Actividad 2 – Monitoreo de red

Seguridad informática II

Ingeniería en Desarrollo de Software

Tutor:

Jessica Hernández Romero

Alumno:

Alejandro Abarca Gerónimo

Fecha:

23 de septiembre de 2024

Indice

Introducción

Los encargaos de realizar el análisis o auditorias de la red son personal de TI esto con el fin de obtener un resumen general o resolver problemas específicos. Existen diferentes herramientas diseñadas especialmente para efectuar las auditorias de red, muchas de las veces los problemas de red surgen ya que estas no se supervisan de forma permanente lo cual conlleva a incidencias, cortes, errores críticos que para los administradores de sistemas significa la pérdida de control de las redes.

Algunas herramientas pueden supervisar las redes durante todo el día incluidos equipos de hardware, aplicaciones, ancho de banda, tráfico de red entre otros componentes de la red. Estas herramientas notifican de inmediato en caso de que un servidor, switch o router este causando problemas para poder aplicar las medidas rápidamente asegurándose de que el equipo en general se mantenga en condiciones óptimas. También permiten mantener las interrupciones y bloqueos al mínimo, asi como realizar monitoreo constante de toda la red, al instalar una herramienta de este tipo se escanean y agregan automáticamente todos los dispositivos dentro de rango de IP concreta.

Descripción

Para el desarrollo de la actividad utilizaremos algunas técnicas de protección ante ataques de explotación y obtención de acceso a sistemas auditando y monitoreando la red. Se realizará un análisis de 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.
- Validar las licencias de sus recursos por cuestiones de los aspectos legales y regulatorios.

- Control total y auditoría cada semana del sistema, hardware, software, licencias y red.
- 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.

Para lograrlo realizaremos la instalación de un software de monitoreo para 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 auditoría cada semana desde la opción Programación de auditoría.

Justificación

La ciberseguridad proporciona a los clientes y empresas protección contra los ciberataques. Si su información no está protegida, puede causar pérdidas financieras importantes y afectar su reputación como organización.

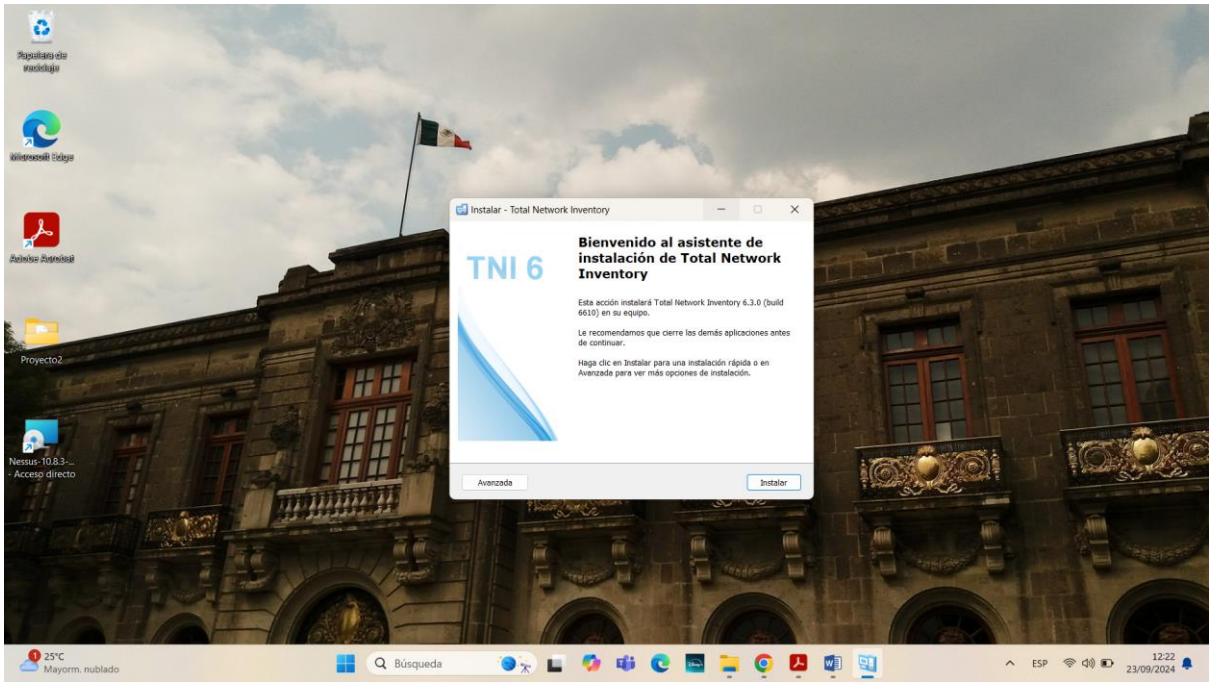
Los ciberataques representan una amenaza cada vez mayor para las empresas de todo el mundo. En los últimos años, con el aumento de los ataques a la información, los cortafuegos, el software antivirus y el software antispyware son esenciales para la seguridad operativa. Todos ellos incluyen un conjunto de procesos y herramientas, cuyo objetivo principal es proteger los recursos informáticos de la organización del uso no autorizado de los sistemas informáticos y sus recursos.

La protección incluye servidores e infraestructura de comunicaciones, sistemas informáticos, bases de datos, archivos y equipos terminales o puntos finales. En

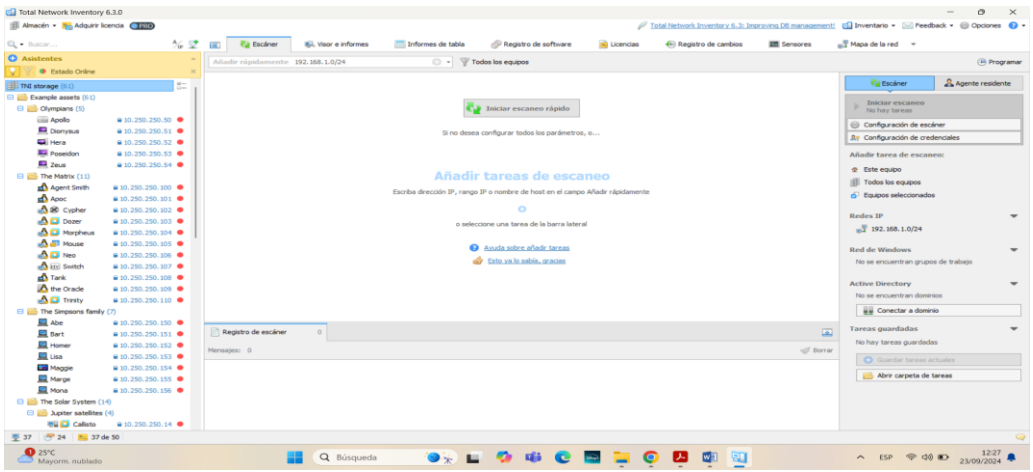
definitiva, todos los componentes informáticos que ayudan al funcionamiento de una empresa. Cuando se trata de ciberseguridad, la prevención es siempre la mejor opción, porque una vez que eres víctima de un ataque, la recuperación puede ser difícil. Por ello, es importante identificar los elementos que hacen de la ciberseguridad un aspecto importante.

Desarrollo:

Instalación de Total Network Inventory en el equipo de cómputo.

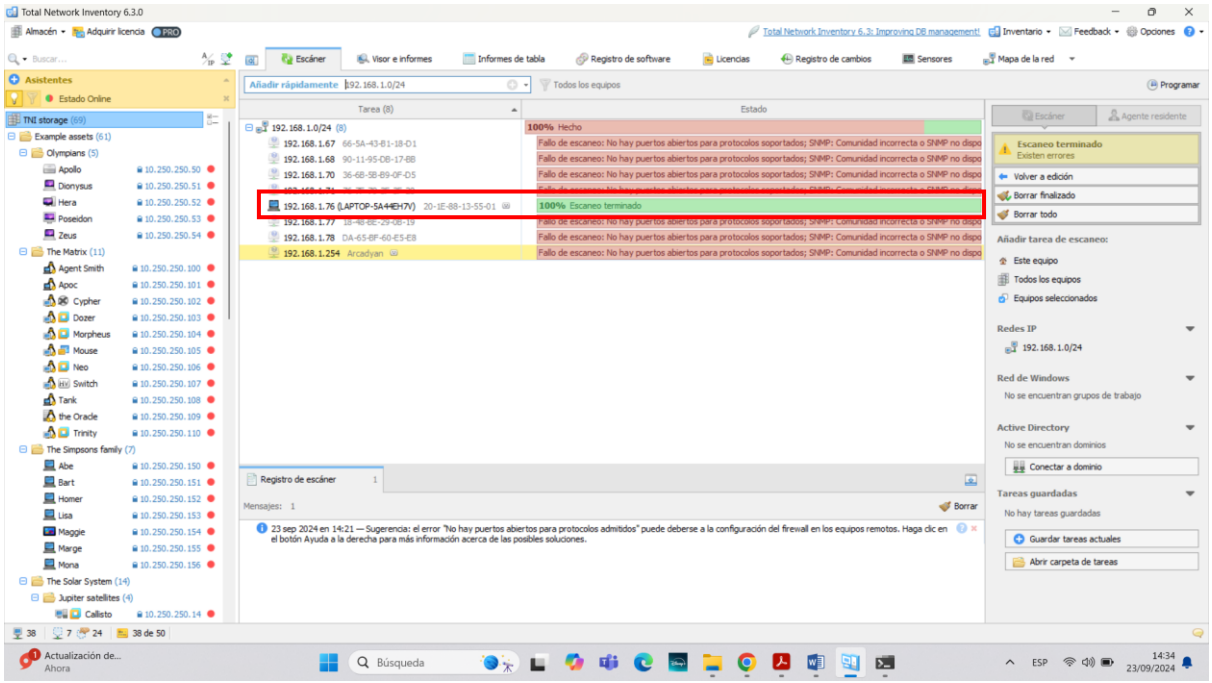


Ingreso a la herramienta una vez que finalizo la instalación, podemos acceder a toda la interfaz para irnos familiarizando con ella y poder realizar las actividades y reportes solicitados.



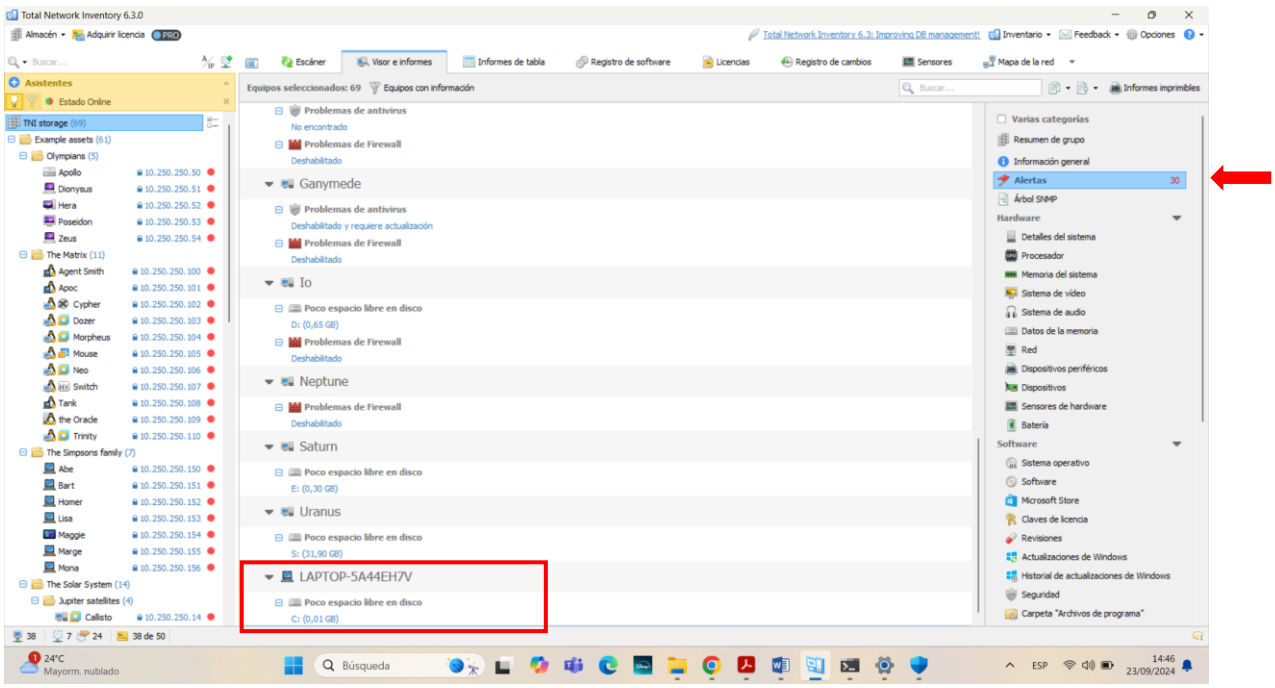
Resultado del escaneo

Se colocó la IP del equipo de cómputo para realizar el escaneo y visualizar los resultados dentro de la herramienta.



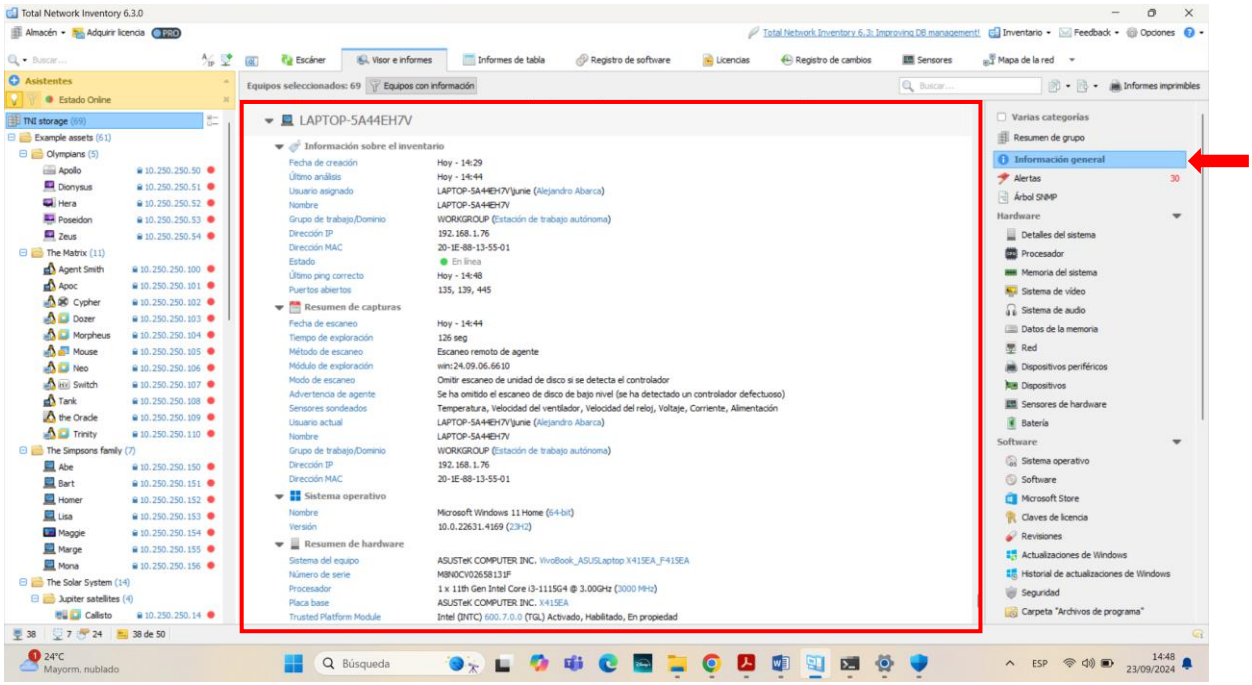
Reportes

Alertas encontradas al realizar el escaneo del equipo el cual se muestra en la parte inferior y a continuación se muestra detalladamente.



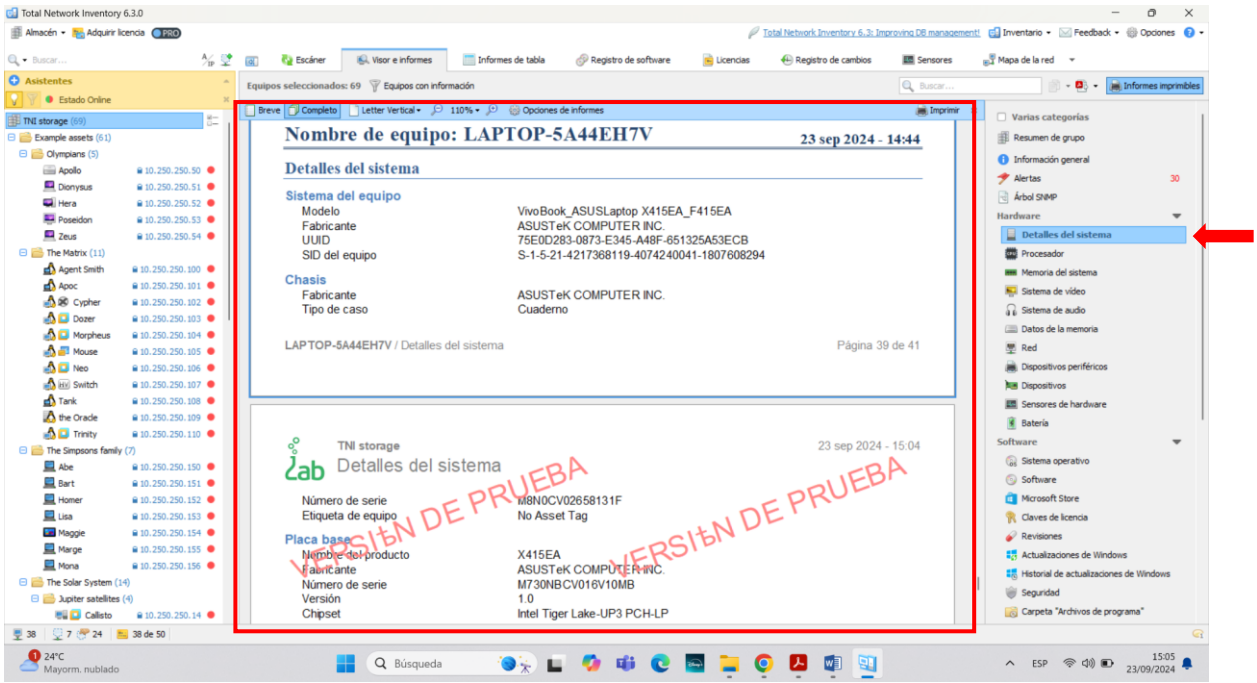
Pestaña de “Información general”

Link del reporte generado: https://drive.google.com/file/d/12-ZpwnykP_Y09-0GoRH2IisvlnAJHOTB/view?usp=drive_link



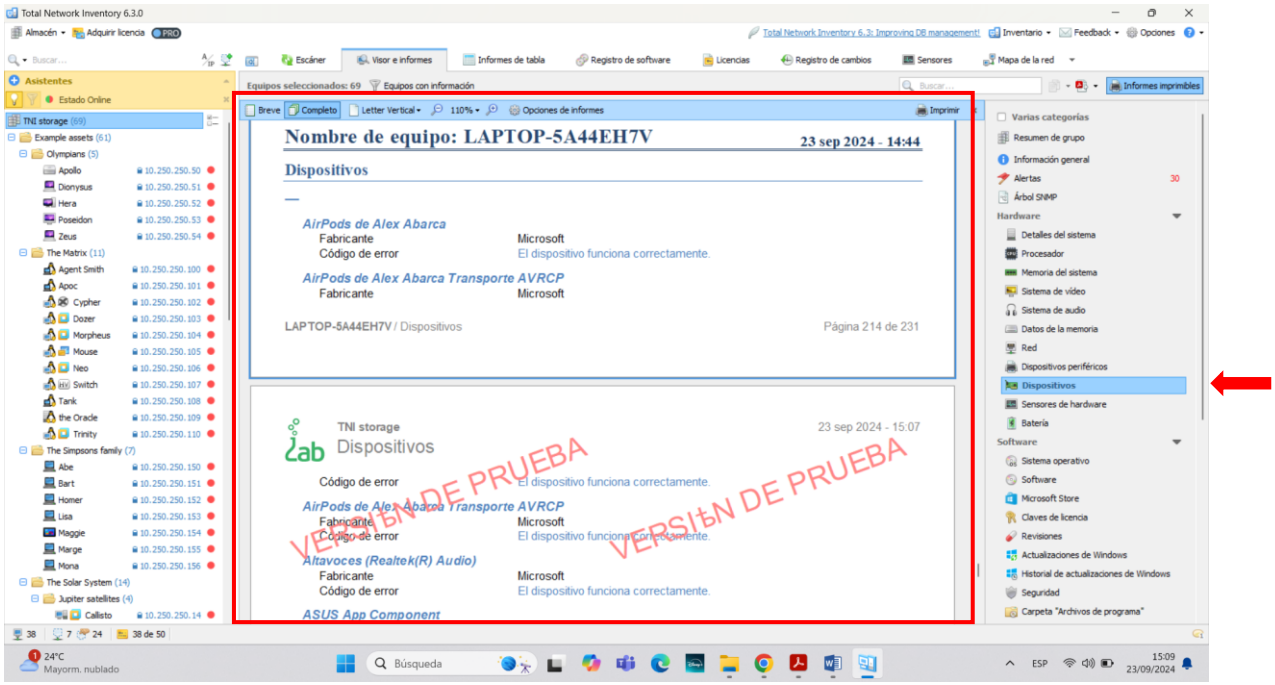
Informe sobre los detalles del sistema.

Link del reporte generado: https://drive.google.com/file/d/1Vqcjsl8ye-4ZfCmvPW3hctvrs3JKyJDs/view?usp=drive_link



Apartado de dispositivos conectados.

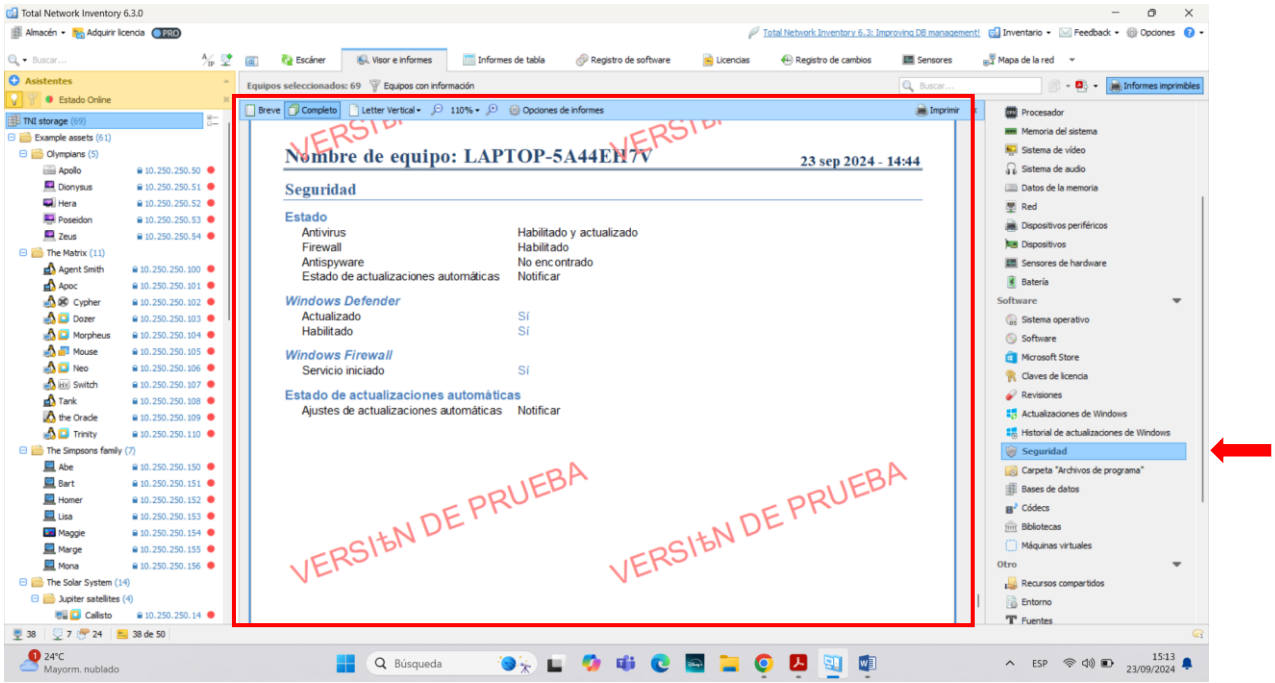
Link del reporte generado: https://drive.google.com/file/d/1vRTuXV5wXBwy0aZPddtxif-NL7GfTH2E/view?usp=drive_link



Pantalla de seguridad.

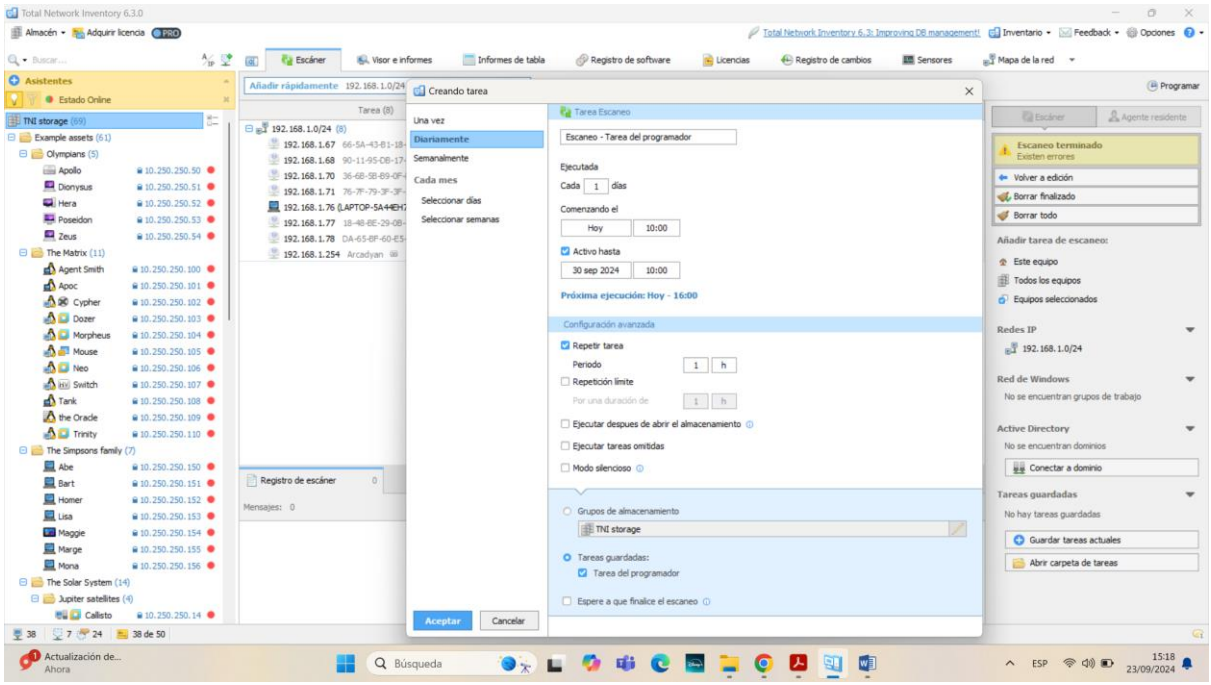
Link del reporte generado:

https://drive.google.com/file/d/1yTmnbjpUuRDhnpSJ1Y211YUb482X60XK/view?usp=drive_link



Auditoría semanal y reporte

Por ultimo realizamos la programación semanal del reporte solicitado dentro de la actividad para que de esta manera se realicen los análisis de manera diaria y asi evitar y prevenir cualquier inconveniente con nuestro equipo.



Conclusión

La auditoría de redes es esencial para garantizar la seguridad, eficiencia y cumplimiento de los sistemas de información. La aplicación de las auditorías ayudan a prevenir los ciberataques y la pérdida de datos al identificar vulnerabilidades, mejorar el rendimiento y garantizar la protección de los datos, aumentando así la confianza de los usuarios y la reputación de la organización. En un entorno digital cada vez más complejo, las auditorías periódicas se han vuelto fundamentales para mantener la integridad y continuidad del negocio.

Para ello se realizó la programación de una escaneo automático para detectar posibles vulnerabilidades en un periodo de tiempo establecido.

La auditoría en redes es un proceso que evalúa la infraestructura de red de una organización para identificar vulnerabilidades, asegurar el cumplimiento de políticas y normativas, y mejorar el rendimiento general, aplicando lo siguiente:

1. Evaluación de Seguridad
2. Monitoreo de Tráfico
3. Cumplimiento Normativo
4. Evaluación de Rendimiento
5. Documentación

La auditoría en redes es una herramienta vital para cualquier organización que busque proteger sus activos digitales, mejorar la eficiencia operativa y cumplir con las normativas vigentes. Implementar auditorías de manera regular ayuda a anticiparse a problemas y fortalece la infraestructura de red ante las amenazas emergentes.

Referencias

1. *Auditorías de red: herramientas, informes y procedimientos*. (s. f.). https://www.paessler.com/es/network-audit?utm_term=&utm_campaign=1635204137&utm_content=&utm_source=google&utm_medium=cpc&utm_adgroup=94233284309&utm_device=c&gad_source=1&gclid=Cj0KCQjwo8S3BhDeARIsAFRmkOOsKakmZFCDd2Fyt1lqhl4qMYH259v7lQz52JqlvS0WTbZ5imwH_W4aAvXDEALw_wcB
2. *SEGURIDAD INFORMATICA*. (2024). HEWLETT PACKARD ENTERPRISE. Recuperado 1 de abril de 2024, de https://www.hpe.com/mx/es/what-is/it-security.html#:~:text=La%20seguridad%20de%20la%20tecnolog%C3%ADa,de%20informaci%C3%B3n%20privada%20o%20ataque