

FLOWTRIX

Sistema de Monitoreo Inteligente de Protocolos de Red



Introducción al Manual de Usuario

Este documento sirve como la guía definitiva para la implementación del *Sistema de Monitoreo Inteligente de Protocolos de Red*. Aquí se detallan los procedimientos técnicos necesarios para desplegar el software correctamente en su entorno operativo.

El propósito de este manual es facilitar una instalación limpia y proporcionar una comprensión clara de cómo FLOWTRIX interactúa con sus interfaces de red para el análisis de paquetes. Ya sea que esté configurando el sistema por primera vez o realizando una reinstalación, estas instrucciones le garantizarán un despliegue exitoso.

"Le recomendamos leer detenidamente cada sección antes de iniciar los procesos de configuración."

Atentamente

EL equipo de Desarrollo de FlowTrix



ÍNDICE

01. Registro y acceso	1 - 3
02. Instalación del agente	4 - 7
03. Panel de control	8 - 14

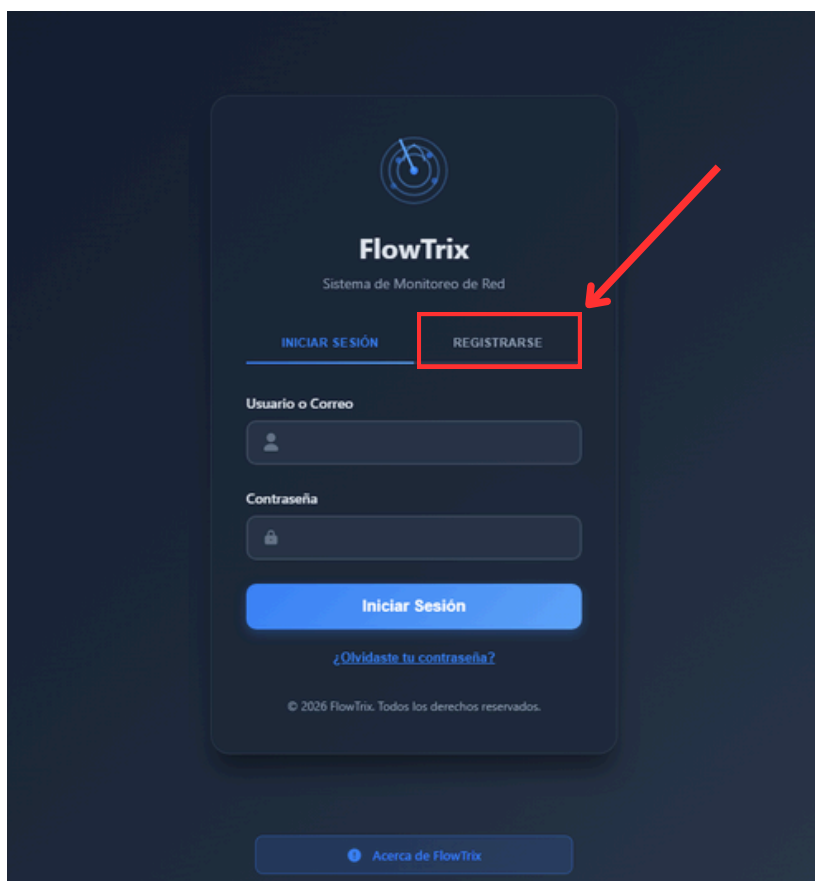




01. Registro y Acceso

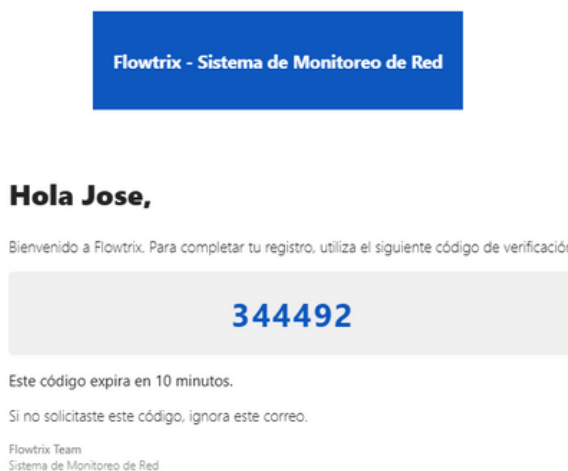
Crear Una cuenta de usuario en el portal de FlowTrix

1. *Acceda al portal:* Abra su navegador web e ingrese a la dirección flowtrix.uas.edu.mx.
2. *Navegue al registro:* En la pantalla de inicio de sesión, haga clic en la pestaña o botón "REGISTRARSE".
3. *Complete el formulario:* Introduzca sus datos personales y credenciales en los campos correspondientes.

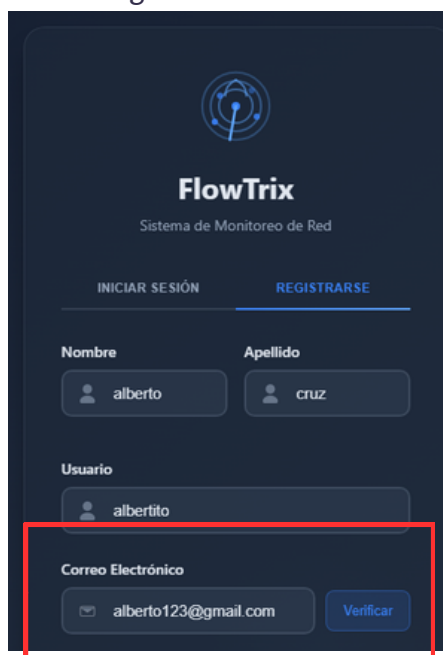




4. Verifique su correo: ingrese su correo en el campo correspondiente y presione el botón Validar, esto enviara un correo con un código a su correo, este código tiene una validez de 10 minutos.



5. Después de presionar el botón de verificación notarás como aparece un recuadro justo debajo de la casilla del correo, en esta parte ingresarás el código de verificación de 6 dígitos que te llegó al correo, automáticamente verificara el código y aparecerá un aviso si el código es correcto, podrás continuar con el proceso y terminar el registro.





Como iniciar sesión

1. *Acceda al portal:* Abra su navegador web e ingrese a la dirección `flowtrix.uas.edu.mx`.
2. *Navigate al Iniciar sesión:* El portal redirige automáticamente a la pantalla de inicio de sesión al ingresar a la URL principal.
3. *Complete el formulario:* Introduzca su Usuario o Correo electrónico y la contraseña (anteriormente creada por el usuario).



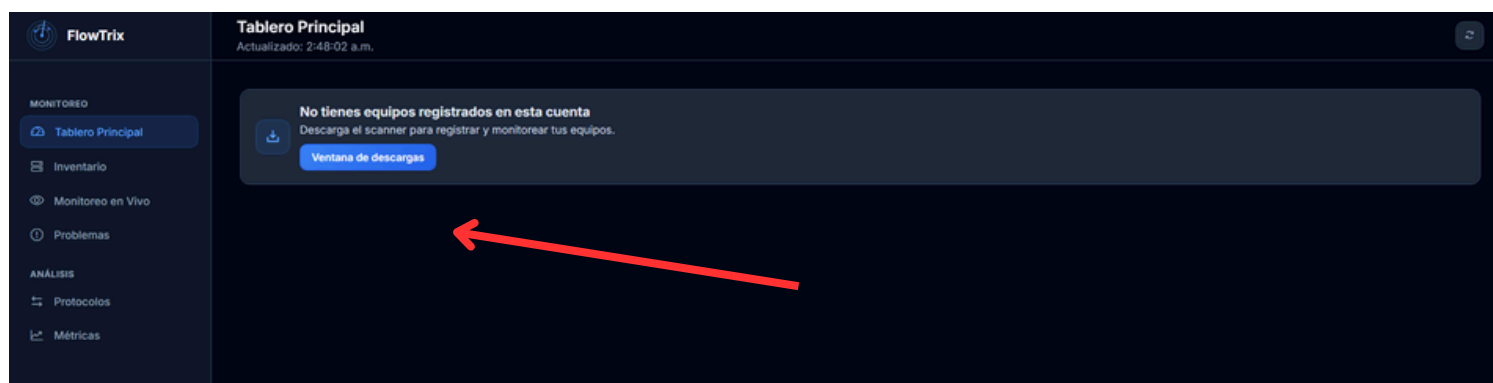


02. Instalación del agente

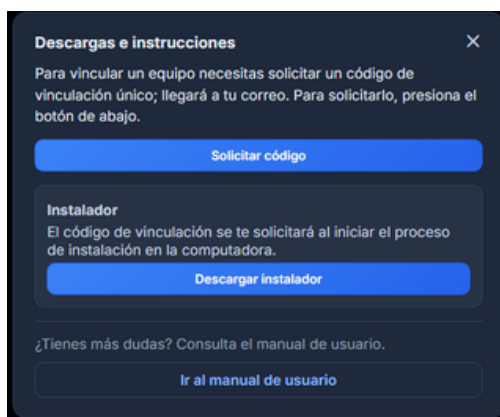
Como empezar a monitorear mis equipos?

Al acceder por primera vez al portal, el tablero principal se mostrará vacío. Esto es normal hasta que se realice el registro del primer equipo mediante el Agente.

1. Ingresa ala ventana de descargas



en la ventana de descargas encontraras varias opciones como “Solicitar código”, “Descargar instalador” “Ir al manual de usuario”, junto con unas breves instrucciones.

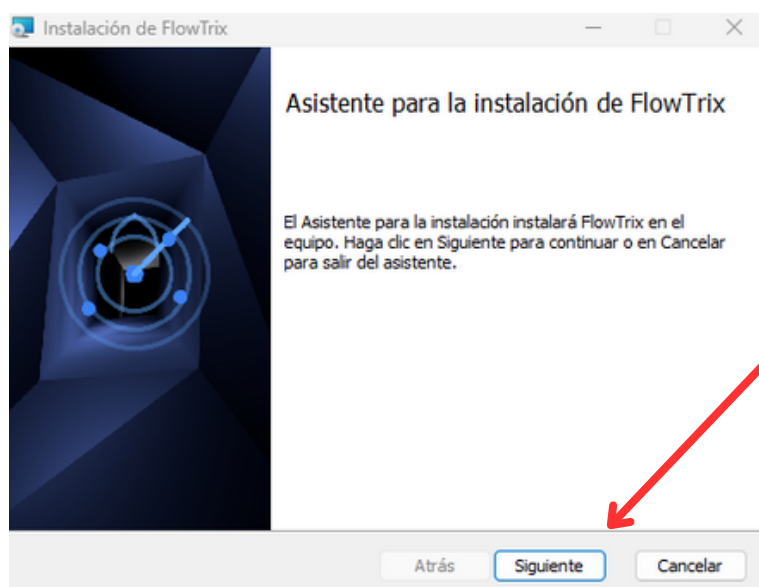


2. Presiona el botón de solicitar Código, llegara un código a tu correo el cual te servirá mas adelante en el proceso de instalación para tus equipos.
3. Presiona el botón de descargar instalador, Comenzara una descarga de un archivo llamado FlowTrix-instalador.msi

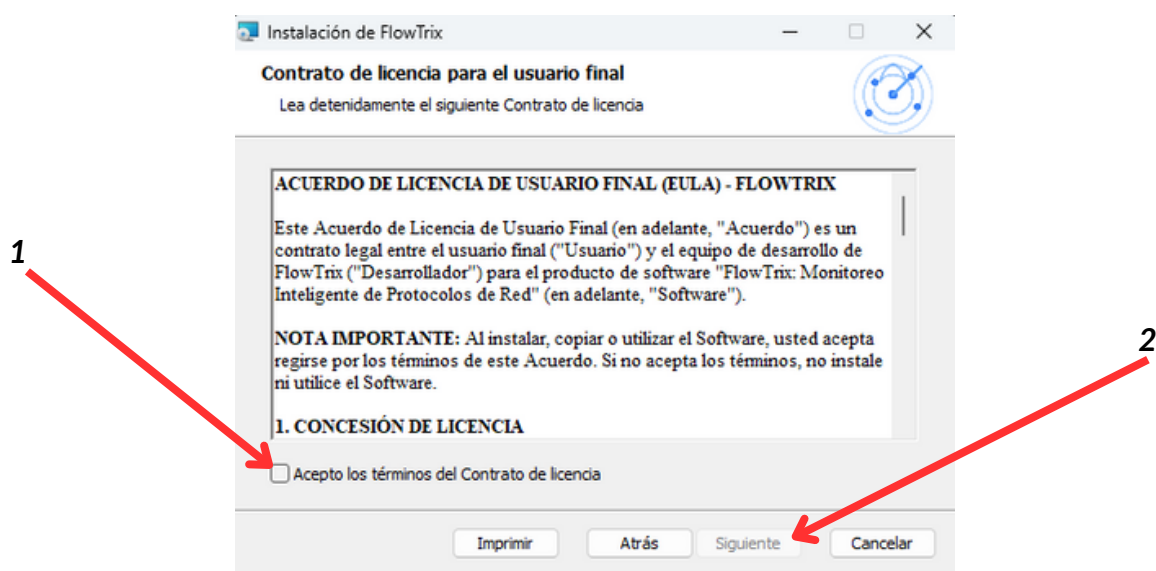




4. Una vez completado la descarga, ejecuta el instalador (FlowTriX-instalador.msi).
5. Pantalla de bienvenida: presiona siguiente.

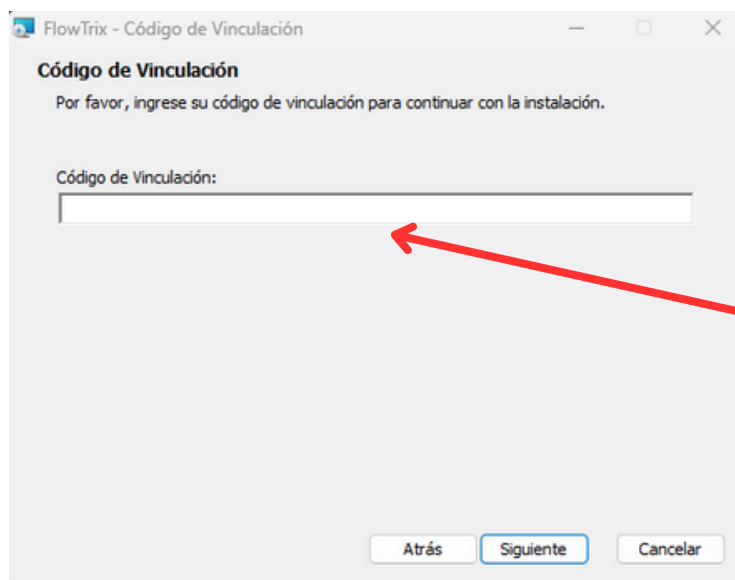


6. Pantalla de licencia: leer la licencia, marcar el recuadro de "Acepto los términos...", presiona siguiente.

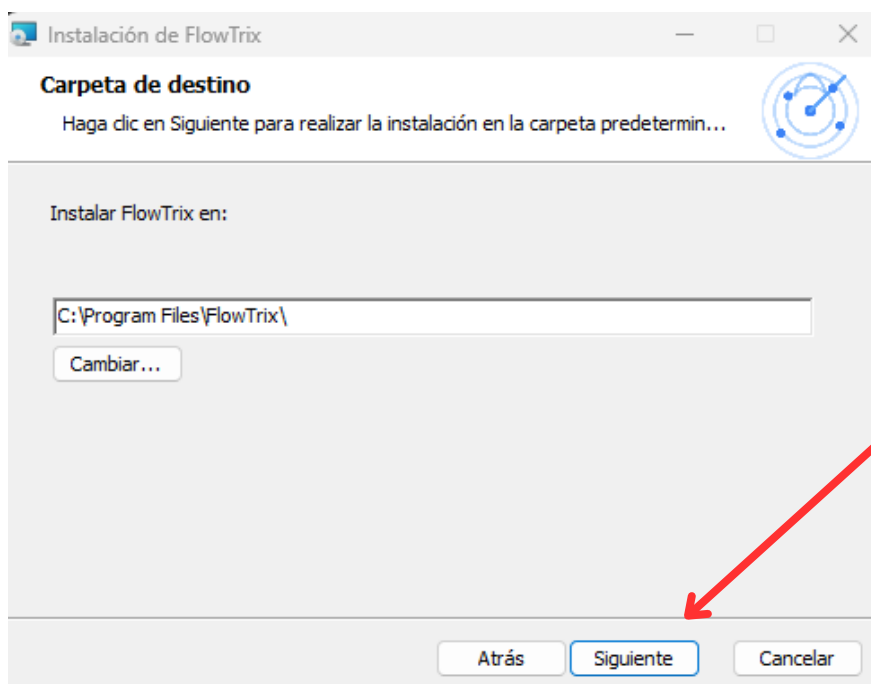




7. Pantalla de código de vinculación: Ingresar el código de vinculación de equipo (previamente solicitado, paso 2), presionar siguiente, en caso de equivocación saldrá un mensaje de error.

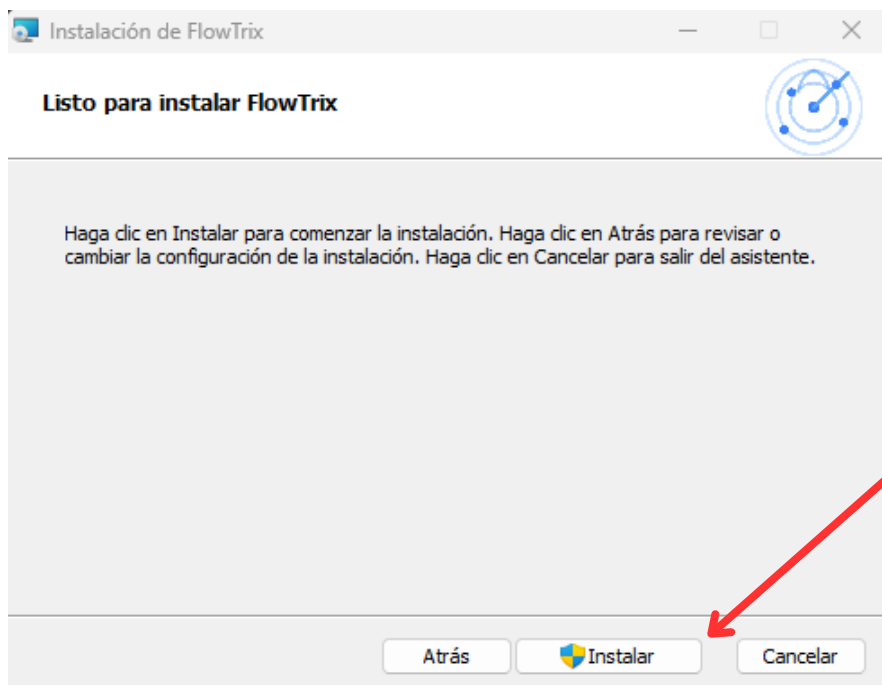


8. Pantalla de carpeta de instalación: En esta parte de la instalación el usuario puede elegir el lugar en donde se instalara el programa (se recomienda dejarlo por defecto), presionar siguiente.





9. *Pantalla de confirmación: en este punto ya estamos listos para instalarlo, presionar instalar, Windows pedirá permiso de administrador, acéptalos y la instalación empezara*





03. Panel de control

Que veo en el panel de control?

Al acceder a la página principal de FlowTrix te encontraras con el panel de control este tiene un menú lateral del lado izquierdo en el que encontraras varias opciones para ver la actividad de tus equipos.

Tablero principal

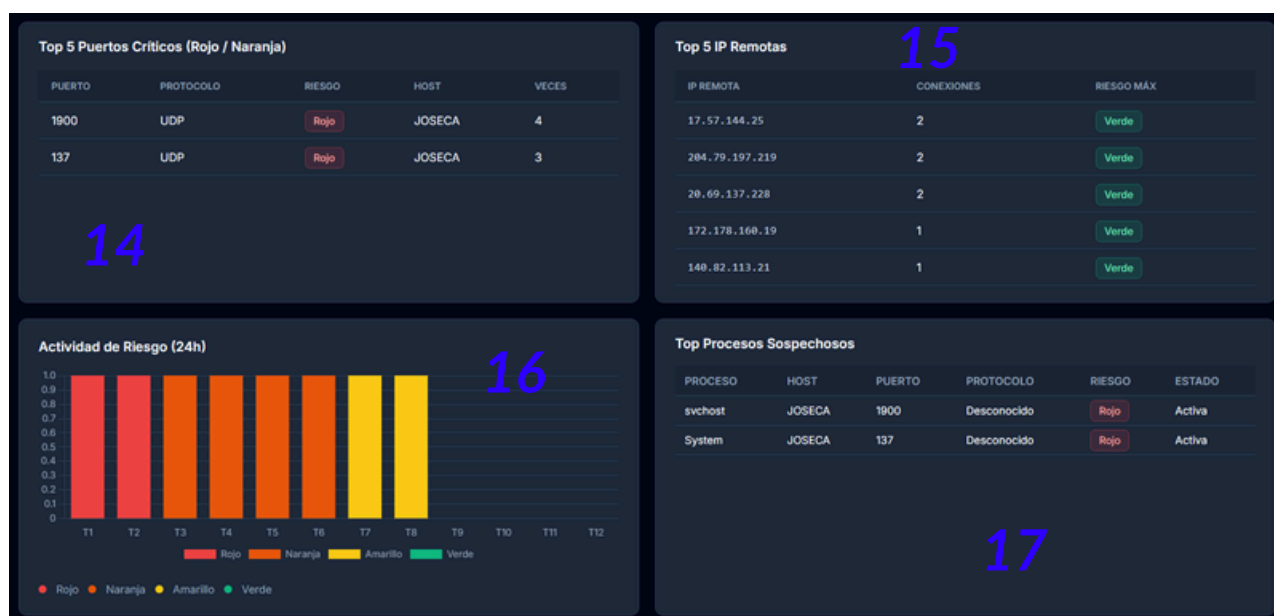
¿Qué elementos lo componen?

- 1.Sistemas operativos: una gráfica circular en la cual te muestra los diferentes sistemas operativos que están instalados en tus equipos.
- 2.Riesgo Global: conteo de protocolos usados por los equipos y representados en una gráfica de barras.
- 3.Riesgo por host: conteo de puertos en rojo usados por equipo.
- 4.Alerta recientes: en esta sección salen las alertas mas recientes que algún equipo haya mandado .
- 5.Equipos totales: conteo de los equipos registrados en tu cuenta.
- 6.Conexiones activas: total de conexiones por protocolos establecidas de todos los equipos.
- 7.Alertas de seguridad: alertas de amenazas (conexiones en rojo detectadas).
- 8.Carga de red: porcentaje de carga de red de tus equipos
- 9.Uptime: porcentaje de los equipos que están mandando datos en ese momento.
- 10.Host críticos: Host con puertos en rojo abiertos.
- 11.Host advertencias: advertencias menos graves como alta cpu o ram.
- 12.Conexiones sospechosas: puertos amarillos o naranjas con conexiones.
- 13.Alertas 24h: Alertas generales de las ultimas 24h.





14. Top 5 Puertos críticos (Rojo / Naranja): muestra los 5 protocolos de este tipo mas usados por los equipos.
15. Top 5 ip remotas: muestra las 5 ip remotas que mas se conectan a tus equipos
16. Actividad de riegos (24h): una gráfica de barras que muestra los riesgos atreves de las horas.
17. Top procesos sospechosos: te da una lista de los procesos de puertos en rojo que son sospechosos ya que se basa en las ultimas conexiones que ha establecido estos equipos.





Inventario

¿Qué elementos lo componen?

En esta sección encontraras todos los equipos que has registrado en tu cuenta, listados, mostrando información útil como nombre del equipo, ip, mac, etc. Podrás presionar un botón “Ver” en cada equipo para tener una visualización de todos los datos del equipo, puertos que esta usando, conexiones remotas establecidas, ip remota, nombre del servicio, etc.

Inventario de Equipos										Buscar equipo...
ESTADO	HOSTNAME	IP	MAC	SO	CPU	RAM	DISCO	ULT. VEZ	ACCIÓN	
Offline	DESKTOP-I13SQLQ	192.168.1.82	08-00-27-CE-67-24	Win 10 Pro 10.0.19045 (64	100.00%	68%	22.60 GB	5d	Ver	
Offline	JOSECA	192.168.1.105	E8-9C-25-80-28-6F	Win 11 Home Single Langua	20.30%	51%	9.22 GB	16h	Ver	

Detalles del Equipo

INFORMACIÓN GENERAL

Hostname

JOSECA

IP

192.168.1.105

MAC

E8-9C-25-80-28-6F

Fabricante

ASUSTek COMPUTER INC.

SO

Microsoft Windows 11 Home Single Language 10.0.26100 (64 bits)

ESTADO DE RECURSOS

CPU

20.30%

RAM

51%

Disco Libre

9.22 GB

PROTOCOLOS DETECTADOS

IKE

HTTPS

mDNS

SSDP

NetBIOS

IPSec NAT

Steam

XMPP SSL

SSH

AUDITORÍA DE CONEXIONES

PROCESO	PUERTO	IP REMOTA	PROTOCOLO	ESTADO	INICIO	FIN / ACT.	RIESGO
svchost	UDP 500	-	IKE	Activa	12:11:08 a.m.	...	Amarillo
svchost	TCP 33062	20.69.137.228	HTTPS	Activa	12:11:08 a.m.	...	Verde
msedge	TCP 58353	135.234.174.40	HTTPS	Activa	12:11:08 a.m.	...	Verde
mDNSResponder	UDP 5353	-	mDNS	Activa	12:11:08 a.m.	...	Amarillo





Monitoreo en vivo ¿Qué elementos lo componen?

Esta sección encontrarás tarjetas tipo mosaicos en la que saldrán todos los equipos mostrando datos como si el equipo esta en linea, ip, sistema operativo, uso de cpu y uso de ram





Problemas

¿Qué elementos lo componen?

Esta sección es crítica para la monitorización, ya que visualiza las alertas activas clasificadas por severidad: Problemas Críticos, Advertencias y Equipos Desconectados.

Problemas críticos (Rojo)

JOSECA

192.168.1.105

ROJO ACTIVO SSDP

Puerto 1900 (SSDP)

16h

Critico

JOSECA

192.168.1.105

ROJO ACTIVO NetBIOS

Puerto 137 (NetBIOS)

16h

Critico

Advertencias (CPU/RAM altas o conexiones Naranja/Amarillo)

JOSECA

192.168.1.105

AMARILLO Steam

Puerto 27036 (Steam)

16h

Alto

JOSECA

192.168.1.105

AMARILLO IKE

Puerto 500 (IKE)

16h

Alto

JOSECA

192.168.1.105

AMARILLO mDNS

Puerto 5353 (mDNS)

16h

Alto

JOSECA

192.168.1.105

AMARILLO IPSec NAT

Puerto 4500 (IPSec NAT)

16h

Alto

Equipos desconectados

DESKTOP-II3SQLQ

192.168.1.82

OFFLINE

Desconectado 5d

5d

Offline

JOSECA

192.168.1.105

OFFLINE

Desconectado 16h

16h

Offline

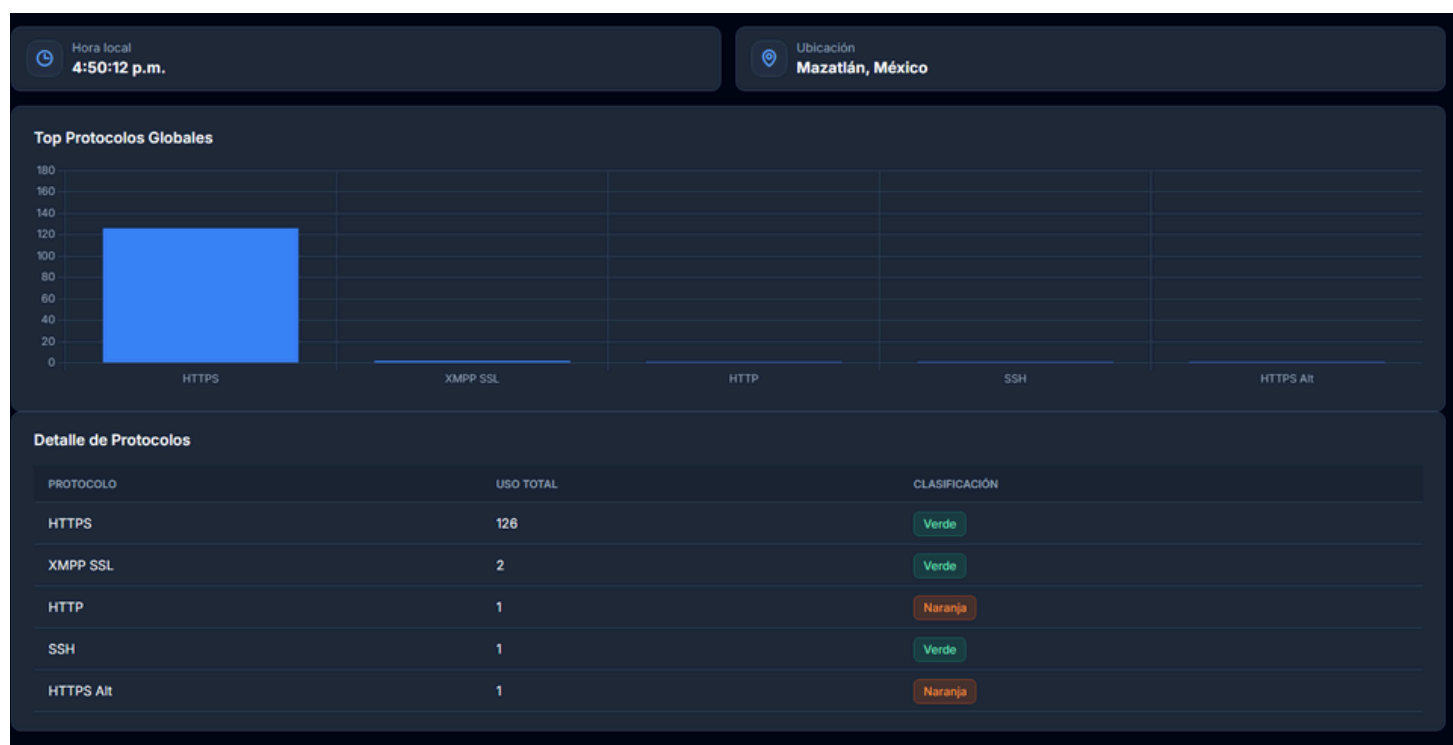




Protocolos

¿Qué elementos lo componen?

Aquí se listan y representan en una gráfica de barras todos lo protocolos mas usados de todos los equipos registrados.





Métricas

¿Qué elementos lo componen?

En esta parte se muestran tres gráficas de un equipo (este lo puedes seleccionar en la barra de arriba), tenemos una gráfica de perfil de riesgos en la que muestra los puertos que esta utilizando el equipo clasificados por colores dependiendo de la gravedad (verde, amarillo, naranja, rojo), tenemos una segunda gráfica la cual es para las conexiones activas (conexiones externas al equipo por algún puerto), manteniendo la misma clasificación de colores, y la tercera gráfica la cual es un grafico de líneas para ver el historial de uso del cpu y ram del equipo



Tienes mas dudas o preguntas?

Visita la página del manual en la que encontraras respuesta a preguntas frecuentes o pedir asistencia en caso de necesitarla

