

Manual de usuario InprOTech Guardian

Fecha: 07/2023

Referencia documento: IN-Manual de usuario InprOTech Guardian

Versión: 0.11

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 Introducción	4
2 Primeros pasos	5
2.1 Acceso a la consola web	5
2.2 Organización de lista de dispositivos	6
2.3 Configuración de reglas	7
2.4 Ajustes	9
2.5 Configuración de reportes	9
2.6 Dashboard continuo (opcional)	9
2.7 Exportación de alertas (opcional)	9
3 Guía rápida	10
3.1 Ventana de accesos	10
3.2 Dashboard principal	11
3.3 Mapa de red	12
3.4 Lista de dispositivos	13
3.5 Panel de alertas	14
3.6 Lista de vulnerabilidades	15
3.7 Lista de comunicaciones	15
3.8 Lista de informes	15
3.9 Ajustes	17
3.9.1 Datos de perfil	17
3.9.2 Seguridad	18
3.9.3 Notificaciones	19
3.10 Ayuda	20
4 Manejo de aplicación web	21
4.1 Dashboard principal	21
4.1.1 Resumen de activos	22
4.1.2 Accesos rápidos	22
4.1.3 Gráfico de tráfico de red	23
4.1.4 Gráfico de alertas	23
4.1.5 Últimos reportes	24
4.2 Mapa de red y lista de dispositivos	24
4.2.1 Mapa de red	24
4.2.2 Lista de dispositivos	26
4.3 Panel de alertas	29
4.4 Vulnerabilidades	31
4.5 Comunicaciones	31
4.6 Informes	32
4.7 Ajustes	32
5 ANEXO I: Clasificación de dispositivos y alarmas	32
5.1 Clasificación de dispositivos	32
5.1.1 Según su estado	32
5.2 Clasificación de alarmas	33



5.2.1 Según su estado	33
5.2.2 Según su severidad	33
6 ANEXO II: Iconos representativos de dispositivos	34
7 ANEXO III: Iconos representativos de tipos de alertas	37



pág. 3



1 Introducción

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

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

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

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

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



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

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

2 Primeros pasos

2.1 Acceso a la consola web

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

	Login	¢
		=
InproTech		=
~		
	INICIAR SES	IÓN

Pantalla de acceso a InprOTech Guardian

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

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

El usuario podrá ser:

- **Admin Inprotech:** Tendrá acceso a toda la información presentada por la aplicación y podrá realizar las configuraciones que considere oportunas de algoritmos, Ids de fábrica, modos de producción, etc.
- **Admin Fábrica:** Acceso similar a el caso anterior, excepto a la parte especifica de configuración mencionada.



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

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



Pantalla de recuperación de contraseña

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

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

2.2 Organización de lista de dispositivos

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

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

Manual de usuario InprOTech Guardian



8	Guar	dian prOTech					Admin Último acceso: 1	/06/2023 09:30:00	⊕ ⁵⁾ [→ <u>salir</u>
ធ	M	apa de red	Lista de dispositivos						
•	P	anel de	dispositivos 🕕 73 de 1	9 Dispositivos				₹ @	+ Crear dispositivo
<u>ک</u> (ل) ه	IDs Sc Too Dispo	anda tos (isitivos fijados No () Todos	Nombre Fabricante Dispositivos críticos Dispositivo Si No Todos Si No C	a autorizados	Nivel Purdue DI	Irección IP Dirección MAC	Ver MACs virtuales SI O No ®		
*	A	ESTADO	NOMBRE	TIPO	NIVEL	MAC	DIRECCIONES IP	SCORING	OPCIONES
Ľ	-	•00	011101-010-0108	Firewall	4	00000000	+13	3 MEDIUM	
₽ _	80	•00	10001412-08	Servidor	2	#100##101	00000	нон	
	-	•00	101100 - 101100 - 101	Firewall	1	ALC: U.S. (1997)	0000	MEDIUM	3 - 8
-	5	•00	M000010	PLC	2	0.0010-0.0010-0.00		MEDIUM	8 0 8
		•00	And and the second seco	Otro	0	1000 00 00 m	0.0000	MEDIUM	
		•00	Andreader sales (Lorenzeed) Londer Recordsory	Otro	0	1000000	0.0000	LOW	8 0 8
		•00	Company Static Int	Otro	0	MACHINESS OF	0.0000	MEDIUM	
		•00	Contractor Western Sale on Spreasers	Otro	0	4000044	0.00000	MEDIUM	
		•00	solution was brought to state	Otro	0		0.000	2 MEDIUM	8 - 8

Pantalla de listado de dispositivos

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

lombre		
R000000-008		
Гіро	Nivel Purdue	
Freedor	Nivel 4	
ijado*	Critico*	Autorizado*
Sí 🔿 No 🖲	Sí 🔘 No 🖲	Sí 🖲 No 🔿
Campos obligatorios		

Pantalla de editado de dispositivos

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

Para hacer cambios masivos de manera más ágil, esta configuración anterior puede

realizarse directamente en la lista de activos pulsando el icono del candado . y aceptando en el pop-up de confirmación.

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

2.3 Configuración de reglas

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

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

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



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

Adicionalmente, podrán configurarse otros parámetros. Se detallará más adelante. Para

la configuración de estos rangos de tiempo, pulsaremos el botón izquierdo de la pantalla y pincharemos en Detección de Amenazas > General > Amenazas basadas en reglas, VER ESTADO.

Configuración						
PERFIL	Estado general					
DETECCIÓN DE AMENAZAS	Estado de mecanismos de detección (1)					
 Vulnerabilidades pasivo Vulnerabilidades activo 	Amenazas Am	nenazas sadas basadas				
AVANZADOS ଊ୍ରି General	en reglas en l <u>VER ESTADO</u> <u>VER ESTADO</u>	IA/ML en firmas <u>VER ESTADO</u>				
Preferencias						
Motor de reglas 🕚 GReglas						
NOMBRE	ESTADO	UMBRALES	ACCIONES			
NuevoDispositivo	Production	1 (j)	2			
NuevaConexion	Production	1 (1)	2			
AnomaliaEnPuerto	Production	1 (j)	2			
Ppublica	Production	1 🔅	2			
Fingerprinting	Production	5-3-3 (j)	2			
			_			

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

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

En la columna de acciones podremos editar estos parámetros.



Editar regla	
Umbral	
1	
Estado	
Producción	
* Campos obligatorios	
Capcelar	Guardar

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

2.4 Ajustes

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

2.5 Configuración de reportes

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

2.6 Dashboard continuo (opcional)

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

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

2.7 Exportación de alertas (opcional)

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

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

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



3 Guía rápida

3.1 Ventana de accesos

	T	InprOTec	h
	ធ	Inicio	С
		Red	٦
	∕∆	Alertas	4
a	4	Vulnerabilidades	
	뢂	Comunicaciones	
	Ľ	Informes	2
a	Û	Notificaciones	
	භ	Ajustes	
			1
			C
			e
			1
			3
			S
	i	Ayuda	

Detalle de ventana de accesos

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



- 7: Notificaciones: Menú de notificaciones del servicio (en construcción)
- 8: Ajustes: Ventana de ajuste de parámetros
- 9: Documentación de ayuda

3.2 Dashboard principal

3	Guardian by ImproTech	💽 Admin Access anteror 20/07/2023 8:00.40
ណ	Bienvenido Admin	Dispositivos no autorizados 🚳
•	Resumen de activos hardware 🛈 VER TODO	Tráfico de red () (Itro ectualescio.34 ja 2023 that () VER DETAILE
⊿	Nivel Purdue 4	12 M3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
a ()		9.M8 00 00
器	1Switch 1PC 2 Firewall 4 Otro	6 M3
C	Nivel Purdue 3	3 MB _ 0 0
ê Ļ		0 M3 1100 1200 1300 1400 1500 1600 1700 1800 1900 2000 2100 2200 2800 000 0100 0200 6800 0400 6500 0600 0700 0600 1000 1100
-	2 Servidor	Alertas 🕕
	Nivel Purdue 2	600 Maming Emergency Ale
		500
	Accesos rápidos	20 20
	3 Algoritmos +99 Alertas	100
	VER LISTADO	0 12 julio 13 julio 14 julio 15 julio 16 julio 17 julio 18 julio 19 julio 20 julio 21 julio 22 julio 23 julio 24 julio 26 julio 26 julio
		Últimos reportes 🛈 VIR TODO
	6 Reglas – Vulnerabilidades activas	24/07/2023 10 57.54
	VERLISTADO	24(0)/003 105754 (http://doi.org/10.1006/004/0000000000000000000000000000000
i		

Ventana explicativa del dashboard principal

Barra superior:

Tipo de sesión y fecha del anterior acceso

Cambio de idioma de la aplicación

Salir de la sesión iniciada

Contador de dispositivos no autorizados

Widget superior izquierdo:

Número de activos de la organización clasificados por modelo Purdue

Widget superior derecho:

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

Widget inferior izquierdo:

Accesos rápidos a listados

Vulnerabilidades activas (en construcción)



Widgets inferiores derechos:

Representación gráfica de número de alertas según su severidad

Acceso a lista de reportes generados

3.3 Mapa de red

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

En el primer caso, tenemos lo siguiente:



Ventana de mapa de red en vista clásica

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

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

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

Destacar que:

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

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



Guardian	Admin Uttimo occeso: 13/08/2023 09 30.00	🕒 🕞 Salir
Mapa de red Lista de dispositivos		
Mapa de red 🛈 Actualizado: 13/06/2023 15:51		S Q Ver
IDs Sonda Fecha y hora Topología de red Protocolo Dirección IP Puerto Ver MACS virtuales Todos () 13/6/2023 (2) 15:51 Purdue () () () () () () () () () () () () ()		
Nwi sh avgnar		
<u>.</u>	Warnings Nivel 4	^
Néwi O	Severidad de warnings ALTA (con nivel 2)	~
	Severidad de warnings BAJA	~
ma ma una ulla ma ma mia mia mia ala, ala, ala, una un	Warnings Nivel 2	^
Novel 1	Severidad de warnings ALTA (con nivel sin asignar)	~
	Severidad de warnings ALTA (con nivel 4)	~
THE TTE THE SHE SHE SHE SHE SHE	Severidad de warnings ALTA (con nivel 0)	~
Novel 2	Severidad de warnings MEDIA	~
	Warnings Nivel 1	~
	Severidad de warnings ALTA (con nivel 4)	~
NVVI J	Severidad de warnings BAJA	~
	Warnings Nivel 0	^
Novel 4	Severidad de warnings ALTA (con nivel 2)	~
	Warnings Nivel sin asignar	^
and and your ages	Severidad de warnings BAJA	~

Mapa de red en vista PURDUE

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

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

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

										-
3	Guard	dian mOTech					Admin Útimo d			⊕ ⁵⁵ [→ <u>Salir</u>
ស	Ma	ipa de red	Lista de dispositivos							
•	Po	nel d	e dispositivos 🕕 73 de 109 D	ispositivos					ৰ ⇒ +	Crear dispositivo
A du	Tode	nda os	Nombre Fabricante Dispositivos críticos	Tipo Rol Ni	ivel Purdue D	Irección IP Dirección MAC	Ver MACs virtuales SI 🔵 No 🖲			
	si 🔿	No O Tod		iodos 🖲						
55	8	ESTADO	NOMBRE	TIPO	NIVEL PURDUE	MAC	DIRECCIONES IP		SCORING	OPCIONES
C	-	•00	611/10/07A - 10AA	Firewall	4	00000000	0000	+133	MEDIUM	
≞ <u>∩</u>	80	•00	CONTRACT - HA	Servidor	2	#103#C00	00000	+5	HIGH	2 - 0
63		•00	101000 - 010100 Million	Firewall	1	40-10-10-10-10-10-10-10-10-10-10-10-10-10		•1	MEDIUM	3 - 8
-	5	•00	4000010	PLC	2	0.0010.0000.00		+5	MEDIUM	8 0 8
		•00	And and the second seco	Otro	0	1010 (0.000) A	0.0000		MEDIUM	
		•00	Andrease said Longard Longs	Otro	0	100000000	0.0000		LOW	8 0
		•00	And the second sec	Otro	0	BACKLOOP .	0.0000		MEDIUM	8 6 8
		•00	Contrabular Victory Sale (Array Contra	Otro	0	#000040	0.000000		MEDIUM	
		•00	and the second second	Otro	0	******	0.000	+2	MEDIUM	8 - 8

3.4 Lista de dispositivos

Ventana de listado de dispositivos



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

La siguiente fila, incluye los posibles filtros aplicables para quedarnos con los dispositivos de nuestro interés.

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

3.5 Panel de alertas

3	Guardian					Admin Acceso anterior: 22/07/2	023 010:00	D [→ <u>Salir</u>
ធ	Panel de alertas							
•	Panel de a	ilertas 🕕 3467 de 3467 Alertas					N 🔒 +	Crear alerta
	IDs Sonda	Búsqueda general Direc	Dirección MAC	Fecha y hora de inicio	Fecha y hora de fin	everidad Categoria		
a ()	Ver resueltas	Ver slienclodas						
~	Si 🔿 No 🔿 Todos 🖲	Si 🔿 No 🔿 Todos 🖲						
	SEVERIDAD	NOMBRE	MAC ORIGEN	MAC DESTINO	IP ORIGEN	IP DESTINO	FECHA	OPCIONES
3	I WARNING	Anomaly detected in netflow traffic			000000	00000	22/07/2023 05:04	
≞ <u>∩</u>	- WARNING	Anomaly detected in netflow traffic		0.0000	000000	00000	22/07/2023 02:11	× <
63	-	Anomaly detected in netflow traffic		i) di ni ili an tran	000000		22/07/2023 01:58	💌 🔍 🐵
-		Anomaly detected in netflow traffic			000000	000000	22/07/2023 01:35	··· • •
		Anomaly detected in netflow traffic			000000	000000	22/07/2023 01:07	* • •
		Anomaly detected in netflow traffic	and the second second	1	000000	00000	21/07/2023 22:57	· · ·
	-	Anomaly detected in netflow traffic)	000000		21/07/2023 21:50	
	-	Anomaly detected in netflow traffic		1	00000	00000	21/07/2023 21:50	
		Anomaly detected in netflow traffic	and the second second		000002	00000	21/07/2023 21:49	× < *
		Anomaly detected in netflow traffic	an operation of the second sec		903003	000000	21/07/2023 21:49	 N
		Anomaly detected in netflow traffic	iliaine en como		000000	00000	21/07/2023 21:34	· · ·
	-	Anomaly detected in netflow traffic	and the second s		000000		21/07/2023 21:34	
		Anomaly detected in netflow traffic			000000	000000	21/07/2023 21:32	
i	-	Anomaly detected in netflow traffic			0000000	000000	21/07/2023 21:32	

Ventana explicativa de listado de alertas

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

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

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

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

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

3.6 Lista de vulnerabilidades

(En construcción.

3.7 Lista de comunicaciones

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

3	Guardia	n _{reh}				Admin Otimo acceso 18	(08/2023 09:30:00 🌐 🕞 Salir
ណៈ	Comun	icaciones					
	Pane	el de comunicacio	nes 🕕 36028 de 36028 Conextones				1
	Todos	Dirección IP	Dirección MAC Puerto Proto	colo			
a ()///		MAC ORIGEN	MAC DESTINO	IP ORIGEN	IP DESTINO	PUERTO DESTINO	PROTOCOLO
ഷം	2%	0.00000000	0.0000000000	40101100	000000	0	ARP
0	22	******	100000	MONOTON D	000000	0	ARP
A 0	**	ALC: NO. OF CO.	0.0000000	Internation in the local distance in the loc	000000	5353	UDP
and The constraints	20	107108-0010	#1000000M	OCIMITATION IN CONTRACTOR OF C	201020	5353	UDP
- 6 8-1	***	1070804410	#100/00/00/00	00040300	000000	5355	UDP
	88	ACCORDING NO.	0.0000.00014	002042030	01000000	1900	UDP
	2%	1000000000	PAUL TOTAL	NUMERON OF	00000000000	1900	UDP
	56	REPORTED IN CO.	100000000	And the Person number of	800	0	
	20	0.7480.04710	10.00.00.00.00.00	And in case of the	000	5353	UDP
	282	411100-0010-001	0.0000000	And the little staff time?	0000	547	UDP
	-	10000	accession.	Manual Contract Cont	0000	5355	UDP
	20	101030-00110	CREEK CONTRACTOR	0000000	903033	53	UDP
	**	4110303040	COURSE OFFICE	00000000	000000	53	UDP
	88	ALCOHOLD NO.	CONTRACTOR OF TAXABLE PARTY.	0000000	803070	53	UDP
	28	0.7480.0010	4040000000	0000000	******	80	TCP

Ventana de listado de comunicaciones

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

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

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

3.8 Lista de informes

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

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

Manual de usuario InprOTech Guardian



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

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

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



8	Guardian		Admin Access anterior 28/07/2023 1106:40
ធ	Bienvenido Admin		Dispasitivos no autorizados (55)
•	Resumen de activos hardware 🕕 🛛 🛛 🛛 VERTODO	Tráfico de red 🕕	Última actualización 26 jul 2023 Ib41 C VER DETALLE
	Nivel Purdue 4	12 MB	0° °° 0° 0°
.		9 M8 - • • • • •	••
20	1 Switch 1 PC 2 Firewall 4 Otro	6 M8	
Ľ	Nivel Purdue 3	3 MB ••	
ê Ļ	1 0	D MH 11:00 12:00 13:00 16:00 16:00 17:00 18:00 18:00 20:00 21:00 22:00 23:00 00:00 0	11:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00
8	2 Servidor	Alertas 🛈	Útima actualización 28 jul 2023 Ib41 (2) VER TODO
	Nivel Purdue 2	600	Warning Emergency Alert
		500	
	Accesos rápidos	200	
	3 Algoritmos activos +99 Alertas		
	VERLISTADO	12 julio 13 julio 14 julio 15 julio 16 julio 17 julio 18 julio 19 julio 20 juli	io 21 julio 22 julio 23 julio 24 julio 25 julio 26 julio
		Últimos reportes 💿	VER TODO
	6 Reglas activas – Vulnerabilidades activas	24/07/2023 12:57:54 report_UnouthorizedDevices_2023072410858.csv	
	VERLISTADO	24/07/2023 155/54 report_unauthorizedDevices_0023072410858.pdf 24/07/2023 155/54 report_Alerts_2023072410858.cev	
i			

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:

3	InprOTec	h	Admin_Gu (itimo access	ardian x:16/05/2023 13:01:40	🗳 🕞 Salir					
ធ	Informes									
•	Panel de reportes Zapartes									
	Tipo	Formato Fecha y hora de inicio Fecha y hora de fin Image: Image								
A ()		TIPO DE FICHERO	FECHA DE CREACIÓN	FORMATO	OPCIONES					
**	0	Dispositivos no autorizados	08/05/2023 04:00	PDF	4					
C	D	Dispositivos no outorizados	08/05/2023 04:00	CSV	±					
A Ó	C	Alertas	08/05/2023 04:00	PDF	<u>a</u>					
an Aga	Ľ	Alertas	08/05/2023 04:00	CSV	<u>ه</u>					
8	D	MACS & IPs	08/05/2023 04:00	PDF	٨					
	0	MACS & IPs	08/05/2023 04:00	CSV	<u>له</u>					
	D	Scoring	08/05/2023 04:00	PDF	±					
	0	Scoring	08/05/2023 04:00	CSV	<u>ه</u>					
	13	IPs públicos	08/05/2023 04:00	PDF	<u>له</u>					
	0	IPs públicos	08/05/2023 04:00	CSV	<u>له</u>					
	0	KPIs	08/05/2023 04:00	PDF	<u>له</u>					

Vista del listado de reportes

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

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

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

3.9 Ajustes

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

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

3.9.1 Datos de perfil

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



0						Acceso anterior: 22/1			[→ Salir
00	Configuración								
⊕ ∡	PERFIL Usuario	Datos de perfil							
a (j)	B General	Nombre	idioma			Teléfono			_
*	🕼 Vulnerabilidades pasivo		63		0	60000003			
19	Vulnerabilidades activo	Email	Acceso actual 24/7/2023	10:30		Acceso anterior 22/7/2023	01:10		
₽ û	AVARZADOS ③ General ≵ Preferencias							Guardar	
i									

Vista de datos del perfil de usuario

3.9.2 Seguridad

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

5	Guardian			Admin Acceso anterior: 22/07/2023 0110:00	6	[→ Salir
ធ	Configuración					
⊕ ▲ ⊕ ()	PERFIL Usuario DETECCIÓN DE AMENAZAS Gi General	Exportación Máximos registros de exportación			50	
* C 4 () 8	Culterabilidades parto Vulnerabilidades activo AVANZADOS Ceneral Preferencias	Seguridad & MFA Notifitato SI ◯ No ®	Millode Ernoll		Guardar	•
		Notificaciones de alertas Hestituse 10 № ® Internación setatesta Resumen St 1 ® 10 0	Mitodo final C Netodicidad Instantione C N/ML zi ® No ()	seventad misima hotice Neglos extáticos si (8): no ()		Θ
i					Guardar	

Vista de datos de sección Seguridad & MFA

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

- Administrador InprOTech
- Administrador de planta
- Operador de planta

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



3.9.3 Notificaciones

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

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

El usuario por tanto podrá:

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

K	Guardian			Admin Accesso anterior: 22/07/2023 0110:00	÷	[→ Salir
ធ	Configuración					
⊕ ▲	PERFIL LUSUARIO DETECCIÓN DE AMENAZAS B General	Exportación Máximos registros de exportación			50	
# □ # ↓ ®	 Uninerabilidades pasivo Vuinerabilidades activo AVANZADOS General Preferencias 	Seguridad & MFA Hobilitada SI⊖ No®	Mélode Emol	-	Guardar	
		Notificaciones de alertas Hotimade 1 0 90 Hotomoción defatidad Recurren C 10 1 0 10	Milloda Email () Perilodicidad Instantanee () M/At. SI ® No ()	Severated minima Notice Region estations SIN No ()	Guardar	e

Vista de datos de sección Notificaciones de alertas

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

Importante:

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

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



Soporte Guardian Para $ \begin{array}{c c} \hline & & \\ \hline \\ \hline & & \\ \hline \\ \hline$
A new alert has been generated in the severity level system: emergency
Creation date: 28/07/2023 20:34:42 +0000 Type: STATIC Name: Possible ARP spoofing Src MAC Dst MAC: Src IP: Dst IP Value:
Access the alert for its management in Guardian.
Once managed, if applicable, proceed to silence or resolve it to avoid unnecessary noise. For more information, consult the alerts playbook or the user manual in the reference documentation.
Remember that you can modify your preferences for receiving notifications, their level of severity, format and periodicity, from the user settings.
InprOTech Guardian Support Team <u>https://inprotech.es/</u>

Formato de alerta individual resumida

Daily summary of ale	erts fro	om Nombre	Fabrica											
SG Soporte Guardia Para	n												③ ← Responder ≪ Responder a todos →	Reenviar 👪 mi. 26/07/2023 17:14
on 26/07/2023 15:11:50 +0000, 50 new alerts have been 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	Probe	Protocol	Description	Value]	
19/10/2018 06:44:56 +0000	STATIC	New IP	2010/16/24/6/5	activity of the late	175,281.00		170.04.0.02		sondal	6	New IP discovered	119-14-1.52		
19/10/2018 06:44:56 +0000	STATIC	New connection	sealing outputs	echten in de la	172.161.080		170.16.2.12		sonda1	6	New connection discovered	100]	
19/10/2018 06:44:56 +0000	STATIC	New IP	1046/00/00/00/0	40763a077865a	111.081.00		1000048		sonda1	6	New IP discovered	170.08.0.40		
19/10/2018 06:44:56 +0000	STATIC	New connection	seasify units to	ac 16/66/07/08/08	10.000.000		175.56.5.45		sondal	6	New connection discovered	100]	
19/10/2018 06:44:56 +0000	STATIC	New IP	3945/5 Julie 1	er. No. loss 275 Million	175.16.048		175.060.08		sonda1	1	New IP discovered	175,010,014]	
19/10/2018 06:44:56 +0000	STATIC	New connection	protection and the local division of the loc	e: 20.5e (21.0e (a))	175.08.0.40		170.004.00		sondal	1	New connection discovered	NA]	
19/10/2018 06:44:56 +0000	STATIC	New IP	read to switch a	00.7930e.775.06cm	170.081.00		175-10-1-15		sonda1	6	New IP discovered	100,083.00]	
19/10/2018 06:44:56 +0000	STATIC	New connection	NUMBER OF STREET	an inclusion of the last	170.04(1.00		270.06.0.10		sonda1	6	New connection discovered	192		
19/10/2018 06:44:56 +0000	STATIC	New IP	19485-79-24/075	and the local division of	171.083.48		179.0644.07		sonda1	6	New IP discovered	170.064.12		
19/10/2018 06:44:56 +0000	STATIC	New connection	personal resources on	an 100 km in 100 km	171.183.60		179-28-0.02		sonda1	6	New connection discovered	200		
19/10/2018 06:44:56 +0000	STATIC	New IP	man/soudars	ec 74 los 37 36 los	170,060.00		170.080.012		sonda1	6	New IP discovered	170.063.02		
19/10/2018 06:44:56 +0000	STATIC	New connection	perior banking	an Property States	170.080.00		175.06.0.03		sondal	6	New connection discovered	200		
19/10/2018 06:44:56 +0000	STATIC	New device	annaile.						sonda1	17	New device discovered	*****		
19/10/2018 06:44:56 +0000	STATIC	New IP		0.0.044	175,000,000		0.000	i	sonda1	17	New IP discovered	270.083-01		
19/10/2018 06:44:56 +0000	STATIC	New IP	******	******	110.085.01		1000		sonda1	17	New IP discovered	1000		
19/10/2018 06:44:56 +0000	STATIC	New connection	******	*****	175.08.040		#0.00	i	sonda1	17	New connection discovered	192		
19/10/2018 06:44:56 +0000	STATIC	New IP	to the second se	-	478.017.01.14	1	175-19-1-10	i	sondal	6	New IP discovered	170.237 (00.09)		
19/10/2018 06:44:56 +0000	STATIC	New connection	Section in public to	the local division of	170.008.00.04		100.084.08	i	sonda1	6	New connection discovered	182		
19/10/2018 06:44:56 +0000	STATIC	New public IP	NAME OF GROOM	and in case of the last	10.001-01.04		110-00-042		sonda1	6	Connection with public IP (source IP: 1000000000000000000000000000000000000	ATRACTOR OF		
19/10/2018 06:44:56 +0000	STATIC	New connection	No. and To purchase	and the local division of	1012.001.00.00		170.064.07		sonda1	6	New connection discovered	10		
19/10/2018 06:44:56 +0000	STATIC	New device	100003-0040-0010					i	sonda1	6	New device discovered	104070-0480		
19/10/2018 06:44:56 +0000	STATIC	New IP	Property and the		10000		100,000.000	i i	sonda1	6	New IP discovered	100.007.00.04		
19/10/2018 06:44:56 +0000	STATIC	New device	10 Co. 44 Street St.	1. The loss of the loss				i Ti	sonda1	6	New device discovered	2010/02/20 10:44:55		
19/10/2018 06:44:55 +0000	STATIC	New IP		ter Miller (* 18. ja	1170-217-22-34		170.04.02	i	sonda1	6	New IP discovered	178.007.00.08		
19/10/2018 06:44:55 +0000	STATIC	New device	1040-0140-0140-01	an Notes 11 Holds		i		i	sonda1	6	New device discovered	100003-0400		
19/10/2018 06:44:55 +0000	STATIC	New IP	10000-0010-0010-001	and the local division of	10000		175.36.3.10	i Tì	sonda1	6	New IP discovered	171.08.0.48		
19/10/2018 06:44:55 +0000	STATIC	New device	private in the last	-		i		i i	sonda1	6	New device discovered	es Philes (17 Berlin		
10/10/2010 05-54-55 40000	STATIC	Advance 10	summer the local division				_		rondal	6	New ID discovered	100.00.00	1	٠

Formato de resumen diario de alertas

3.10 **Ayuda**

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



E	Guardian		Admin Acceso anterior: 26/07/2023 II:06:40
ធ	Bienvenido Admin		Dispositivos no autorizados 65
•	Resumen de activos hardware 🛈 VER TODO	Tráfico de red	Última actualización 26 jul 2023 Tost C VER DETALLE
	Nivel Purdue 4	12 MB	
.		9 MB	
윦	1 Switch 1 PC 2 Firewall 4 Otro	6 MB	
Ľ	Nivel Purdue 3	3 MB - 00	
≞ ∴	i ()	0 MB 11:00 12:00 13:00 15:00 15:00 17:00 18:00 19:00 20:00 21:00 22:00 20:00	
8	2 Servidor	Alertas 🕕	Ottima actualización 28 jul 2023 11:41 (C) VER TODO
	Nivel Purdue 2	600	Warning Emergency Alert
		400	
	Accesos rápidos	300	
	3 Algoritmos activos VERLISTADO	100 0 - 12 julo 13 julo 14 julo 15 julo 16 julo 17 julo 18 julo 19 julo 20 j	juto 21 juto 22 juto 23 juto 24 juto 25 juto 26 juto
		Últimos reportes 🕕	VER TODO
	6 Regias – Vulnerabilidades activas	24/07/202310.87.84	
	VERUSTADO	24/07/2023105254 report_UnouthorizedDevices_2023072410555.pdf	
i		24/07/2023 10:57:54 report_Alerts_20230724T0858.csx	

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**



Dashboard principal



4.1.1 Resumen de activos

Resume	n de acti	VOS 🔅	
Nivel 04			
Router	9 PC	11 Teléfono	
Nivel 03			
0	Ċ		
12 HMI	2 SCADA	7 DCS	
Nivel 02			

Resumen de activos

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

4.1.2 Accesos rápidos



Accesos rápidos

4.1.2.1 Algoritmos Activos

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

4.1.2.2 Alertas Activas

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



4.1.2.3 Reglas Activas

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

4.1.2.4 Vulnerabilidades Activas

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

4.1.3 Gráfico de tráfico de red



Tráfico de red

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

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



4.1.4 Gráfico de alertas

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

8	Inp	rOTeo	ch	Admin_G Lost occess	uardian 18/04/2023 18:33:20	6	[→ Log_Out
ធ		Reports					
•	F	Repor	ts panel (i) 22 Reports				3
	Тур	96	Format Start datetime End datetime	B			
8			FILE TYPE	CREATION DATE	FORMAT		
*	C	3	Unauthorized devices	17/04/2023 03:30	PDF		4
ß	C	5	Unauthorized devices	17/04/2023 03:30	CSV		۵.
a n	C	5	Alerts	17/04/2023 03:30	PDF		<u>ه</u>
- 4	C	3	Alerts	17/04/2023 03:30	CSV		d.
\$	C	3	Scoring	17/04/2023 03:30	PDF		±
	C	3	Scoring	17/04/2023 03:30	CSV		<u>ه</u>
	C	3	Public IPs	17/04/2023 03:30	PDF		<u>الم</u>
	C	5	Public IPs	17/04/2023 03:30	CSV		<u>الله</u>

Acceso o	últimos	renortes	disne	nihles
ALLESU U	unumos	reportes	uispe	minues

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

Actualmente, los reportes generados con periodicidad semanal, son:

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

4.2 Mapa de red y lista de dispositivos

4.2.1 Mapa de red

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



Ventana de mapa de red





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

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

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



Dispositivo no autorizado

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



Información básica de dispositivo

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

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



InprOTech

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"

Mapa de r	d (i) Actualizado: 13/06/2023 15:	51		
	Fecha y hora	Topología de red Protocolo	Dirección IP Puerto	Ver M

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	Guar	dian wOTech								Admin Utimo acceso: 13/1	06/2023 09:30:00	÷	[→ <u>Salir</u>
ស	Mo	ipa de red	Lista de dispositivos										
•	Po	nel de	dispositivos 🕕	73 de 109 Dispositivos							₹ 👜	+ Crear d	Ispositivo
▲ ()	IDs So Tod Dispos Si ()	nda os l sittivos fijados No () Todos	Nombre Fab Dispositivos críticos Si O No O Todos O Si	ricante Tipo	C Rol	Nivel Pur	due Dirección IF	Dirección MAC	Ver MACs virtuales				
*	8	ESTADO	NOMBRE		TIPO	1	IIVEL JRDUE	MAC	DIREC	CIONES IP	SCORING		OPCIONES
ß	1001	•00	00000-008		Firewall		4	10000000		+133	MEDIUM	6	1 - 0
⊕ <u>∩</u>	80	•00	10001000-00		Servidor		2	#100 Back (0.1)	-		HIGH		1 - 0
63	-	00	100.000 - 000.000 M		Firewall		1	ALC: U.S. (1997)		-1	MEDIUM		1 - 8
-	51	•00	100000		PLC		2	0.00100000000		-1	MEDIUM		1 - 0
		•00	manager colle becaused		Otro		0	101010-0010-00			MEDIUM		1 🕤 🛛
		•00	Andreastic states (a second of)		Otro		0	100000000000	-		LOW		1 - 8
		00	Contractor Marine 198		Otro		0	000000000	-		MEDIUM		1 - 8
		•00	Contradic Victory Sale (1979)		Otro		0	#1000 Million	-		MEDIUM	6	1 - 0
		•00	solution was broad as	-	Otro		0			+2	MEDIUM		

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
 - o El primero de los círculos indicará si el dispositivo está autorizado (color verde) o no autorizado (color rojo).
 - o El segundo de los círculos indicará si el dispositivo es crítico (color naranja con relleno) o no crítico (color naranja sin relleno).
 - o El tercero de los círculos indicará si el dispositivo se encuentra fijado (color gris con relleno) o no fijado (color gris sin relleno).
- NOMBRE: Nombre que se le ha asignado a cada dispositivo.
- TIPO: Diferenciación del tipo de dispositivo (PLC, RTU, SCADA, etc..).
- NIVEL PURDUE: Nivel de clasificación según el modelo de Purdue.
- MAC: Dirección MAC asignada del dispositivo.
- DIRECCIONES IP: Dirección IP asignada del dispositivo.
- ACCIONES:
 - 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
ripo No informado	NO AUTORIZADO NO FIJADO
NIVEL PURDUE No informado	
FABRICANTE	AND ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS
D SEDE	MERCENTER
D SONDA	

Ventana de información ampliada de dispositivo





0	Leditor	Botón para modificar	parámetros del dispositivo.	
		Editar Dispositivo	Ir a detailes	



Ventana de parámetros de dispositivo

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

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

Panel	de <mark>disposit</mark>	ivos 🕕 71 de 105 D	spositivos							S	+ Crear dispositivo
IDs Sonda	Nombre	Fabricante	Tipo	Rol	Nivel Purdue Dirección IP	Dirección MAC	Ver MACs virtuales	Dispositivos fijados	Dispositivos críticos	Dispositivos autorizados	
Todos		8		0) si⊖ No⊛	Si No Todos	Si No Todos 🖲	Si No 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
- Fabricante del dispositivo
- Tipo de dispositivo (PLC, RTU, SCADA, FIREWALL, etc.)
- Rol del dispositivo (Emisor, receptor o ambos)
- Nivel de Purdue, según anexo II
- Dirección IP del dispositivo
- Dirección MAC del dispositivo
- Visión de MACs virtuales reservadas de broadcast
- Dispositivos fijados, ver anexo I
- Dispositivos críticos, ver anexo I
- Dispositivos autorizados, ver anexo I

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

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

Es posible añadir manualmente un dispositivo nuevo a la red de la organización y

+ CREAR DISPOSITIVO

listado, mediante el botón

Aparecerá la siguiente ventana emergente:



			+ Anddir IP
El campo es obligato	rio		
Nombre			
Тіро			
El campo es obligato	rio Nivol Durdu	10	
	El campo es	obligatorio	
Fijado*	Crítico*	Autorizado*	
		Sí O No O	
El campo es	El campo es	El campo es	

Filtros disponibles en listado de dispositivos

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

4.3 Panel de alertas

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

8	Guardian					Admin Acceso anterior: 22/07/5	023 0110.00) [→ <u>Salir</u>
ស	Panel de alertas							
•	Panel de d	alertas () 3467 de 3467 Alertas					N B +	Crear alerta
	IDs Sonda Todos 🕞	Bûsqueda general Direccii Texto libre	ón IP Dirección MAC	Fecha y hora de inicio	Fecha y hora de fin	Severidad Categoria	G	
B (b)	Ver resueltas Si 🔿 No 🔿 Todos 🖲	Ver silenciadas Si O No O Todos 💿						
88	SEVERIDAD	NOMBRE	MAC ORIGEN	MAC DESTINO	IP ORIGEN	IP DESTINO	FECHA	OPCIONES
	-	Anomaly detected in netflow traffic		CONTRACTOR .	000000	00000	22/07/2023 05:04	💌 🔍 💿
۵.	-	Anomaly detected in netflow traffic		0.0004-0.000	000000	20030230	22/07/2023 02:11	
8	-	Anomaly detected in netflow traffic		0.00.00.40.00.00	000000		22/07/2023 01:58	··· · ·
	-	Anomaly detected in netflow traffic		0.0040.00410	000000	000000	22/07/2023 01:35	
	-	Anomaly detected in netflow traffic		0.0000.0000	000000	000000	22/07/2023 01:07	× 4 8
	-	Anomaly detected in netflow traffic		0.0010.0004	000000	CONTRACTOR NO.	21/07/2023 22:57	💌 🖪 💿
	-	Anomaly detected in netflow traffic		10000000	000000	00000	21/07/2023 21:50	💌 🔍 💿
	-	Anomaly detected in netflow traffic		1000.0000	00000	00000	21/07/2023 21:50	··· •
	- ALERT	Anomaly detected in netflow traffic		Report Franks	000002	00000	21/07/2023 21:49	
	-	Anomaly detected in netflow traffic		440346104	0000000	000000	21/07/2023 21:49	 N
	-	Anomaly detected in netflow traffic	(i)	10000-000	000803	000000	21/07/2023 21:34	💌 🔍 💿
	-	Anomaly detected in netflow traffic		******	000000	00000	21/07/2023 21:34	× A 0
	-	Anomaly detected in netflow traffic		00000000	000000	000000	21/07/2023 21:32	💌 🖪 💿
i	-	Anomaly detected in netflow traffic	(and the section.	0000000	000000	21/07/2023 21:32	

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 NOT/ No informad
CATEGORÍA STATIC PROTOCOLO ARP SEVERIDAD (ALERT) ESTADO (ACTIVA) ID SEDE	MAC ORIGEN MAC DESTINO IP ORIGEN IP DESTINO TIPO ORIGEN	NOMERE DESTINO VALOR https://0 Descencion Network port anomaly 0: expected protocol -> ICMP; found -> 2054	CREADOR NOT/ No informade
ID SONDA	No aplica TIPO DESTINO No aplica	No informado	

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 a	lertas (i) 34482	de 34482 Alertas					8	🗟 🕂 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 resueltas Ver Si No Todos • Si	r silenciadas 🔿 No 🔿 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 er 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:

ampo os obligatorio	
Drigen	Descripción*
	El campo es obligatorio
Destino	Severidad*
	El campo es obligatorio
C Origen	Fecha
C Destino	Categoría*
C Destino	Categoría*

Ventana de creación de alertas

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

4.4 Vulnerabilidades

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

4.5 **Comunicaciones**

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

C	Guardia	1 n Tech				Admin Ottimo acceso 15	108/2023 09 30:00 🌐 🕞 Salit
ណ	Comur	nicaciones					
•	Pane	el de comunicacio	nes () 36028 de 36028 Conexiones				6
	Todos	Dirección IP	Dirección MAC Puerto Proto				
a (j) / (MAC ORIGEN	MAC DESTINO	IP ORIGEN	IP DESTINO	PUERTO DESTINO	PROTOCOLO
ഷം	2%	NOVEMBER OF STREET, ST	0.0000000000	40101100	000000	0	ARP
0	22	******	0000000	0000000	000000	0	ARP
A ()	**	ALCOHOLD IN	0000000	Internation in the local data	0040330	5353	UDP
and T ^a Terro	26	107108-00403	#100000mm	0004000	000000	5353	UDP
- 6 8 -)	***	ACCORDANCES.	#38/00/00/1	00040300	000000	5355	UDP
	88	ACCORDING NO.	0.0040.77774	0020420200	00000000	1900	UDP
	2%	1000000000	PAGE TOTAL	0000000	000.000.000.000	1900	UDP
	58	ACT ADDRESS TO A	\$100 M AND \$2	And the Person number of	800	0	
	***	0.74803473	10.00.00.00.00	And in case of the second second	000	5353	UDP
	22	411140-0010-0	0.00000000	And the local distance of the local distance	0000	547	UDP
	**	411100 (MARK)	accession in the	And in case of the second second	0000	5355	UDP
	86	0.000000000	0003070003	1000000	9039333	53	UDP
	**	and the second second	00004000	00000000	000000	53	UDP
	88	ALCOHOLD NO.	CONTRACTOR IN	0000000	000000	53	UDP
	22	0.1480.010	494000000	1000000	000000	80	TCP

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.



76 60

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 de	e comunica	ciones 🕕 242	186 de 24286 Cone	xiones
IDs Sonda	Dirección IP	Dirección MAC	Puerto	Protocolo
Todos	0			

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.

C	InprO	fech	Admin, G Last access	uardian 18/04/2023 18:33:20	⊕ Log_Out
ស	Repo	ts			
•	Rep	orts panel () 22 Reports			8
	Туре	Format Start datetime End datetime	8 0		
80		FILE TYPE	CREATION DATE	FORMAT	OPTIONS
器	۵	Unauthorized devices	17/04/2023 03:30	PDF	٤
Ľ	۵	Unauthorized devices	17/04/2023 03:30	CSV	٤
a c	D	Alerts	17/04/2023 03:30	PDF	٤
and they	C	Alerts	17/04/2023 03:30	CSV	٤
\$	C	Scoring	17/04/2023 03:30	PDF	٤
	0	Scoring	17/04/2023 03:30	CSV	۵.
	0	Public IPs	17/04/2023 03:30	PDF	۵
	ß	Public IPs	17/04/2023 03:30	csv	۵

Acceso a últimos reportes disponibles

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

4.7 Ajustes

Ver sección homónima en el apartado Guía rápida.

5 ANEXO I: Clasificación de dispositivos y alarmas

5.1 Clasificación de dispositivos

5.1.1 Según su estado

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



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

5.2 **Clasificación de alarmas**

5.2.1 Según su estado

- **Resueltas/No resueltas**: Las alarmas marcadas como resueltas son aquellas que han sido tratadas, pero se quiere mantener la aparición de la alarma en futuras situaciones idénticas (misma tipología, MACs, IPs y puertos involucrados). Las no resueltas, están pendientes de gestión.
- Silenciadas/No silenciadas: Las alarmas declaradas como silenciadas no volverán a surgir en el mismo contexto de red*. P.ej. un dispositivo que se comunica con una IP pública conocida y controlada por la organización, y no se desea que se generen alarmas para esta situación.

* Cabe mencionar que las alarmas silenciadas, a pesar de no mostrarse al usuario, se almacenan igualmente en base de datos para consulta posterior por el personal de InprOTech a petición del cliente, si fuese necesario.

5.2.2 Según su severidad

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

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

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



6 ANEXO II: Iconos representativos de dispositivos

Icono	Descripción	Nivel PURDUE
	РС	2
	SCADA	2
	DCS	2
	Virtual	2
	НМІ	2
	TABLET	2
	TELÉFONO VOIP	2
	SERVIDOR	2
	TELÉFONO MÓVIL	2



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



FIREWALL	Según ubicación
OTHER	Según ubicación

Tabla 1: Iconos representativos de dispositivos





7 ANEXO III: Iconos representativos de tipos de alertas

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