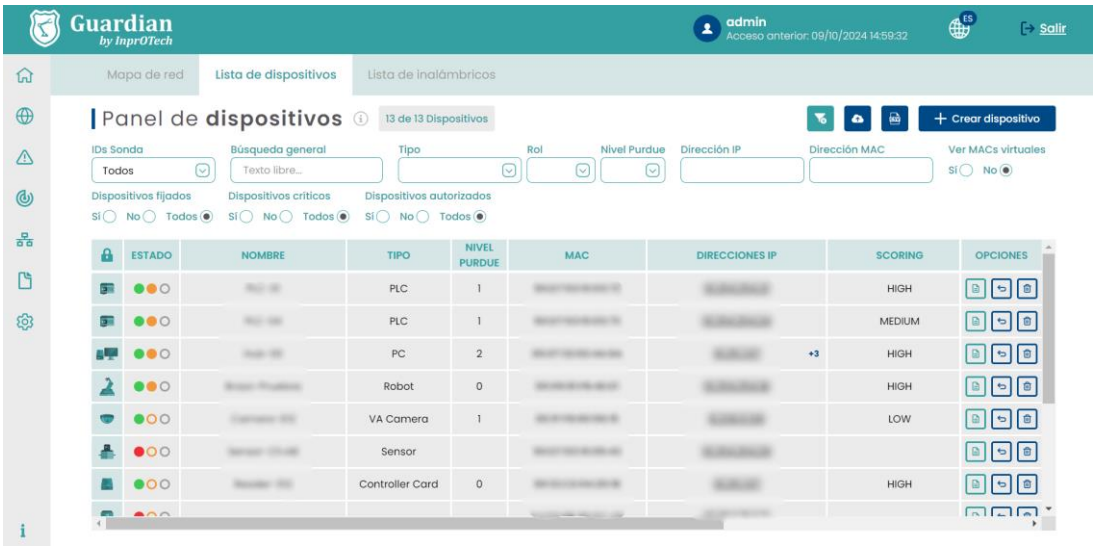
Filtros disponibles en mapa de red

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

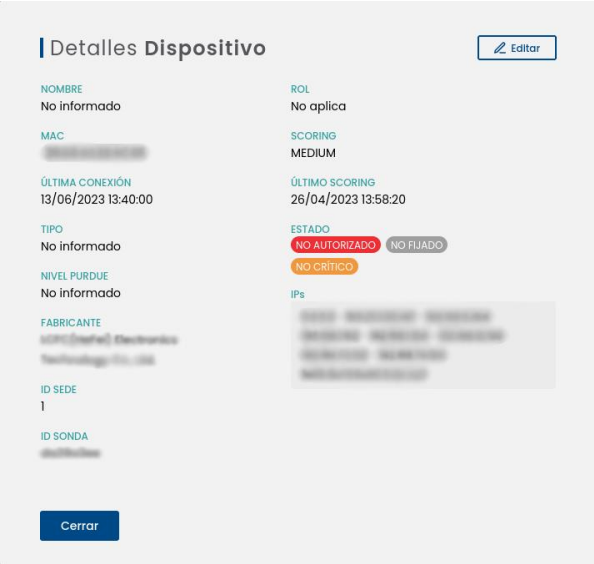
Para acceder a la lista de dispositivos, el usuario deberá pulsar sobre el icono que aparece en la parte izquierda de la pantalla y seleccionar la pestaña de “Lista de dispositivos”.



Ventana de lista de dispositivos

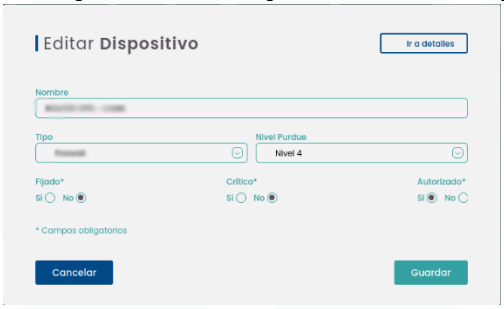
Se mostrará un listado con todos los dispositivos presentes en la organización junto con su información de forma más ampliada:

- 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, Honeypot etc..).
- NIVEL PURDUE: Nivel de clasificación según el modelo de Purdue.
- MAC: Dirección MAC asignada del dispositivo.
- DIRECCIONES IP: Dirección IP asignada del dispositivo.
- SCORING: importancia/riesgo del dispositivo (baja, media o alta).
- VULN RISK: nivel de criticidad más alto para todas las vulnerabilidades del dispositivo.
- VENDOR: fabricante del dispositivo, identificado con los tres primeros campos de su dirección MAC.
- FIRMWARE: firmware integrado en el dispositivo.
- CAMPOS PERSONALIZABLES: además de los campos existentes, el usuario podrá crear sus propios campos 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 reportes.
  Las columnas creadas como campos personalizables formarán parte de un inventario virtual. Sobre él, podrán aplicarse filtros de búsqueda según se desee. Este inventario de campos también es exportable.
- ACCIONES:
  -  : Botón para ver en detalle la información del dispositivo.



Ventana de información ampliada de dispositivo

- Editar: Botón para modificar parámetros del dispositivo.



Ventana de parámetros de dispositivo

- : Botón para realizar otras acciones en el dispositivo, como acceso con vista filtrada previamente 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
- Tipo de dispositivo (PLC, RTU, SCADA, Honeypot, 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 (S/N).
- Dispositivos fijados (S/N), ver anexo I.
- Dispositivos críticos (S/N), ver anexo I.
- Dispositivos autorizados (S/N), ver anexo I.

También se puede realizar una búsqueda general a partir de una cadena de texto.

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

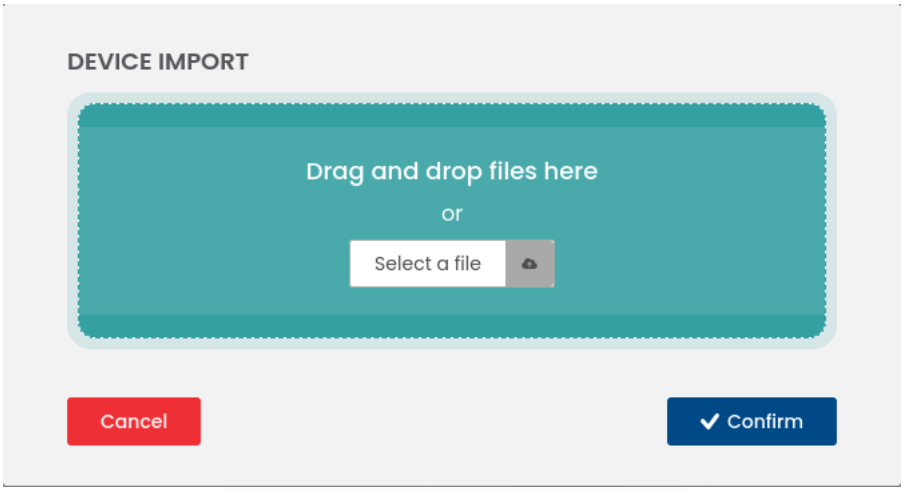
Se ha de introducir manualmente la información solicitada sobre el dispositivo a añadir y para hacer efectiva esa creación se ha de pulsar en el botón de “Guardar”.

4.2.2.1 Importación de CSV

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

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

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



Importación CSV pop-up

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

- Un máximo de 250 registros.
- Encabezado con las siguientes columnas (podremos poner el nombre que deseemos a las columnas):
    - MAC
    - Nombre del dispositivo
    - Autorizado (S/N)
    - Critico (S/N)
    - Fijado (S/N)
    - Tipo de dispositivo (de la lista permitida: virtual, plc, rtu, switch, rúter, robot, pc, scada, hmi, firewall, adjustable_frequency_drive, controller_card, sensor, va_camera, tableta, voip_phone, servidor, code_bar_scanner, other)
    - nivel PURDUE (de 0 a 4, tal y como se explica en el Anexo II)
    - Campos personalizables.
- El delimitador de campos será ";"
- No podrá contener campos vacíos.
- Podrá contener registros de dispositivos nuevos, o dispositivos existentes en la base de datos a los que se le quiere cambiar alguno o varios de los atributos mencionados en el punto anterior. Se requiere una fila por dispositivo, con el formato indicado.
- Los nuevos registros simplemente tendrán todos los campos del CSV cubiertos con la información deseada.
- Los registros existentes que queramos modificar contendrán el literal **CURRENT** en todos aquellos campos que deban permanecer fijos. En los campos a actualizar, simplemente pondremos la nueva información en base a lo establecido previamente.
- Los que queremos modificar deberán llevar **CURRENT** en alguna de sus propiedades; esto nos permite distinguir estos registros de los nuevos.
- El campo MAC no podrán llevar el literal **CURRENT**, puesto que identifica unívocamente al dispositivo.

- Los nuevos registros también podrán contener el literal **CURRENT** en algunos de sus campos; esto se traduce en dejar esos campos con los valores por defecto. En el caso de los datos tipo *bolean* será *false*, y en los campos de texto, como el nombre, Purdue y tipo de dispositivo, quedarán como *NULL*, pudiendo ser modificados por el usuario a través de la interfaz web
- Existen dos formas posibles en las que se puede definir un conjunto de campos personalizables, respetando su estructura de clave-valor:
    - Formato .json: {"clave1": "valor1", "clave2": "valor2"}
    - Barras: clave1 | valor1 | clave2 | valor2

Se podrán eliminar los campos personalizables definidos previamente sobrescribiendo los datos con un nuevo documento CSV que contenga el literal *DELETE* en el lugar de dichos campos, de una manera parecida a la que se utiliza con el literal CURRENT.

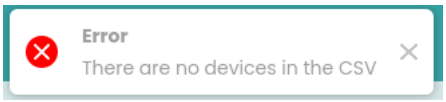
- Es importante escribir los literales entre asteriscos.

Aviso. Consultar a Soporte en caso de duda, puesto que un uso inadecuado de esta funcionalidad puede tener bastante impacto en cuanto a integridad de la información de los nodos.

Una vez que se haya seleccionado el archivo, se hará clic en "Confirmar", dado que es una operación de alto impacto (permite tanto añadir como modificar propiedades de los dispositivos):

Desplegable importación de dispositivos

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



Error en importación

En caso de que existan errores en los datos dentro del archivo ".csv", se mostrará un mensaje que incluirá los detalles de los errores encontrados, junto con el número de línea en la que se encuentra cada error.

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

Error en importación

4.2.2.2 Air Watcher (Lista de dispositivos inalámbricos)

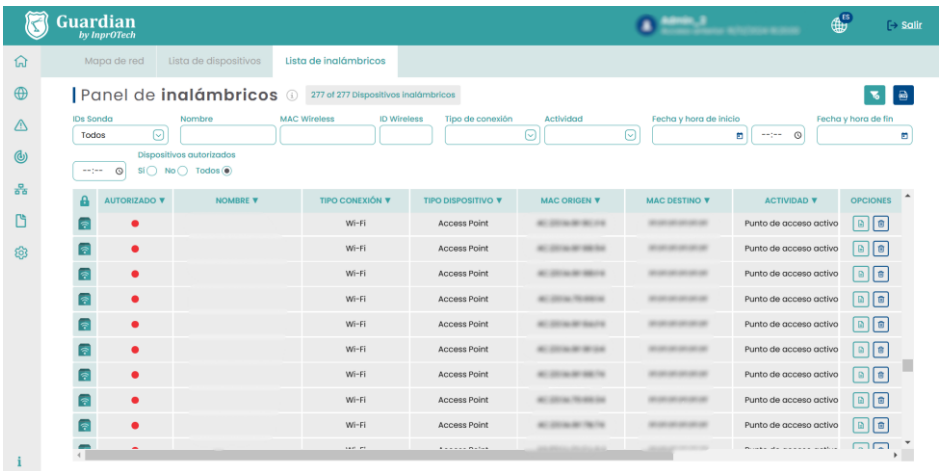
En la sección de red, existen tres pestañas, entre las que se encuentra la que permite acceder a la vista del listado de dispositivos inalámbricos registrados en la red (tercera pestaña).

En la parte superior, podremos ver el número total de dispositivos en la base de datos y, si tenemos algún filtro aplicado, veremos cuántos coinciden con dicho filtro en relación con el total.

En la zona derecha, encontraremos la botonera para eliminar los filtros previamente aplicados y exportar la lista de dispositivos en formato CSV.

La información que nos dará este apartado será el siguiente, para todos aquellos dispositivos con capacidad Wi-Fi o Bluetooth detectados en las inmediaciones de la sonda:

- **Autorizado**: determina si el dispositivo ha sido autorizado por un administrador (verde) o no (rojo).
- **Nombre**: se corresponde con el nombre del dispositivo.
- **Tipo de conexión**: podría ser Wi-Fi o Bluetooth.
- **Tipo de dispositivo**: los valores pueden ser diversos en los dispositivos Bluetooth, en los dispositivos Wi-Fi puede coger los valores de "Punto de Acceso" o "Smartphone or Laptop", además de "Unknown"
- **MAC origen**: dirección MAC origen del paquete. Identifica al propio dispositivo en la comunicación capturada.
- **MAC destino**: dirección MAC destino del paquete. Identifica al dispositivo receptor del paquete
- **Actividad**: refleja en qué estado de se encuentra el dispositivo o el tipo de actividad que ha realizado; buscando redes, realizando un intento de conexión, siendo un punto de acceso activo, transmitiendo datos o, simplemente, mostrándose como un dispositivo visible.
- **ID Wireless**: Nombre o identificador de la red WiFi (podría estar vacío en el caso de que, por ejemplo, la conexión fuese Buetooth).
- **Visto primera vez**: formato dd/mm/aaaa hh:mm
- **Visto última vez**: formato dd/mm/aaaa hh:mm



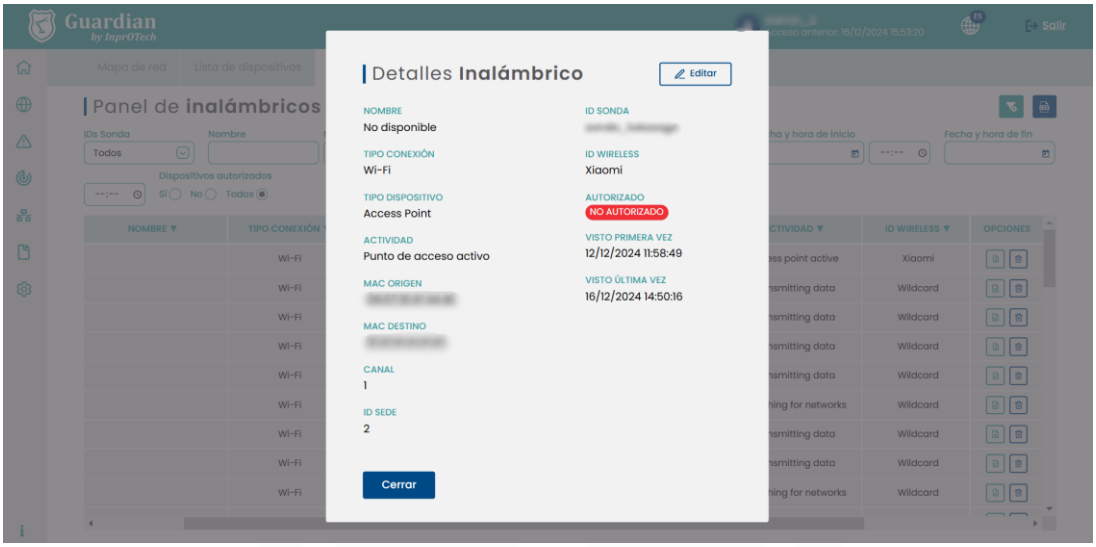
Lista de dispositivos inalámbricos

A continuación, se incluyen los posibles filtros aplicables para quedarnos con los dispositivos de nuestro interés:

Filtros de dispositivos inalámbricos

Hay que recordar que es posible ordenar los dispositivos alfabéticamente de forma directa o inversa haciendo clic en cualquiera de las columnas.

Por último, el listado en sí de los activos contiene información sobre ellos, además de botones para realizar ciertas acciones (ver detalles o eliminar).



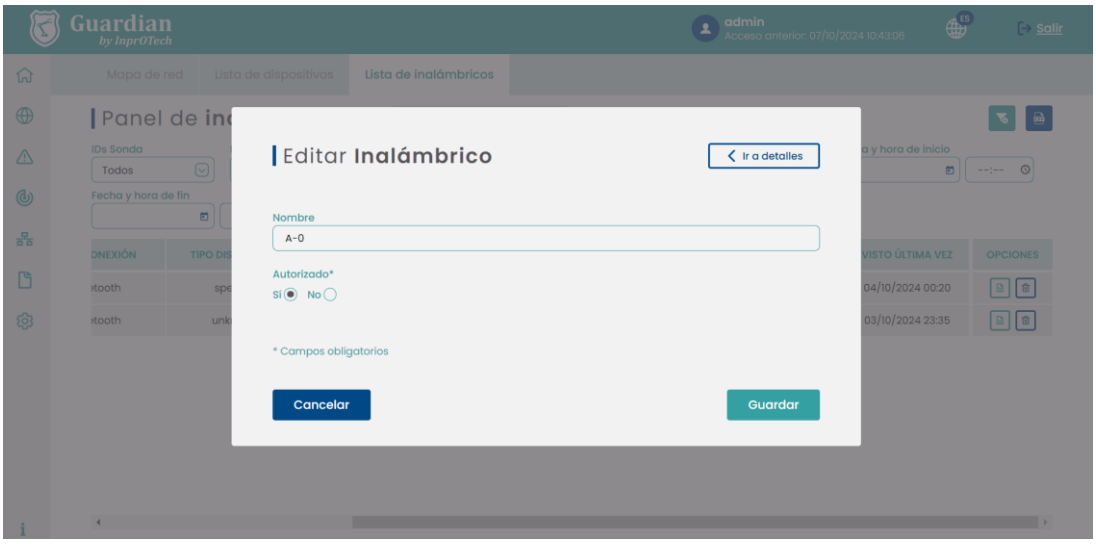
Detalles de dispositivo inalámbrico

También podremos ver algunos campos adicionales en este nuevo modal:

- Canal: identificador del canal de transmisión
- ID sede: representa la fábrica
- ID sonda: identifica la sonda.
- ID Wireless: identificador único de la red del dispositivo

Si pulsamos el botón 

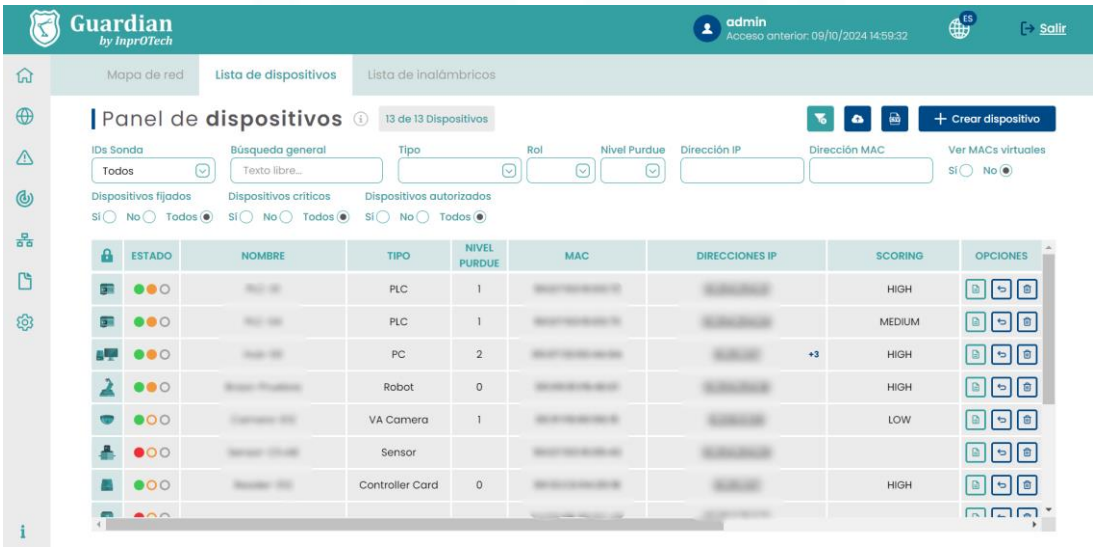
, podemos renombrar el dispositivo y determinar si está o no autorizado.



4.2.2.3 Smart View (Escáner de dispositivos)

Esta capacidad permite realizar un escáner activo de los dispositivos en la red OT, para mediante un fingerprinting ligero identificar algunas propiedades adicionales de cada nodo: versión del dispositivo, firmware, puertos abiertos, y servicios en ejecución en la propia máquina.

Para ello se utilizará la herramienta nmap, y se escanearán los puertos en 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 refrescarán mediante un barrido periódico.

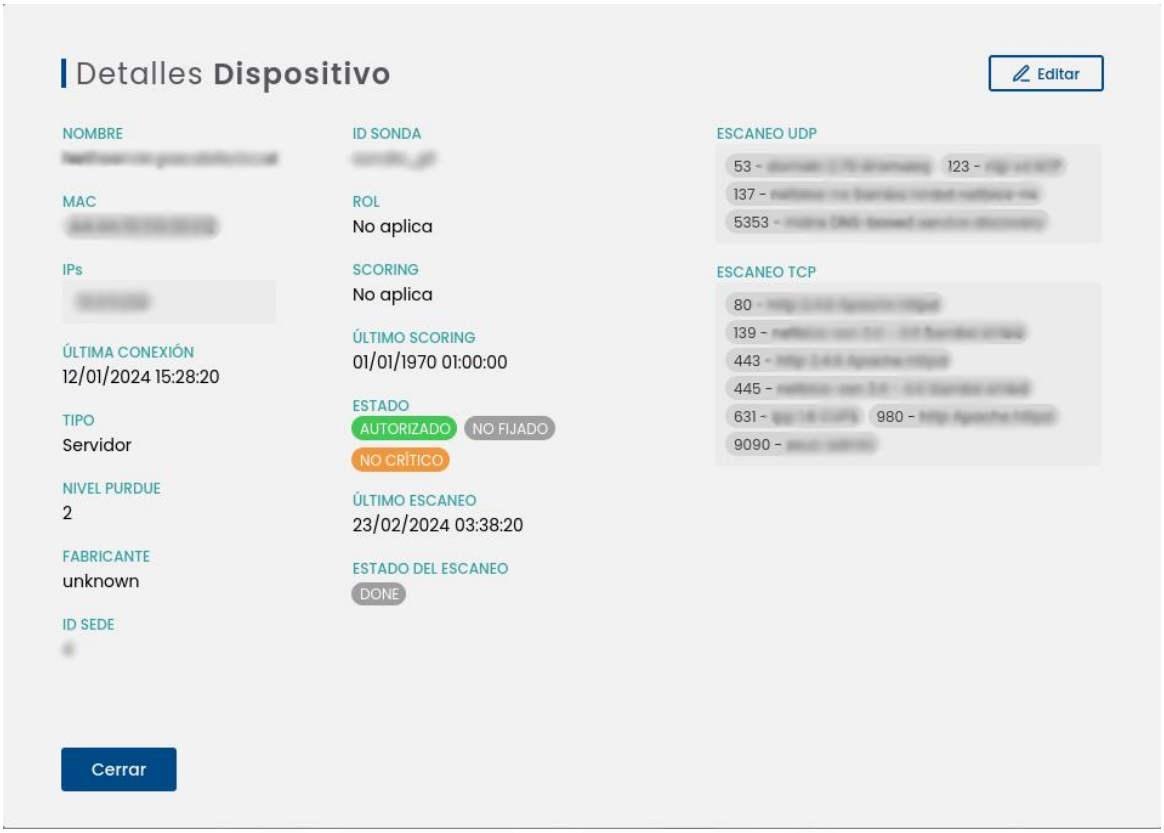


Lista de dispositivos

Como se puede apreciar, una vez ejecutado el escáner tendremos información asociada al firmware de algunos de los dispositivos.

El resto de información del escáner, podremos visualizarla en icono de la derecha y haciendo clic. En el pop-up podremos ver toda la información del dispositivo en cuestión, y aparecerán dos apartados llamados “Escaneo TCP” y “Escaneo UDP”, donde

se visualizarán todos los puertos abiertos que ha encontrado para un dispositivo dado, así como la fecha del último escaneo y si ha finalizado correctamente o ha habido algún tipo de error.



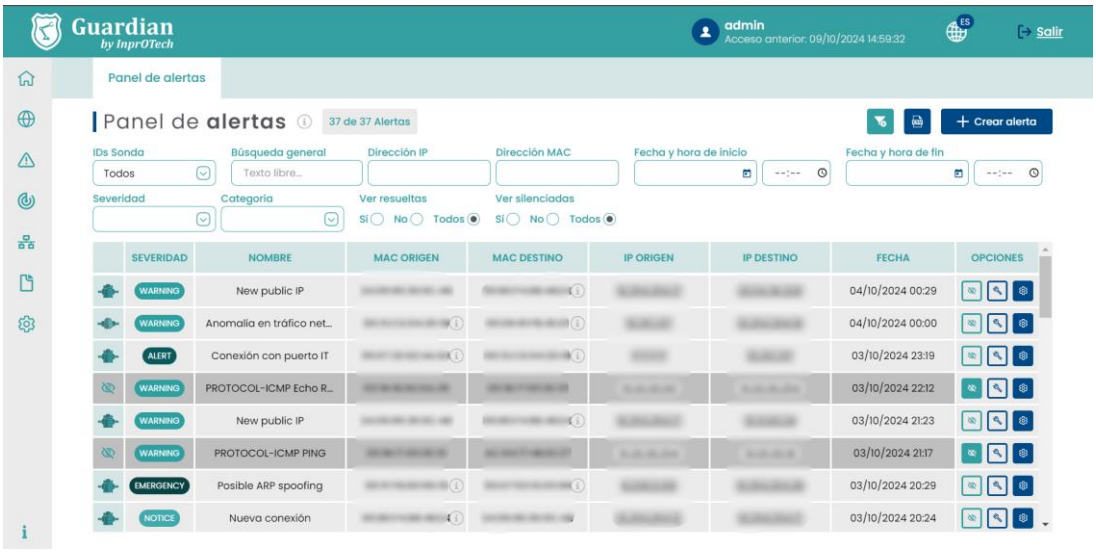
Detalles del dispositivo

DISCLAIMER: Dado el carácter activo de esta funcionalidad, aunque no se ha observado impacto operativo no puede descartarse completamente. Por ello, es decisión del cliente si activar o no esta funcionalidad (para lo que debe consultar al soporte de InprOTech). Si quisiera activarlo en su planta industrial, pero dejar algún subconjunto de dispositivos excluido de la lista de nodos a analizar, basta con etiquetarlos con la propiedad "Crítico" habilitada en el inventario de dispositivos (de forma individual o mediante una actualización masiva).

Adicionalmente, los dispositivos de tipo honeypot y etiquetados como tal también están exentos, debido a su comportamiento como señuelos con puertos vulnerables. Esto evita el envío excesivo de falsos positivos.

4.3 Panel de alertas

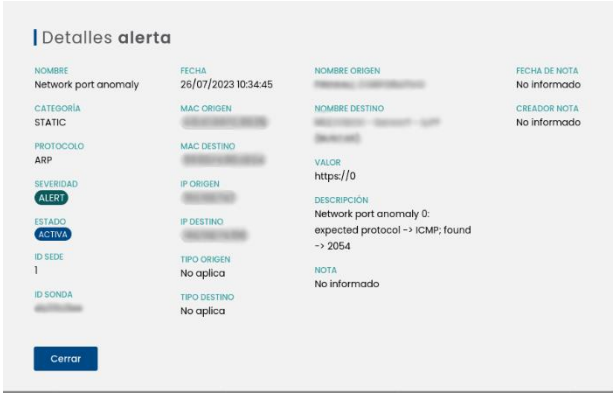
Para acceder al listado de alertas, el usuario deberá pulsar sobre el icono  que aparece en la parte izquierda de la pantalla.



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

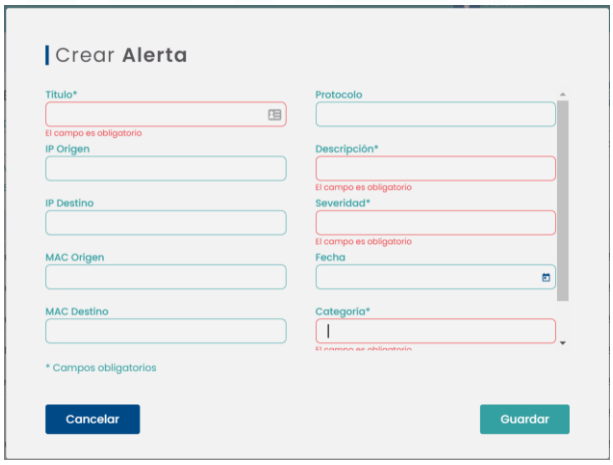
Al pulsar el botón  se realizará un reinicio de los valores de filtrado y se mostrará nuevamente la lista completa con todas las alarmas.

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 

.

Aparecerá la siguiente ventana emergente:



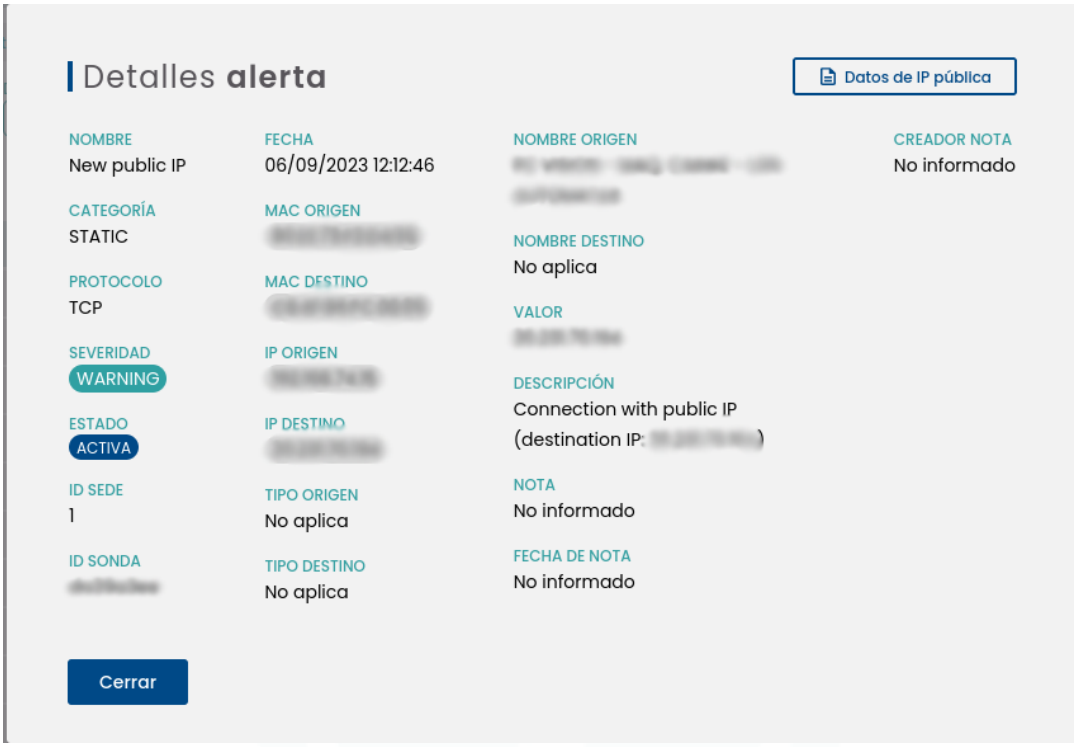
Ventana de creación de alertas

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”.

4.3.1 IP Públicas

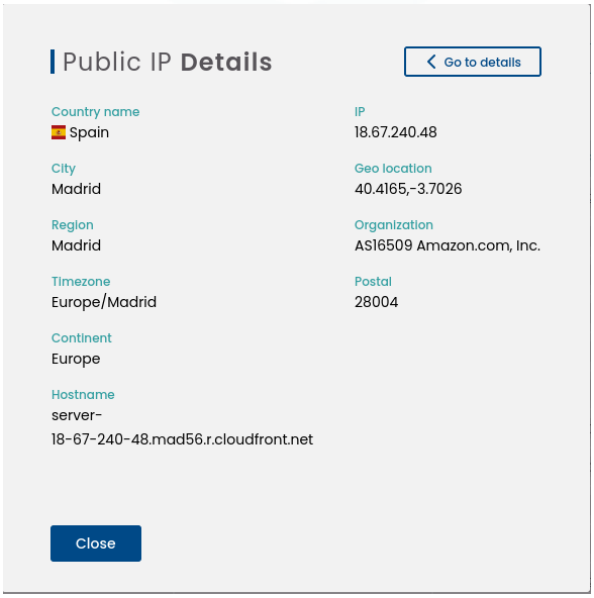
Esta alerta está conectada con un servicio de ciber inteligencia que permite obtener más información sobre el extremo de la comunicación fuera de la red confiable, para tratar de determinar si puede ser maliciosa.

Para acceder al detalle de la alerta, se hará clic en el icono del engranaje, que podemos ver en la parte derecha del panel. A continuación, pinchando en "Ver detalles", accederemos a esta información:



Pantalla con los detalles de alerta

En la parte superior de esta pestaña, podremos observar un botón llamado 'Datos de IP Pública'. Al hacer clic en este botón, se accede a la información adicional sobre la IP, que



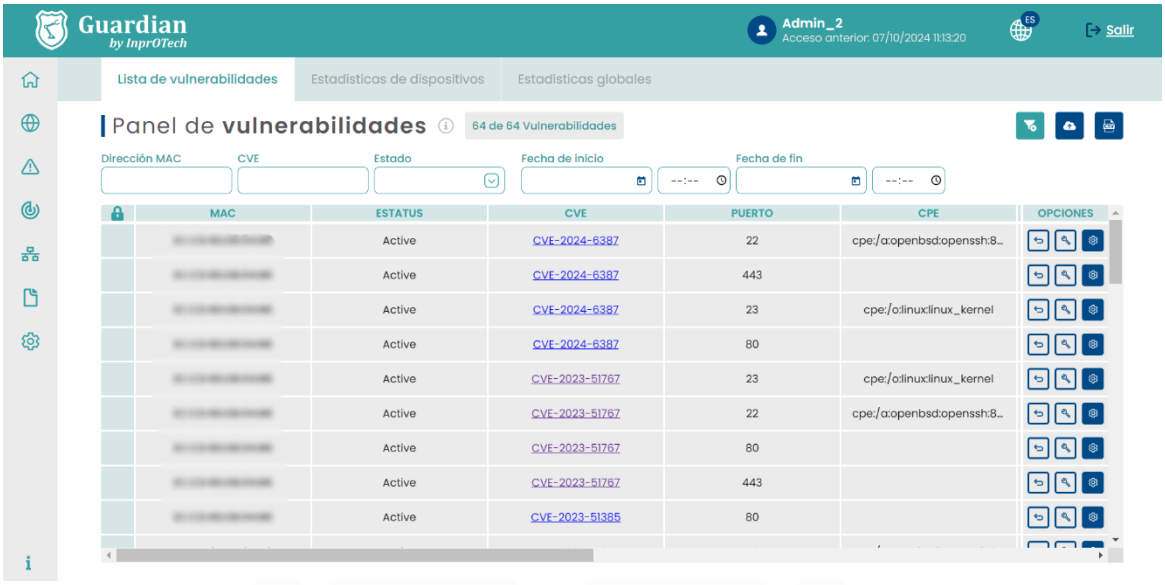
puede incluir detalles como la ciudad de origen, región, zona horaria, continente, nombre del país, dirección IP pública, coordenadas, organización y código postal.

Detalles de IP Pública

4.4 Análisis de vulnerabilidades

4.4.1 Panel de vulnerabilidades

Para acceder al panel de vulnerabilidades, el usuario deberá pulsar sobre el icono que aparece en la parte izquierda de la pantalla y seleccionar la pestaña "Panel de vulnerabilidades".



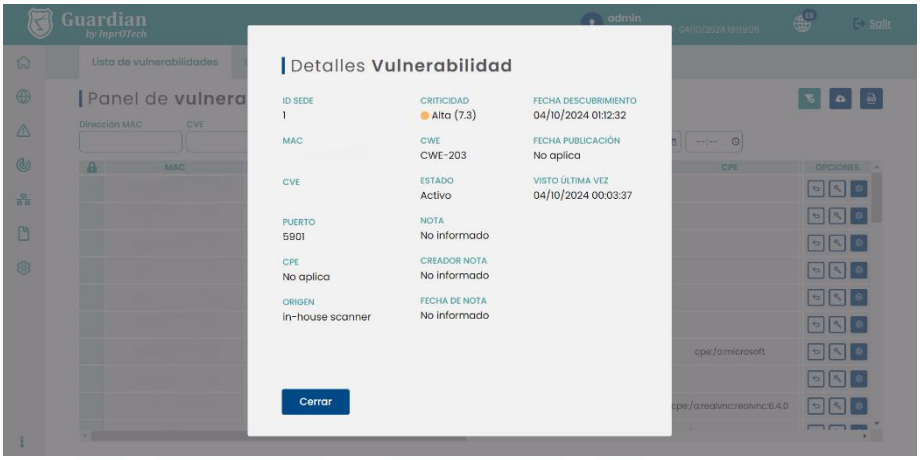
Vista del panel de vulnerabilidades

En la pestaña de panel de vulnerabilidades, el usuario podrá visualizar un listado con todas las vulnerabilidades que presenta la red. Estas son encontradas en los servicios detectados tras los puertos abiertos hallados por Smart View y comprobadas contra la base de datos de vulnerabilidades del NIST, la "*National Vulnerability Database* (NVD).

La información mostrada en cada fila es la siguiente:

- Dirección MAC: la dirección MAC del dispositivo en el que se ha detectado la vulnerabilidad.
- Estado: indica si la vulnerabilidad se encuentra activa, resuelta, silenciada o si ha sido un falso positivo.
- CVE: "Common Vulnerabilities and Exposures". Identificador según el glosario de clasificación de vulnerabilidades.
- Puerto: puerto del dispositivo.
- CPE: "Common Platform Enumeration". Identificador del producto o sistema afectado por la vulnerabilidad en cuestión.
- Fuente: sistema o dispositivo que ha encontrado la vulnerabilidad.
- Criticidad: puntuación del 0 al 10 asignada según el nivel de criticidad de la vulnerabilidad
- CWE: "Common Weakness Enumeration". Identificador de la debilidad común asociada a la vulnerabilidad encontrada.

- Fecha de descubrimiento: fecha en la que la vulnerabilidad se ha encontrado.
- Fecha de publicación: fecha en la que la vulnerabilidad con el CVE referenciado fue documentada en la base de datos de vulnerabilidades NVD.
- Visto última vez: marca de tiempo en la que se vio esta vulnerabilidad por última vez.
- Opciones (Acciones):
  - Ir a: permite ver alertas que ha generado esta vulnerabilidad, o bien los dispositivos en los que se presenta.
  - Cambiar estado (activa, resuelta, silenciada o falso positivo).
  - Otras acciones: permite ver los detalles de una vulnerabilidad y añadir una nota.



Detalles de una vulnerabilidad

Junto al encabezado, vemos el número de vulnerabilidades mostradas junto con el conteo total.

Número de vulnerabilidades y filtros

Vemos también en la imagen superior que existe la posibilidad de realizar un filtrado para que la pantalla muestre únicamente las vulnerabilidades deseadas. Este filtrado se puede realizar según:

- Dirección MAC
- CVE
- Estado
- Fecha (dd/mm/aaaa) y hora (hh:mm) de inicio
- Fecha (dd/mm/aaaa) y hora (hh:mm) de fin

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

Mediante el botón se podrá realizar una importación de un archivo con extensión ".csv" que contenga las vulnerabilidades que se desean añadir. Deben contener los

siguientes campos, manteniendo las fechas el formato YYY-MM-DDTHH:MM:SS.000GMT+XX:XX:

- ID de fábrica
- Dirección MAC
- CVE
- Puerto
- CPE (Opcional)
- Fuente
- Criticidad
- CWE (Opcional)
- Estado
- URL
- Nota (opcional)
- Nota del creador (opcional)
- Fecha encontrada
- Fecha publicada
- Fecha última vez visto

Por otro lado, mediante el botón  se realizará una exportación de un archivo en formato CSV del listado de dispositivos con su información.

4.4.2 Estadísticas de dispositivos

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 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

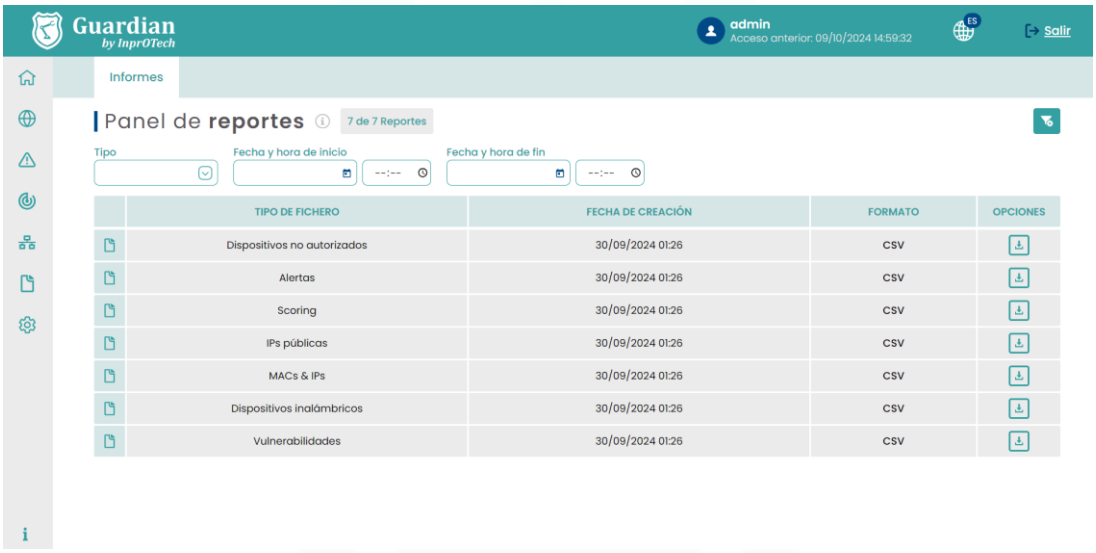
Se mostrará un listado con todas las comunicaciones que se han realizado entre los dispositivos OT de la red de la organización, e información acerca de ellas.

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.



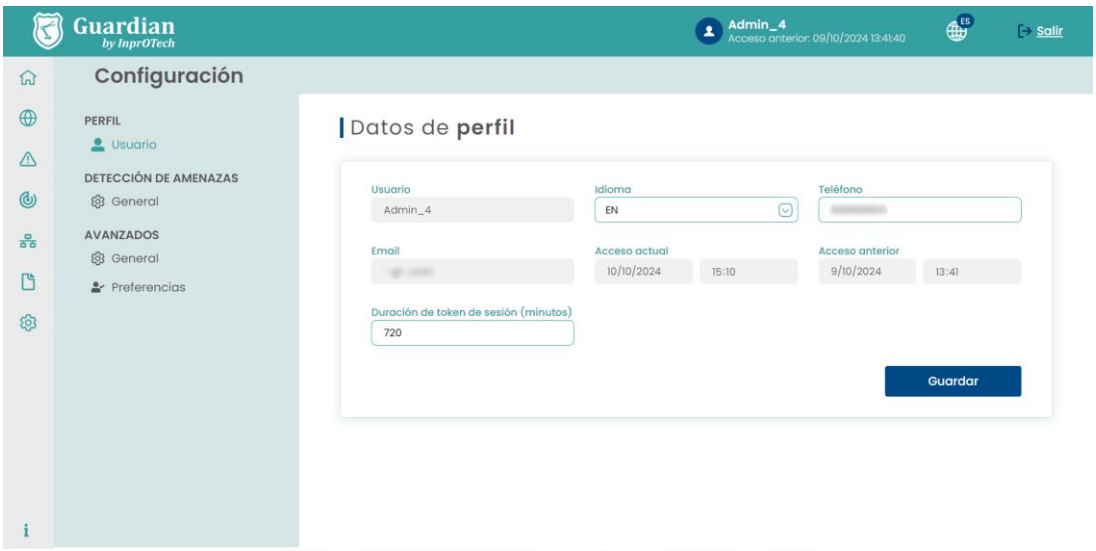
Acceso a últimos reportes disponibles

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 Otros ajustes

En Configuración, podemos parametrizar diferentes aspectos del servicio.

En el perfil de usuario, podremos ver toda la información asociada a la identidad con la que se accede al sistema. Algunos de los campos pueden ser editados, como son el idioma, el teléfono y la duración del token de sesión en minutos:



Pantalla de datos de perfil

En Detección de Amenazas, se presenta inicialmente el estado global de las diferentes estrategias de detección de anomalías en modo semáforo (rojo, naranja, verde):

Pantalla general de reglas y algoritmos

Amenazas basadas en reglas

- Rojo: todas las reglas están en modo training, inactive o alguno no contemplado en su campo status.
- Naranja: alguna de las reglas tiene el status producción, pero no todas ellas.
- Verde: todas las reglas están en modo producción.
- Gris: no existen reglas.

Amenazas basadas en IA/ML

- Rojo: todos los algoritmos están en modo training, inactive o alguno no contemplado en su campo status.
- Naranja: alguno de los algoritmos está en modo producción, pero no todos ellos.
- Verde: todos los algoritmos están en modo producción.
- Gris: no existen algoritmos.

Amenazas basadas en firmas

- Rojo: todos los elementos tienen un valor training, inactive o alguno no contemplado en su campo status.
- Naranja: alguno de los elementos tiene un valor diferente a active, pero no todos ellos.
- Verde: todos los elementos tienen un status igual a active y el campo signature_timestamp tiene una antigüedad inferior a siete días.
- Gris: no existen elementos.

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 y nivel Purdue

Por lo general, el modelo Purdue define los siguientes niveles para los dispositivos existentes:

Nivel 0: Dispositivos de campo, tales como sensores o actuadores.

Nivel 1: Controladores básicos, PLC, dispositivos I/O y 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 BBDD y MES. Control de planificación y producción en tiempo real.

Nivel 4: Dispositivos de gestiones empresariales como los ERP, CRM o 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
	TABLET	2
	TELÉFONO VOIP	2
	SERVIDOR	2

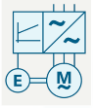
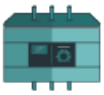
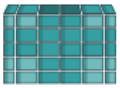
	TELÉFONO MÓVIL	2
	RTU	1
	CÁMARA V.A.	1
	LECTOR CODIGO BARRAS	1
	PLC	1
	ROBOT	0
	VARIADOR DE FRECUENCIA	0
	TARJETA CONTROLADORA	0
	SENSOR	0
	AFD	0
	SWITCH	Según ubicación
	ROUTER	Según ubicación
	FIREWALL	Según ubicación
	HONEYPOT	Según ubicación
	OTHER	Según ubicación

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)
	Alertas UEBA y Process Mining
	Alerta de Honeypot