

Manual de usuario InprOTech Guardian

Fecha: 07/2025

Referencia documento: IN-Manual de usuario InprOTech Guardian

Versión: 0.17

Este documento ha sido generado por **InprOTech** para uso exclusivo de **CLIENTE** y su contenido es confidencial. Este documento no puede ser difundido a terceros, ni utilizado para otros propósitos que los que han originado su entrega, sin el previo permiso escrito de **InprOTech**. En el caso de ser entregado en virtud de un contrato, su utilización y difusión estarán limitadas a lo expresamente autorizado en dicho contrato. **InprOTech** no podrá ser considerada responsable de eventuales errores u omisiones en la edición del documento.



INDICE

1	Intro	oducción	4				
2	2 Primeros pasos						
	2.1	Acceso a la consola web	5				
	2.2	Organización de lista de dispositivos	7				
	2.3	Configuración de reglas	8				
	2.4	Ajustes	10				
	2.5	Configuración de reportes	10				
	2.6	Dashboard continuo (opcional)	10				
	2.7	Exportación de alertas (opcional)	10				
	2.8	Escáner activo de dispositivos (opcional)	11				
	2.9	Análisis de dispositivos inalámbricos (opcional)	11				
	2.10	Licencias	11				
	2.11	Control de acceso y roles	12				
	2.12	Campos personalizables	12				
3	Guía	rápida	. 14				
	3.1	Ventana de accesos	14				
	3.2	Dashboard principal	15				
	3.3	Mapa de red	16				
	3.4	Lista de dispositivos	17				
	3.5	Panel de alertas	18				
	3.6	Lista de comunicaciones	19				
	3.7	Lista de informes	19				
	3.8	Ventana de ajuste de parámetros	22				
	3.8.1	Perfil de usuario	22				
	3.8.2	Seguridad	23				
	3.8.3	Notificaciones de alertas	24				
	3.9	Ayuda	25				
4	Man	ejo de aplicación web	.26				
	4.1	Dashboard principal	26				
	4.1.1	Resumen de activos	27				
	4.1.2	Accesos rápidos	27				
	4.1.3	Gráfico de tráfico de red	29				
	4.1.4	Gráfico de alertas	29				
	4.1.5	Últimos reportes	30				
	4.2	Mapa de red y lista de dispositivos	30				







	4.2.1	Mapa de red	.30
	4.2.2	Lista de dispositivos	.32
	4.3	Panel de alertas	.41
	4.3.1	IP Públicas	.44
	4.4	Análisis de vulnerabilidades	.48
	4.4.1	Panel de vulnerabilidades	.48
	4.4.2	Estadísticas de dispositivos	.50
	4.4.3	Estadísticas globales	.50
	4.5	Comunicaciones	.50
	4.6	Informes	.51
	4.7	Otros ajustes	.53
5	ANE	XO I: Clasificación de dispositivos y alarmas	54
	5.1	Clasificación de dispositivos	.54
	5.1.1	Según su estado	.54
	5.2	Clasificación de alarmas	.54
	5.2.1	Según su estado	.54
	5.2.2	Según su severidad	.55
6	ANE	XO II: Iconos representativos de dispositivos y nivel Purdue	56
7	ANE	XO III: Iconos representativos de tipos de alertas	58





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 <u>PURDUE</u>.
- 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).
- **Reputación de IPs públicas:** Las conexiones con direcciones IP públicas serán analizadas para comprobar la reputación de dicha dirección. En caso de determinar que es una IP listada como maliciosa, la alerta correspondiente quedará convenientemente resaltada en el panel.
- **Bloqueo de tráfico malicioso:** Posibilidad de, ante conexiones con direcciones IP públicas consideradas maliciosas, establecer estrategias para comunicarnos con el cortafuegos del sistema e incluir dicha dirección en una lista de IPs no permitida. Entre estas estrategias contamos con un modo informativo, donde solo informamos de la situación, uno manual, donde el propio usuario bloquea o desbloquea las conexiones, y uno automático, donde la comunicación con el firewall se realiza sin intervención humana (políticas manual y automática 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 <u>http://[IP]:9000</u>, 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 <u>PURDUE</u> 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".

S	Guar	dian aprOTech					0 *****		∰ [→ <u>Sali</u>
ណ	Mc	ıpa de red	Lista de dispositivos	Lista de inal	ámbricos				
•	Po	anel de	dispositivos	(i) 587 de 810) Dispositivos			6	+ Crear dispositivo
	Tod	nda os	Búsqueda general Texto libre	Тіро	G	Rol Nivel Purd	Dirección IP	Dirección MAC	Ver MACs virtuales Sí 🔵 No 🖲
6	Dispo Sí 🔵	sitivos fijados No 🔿 Todos	Dispositivos críticos Si No Todos e	Dispositivos a	utorizados Todos 💿				
*	8	ESTADO	NOMBRE	TIPO	NIVEL PURDUE	MAC	DIRECCIONES IP	SCORING	OPCIONES
Ľ	0.00	•00	100,1001,1001	HMI		10100-0010-0017	-		
ŝ		•00				10100-001-001-001-001	-		
		•00				10100-00140-00140	1000		
	N [54	•••	100,1000,1000	НМІ		10100-00-00-70-70	10000		
		•00	Institute_101	Other		10100-0010-0114	100.00		
		00				10.00.00.00.00.0	No. of Lot, No. of		
		000				MORE REPORTED	No.		
	<	••••							

Pantalla de listado de dispositivos

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

count rewall co	Work Parabut 4 Fase:CANTE Check Point Software Technologies D Stor ID Stor ID Sono A Rot No aptica	ISANO CONTROL CONTROL Ulas Jonatian Ulas Jonatian Escando Ulas	
ktma.comtx0n 4/06/2024 12:03:20 IPO Itewali	HIGH <u>Último Scoring</u> 27/05/2024 09:38:20		

Desplegable de detalles de dispositivo

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







Nivel Purdue	0
Crítico*	Autorizado*
Sí 🔿 No 🖲	Sí No
	Nivel Purdue Nivel 4 Crítico* Si () No ()

Pantalla de editado de dispositivos

Y rellenar manualmente los campos de nombre de dispositivo, nivel <u>PURDUE</u> 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 (a), 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 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 ⁴²⁹ del menú izquierdo de la pantalla y pincharemos en Detección de Amenazas > General > Amenazas basadas en reglas, VER ESTADO.





3	Guardian		Adl	min eso anterior: 03/07/2025 12:20:00	[→ <u>Salir</u>
ធ	Configuración				
⊕ ∧	PERFIL	Estado general			
6	DETECCIÓN DE AMENAZAS	Estado de mecanismos de de	tección 🕕		
윪 ()		Amenazas basadas en reglas	Amenazas basadas en IA/ML	Amenazas basadas en firmas	
ø	 Beneral Preferencias 	VER ESTADO	VER ESTADO	VER ESTADO	

Pantalla de estados mecanismos de detección

Motor de reglas 🕕 GReglas								
	NOMBRE	ESTADO	UMBRALES	ACCIONES				
۲	NuevoDispositivo	Production	1 (1)	L				
۲	NuevaConexion	Production	1 (j)	Z				
۲	AnomaliaEnPuerto	Production	1 (i)	L				
۲	IPpublica	Production	1 (j)	Z				
۲	Fingerprinting	Production	5-3-3 🚯	L				
۲	AtaqueARP	Production	1 (j)	L				

Pantalla motor de reglas

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

UMBRALES	ACCIONES
1 (j)	L
5-3-3 (i)	L
1 (j)	Z

Pantalla de umbrales

En la columna de acciones podremos editar estos parámetros.







	Production
Editar reala	
, Louison , Cogica	
Umbrai	
1	
Estado	
Producción	
* Campos obligatorios	
Cancelar	Guardar

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.

Si al iniciar sesión aparece el mensaje **"Error de licencia. Contacte con soporte."**, significa que los archivos de licencia no se encuentran o la licencia ha expirado.











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".













3 Guía rápida

3.1 Ventana de accesos

K	Guardian	
ណ៍	Inicio	
	Red	
	Alertas	
@	Vulnerabilidades	
器	Comunicaciones	
ß	Informes	
තු	Ajustes	
i	Ayuda	
Detalle d	le 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

K	Guardian			Admin_2 Acceso anterior: 08/10/2024 16:15:00	⊕ <u>Salir</u>
ធ	Bienvenido Admin_2	2		Dispositiv	os no autorizados 737
	Resumen de activos h	nardware i VER TODO	Tráfico de red 🔅	Última actualización 9 oct 2024 10:38	C ⁴ VER DETALLE
	Nivel Purdue sin asignar	*	10 MB	TX RX	• TX -7d • RX -7d
@			5 MB		
器	10 PLC 32 HMI 514 NI	31 Otro	0 MB 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	00 06:00 08:00 10:00
ß		*	Alertas 🔅	Última actualización 9 oct 2024 10:	38 C ⁴ VER TODO
礅	Accesos rápidos				
	7 Algoritmos activos	+99 Alertas	0		
	VER LISTADO	VER LISTADO	Últimos reportes (i)		VER TODO
	6 Reglas activas	64 Vulnerabilidades activas	24/09/2024 02:58:00 24/09/2024 02:58:00	report_UnauthorizedDevices_2024	40924T0058.csv
i	VERLISTADO	VER LISTADO	24/09/2024 02:58:00	report_MACs_IPs_20240924T0056	3.csv

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 <u>PURDUE</u>.

En el primer caso, tenemos lo siguiente:

T	Guardian						Admin_4 Acceso anterior: 0	13/10/2024 12:38:20	⊕	[→ <u>Salir</u>
ភ	Mapa de red	Lista de dispositiv	ros Lista de inc	alámbricos						
\oplus	Mapa de	e red i Actua	lizado: 09/10/2024 10:	41					7	Q Ver
≙	IDs Sonda Todos	Fecha y hora 9/10/2024	10:41 O	Topología de re Estándar	d Protocolo	Direc	cción IP	Puerto	Ver MACs virtua Sí 🔿 No 💿	les
٩	-		_	-	-	-	-			
-	2	2		2	2	?	2			-
Ľ			1000 (000 Here)	1						
Ø				-						
				_						
				ţ						
				?						
i										સ્વર

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 <u>PURDUE</u> 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).







3	Guardian by InprOTech				Admin_4 Acceso anterio			[→ <u>Salir</u>
ົລ	Mapa de red	Lista de dispositivos 🛛 Lista de inald	imbricos					
Ð	Mapa de	red (i) Actualizado: 09/10/2024 10:41					6	Q Ver
	IDs Sonda Todos	Fecha y hora	Topologia de red Purdue	Protocolo	Dirección IP	Puerto	Ver MACs virtual Si O No 🖲	les
6								
80	Nivel 2			Warnings	Nivel 2			~
<mark>ت</mark>				Severidad de	e warnings ALTA (con niv de tipo Sen en nivel PURD	el sin asignar) ridor en nivel PURDUE 2 est UE sin asignar , Normalmi	tá comunicándose c	on el
\$	and the second	altera altera intera		permiten sol	o entre niveles adyacentes			
	Nivel 1			Warnings	Nivel 1			^
			_	Severidad de	e warnings BAJA			~
	-		1.1	Warnings	Nivel sin asignar			^
	Nivel O			Severidad de	ə warnings BAJA			~

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	Guar	dian					Admin_4		. 🗳 🗗
ì	M	apa de red	Lista de dispositivos	Lista de inal	ámbricos				
Ð	Po	anel d	e dispositivos	(i) 359 de 69	5 Dispositivos			™ 🗛 🖶	+ Crear dispositivo
2	IDs Sc Tod	inda los	Búsqueda general	Тіро	C	Rol Nivel Purd	ue Dirección IP	Dirección MAC	Ver MACs virtuales
)	Dispo SI ()	sitivos fijado No 🔿 Toc	s Dispositivos críticos los Si No Todos	Dispositivos a	utorizados Todos 💿				
5	8	ESTADO	NOMBRE	TIPO	NIVEL PURDUE	MAC	DIRECCIONES IP	scol	RING OPCIONES
i i		000				000000000000		LO	w De
		•00				10102-0017-00140		+ 1 LO	w Dot
		000				1010-1010-00-00	-	LO	w Dom
		•00	a suprementaria	Other	2	10.0017/00170.00		MED	IUM 🖹 🕤 🗊
			Toposition 1	Other	2	-	-	MED	UM 6 50
								MED	
		•00						WILD	
	83 AG	•00 ••0	Name and a real and a subscription of the local division of the lo	Server	2			+515 MED	

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).

T	Guar	dian					Admin_4 Acceso anterior: 03/10		(→ <u>s</u>
3	Po	inel de alerta	IS						
,	P	anel de	alertas 🕕 🎹	566 de 117566 Alertas				5	+ Crear alerta
	IDs Se Too	los I	Búsqueda general	Dirección IP	Dirección MAC	Fecha y horo	a de inicio	Fecha y hora de fin	• ·-: O
	Seve	idad I	Categoria	Ver resueltas Si No O Todos	Ver silenciadas Si No Too	los			
		SEVERIDAD	NOMBRE	MAC ORIGEN	MAC DESTINO	IP ORIGEN	IP DESTINO	FECHA	OPCIONES
	-	EMERGENCY	Possible ARP spoofing	10.00101110	****	-	SCHOOL SECTION.	09/10/2024 13:08	
	-	EMERGENCY	Possible ARP spoofing	And the second second	****	And Address of California	-	09/10/2024 13:07	
	-	EMERGENCY	Possible ARP spoofing	101003-010	******	1000	-	09/10/2024 13:07	· · ·
	-	WARNING	New connection	-	*****	-	-	09/10/2024 13:07	
	-	WARNING	New public IP	maintener	-	-	-	09/10/2024 13:07	
	-	EMERGENCY	Possible ARP spoofing	-	-	-	-	09/10/2024 13:05	a a a
	-	EMERGENCY	Possible ARP spoofing	-	****	-	-	09/10/2024 13:04	
	-	EMERGENCY	Possible ARP spoofing		-	-	-	09/10/2024 13:02	

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.

Guard	lian ^{roTech}				Acceso anterior: 07/10/2024 10:43:06	6 F	→ <u>Salir</u>
Com	nunicaciones						
Pai	nel de comu	inicaciones 🔅 💈	2 de 22 Conexiones			8	•
IDs Sono Todos	Direcc	ión IP Dirección MAC	Puerto	Protocolo			
	MAC ORIGEN	MAC DESTINO	IP ORIGEN	IP DESTINO	PUERTO DESTINO	PROTOCOLO	-
	MATTERATOR	No. of Concession, Name	April 10	Statistics.	53	UDP	
.0 0	BUTTORIES.	MARK TRANSPORT	And states of the local division of the loca	A.BORNER	137	TCP	
	100-107-102-00-102-102	Marco Contractorio del	And the Party of t	S. BALLAND	137	UDP	
888	10000-0000-000-00	Man with Market	And and a second s	Simon a	137	UDP	
8%	-	Man Concession of Concession o	Advance:	ADDRESS OF	53	UDP	
00	800702-0010	And the second second	And the Party of t	STREET, ST	53	UDP	
	101210-0012	1012102-00108	Statistics.	Station of	5353	UDP	
58	-	1000-100-00-00	sources.	Statistics.	53	UDP	
28	-	Manufacture of Concerning of	Name and Address of Concerning	10000	5353	GRE	
	Guard by Inp Corr Do Sone Todos So So So So So So So So So So So So So	Guardian by InproTech Comunicaciones Panel de comu De Sonde Todos Office MAC ORIGEN	Guardian by Inprotection Comunicaciones Panel de comunicaciones () 2 Tos Sonda Dirección IP Dirección IP Dirección MAC MAC ORIGEN MAC DESTINO S S S S S S S S S S S S S	Guardian by Inprotects Comunicaciones Panel de comunicaciones Ibs Sonda Dirección IP Dirección IP MAC ORIGEN MAC ORIGEN <th>Guardian by Inprotects Comunicaciones Panel de comunicaciones Ibs Sonda Dirección IP Dirección MAC Puerto Protocolo MAC ORIGEN MAC ORIGEN MAC DESTINO IP ORIGEN IP ORIGEN</th> <th>Mac ORIGEN Vierto Protocolo Mac ORIGEN IP ORIGEN IP ORIGEN IP DESTINO PUERTO DESTINO Mac ORIGEN Mac DESTINO IP ORIGEN IP ORIGEN IP ORIGEN IP ORIGEN Mac ORIGEN Mac DESTINO IP ORIGEN <</th> <th>Comunicaciones Panel de comunicaciones Dirección IP Dirección MAC Puerto NAC ORIGEN MAC DESTINO IP ORIGEN IP ORIGEN MAC ORIGEN MAC DESTINO IP ORIGEN IP ORIGEN IP ORIGEN IP ORIGEN MAC ORIGEN MAC DESTINO IP ORIGEN IP ORIGEN IP ORIGEN IP ORIGEN</th>	Guardian by Inprotects Comunicaciones Panel de comunicaciones Ibs Sonda Dirección IP Dirección MAC Puerto Protocolo MAC ORIGEN MAC ORIGEN MAC DESTINO IP ORIGEN IP ORIGEN	Mac ORIGEN Vierto Protocolo Mac ORIGEN IP ORIGEN IP ORIGEN IP DESTINO PUERTO DESTINO Mac ORIGEN Mac DESTINO IP ORIGEN IP ORIGEN IP ORIGEN IP ORIGEN Mac ORIGEN Mac DESTINO IP ORIGEN <	Comunicaciones Panel de comunicaciones Dirección IP Dirección MAC Puerto NAC ORIGEN MAC DESTINO IP ORIGEN IP ORIGEN MAC ORIGEN MAC DESTINO IP ORIGEN IP ORIGEN IP ORIGEN IP ORIGEN MAC ORIGEN MAC DESTINO IP ORIGEN IP ORIGEN IP ORIGEN IP ORIGEN

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":
 - \circ Nombre
 - o MAC
 - Fabricante





- Rol 0
- Fecha de descubrimiento 0
- IPs 0
- **Nivel Purdue** 0
- Solucionado (S/N) 0
- Crítico (S/N) 0
- Tipo de dispositivo 0
- Puntuación y su registro de tiempo 0
- Scan status y último escaneo 0
- N.º de riesgo de vulnerabilidad 0
- Etiqueta de riesgo de vulnerabilidad 0
- SO 0
- Bloqueado (Permitido / No permitido) 0
- Campo personalizable (desglosando cada campo en columnas) 0
- Informe de alertas detectadas:
 - Título informativo de la alerta 0
 - 0 Categoría
 - Severidad 0
 - Silenciada 0
 - Resuelta 0
 - Valor 0
 - IP origen 0
 - MAC origen 0
 - IP destino 0
 - MAC destino 0
 - Protocolo 0
 - Fecha 0
 - Ubicación (Ciudad / Continente / País / Latitud / Longitud...) 0
 - Nombre del anfitrión 0
 - 0 IP
 - Dispositivo origen (nombre/tipo) 0
 - Dispositivo destino (nombre/tipo) 0
 - 0 Creador
- Relación MAC-IP
 - MAC
 - Fabricante 0
 - o IP
 - Pública 0
 - 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
 - o Puntuación individual
 - Fecha de puntuación 0
 - o Puntuación global de fabrica
 - Puntuación global de cloud 0
 - Dispositivos inalámbricos
 - o IP
 - MAC 0

C/ María Berdiales, 20 4ª planta 36203 Vigo, España .Tlfn: (+34) 886113106







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





S	Guardian	n ^{ch}	Admir Lost oc	0_2 cess: 04/10/2024 10:46:40 ⊕	[→ <u>Log Out</u>
ធ	Reports				
\oplus	Repor	ts panel (1) 7 of 7 Reports			~
	Туре	Start datetime End	i datetime		
Q		FILE TYPE	CREATION DATE	FORMAT	OPTIONS
格		Unauthorized devices	24/09/2024 02:58	CSV	٤
ß	ß	Alerts	24/09/2024 02:58	CSV	±.
53	ß	MACs & IPs	24/09/2024 02:58	CSV	<u>ٿ</u>
~	C	Scoring	24/09/2024 02:58	CSV	<u>ا</u>
	ß	Public IPs	24/09/2024 02:58	CSV	٤
	ß	Wireless devices	24/09/2024 02:58	CSV	<u>ا</u>
	Ľ	Vulnerabilities	24/09/2024 02:58	CSV	<u>ا</u>
i					

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.







K	Guardian			Admin Acceso an		B	[→ <u>Salir</u>
ណ	Configuración						
⊕ ∧	PERFIL	Datos de perfil					
٩	DETECCIÓN DE AMENAZAS ଷ୍ଟି General	<mark>Usuario</mark> Admin	Idloma ES		Teléfono 612345678		
** (*)	NETWORK Bloqueo AVANZADOS	Email user@test.com	Acceso actual 04/07/2025	02 : 21	Acceso anterior 04/07/2025	02:21	
礅	ĝ: General 삶 Preferencias	Duración de token de sesión (minutos) 720					
						Guardar	
i							

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).

C	Guardian		0	Admin Acceso anterior: 04/07/2025 02:21:40	B	(→ <u>Salir</u>
ណ	Configuración					
⊕ 	PERFIL	Preferencias de usuario				
٩	DETECCIÓN DE AMENAZAS හු General	Seguridad & MFA				
묾	NETWORK Bloqueo	Habilitado SI 🔵 No 🖲	Método Email			
۲ چ	AVANZADOS				Guardar	
	Preferencias	Notificaciones de alertas				
		Habilitado Sí 🖲 No 🔿	Método Email	Severidad mínima Notice		J
		Información detallada Verboso	Periodicidad Instantáneo	Reglas estáticas		
		IDS SI ● No ◯	IA/ML Sí ● No ◯	Honeypot Sí 🔵 No 🖲		
i					Guardar	

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:

Notificaciones de alertas

- 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.

Habilitado	Método	Severidad mínima
Sí 🔵 No 💿	Email	Notice
Información detallada	Periodicidad	Reglas estáticas
Verboso	Instantáneo	Sí
IDS	IA/ML	Honeypot
Sí No	Sí	Sí 🔵 No 🔵
		Guardar

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:

SG Soporte Guardian Para	$\textcircled{\textcircled{\baselineskip}{0.5ex} \textcircled{\baselineskip}{0.5ex} \xrightarrow{\baselineskip}{0.5ex} \xrightarrow{\baselineskip}{0.5ex} \overrightarrow{\baselineskip}{0.5ex} \overrightarrow{\baselineskip}{0.5ex} \overrightarrow{\baselineskip}{0.5ex} $
A new alert has been generated in the severity level system: emergency	
Creation date: 28/07/2023 20:34:42 +0000 Type: STATIC Name: Possible ARP spoofing Src MAC Dst MAC: Src IP: Dst IP: Value:	
Access the alert for its management in Guardian.	
Once managed, if applicable, proceed to silence or resolve it to avoid unne information, consult the alerts playbook or the user manual in the referen	ecessary noise. For more ice documentation.
Remember that you can modify your preferences for receiving notification and periodicity, from the user settings.	ns, their level of severity, format
InprOTech Guardian Support Team https://inprotech.es/	
Ejemplo de notificación de alerta individuo	al resumida

Sonorte Guardia	ensin	onnivonibre	rabrica										Besponder	() Responder a todos	-) Reenviar	45	
SG Para															mi 2	6/07/2023 1	(7)14
																	F
On 26/07/2023 15:13:50 +00	00, 50 ni	w alerts have bee	in generated in the	system in the last 24	hours.												
Summary:																	
Creation date	Туре	Name	Src MAC	Dst MAC	Src IP	Src Type	Dst IP	Dst Type 8	robe	Protocol	Description	Value					
19/10/2018 06:44:56 +0000	STATIC	New IP	2040/1644/60	en Principalitation	175,0811-00		175-18-1-12	S	onda1	6	New IP discovered	110-04-0.50					
19/10/2018 06:44:56 +0000	STATIC	New connection	Statistic Incoments	ec/Mileci/1011a	172.181.080		170.142.12	9	nda1	6	New connection discovered	1000					
19/10/2018 06:44:56 +0000	STATIC	New IP	0046-01-0-002	ec.7656.01186.54	275.08.5.00		101010-00	2	nda1	6	New IP discovered	170.08.6.40					
19/10/2018 06:44:56 +0000	STATIC	New connection	search in a debit	en hannen site de	210.000.000		175.56.3-65	5	onda1	6	New connection discovered	(868)					
19/10/2018 06:44:55 +0000	STATIC	New IP	1040/0-0-0-0-0	et. No. interior design	170.185.140		170.040.00	5	onda1	1	New IP discovered	170,000,000					
19/10/2018 06:44:56 +0000	STATIC	New connection	presenting and price	ecchildren of the La	175-2612-00		110.054.05	s	indal	1	New connection discovered	NA					
19/10/2018 06:44:56 +0000	STATIC	New IP	real months in	11.76 av. 77.86.14	210.061-00		170.063.03	9	onda1	6	New IP discovered	110,064-30					
19/10/2018 06:44:56 +0000	STATIC	New connection	And And And And And And	41 10 10 10 Total Table	101030-008		275.58.5.10	5	ondal	6	New connection discovered	1012					
19/10/2018 06:44:56 +0000	STATIC	New IP	method surface	and Performance of Street or	170.0816-88		171.064-02	5	onda1	6	New IP discovered	170.064.02					
19/10/2018 06:44:56 +0000	STATIC	New connection	Steas to united	and the local difference	175.183.00	0	17040108	5	onda1	6	New connection discovered	194					
19/10/2018 06:44:56 +0000	STATIC	New IP	man hourselfs	ec 76 log 27 30 ha	110.000		170.080.018	9	onda1	6	New IP discovered	170.068.015					
19/10/2018 06:44:56 +0000	STATIC	New connection	2010/5-24/6/5	and in case of the	270 284 280		170.0610.05	5	ondal	6	New connection discovered	200					
19/10/2018 06:44:56 +0000	STATIC	New device	******	0.0555.07				9	onda1	17	New device discovered	*****					
19/10/2018 06:44:56 +0000	STATIC	New IP	CONTRACT.	0.0.044.0	175-280-05		4000	5	onda1	17	New IP discovered	171194-0-01					
19/10/2018 06:44:56 +0000	STATIC	New IP	******	******	101.08.6.00		4552	5	ondal	17	New IP discovered	6008					
19/10/2018 06:44:56 +0000	STATIC	New connection	******	558665	175.00140		0.0.00	5	onda1	17	New connection discovered	582					
19/10/2018 06:44:56 +0000	STATIC	New IP	mentionedada	a transition of	2,75,217,21,14		175-18-1-18	S	ondal	6	New IP discovered	172-257 (80-08					
19/10/2018 06:44:56 +0000	STATIC	New connection	Manager and Party	in the same of the last	270.000.00.00		170.084.08	9	onda1	6	New connection discovered	191					
19/10/2018 06:44:56 +0000	STATIC	New public IP	101010-0010-0010	and the second second	10.00.00		Paintie	5	onda1	6	Connection with public IP (source IP:	151417-00-08					
19/10/2018 06:44:55 +0000	STATIC	New connection	Seale for purport	and the local division of	NIS / 11 - 10 - 10		10038412	9	onda1	6	New connection discovered	20					
19/10/2018 06:44:56 +0000	STATIC	New device	Personal States and Party	10.75 her (11.96 her				5	onda1	6	New device discovered	10107-04105					
19/10/2018 06:44:56 +0000	STATIC	New IP	POST OF STREET,	and the local day	STREET, STORE		100,084410	9	onda1	6	New IP discovered	100.007.02.14					
19/10/2018 06:44:56 +0000	STATIC	New device	di venis lo mero	the research the sec				5	ondal	6	New device discovered	PR 65-82.00 M(3)					
19/10/2018 06:44:56 +0000	STATIC	New IP	ALC: 12.01 all 10	the Patrice Children in	1010-2019 20-34		170.084.02	9	onda1	6	New IP discovered	170.007.00.00					
19/10/2018 06:44:55 +0000	STATIC	New device	50.00.00.00.00.00	No. No. of Concession, Name		1		5	mda1	6	New device discovered	THE R. D. LEWIS CO., LANSING MICH.					
19/10/2018 06:44:55 +0000	STATIC	New IP	MARK TO LODGE	and the latter of the latter of	10.000		171.063-00	9	onda1	6	New IP discovered	170.051-00					
19/10/2018 06:44:55 +0000	STATIC	New device	parallel in the Area	and the second second				5	onda1	6	New device discovered	au Phile 27 Belle					
an Inn Innan march an An Innan	Long to the local division of the local divi			1	· · · · · · · · · · · · · · · · · · ·	1		1			Annual State Annual						

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.





K	Guardian			Acceso anterior: 09/10/2024 14:59:32	S	[→ <u>Salir</u>
ធ	Documentación					
\oplus	Document	ación del ser	vicio			
	Documentació	. I C				
٩	de uso					
뢂	Ira					
5						
63						
i						
i						

Pantalla principal

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

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).





K	Guardian				Admin_4 Access ant	erior: 09/10/2024 13:41:40	E S	[→ Salir
ធ	Configuración							
•	PERFIL	Amenazas	basadas en I	A/ML				
<u>د</u>	DETECCIÓN DE AMENAZAS	Gestión de algo IDs Sonda	oritmos IA/ML Búsqueda general					
ß	 Ø General Preferencias 	Todos	ALGORITMO	ESTADO		ACCIONES		
鐐		¥ 📁	_anagram	Inactivo				
		Ŷ	deep-payload	Inactivo				
		w and	_autoencoder	Inactivo				
		¥	_isolation-forest	Inactivo				
		v	_ext-iforest	Inactivo				
i								

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).

K	Guardian			e	Admin_4 Acceso anterior: 09/10/2024 13:41:40	⊕ [→ Salir
ធ	Configuración					
⊕ ∡	PERFIL	Mot	or de reglas i Grega			8
ക	DETECCIÓN DE AMENAZAS		NOMBRE	ESTADO	UMBRALES	OPCIONES
		•	New device	Production	15 (i)	2
**	General	•	New connection	Production	15 (j.)	2
Ľ	🛓 Preferencias	•	Network port anomaly	Production	15 (i)	2
ŵ		•	New public IP	Production	15 (i)	2
		•	Possible fingerprinting	Production	5-3-3 (i)	2
		•	Possible ARP spoofing	Production	1 (j)	

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



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

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

K	Guardia	n _{ch}	admin Acceso anterior	r: 09/10/2024 14:59:32	s [→ <u>Salir</u>
ធ	Informes				
۲	Pane	de reportes (i) 7 de 7 Reportes			8
	Тіро	Fecha y hora de inicio	Fecha y hora de fin		
(TIPO DE FICHERO	FECHA DE CREACIÓN	FORMATO	OPCIONES
꾦	C	Dispositivos no autorizados	30/09/2024 01:26	CSV	Ł
Ľ	ß	Alertas	30/09/2024 01:26	CSV	±.
ഹ	Ľ	Scoring	30/09/2024 01:26	CSV	<u>الله</u>
~~	ß	IPs públicas	30/09/2024 01:26	CSV	<u>الله</u>
	ß	MACs & IPs	30/09/2024 01:26	CSV	Ł
		Dispositivos inalámbricos	30/09/2024 01:26	CSV	<u>الله</u>
	C	Vulnerabilidades	30/09/2024 01:26	CSV	٤
i					

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".

T	Guardian			(admin Acceso anterior: 09/10,	2024 14:59:32	₽	[→ <u>Salir</u>
ធ	Mapa de red	Lista de dispositivos Lis	ta de inalámbricos					
•	Mapa de	red (i) Actualizado: 10/10	/2024 15:50				6	Q, Ver
	IDs Sonda Todos	Fecha y hora	:50 O Estándar (Protocolo I	Dirección IP Pu	ierto	Ver MACs virtuales Sí () No ()	
6					/			
Ľ			-11					
©								
				C.				
		1	T	1				
		S.		-	-	-		
								0.0.11
i								स् स्







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".







3		dian					admin Acceso anterio	r: 09/10/2024 14:59:32	⊕ ^{ss} (→ <u>sa</u>
ລ	Mo	ipa de red	Lista de dispositivos	Lista de inală	mbricos				
Ð	Po	anel de	dispositivos	i 13 de 13 Disp	ositivos			5 4	+ Crear dispositivo
) 2	IDs So Tod Dispo Si	nda os sitivos fijados No 🔵 Todos	Búsqueda general Texto libre Dispositivos críticos S Sí No Todos @	Dispositivos aut	orizados odos 💿	Rol Nivel Purd	ue Dirección IP	Dirección MAC	Ver MACs virtuales
2	8	ESTADO	NOMBRE	TIPO	NIVEL	MAC	DIRECCIONES IP	SCORING	OPCIONES
5	51		2010	PLC	1	-	ALCOHOM 2	HIGH	8 - 6
3			102-04	PLC	1	-	STREET, ST	MEDIUM	
	-		140-10	PC	2		1000	+3 HIGH	
	2		Reason Providence	Robot	0	-	10.000	HIGH	
	•	000	Carrane IX	VA Camera	1	-	10000	LOW	
		000	100 miles - 12 milli	Sensor		-	Second Second		
		000	Annales (11)	Controller Card	0	-	10000	HIGH	
	-								

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:
 - o 🔋 : Botón para ver en detalle la información del dispositivo.





NOMBRE No informado	ROL No aplica
MAC	SCORING MEDIUM
última conexión 13/06/2023 13:40:00	ÚLTIMO SCORING 26/04/2023 13:58:20
TIPO No informado	ESTADO NO AUTORIZADO NO FIJADO NO CRITICO
No informado	IPs
FABRICANTE	DES MULTICO DESERSA DESERS ACTUES CONTRA DESERSA DESERSA MULTICOMULTICO
I ID SONDA	
digitifications.	

Ventana de información ampliada de dispositivo

o **Editor**: Botón para modificar parámetros del dispositivo.

Nombre		
And the second second		
Tipo	Nivel 4	
Fijado*	Crítico*	Autorizado
Si 🔿 No 🖲	Si 🔘 No 🖲	Si 🖲 No (
* Campos obligatorios		

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.

Panel de d	ispositivos 🔅	13 de 13 Dispositivos				▶ •	+ Crear dispositivo
Todos	Búsqueda general Texto libre	Tipo	Rol	Nivel Purdue	Dirección IP	Dirección MAC	Ver MACs virtuales
Dispositivos fijados Sí O No O Todos 💿	Dispositivos críticos Dis Sí O No O Todos O Sí	spositivos autorizados O No O Todos 🖲					

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:

MACT			+ Añadir IP
El campo es obligator	0		
Nombre			
Tipo			
El campo es obligator	0		
Rol	Nivel Purdu	10	
	El campo es o	obligatorio	
Fijado*	Crítico*	Autorizado*	
Sí No C El campo es obligatorio	Sí No Si El campo es obligatorio	Sí No El campo es obligatorio	
oongatorio	obligatorio	obligatorio	

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.

Dra	a and drop fi	les here	
DIG	or		
	Select a file	۵	

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):

IMPORTACIÓN DE DISPOSITIVOS	
Realmente desea in; Se recomienda realizar una copia de segu report_Public;	nportar nuevos dispositivos? Iridad de los dispositivos antes de la importación. _IPs_20231020T0945.csv
Cancelar	✔ Confirmar

Desplegable importación de dispositivos

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



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.

8	Error Line 3: MAC duplicated in database	×		8	Error Line 1: Invalid File Header	×
		Erro	or en importa	ación		









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: el dispositivo tiene la antena Wi-Fi encendida y se encuentra buscando puntos de acceso.
 - Intento de conexión: el dispositivo ha intentado conectarse a un punto de acceso.
 - Punto de acceso activo: el dispositivo ejerce la actividad de punto de acceso.
 - Transmitiendo datos: el dispositivo está enviando información a un punto de acceso.
 - Dispositivo visible: solo aplica a dispositivos bluetooth; el dispositivo tiene el bluetooth activado y esta visible para los demás dispositivos.
- **ID Wireless**: Nombre o identificador de la red WiFi (podría estar vacío en el caso de que, por ejemplo, la conexión fuese Bluetooth).
- Visto primera vez: formato dd/mm/aaaa hh:mm
- Visto última vez: formato dd/mm/aaaa hh:mm



C	Guar	dian					0 ****		tis g [→ Salir	
ធ	M	apa de red	Lista de dispositivos	Lista de inalámbricos						
•	Po	anel de i l	nalámbricos	(i) 277 of 277 Dispositivos	inalámbricos				₹ 🗎	
	Dis Sondo Nombre MAC Wireless Dia Viseless Tipo de conexión Actividad Fecha y hora de inicio Fecha y hora de línicio Fecha y									
٩		Disposit	ivos autorizados							
-				TIPO CONEXIÓN ¥		MAC ORIGEN ¥	MAC DESTING V		OPCIONES *	
C		•		Wi-Fi	Access Point	#1.00%#1#1.014	*****	Punto de acceso activo		
-		•		Wi-Fi	Access Point	10000000	******	Punto de acceso activo		
		•		Wi-Fi	Access Point	40,000,000,0014	******	Punto de acceso activo	8	
		•		Wi-Fi	Access Point	40,000,70,0004		Punto de acceso activo		
		•		Wi-Fi	Access Point	40.0016-0156-14	10 (0 (0 (0 (0 (0 (0 (0 (0 (0 (0 (0 (0 (0	Punto de acceso activo		
		•		Wi+Fi	Access Point	40,000,000,000,000	and the second second	Punto de acceso activo		
		•		Wi-Fi	Access Point	AC 2014-07-08-14	*****	Punto de acceso activo		
		•		Wi+Fi	Access Point	#C 3014-70-80.04	and the second second	Punto de acceso activo		
		•		Wi-Fi	Access Point	A. (1) A. (1) A. (4)		Punto de acceso activo		
4	4	-		117 P				A	· · · · · · ·	

Lista de dispositivos inalámbricos

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

Panel	de inalámbricos	i	134 of 134 Dispo	sitivos inalámbric	os						6
IDs Sonda Todos	Nombre		Wireless	ID Wireless	Tipo de conexión	\odot	Actividad	Fec	cha y hora de inicio	Fecha y hora de l	fin
:	Dispositivos autorizados Sí () No () Todos ()										

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).

G	uardian by InprOTech				cceso anterior: 16/12,	(2024 15:53:20	
		de dispositivos	Detalles Inalám	brico 🖉 Editor			
	Panel de ina	lámbricos	NOMBRE No disponible	ID SONDA			
	Todos		TIPO CONEXIÓN WI-FI	ID WIRELESS Xiaomi	na y nora de inicio		
		Todos ()	TIPO DISPOSITIVO Access Point	AUTORIZADO NO AUTORIZADO			
	NOMBRE ▼	TIPO CONEXIÓN 1	ACTIVIDAD	VISTO PRIMERA VEZ	CTIVIDAD ¥	ID WIRELESS ¥	
		Wi-Fi	Punto de acceso activo	12/12/2024 11:58:49	ess point active	Xiaomi	
		Wi-Fi	MAC ORIGEN	VISTO ÚLTIMA VEZ 16/12/2024 14:50:16	nsmitting data	Wildcard	
		Wi-Fi	MAC DESTINO		nsmitting data	Wildcard	
		Wi-Fi	and the second s		nsmitting data	Wildcard	
		Wi-Fi	CANAL 1		nsmitting data	Wildcard	
		Wi-Fi	ID SEDE		hing for networks	Wildcard	
		Wi-Fi	2		nsmitting data	Wildcard	
		Wi-Fi	_		nsmitting data	Wildcard	
		Wi-Fi	Cerrar		hing for networks	Wildcard	

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

	Guardian			admin Acceso anterior: 07/10/202	14 10:43:06 € S	alir
ŵ						
	Panel de	ind			₹ 🗎	
	IDe Sonda Todos (Fecha y hora de fin	Editar Inalámi	orico	Ir a detailes	a y hora de inicio	
		A-0			VISTO ÚLTIMA VEZ OPCIONES	
Ľ	itooth	spe Si No			04/10/2024 00:20	
	itooth	unk			03/10/2024 23:35	
		* Campos obligatorios				
		Cancelar		Guardar		
i	4				•	

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.

S	Guar	rdian					admin Acceso ante	rior: 09/10/2024 14:5	9:32	⊕ ^{ES} [→ <u>Salir</u>
ធ	M	apa de red	Lista de dispositivos	Lista de inalá	mbricos					
•	Po	anel de	dispositivos	(i) 13 de 13 Disp	ositivos			5 4	⊜ +	Crear dispositivo
 (1)	IDs Sc Tod Dispo Si	onda dos ositivos fijados No 🔵 Todos	Búsqueda general Texto libre Dispositivos críticos Sí No Todos (Dispositivos aut	orizados odos 💿	Rol Nivel Purd	ue Dirección IP	Dirección MAC		Ver MACs virtuales Si O No O
		ESTADO	NOMBRE	TIPO	NIVEL	MAC	DIRECCIONES IP	sc	ORING	OPCIONES
C	51		2010	PLC	1	-	ADDING:		HIGH	
ŝ			10.0-000	PLC	1	-	STREET, ST	м	EDIUM	
	-		144-18	PC	2		1000	+3	HIGH	
	2		Road Product	Robot	0	100000-000	and the second		HIGH	
	•	•00	Converse HX	VA Camera	1	-	100000		LOW	
		000	100-00-01-08	Sensor		10000000000000000000000000000000000000	Second Second			
		•00	Annales (11)	Controller Card	0	and the second second	-		HIGH	
-	-					1				

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.

OMBRE	ID SONDA	ESCANEO UDP
where is particular.	1000.p	53 - 123 -
MAC	ROL No aplica	5353 -
Ps	SCORING	ESCANEO TCP
0000	No aplica	80
	ÚLTIMO SCORING	139 -
2/01/2024 15:28:20	01/01/1970 01:00:00	443 -
100	ESTADO	445 - 631 - 980 -
Servidor		9090 -
NIVEL PURDUE	ÚLTIMO ESCANEO	
2	23/02/2024 03:38:20	
ABRICANTE unknown	ESTADO DEL ESCANEO	
D SEDE		

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 (4) que aparece en la parte izquierda de la pantalla.





	Guar	dian					Acceso anterior: 09/10		
3	Pa	nel de alerta	s						
)	Po	anel de	alertas 🕕 🔐	de 37 Alertas				8	+ Crear alerta
2	IDs So Tod	nda os (Búsqueda general	Dirección IP	Dirección MAC	Fecha y ho	a de inicio	Fecha y hora de fir	n
e	Sever	dad (Categoria	Ver resueltas Si O No O Todos (Ver silenciadas Sí O No O Todos	۲			
a a a a a a a a a a a a a a a a a a a		SEVERIDAD	NOMBRE	MAC ORIGEN	MAC DESTINO	IP ORIGEN	IP DESTINO	FECHA	OPCIONES
ב	-	WARNING	New public IP		(i)	And the Party of t	-	04/10/2024 00:29	
3	-0-	WARNING	Anomalia en tráfico net			-	Southern Street	04/10/2024 00:00	
	-	ALERT	Conexión con puerto IT			-	-	03/10/2024 23:19	
	B	WARNING	PROTOCOL-ICMP Echo R_		-		(and do not	03/10/2024 22:12	× < 0
	-	WARNING	New public IP		(i)	summer:	0.000	03/10/2024 21:23	A S
	Ø	WARNING	PROTOCOL-ICMP PING		-		[03/10/2024 21:17	
	-	EMERGENCY	Posible ARP spoofing		(i)	-	and the second second	03/10/2024 20:29	* • *
	-	NOTICE	Nueva conexión			And state	and the second	03/10/2024 20:24	

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.

NOMBRE Network port anomaly	FECHA 26/07/2023 10:34:45	NOMBRE ORIGEN	FECHA DE NOTA No informado
CATEGORIA	MAC ORIGEN	NOMBRE DESTINO	CREADOR NOTA
STATIC	Concernance of the local division of the loc	Marriella and an	No informada
PROTOCOLO	MAC DESTINO	(80/81/87)	
ARP		VALOR	
		https://0	
SEVERIDAD	IP ORIGEN	https://o	
ALERT	discount frage	DESCRIPCIÓN	
		Network port anomaly 0:	
ESTADO	IP DESTINO.	expected protocol => ICMP: found	
ACTIVA	CONTRACTOR OF THE OWNER.	> ODE 4	
ID SEDE	TIDO ODICEN	-> 2054	
1	HIPO OKIGEN	NOTA	
	No oplica	No informado	
ID SONDA	TIPO DESTINO		
and the laws	No aplica		

Ventana de información ampliada de alerta







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

Panel de o	alertas 🕕 🚳	482 de 34482 Alertas					7	🖗 🕂 Crear alerta
IDs Sonda Todos 🔍	Búsqueda general Texto libre	Dirección IP	Dirección MAC	Fecha y hora de inicio	Fecha y hora de fin	Severidad Categoria	Ver resueltos	Ver silenciadas Si O No O Todos 🖲

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:

Título*	Protocolo
	13
El campo es obligatorio	
IP Origen	Descripción*
	El campo es obligatorio
IP Destino	Severidad*
	El campo es obligatorio
MAC Origen	Fecha
MAC Destino	Categoría*
	El campo es obligatorio

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:

NOMBRE New public IP	FECHA 06/09/2023 12:12:46	NOMBRE ORIGEN	CREADOR NOT
CATEGORÍA STATIC PROTOCOLO TCP SEVERIDAD WARNING ESTADO	MAC ORIGEN MAC DESTINO IP ORIGEN IP DESTINO	NOMBRE DESTINO No aplica VALOR DESCRIPCIÓN Connection with public IP (destingtion IP:	
ID SEDE	TIPO ORIGEN No aplica	NOTA No informado	
ID SONDA	TIPO DESTINO No aplica	FECHA DE NOTA No informado	

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

Public IP Details	Co to details
Country name	IP 18.67.240.48
City Madrid	Geo location 40.4165,-3.7026
Region Madrid	Organization AS16509 Amazon.com, Inc.
Timezone Europe/Madrid	Postal 28004
Continent Europe	
Hostname server-	
18-67-240-48.mad56.r.cloudfront.net	
Close	







Detalles de IP Pública

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.

4.3.2 Reputación de IPs y Política de Bloqueo

Tras la recepción de una alerta de conexión con IP pública (*New public IP*), Guardian puede conectarse con una serie de listados públicos donde se reportan actividades consideradas abusivas (*spamming, hacking,* etc). La alerta se enriquece con esta información, visible en los detalles de IP pública, y en caso de detectar que la dirección pública involucrada tiene mala reputación, cambia la severidad, la descripción, y la marca en color rojo.

3	Gua	ardian y InprOTech					admin Acceso ani	terior: 11/06/2025 08:46:40	⊕ ^{ES} (→ Salir
ធ		Alertas							
•	Ð	Panel de a	lertas i 42 de 42 Alertas					6	+ Crear alerta
	IDs 1	Sonda Todos 🕞	Búsqueda general Texto libre	Dirección IP Direcció	ón MAC Fecha y hora dd/mm/yy	y D: O	Fecha y hora de fin dd/mm/yyyy 🝵: 💿	Severidad Cate	goría 🕞
٩	Ve	r resueltas	Ver silenciadas						
	51	SEVERIDAD V		MAC ORIGEN T		IP ORIGEN V		FECHA V	
ß	4	WARNING	New public IP	54 2636 30 DOMB	X (1745: 4 14 ()	1.74.841	378.4235	09/06/2025 09:09	
@	4	WARNINO	New public IP	SHOCK MADE	119 2412 C	(EVENUE)	1.757.8510	09/06/2025 09:09	
	-	EMERGENCY	New public IP	310600	106/0119	QUIE ((231.335	09/06/2025 09:09	
	-	EMERGENCY	Posible ARP spoofing	N 2690 X 06918 ()	X (145) 434 ()	8.008.0125	(4.540.540.4)	08/06/2025 09:09	× • •
	-	ALERT	Nuevo dispositivo	SKOCK MACH	X (145: 414 ()			08/06/2025 09:09	× • •
	-	NOTICE	Nueva conexión	N 26 26 26 26 36 36 36 36 36 36 36 36 36 36 36 36 36	1.3-31413-8 (i	0.2 × 3× P	(1.54CN-0.1)	08/06/2025 09:09	× • •

OMBRE	FECHA	NOMBRE ORIGEN	NOTA
New public IP	09/06/2025 09:09:53	No aplica	No disponible
CATEGORÍA	MAC ORIGEN	NOMBRE DESTINO	FECHA DE NOTA
STATIC	N. T. (027/2000)	No aplica	No disponible
PROTOCOLO	MAC DESTINO	VALOR	CREADOR NOTA
TCP	国际公司 (1)	<u>152 885</u>	No disponible
SEVERIDAD	IP ORIGEN	DESCRIPCIÓN	
EMERGENCY	100.8	Connection with public IP	
ESTADO	IP DESTINO	(destination IP: 💁 🚛 📪). Th	is
ACTIVA	00 7 D9 E*	IP has been listed as abusive	
ID SEDE	TIPO ORIGEN	and/or malicious. We	
1	No aplica	and from this IP.	
ID SONDA	TIPO DESTINO		
sonda	No aplica		



C/ María Berdiales, 20 4ª planta 36203 Vigo, España .Tlfn: (+34) 886113106





Nombre del país	Ubicación geográfica
🔵 Japan	345 38 DESCI
Ciudad	Organización
Osaka	All CARLON MOULD AND AN AN
Región	Secondary 1
Osaka	Código postal
Zona horaria	54:-000
Asia/Tokyo	Reputación
Continente	Bad IP
Asia	Fuente de reputación
Nombre de host	abuseipdb
2002.00F	
IP	
89.93	

El Chequeo de Reputación puede activarse y desactivarse en el menú de configuración , sección Network/Bloqueo. Esta opción afecta síncronamente a las alertas que entran, es decir, activar la reputación no afectará retroactivamente a aquellas alertas de IP pública que hayan entrado mientras la reputación estaba desactivada.

K	Guardian		admin Acceso anterior: 11/06/2025 08:46:40	(→ Salir
ណ	Configuración	1		
•	PERFIL	Bloqueo de tráfico		
ക	LUSUATIO DETECCIÓN DE AMENAZAS	Importar fichero Whitelist	Exportar fichero Whitelist Exportar	
뮮	General NETWORK	Chequeo de reputación y P	olítica de bloqueo	
۲ چ	Bloqueo AVANZADOS B General	Chequeo de reputación Habilitar 🔿 Deshabilitar 👁	Política de bloqueo Automático v	
	🛓 Preferencias		Manual Informativo Apagado	Guardar

Ante la recepción de una alerta de IP pública considerada maliciosa, Guardian permite responder aplicando una Política de Bloqueo de las tres disponibles:

-Informativa, donde se informa al usuario y se recomienda revisar y bloquear el tráfico de/hacia esa dirección.

-Manual o semidesatendida, donde se habilita un botón para

bloquear/desbloquear la IP maliciosa enviando al cortafuegos una instrucción para incluir dicha dirección en un filtro.

-Automático, donde se delega a Guardian el envío de esta instrucción al cortafuegos de forma desatendida.

Además, la Política de Bloqueo puede desactivarse. En este caso, toda la información relativa a la reputación de las direcciones en las alertas se desactivará, así como las reglas de bloqueo (vía envío de comando al cortafuegos para levantar la regla de bloqueo de direcciones). Esta información no se borra, y se volverá a aplicar si la





Política de Bloqueo vuelve a seleccionarse a un valor activo. En el mismo menú se puede encontrar un selector desplegable para la Política de Bloqueo. A las alertas de IP pública que llegan al sistema mientras la Política de Bloqueo está desactivada no se les realiza ningún cambio retroactivo al activarla de nuevo.

Las opciones automática y semidesatendida están actualmente en desarrollo.

4.3.3 Lista blanca de IPs

El usuario puede proporcionar al sistema una lista de direcciones IP (o también rangos de direcciones en formato CIDR) que funcionen como una lista de direcciones permitidas (lista blanca). A estas direcciones, en caso de llegar en una alerta de IP pública, no se les calculará la reputación aunque el chequeo esté activado, y solo se especificará en el menú de datos de IP pública que su reputación es *whitelist*.

El fichero de carga deberá tener formato *csv*, con una sola columna por fila, que tendrá que contener bien una dirección IP (*192.168.0.1*) o un rango CIDR (*192.168.1.0/24*). La carga se realiza de forma atómica: un único dato mal formateado o inválido anula toda la operación. Las posibles redundancias en la lista de direcciones y rangos (IPs repetidas, IPs contenidas en rangos CIDR, rangos CIDR superpuestos) no se consideran errores.

La importación se realizará en las opciones de bloqueo, a través de la pantalla desplegada tras presionar el botón mortar bajo la opción "*Importar fichero Whitelist*", que presentará la siguiente ventana emergente donde se podrá bien arrastrar el fichero a la caja verde, o bien encontrarlo en el árbol de ficheros del equipo.



Importaciones sucesivas sustiuirán completamente la lista blanca anterior. Así, si se desea no implementar ninguna lista blanca, se debe simplemente cargar un fichero vacío.







Cargar una nueva lista blanca tiene efectos en las alertas de IP públicas ya existentes en la base de datos:

- a aquellas alertas con IPs que tengan la reputación ya procesada con anterioridad, y que están incluídas en la nueva lista blanca, se les devuelve al estado original con el estado `reputation: Wlisted`.

- a aquellas alertas con IPs dentro de la lista blanca anterior, pero que quedan fuera de la nueva lista blanca, se les calcula la reputación y modifica la descripción de la alerta consecuentemente.

La lista blanca cargada se puede descargar para su examen presionando el botón Exportor, que descargará un fichero en formato csv con los datos guardados.

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".

K	Guar	'dian nprOTech		Admin_: Acceso an	2 iterior: 07/10/2024 11:13:20	€S [→ <u>Salir</u>	
ណ	Lis	ta de vulnerabilidades	Estadísticas de dispositivos	Estadísticas globales			
•	Po	anel de vulne r	abilidades 🔅 🚳	e 64 Vulnerabilidades			8
	Direct	CVE	Estado	Fecha de inicio	Fecha de fin	• : •	
6	6	MAC	ESTATUS	CVE	PUERTO	CPE	OPCIONES 🔺
몷			Active	CVE-2024-6387	22	cpe:/a:openbsd:openssh:8_	€ < ®
		10.000 00.000 00.000	Active	CVE-2024-6387	443		5 🔍 🛞
ß			Active	CVE-2024-6387	23	cpe:/o:linux:linux_kernel	5
ŝ		10.000 Million (10.000	Active	CVE-2024-6387	80		5
		10.000	Active	CVE-2023-51767	23	cpe:/o:linux:linux_kernel	5
		10.000	Active	CVE-2023-51767	22	cpe:/a:openbsd:openssh:8_	← < ®
			Active	CVE-2023-51767	80		5
		10.000	Active	CVE-2023-51767	443		to 🔍 🕘
			Active	CVE-2023-51385	80		5
i	4						· · · · · · · · · · · · · · · · · · ·

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.

T	Guardian			admin	- c4/10/2024 (359 06	🗳 🕞 Salir
	Lista de vulnerabilidades	Detalles Vu	Inerabilidad			
	Panel de vulnera	ID SEDE 1	Alto (7.3)	FECHA DESCUBRIMIENTO 04/10/2024 01:12:32		6
		MAC	CWE CWE-203	FECHA PUBLICACIÓN No aplica	a) ((0)	
	E MAL	CVE	ESTADO Activo	VISTO ÚLTIMA VEZ 04/10/2024 00:03:37	Gri	
ß		PUERTO 5901	NOTA No informado			
		CPE No aplica	CREADOR NOTA No informado			
		ORIGEN in-house scanner	FECHA DE NOTA No informado			
	The second s				cpet/ormicrosoft	
		Cerrar			ope:/azealvnczealvnc:6.4.0	
i				_		—— , *

Detalles de una vulnerabilidad

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

Panel de v	ulnerabilid	ades 🔅	64 de 64 Vulnerabilidades			6
Dirección MAC	CVE	Estado	Fecha de inicio	Fecha de fin	•: O	

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 el 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.





Gua	rdian			3	admin Acceso anterior: 09/10/2024 14:59:32	G	[→
c	Comunicaciones						
	anel de comui	nicaciones ()	22 de 22 Conexiones Puerto	Protocolo			5
	MAC ORIGEN	MAC DESTINO	IP ORIGEN	IP DESTINO	PUERTO DESTINO	PROTOCOLO	
88	500753300374	500753300396	0125425426	3125425428	53	UDP	
80	500753300374	500753300543	(825425426	3525425429	137	TCP	
80	500753300374	50:07:53:10:05:43	025425426	(825425429)	137	UDP	
5	500753300274	50:07:53:10:05:43	3125425428	(0.254,254,29)	137	UDP	
88	50.07.5330.02.73	500753100396	3125425424	3125425428	53	UDP	
88	500752300273	50:07:53:10:05:43	(025425424	3025425428	53	UDP	
80	500753300372	500753300294	32542542	(825425428	5353	UDP	
-	500753300872	500753100543	32542542	3125425429	53	UDP	
	00.0074.084814	00.40.45.08.FF.CC	82542542	(825425426	5353	GRE	

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.

Panel d	le comunica	ciones ① 2428	86 de 24286 Conexi	iones	
onda	Dirección IP	Dirección MAC	Puerto	Protocolo	
Todos					

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.

K	Guardia	an Tech	admin Acceso anterior	r: 09/10/2024 14:59:32	s) → <u>Salir</u>
ធ	Informe	35			
\oplus	Pane	el de reportes 🚯 7 de 7 Reportes			76
	Тіро	Fecha y hora de inicio	Fecha y hora de fin		
0		TIPO DE FICHERO	FECHA DE CREACIÓN	FORMATO	OPCIONES
器	ß	Dispositivos no autorizados	30/09/2024 01:26	CSV	Ł
ß	ß	Alertas	30/09/2024 01:26	CSV	±.
ന	ß	Scoring	30/09/2024 01:26	CSV	Ł
~~~	ß	IPs públicas	30/09/2024 01:26	CSV	Ł
	ß	MACs & IPs	30/09/2024 01:26	CSV	Ł
	Ľ	Dispositivos inalámbricos	30/09/2024 01:26	CSV	±.
	Ľ	Vulnerabilidades	30/09/2024 01:26	CSV	٤
i					

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:

T	Guardian by InprOTech			Admin Acceso an	terior: 04/07/2025 02:21:40	<b></b>	[→ <u>Salir</u>
ណ	Configuración						
•	PERFIL	Datos de <b>perfil</b>					
<u>دی</u>	<b>DETECCIÓN DE AMENAZAS</b> ැහි General	Usuario Admin	Idioma ES	$\odot$	Teléfono 612345678		
몲	NETWORK	Email user@test.com	Acceso actual	02:21	Acceso anterior 04/07/2025	02:21	
¢	AVANZADOS	Duración de token de sesión (minutos)					
	Y Preterencias					Guardar	
i							

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):

T	Guardian	▲ Admin Accesso anterior: 03/07/2025 122000 ● S	alir
ធ	Configuración		
⊕  & & & & & & &	PERFIL ▲ Usuario DETECCIÓN DE AMENAZAS ③ General METWORK ▲ Bloqueo AVANZADOS ③ General ▲ Preferencias	Estado general Estado de mecanismos de detección () Amenazas basadas en reglas VERESTADO VERESTADO VERESTADO VERESTADO	

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
	РС	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
7	LECTOR CODIGO BARRAS	1
•	PLC	1
3	ROBOT	0
	VARIADOR DE FRECUENCIA	0
	TARJETA CONTROLADORA	0
	SENSOR	0
	AFD	0
	SWITCH	Según ubicación
	ROUTER	Según ubicación
	FIREWALL	Según ubicación
働	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	
4	Alerta del IDS (sistema de detección de intrusiones)	
	Alertas UEBA y Process Mining	
	Alerta de Honeypot	

