Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad |2| Monitoreo de red.

Seguridad informática II.

Ingeniería en Desarrollo de Sofwtare.

academia global

TUTOR: Jessica Hernández

ALUMNO: Carlos Ariel Nicolini

FECHA: 30/05/2025

Índice

Introducción **3**

Descripción **4**

Justificación **5**

Desarrollo **11**

- **Incidencias encontradas** **11**
- **Reporte** **14**
- **Análisis de identificación de mejoras** **18**

Conclusión **21**

Referencias **22**

Introducción

Monitoreo de red significa utilizar un software de monitoreo de red para monitoreo el estado y la confiabilidad continua de una red informática. Los sistemas de monitoreo de red (NPM) suelen generar mapas de topología e insights prácticos basados en los datos de rendimiento recopilados y analizados.

Como resultado de este mapeo de red, los equipos de TI obtienen una visibilidad completa de los componentes de red, el monitoreo del rendimiento de las aplicaciones y la infraestructura de TI relacionada. Esta visibilidad les permite hacer un seguimiento del estado general de la red, detectar señales de alarma y optimizar el flujo de datos.

Un sistema de monitoreo de red también recopila datos para analizar el flujo de trafico y medir el rendimiento y la disponibilidad. Una forma de supervisar los problemas de rendimiento y los cuellos de botella es configurar umbrales, de modo que reciba alertas instantáneas cuando se produzca una violación del umbral. Algunos umbrales son estáticos simples. Sin embargo, los sistemas NM modernos emplean el aprendizaje automático (ML) para determinar el rendimiento normal de todas las métricas de una red en función de la hora del día y el día de la semana. Los sistemas NPM con tales líneas de base impulsadas por ML crean alertas que suelen ser mas aplicables en la práctica.

Descripción

Contextualización:

Se pretende utilizar algunas técnicas de protección ante ataques de explotación y obtención de accesos a sistemas realizando auditorías a la red mediante herramientas tecnológicas ya sea especializadas o que presenten esta funcionalidad de auditoría.

En este sentido, se requiere analizar los factores que enfatizan la importancia de la seguridad y que se describen a continuación:

- Prevenir los ataques de acceso.
- Prevenir accesos a las redes.
- Monitoreo completo de la red.
- Es importante que se guarde la bitácora, eliminarla e iniciar una nueva para detectar los cambios desde el día 1.

Actividad:

Instalar un software de monitoreo y analizar el equipo.

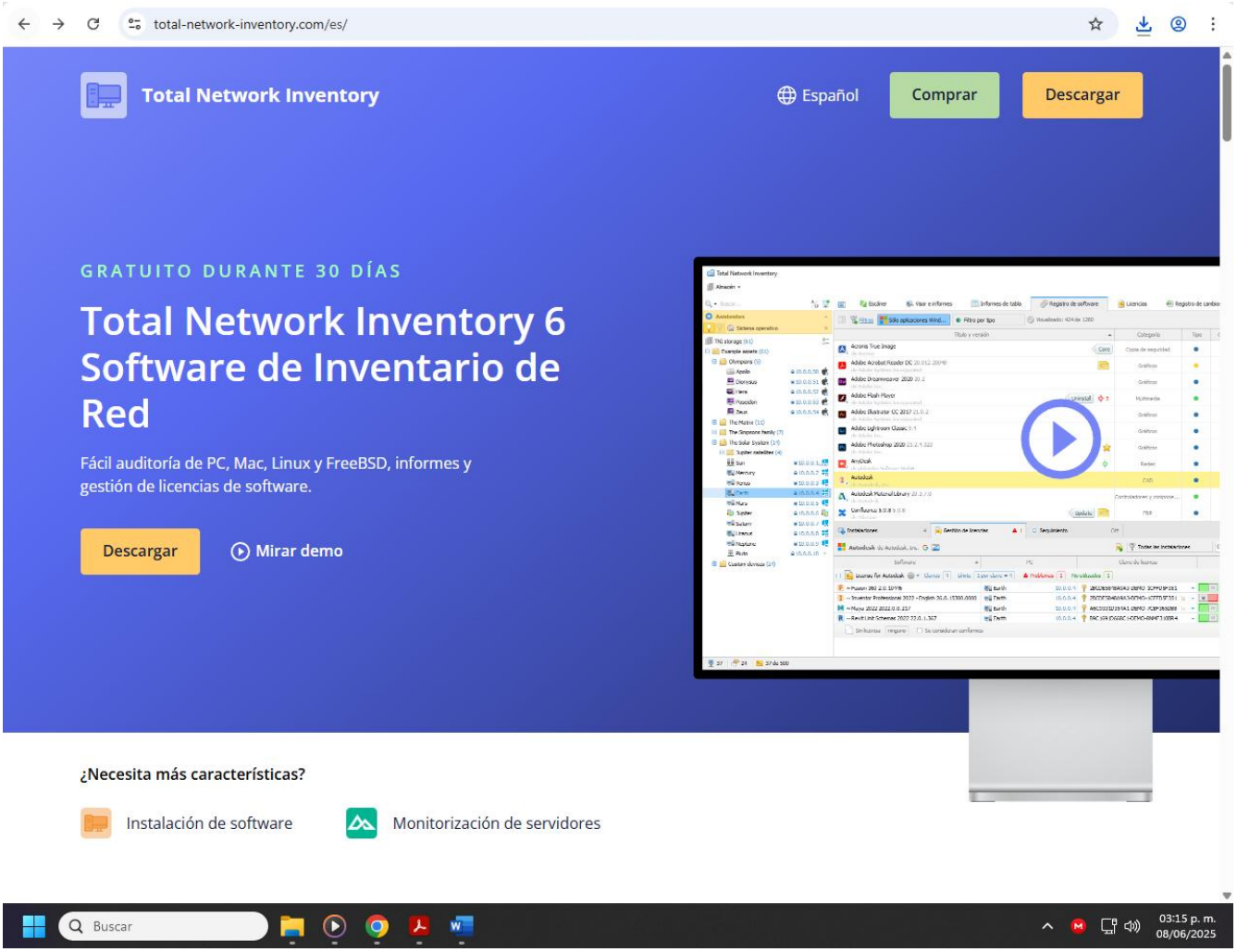
Software de monitoreo:

1. Seleccionar, instalar y analizar el equipo. Escanear la red e identificar los dispositivos conectados en ella. Emitir un reporte que identifique cada uno de sus detalles.
2. Configurar una auditoria cada semana desde la opción Programación de auditoría.

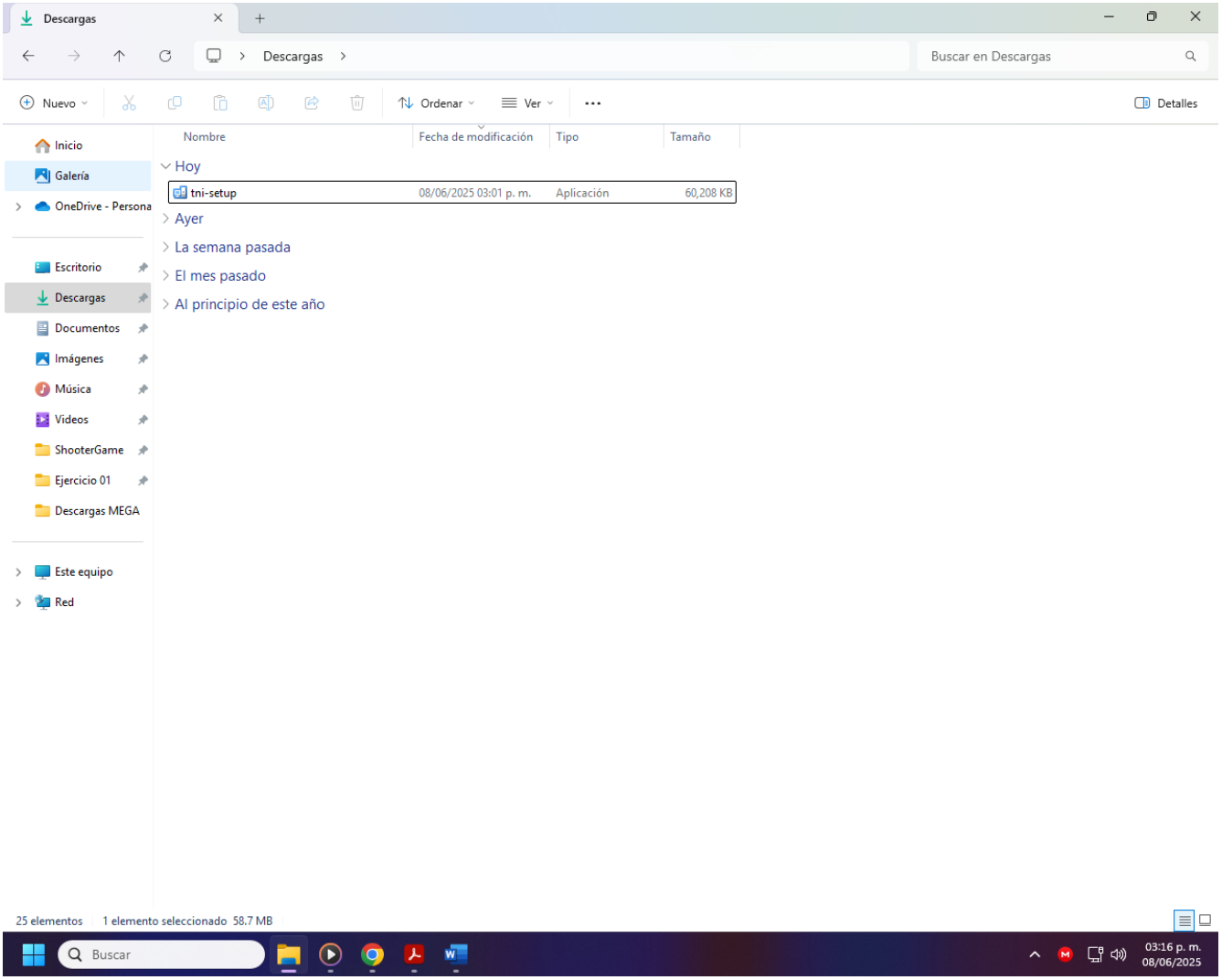
Justificación

En esta actividad continuamos con las herramientas de escaneo de seguridad, en este caso utilizaremos la aplicación Total Network Inventory, ingresamos al sitio https://www.total-network-inventory.com/es/, descargamos la versión de prueba que está en el sitito, realizamos la instalación y ejecutaremos un escaneo de nuestro equipo, generaremos el reporte, lo validaremos y además configuraremos una auditoria semanal durante un mes.

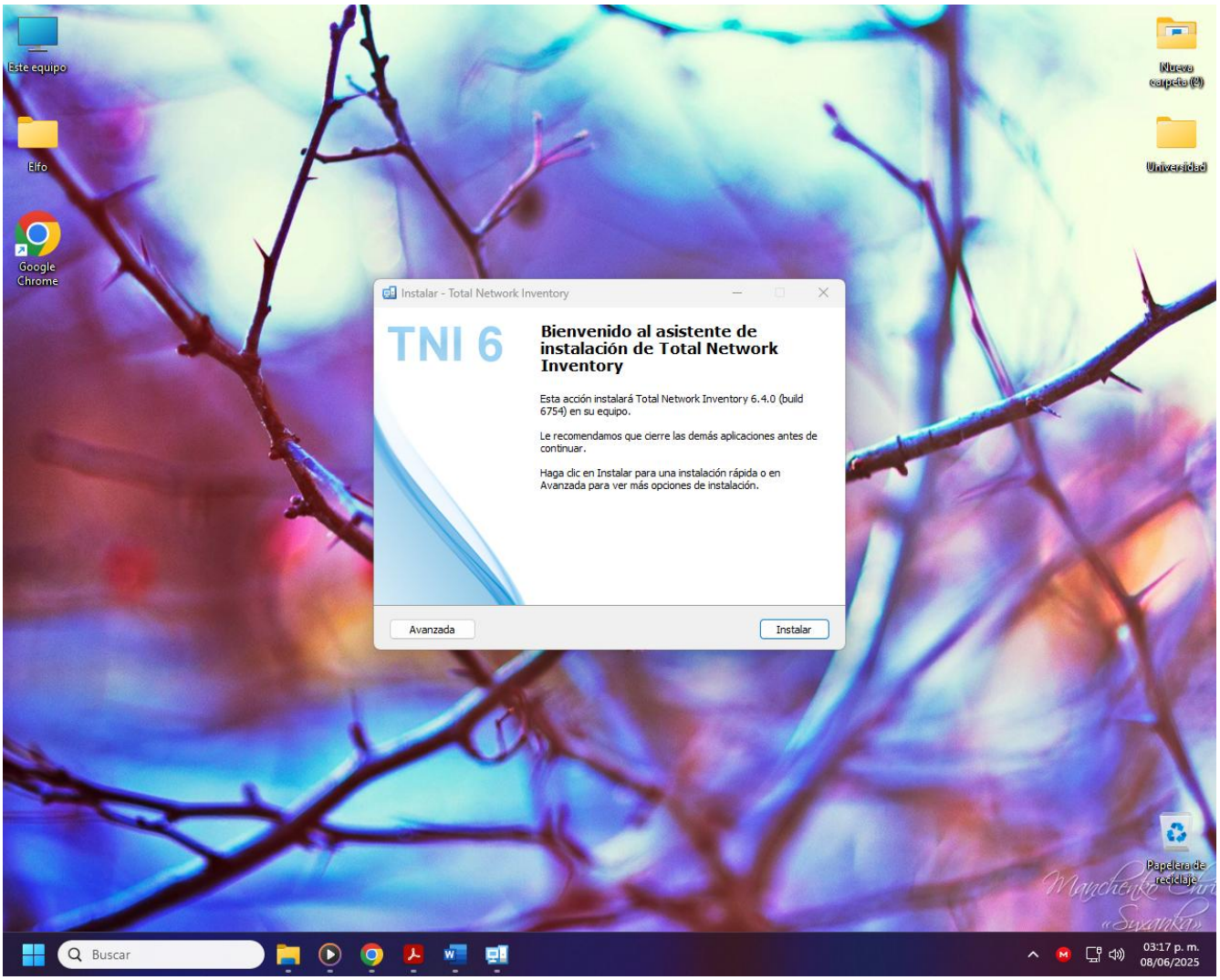
Ingresamos al sitio oficial de la herramienta.



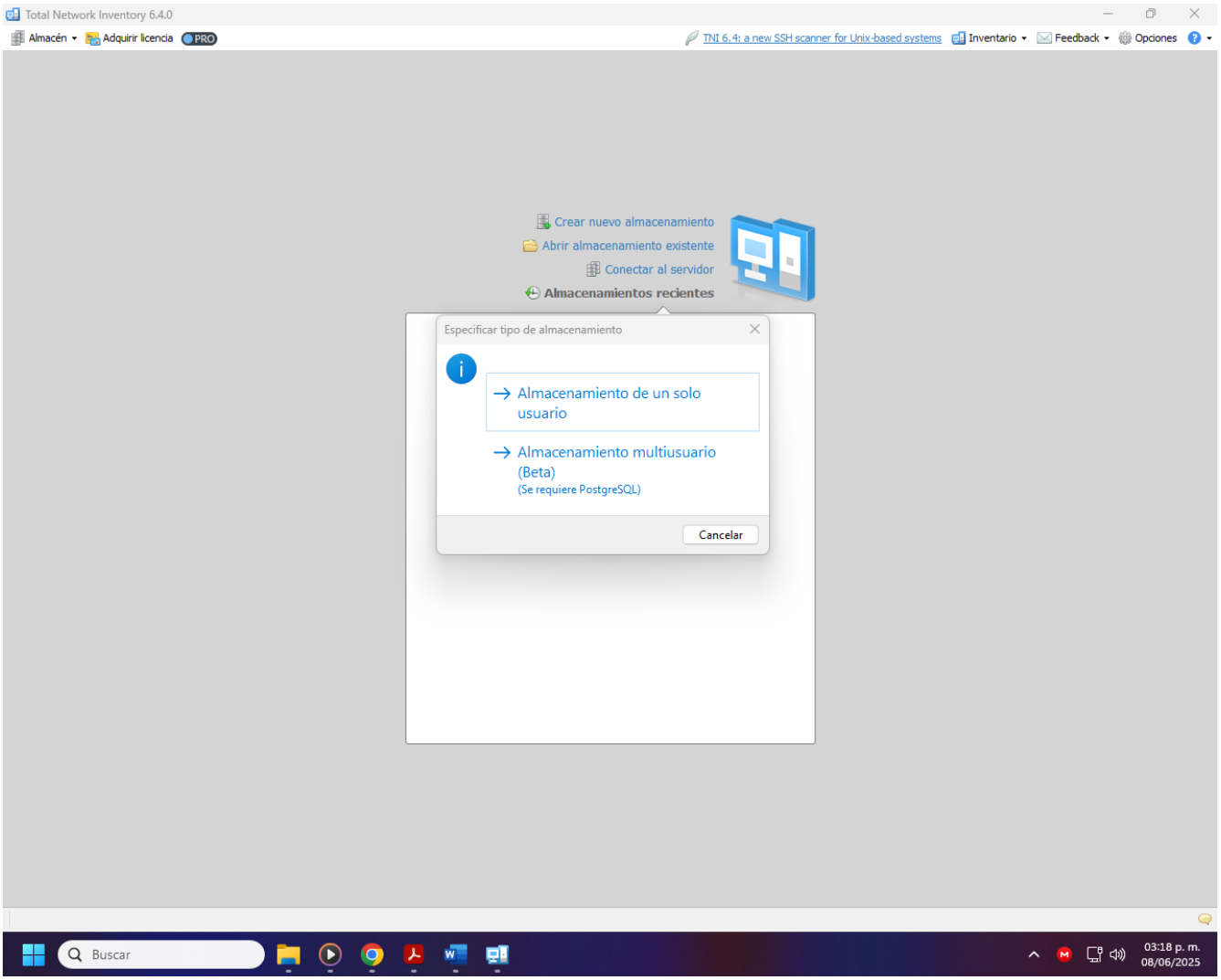
Una vez en el sitio descargamos el instalable (en este caso es la versión de prueba).



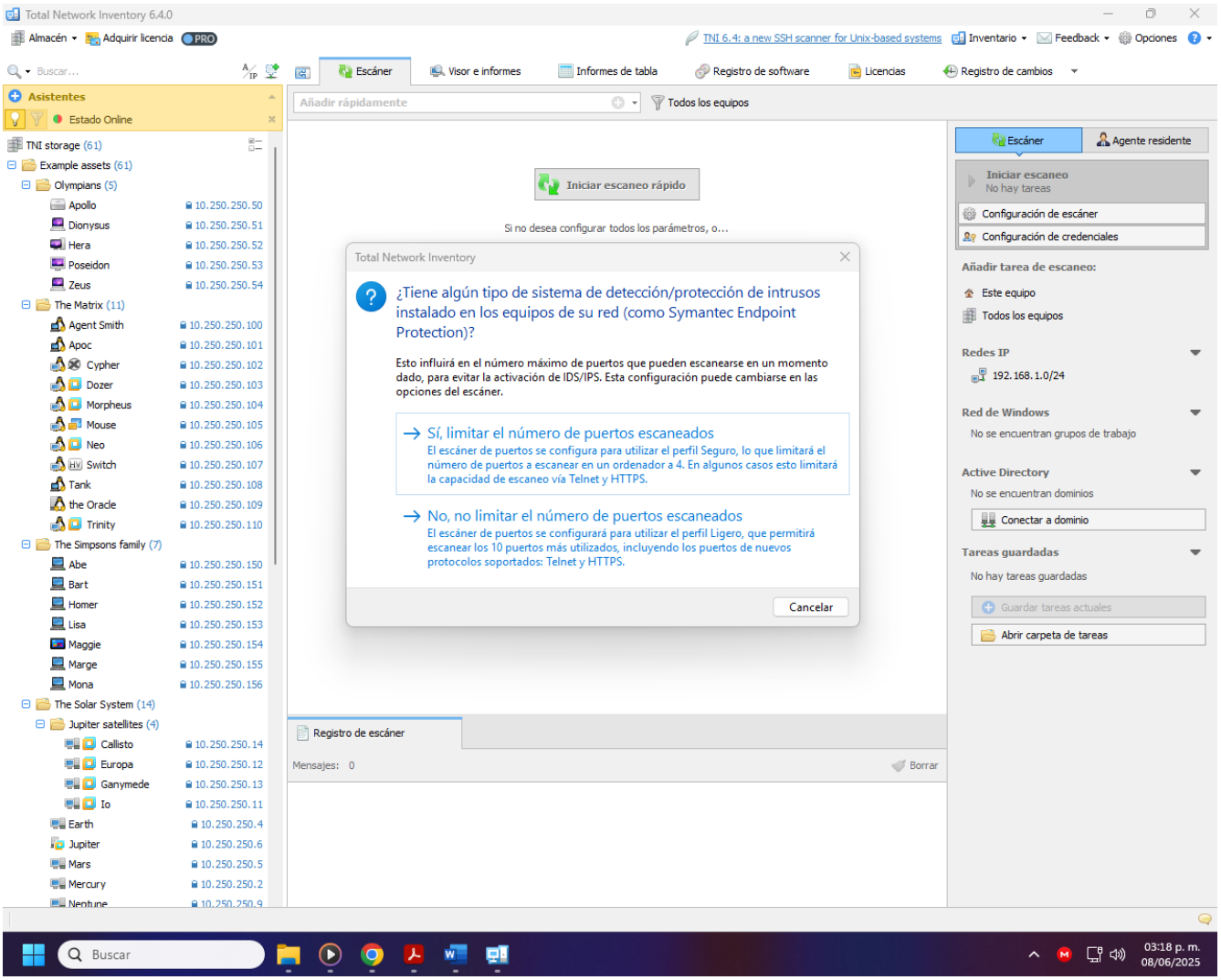
Ejecutamos como administrador la instalación del programa.



Una vez instalado lo ejecutamos. Al iniciar el programa utilizaremos almacenamiento local de un solo usuario.

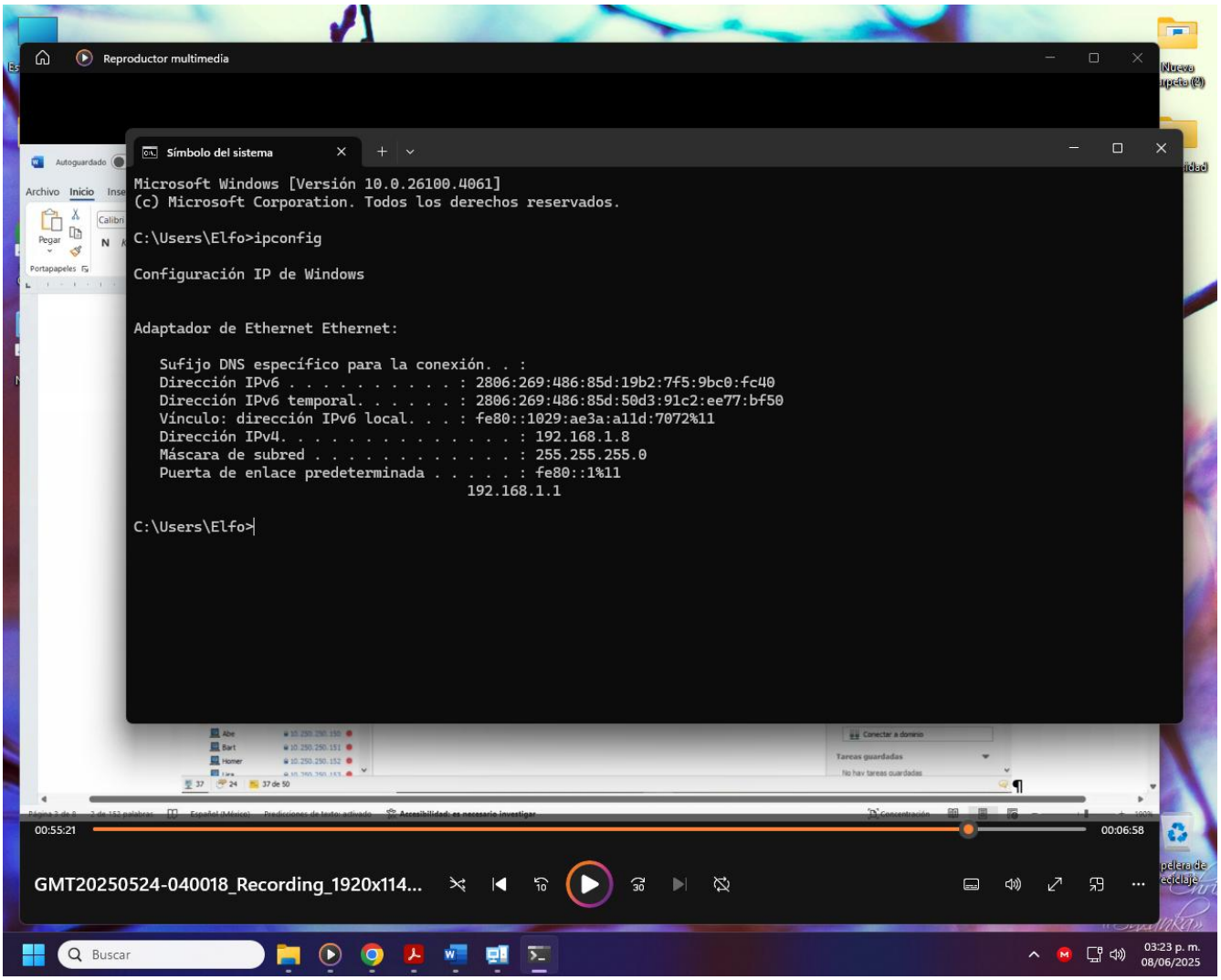


Una vez que ingrese el programa seleccionamos como fue explicado en la clase la opción de no, no liminar el número de puertos escaneados.



Con esto queda listo para realizar los escaneos y demás puntos que necesitamos realizar en esta tarea.

Se adjunta una imagen de la ip del equipo ya que se utilizará en los escaneos.



Este trabajo junto con el reporte fue subido al siguiente enlace de GitHub

https://github.com/CarlosNico/Seguridad-inform-tica-II/

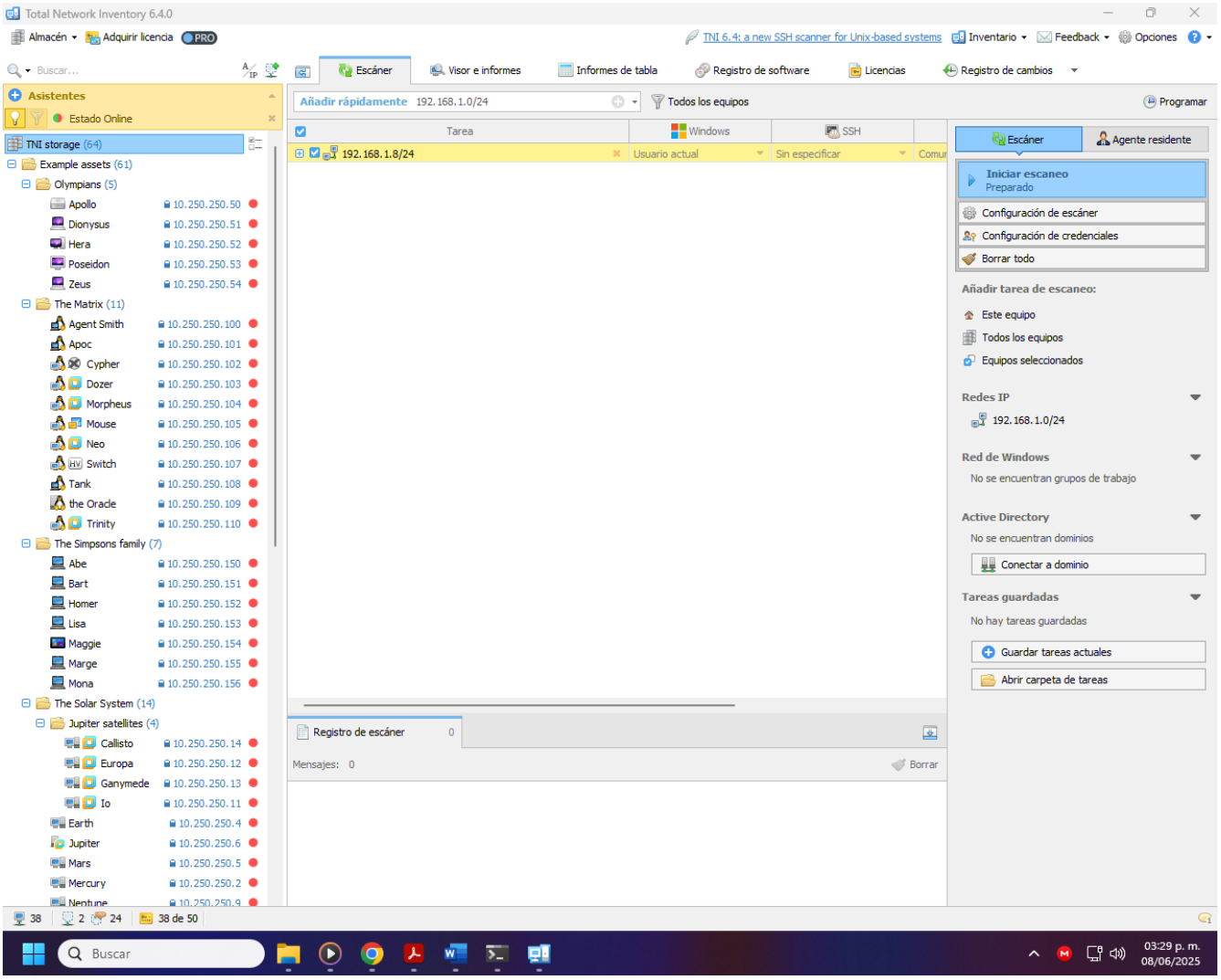
Desarrollo

Resultado del escaneo

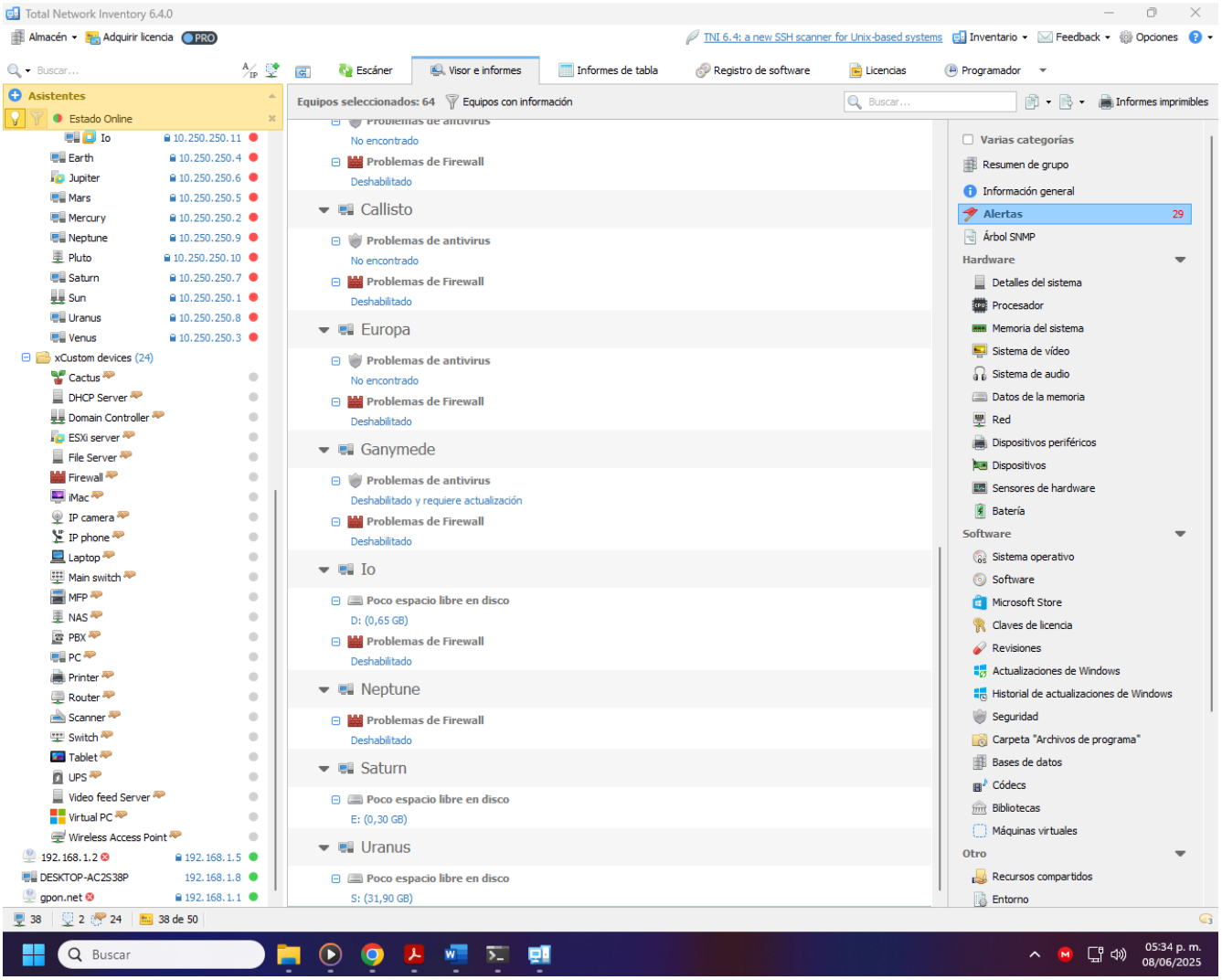
En esta parte del ejercicio instalaremos el software Total Network, lo configuraremos, realizaremos un escaneo, lo analizaremos y programaremos una auditoria semanal.

A continuación, presentamos el resultado del escaneo que nos salió limpio.

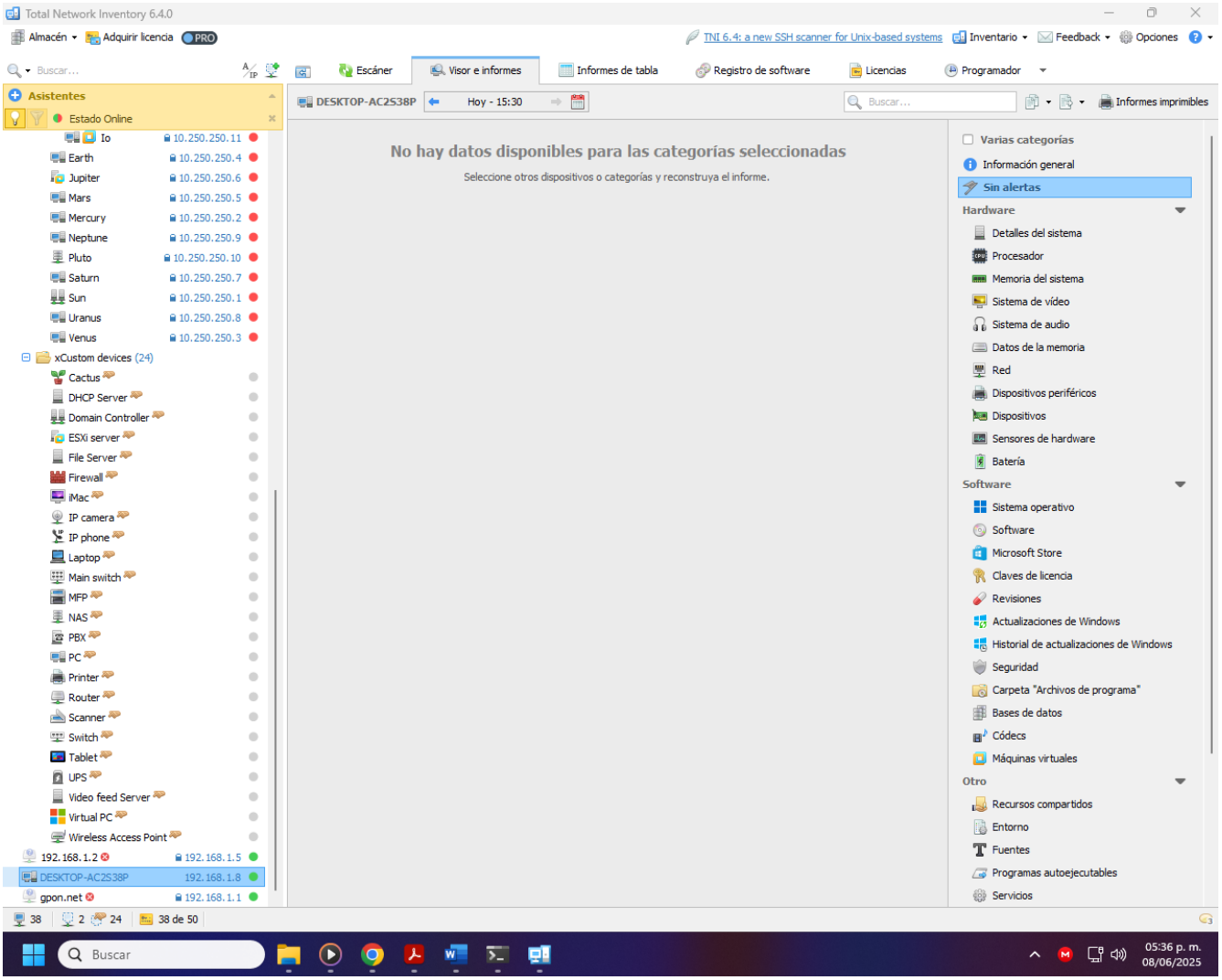
Se configura el escaneo del equipo (ip: 192.168.1.8 y se pone /24 para la red como explicaron en la clase).



En los resultados de alertas no aparece nuestro equipo alarmado

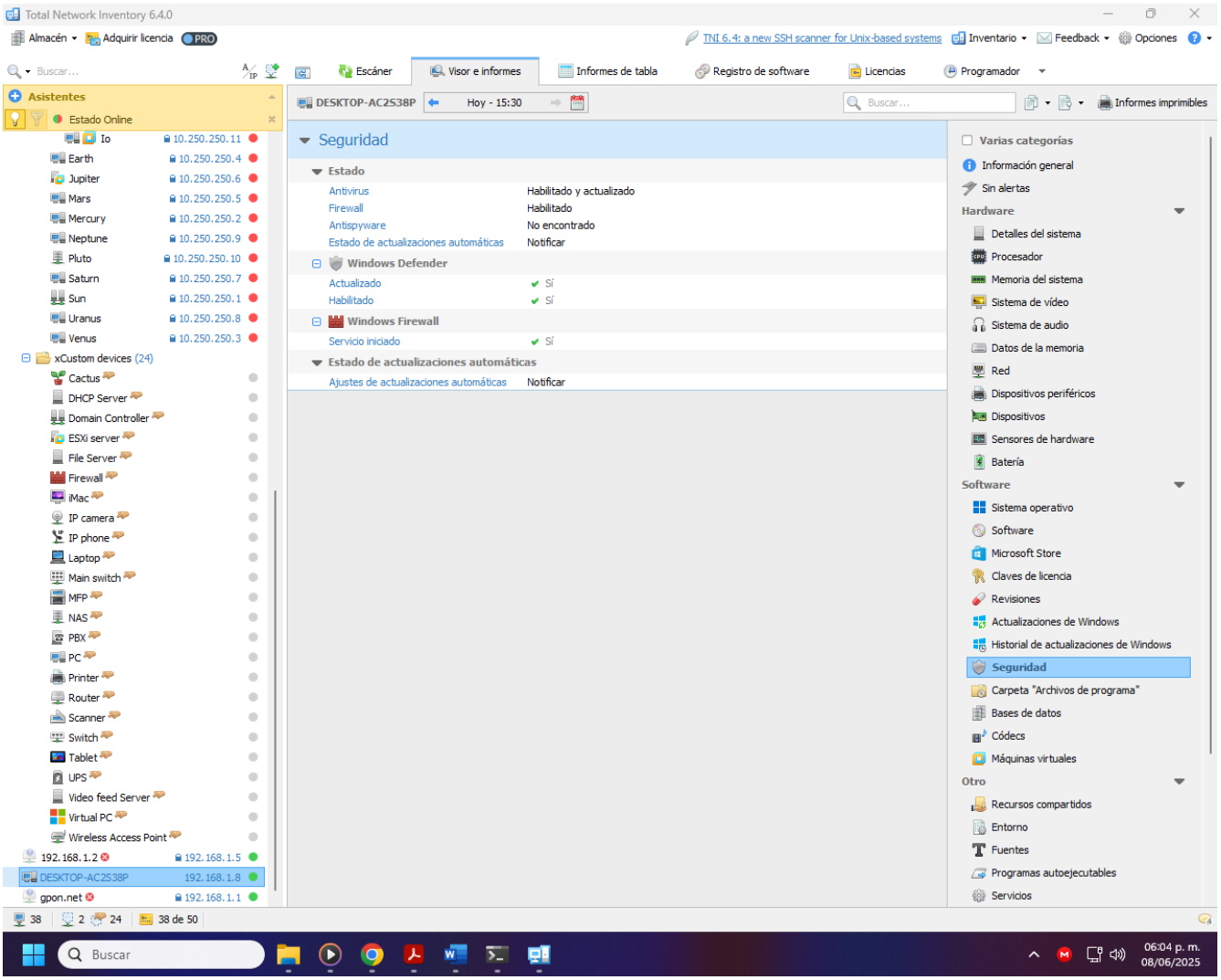


El equipo aparece sin alertas, ya que además lo he formateado hace muy poco.

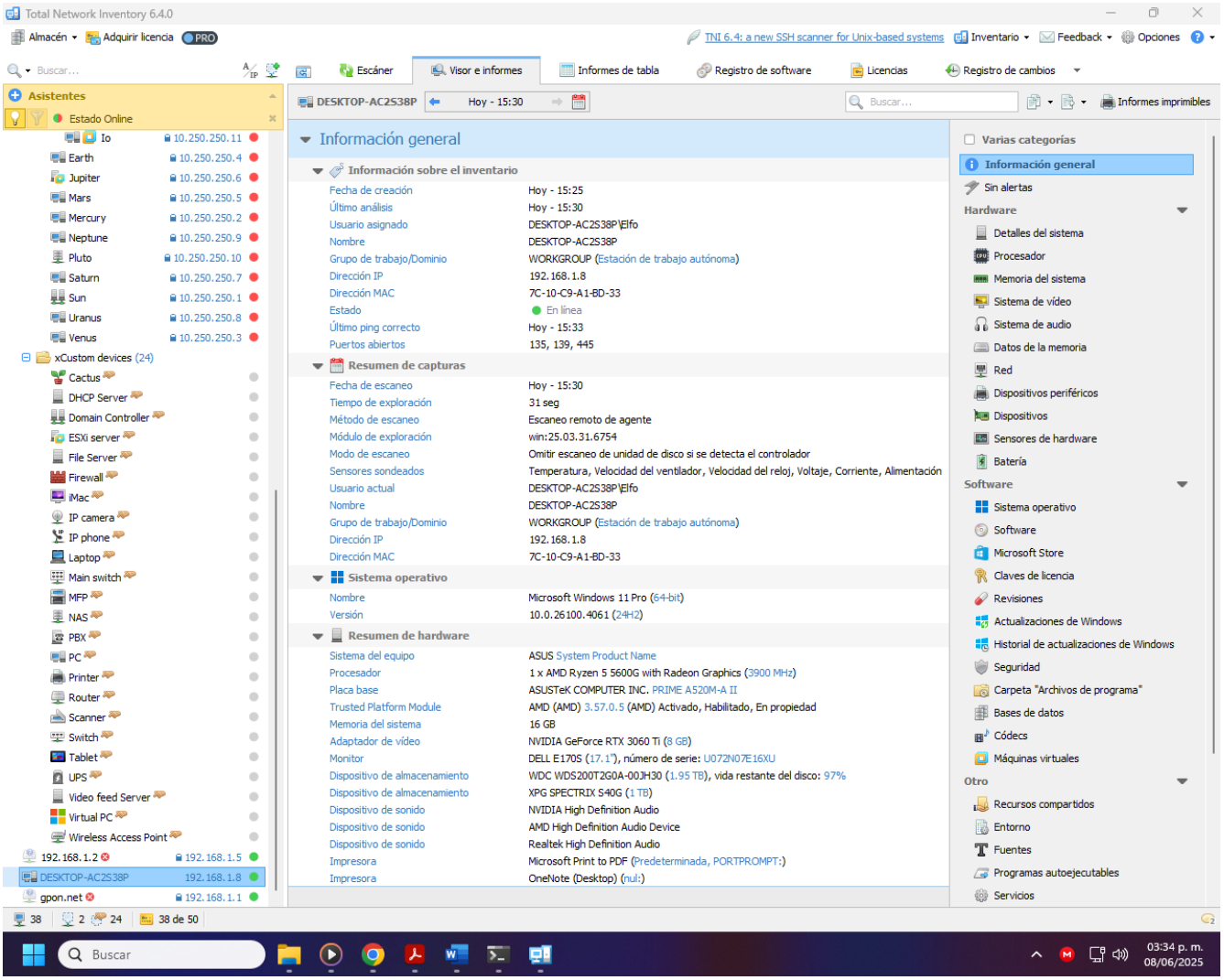


Reporte

Se generan el reporte del equipo en revisión. En este caso el reporte salió en ceros, pero se adjuntan imágenes de la información de seguridad y se adjuntan imágenes del reporte de los detalles del sistema.



Reportes del sistema e información del sistema.



Nombre de equipo: DESKTOP-AC2S38P

8 jun 2025 - 15:30

Detalles del sistema

Sistema del equipo

Modelo	System Product Name
Fabricante	ASUS
UUID	146FC420-C73F-FF4E-4937-7C10C9A1BD33
Número SKU	SKU
SID del equipo	S-1-5-21-1927348829-3880112718-2224142306

Chasis

Fabricante	Default string
Tipo de caso	Escritorio
Número de serie	Default string
Etiqueta de equipo	Default string

Placa base

Nombre del producto	PRIME A520M-A II
Fabricante	ASUSTeK COMPUTER INC.
Número de serie	210686205600181
Versión	Rev X.0x
Chipset	AMD A520 (Promontory PROM19 A)
Ranuras	4xPCI Express x1, 2xPCI Express x4, 1xPCI Express x16
Versión PCI Express	v3.0
Versión USB	v3.1
Chip Super-IO/LPC	Nuvoton NCT6798D
Temperatura	35 °C

Ventiladores

Chassis2

Nombre	Chassis2
Valor	1035 RPM

Información del BIOS

Nombre	2006
Fabricante	American Megatrends Inc.
Fecha de versión	20 mar 2021
Versión de SMBIOS	2006
Número de serie	System Serial Number

Ranuras de memoria

Disponible;
En uso; 16 GB
Disponible;
Disponible;

Ranuras del sistema

Ranura de sistema

Tipo	PCIEX16_1

Uso	En uso
Tipo de bus	PCI Express x16
Ancho del bus	16x / x16
Longitud de la ranura	Long

Ranura de sistema

Tipo	PCIEX1_1
Uso	Disponible
Tipo de bus	PCI Express x1
Ancho del bus	1x / x1
Longitud de la ranura	Short

Ranura de sistema

Tipo	PCIEX1_2
Uso	Disponible
Tipo de bus	PCI Express x1
Ancho del bus	1x / x1
Longitud de la ranura	Short

Puertos

VGA port (Puerto de vídeo / Desconocido)
HDMI port (Puerto de vídeo / Desconocido)
DP port (Puerto de vídeo / Desconocido)
PS/2 Mouse/Keyboard U32G1_56 (Puerto de ratón / PS/2)
USB_56 (USB / Access.bus)
LAN_U32G1_34 (USB / Access.bus)
AUDIO (Puerto de audio / Desconocido)
SATA6G_1 (Compatible con 8251 / Desconocido)
SATA6G_2 (Compatible con 8251 / Desconocido)
SATA6G_3 (Compatible con 8251 / Desconocido)
SATA6G_4 (Compatible con 8251 / Desconocido)
M.2(SOCKET3) (Compatible con 8251 / Desconocido)
RGB_HEADER1 (Ninguno / Desconocido)
RGB_HEADER2 (Ninguno / Desconocido)
USB_12 (USB / Access.bus)
USB_34 (USB / Access.bus)
U32G1_12 (USB / Access.bus)
CPU_FAN (Ninguno / Desconocido)
CHA_FAN1 (Ninguno / Desconocido)
CHA_FAN2 (Ninguno / Desconocido)
AAFP (Puerto de audio / SSA SCSI)
PANEL (Ninguno / Desconocido)
SPDIF_OUT (Ninguno / Desconocido)
SPEAKER (Ninguno / Desconocido)
COM (Compatible con puerto serie 16550A / DB-9)
COM_DEBUG (Ninguno / Desconocido)
TPM (Ninguno / Desconocido)
ADD_GEN2_1 (Ninguno / Desconocido)
ADD_GEN2_2 (Ninguno / Desconocido)

Trusted Platform Module

Activado	Sí

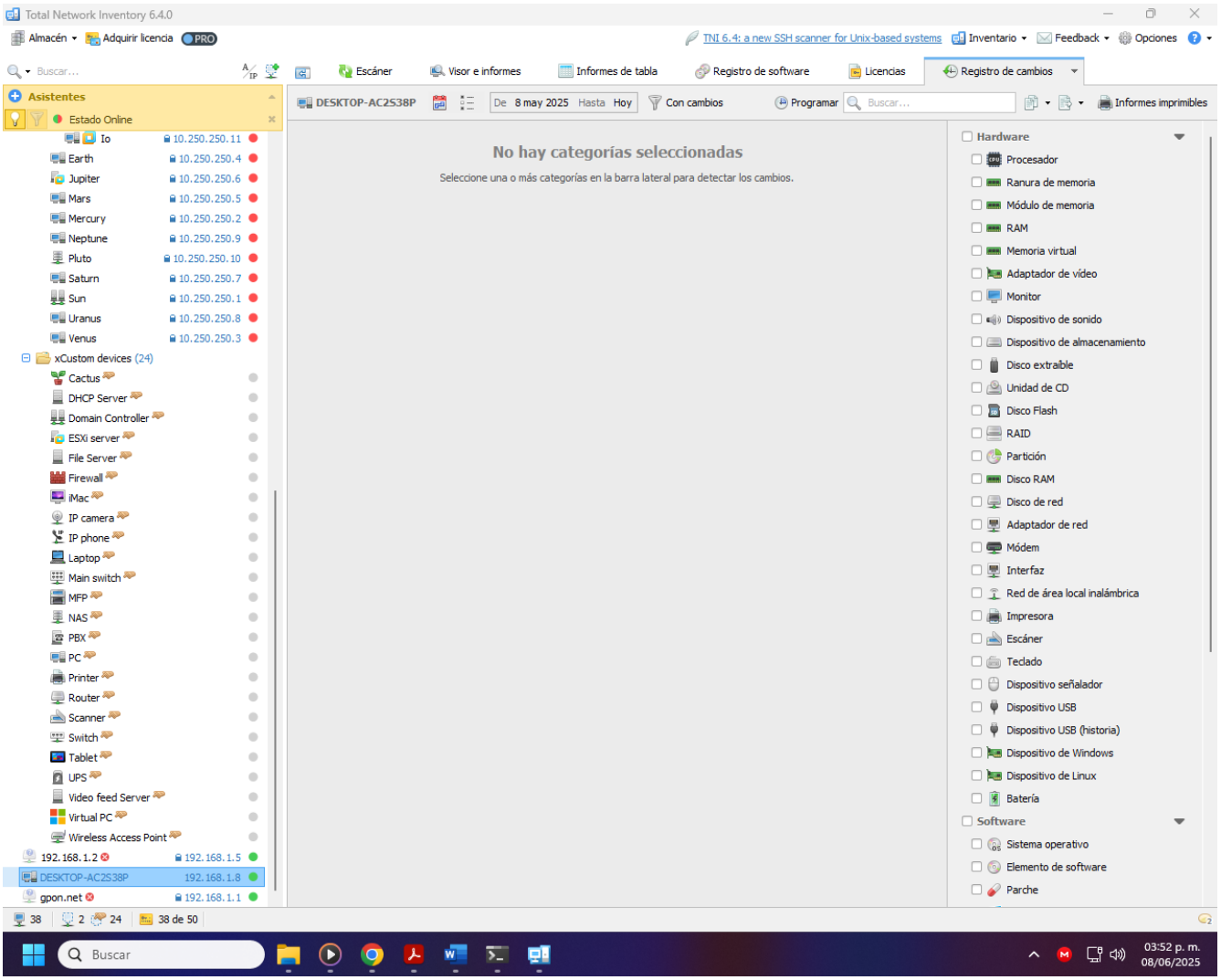
Detalles del sistema

Habilitado	Sí
En propiedad	Sí
Fabricante	AMD (AMD)
Versión del controlador TPM	3.57.0.5
Versión del chip TPM	AMD
Versión de la interfaz de presencia física	1.3
Versión de la especificación de TPM	2.0, 0, 1.38

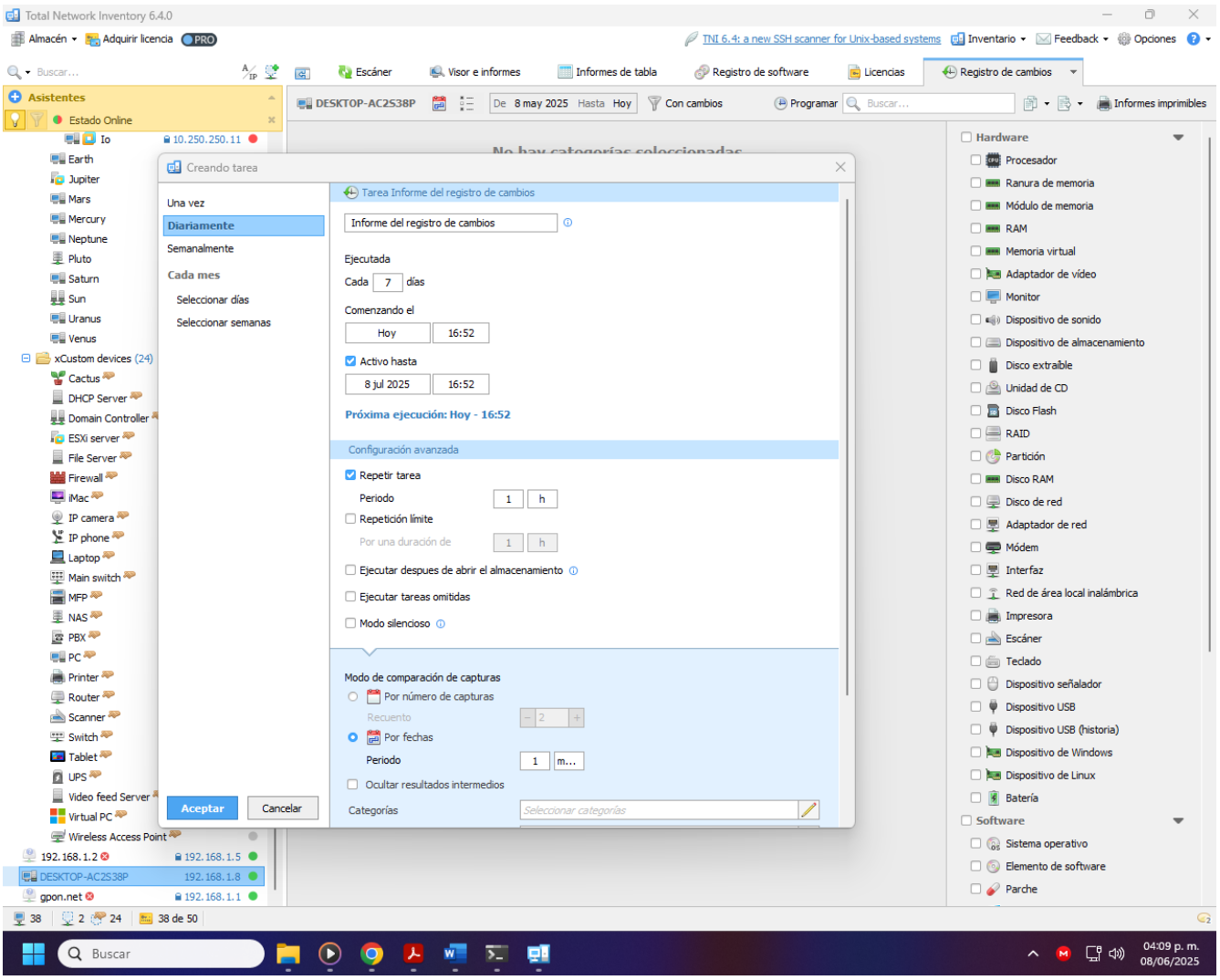
Auditoria semanal y reporte

En esta parte del trabajo se realizará una configuración de una auditoria semanal para tener un escaneo por semana del equipo en cuestión y poder analizar posibles comportamientos anómalos.

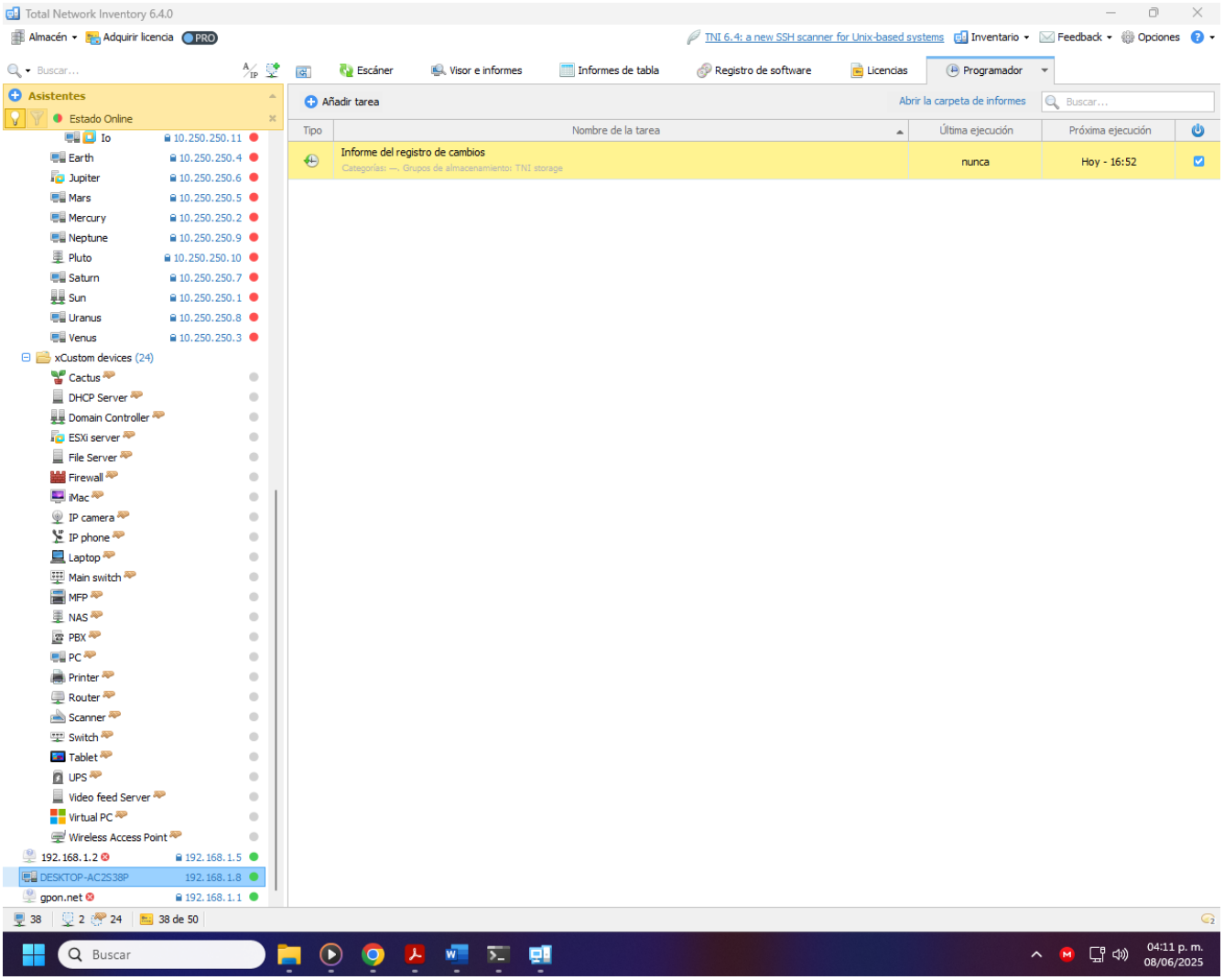
Ingresamos en la pestaña de Registro de cambios y seleccionamos la opción de programar.



Al presionar el botón programar nos aparecerá un menú donde llenaremos la información para su creación, pondremos que se ejecutará cada 7 días a partir de hoy y se deja activo por un mes, además se repetirá la tarea cada una hora. Una vez configurado se da en el botón aceptar.



En la siguiente imagen se aprecia la auditoria configurada y lista para su ejecución de manera automática.



Conclusión

Un correcto monitoreo de red es crucial para la seguridad, estabilidad y correcto funcionamiento de la red informática, con la implementación de herramientas NPM para tener una completa visibilidad de la red y su topología, lo cual nos permitirá de manera anticipada detectar y solucionar problemas antes de que se materialicen y afecten a los usuarios o impacten en la productividad de la empresa. Con este método se previenen interrupciones, se mejora la eficiencia de los recursos, se optimiza el rendimiento y contribuye a la seguridad de la red.

En seguridad y TI es muy importante tener un escaneo constante sobre lo que se conecta a la red y que realiza, cuanto consume y en que periodo de tiempo. En las quincenas o fines de mes en redes productivas de ventas es muy común un alto consumo y transacciones, pero dicha operación debe estar monitoreada y tener bien detectado los destinos y desde donde vienen dichas consultas, ya que no tener bien monitoreado esas actividades puede ocasionarle a la empresa perdidas financieras, ya sea por una intrusión o por un software con un malfuncionamiento que consuma muchos recursos y realice una negación de servicios.

Hace poco me toco estar en una situación así, cuando el equipo de monitoreo detecto un consumo grande no conocido desde unas terminales que estaban enviando muchas solicitudes, se detectó, se estaba revisando y ese detalle ocasiono una caída del sistema y negación de servicios a nivel a nivel cajas de cobro, lo cual se pudo solucionar de manera rápida ya que se habían detectado los equipos que estaban inundando con solicitudes al equipo de red. Gracias al escaneo y la atención a las alarmas se pudo evitar una perdida de servicio de horas lo que habría ocasionado una suspensión de servicios de cobro y esto se reflejaría en una perdía económica y en una pérdida de confianza del cliente.

Este trabajo fue subido al siguiente enlace de GitHub

https://github.com/CarlosNico/Seguridad-inform-tica-II/

Referencias

5 razones por las que las empresas deben monitorizar la red. (2020, March 24). Kyocera. https://www.kyoceradocumentsolutions.es/es/smarter-workspaces/insights-hub/articles/razones-empresas-monitorizar-red.html

ManageEngine. (n.d.). *Monitoreo de tráfico de red*. ManageEngine. Retrieved June 9, 2025, from https://www.manageengine.com/latam/netflow/monitoreo-de-trafico-de-red.html?network=g&device=c&keyword=analisis%20de%20trafico%20de%20red&campaignid=15487243173&creative=571654546305&matchtype=p&adposition=&placement=&adgroup=137193043128&targetid=kwd-355262329676&location=1010154&gad_source=1&gad_campaignid=15487243173&gbraid=0AAAAAChA28DnLPl2ulY03y-R00LN35NPR&gclid=CjwKCAjw6ZTCBhBOEiwAqfwJd0iJBsR16_7sRJKnyuWh5pF39OapHccizvrEwXzRN5B3P9nk0v4HYBoC3koQAvD_BwE

¿Qué es el Monitoreo de red? (2024, November 11). *Ibm.com*. https://www.ibm.com/mx-es/topics/network-monitoring

Total Network Inventory. (n.d.). Total-network-inventory.com. Retrieved June 9, 2025, from https://www.total-network-inventory.com/es/