

## Actividad | 2 |

Monitoreo de Red

### Seguridad Informática II

---

Ingeniería en Desarrollo de Software



TUTOR: Jessica Hernández

---

ALUMNO: Yanira Lizbeth Lopez Navarro

---

FECHA: 22/01/2024

---

# Índice

Introducción ..... 3

Descripción ..... 4

Justificación ..... 5

Desarrollo: ..... 6

Conclusión ..... 15

Referencias ..... 16

## Introducción

En el panorama tecnológico actual, el monitoreo de red se erige como el confidente esencial que vela por nuestra conectividad, desempeñando el papel crucial de un amigo cercano que nos alerta y protege. Este viaje hacia el fascinante mundo del monitoreo de red nos invita a imaginar a esta herramienta como nuestro compañero de confianza, siempre atento a las señales, anticipando anomalías antes de que se conviertan en desafíos significativos.

A medida que nos sumergimos en las técnicas avanzadas y herramientas especializadas que definen al monitoreo de red, descubrimos la riqueza de esta relación basada en la confianza y la proactividad. Subrayamos la importancia vital de la visión en tiempo real, permitiéndonos estar al tanto de los acontecimientos y responder con agilidad y conocimiento.

Exploramos también métricas estratégicas que no solo evalúan el rendimiento, sino que también actúan como un instinto protector, ayudándonos a anticipar posibles contratiempos. En este vínculo de amistad con el monitoreo de red, no solo buscamos garantizar su seguridad, sino también fortalecer su resistencia en este entorno digital en constante cambio. Esto nos permite comprender y apreciar la importancia de esta alianza confiable para mantener nuestras conexiones digitales seguras y resilientes.

## Descripción

En el contexto presentado, se plantea la necesidad de implementar medidas de seguridad para proteger los sistemas contra ataques y accesos no autorizados. La importancia de estas acciones radica en salvaguardar la integridad y confidencialidad de la información almacenada en los sistemas digitales. La prevención de ataques de acceso y la seguridad de las redes se convierten en objetivos fundamentales para garantizar

Además, se destaca la necesidad de validar las licencias de los recursos como un componente crítico para cumplir con aspectos legales y regulaciones, evitando posibles problemas legales y sanciones.

La auditoría semanal completa del sistema

El monitoreo continuo de la red se plantea como una herramienta esencial para detectar y responder de manera inmediata a cualquier actividad sospechosa, mejorando la capacidad de defensa contra posibles amenazas cibernéticas. Finalmente, la gestión de la bitácora, su eliminación y reinicio desde el día 1 se destaca como una estrategia efectiva para rastrear y analizar cambios, facilitando la detección de posibles brechas de seguridad y la implementación de acciones correctivas. En conjunto, estas prácticas forman un enfoque integral para fortalecer la ciberseguridad y garantizar la protección de la información.

## Justificación

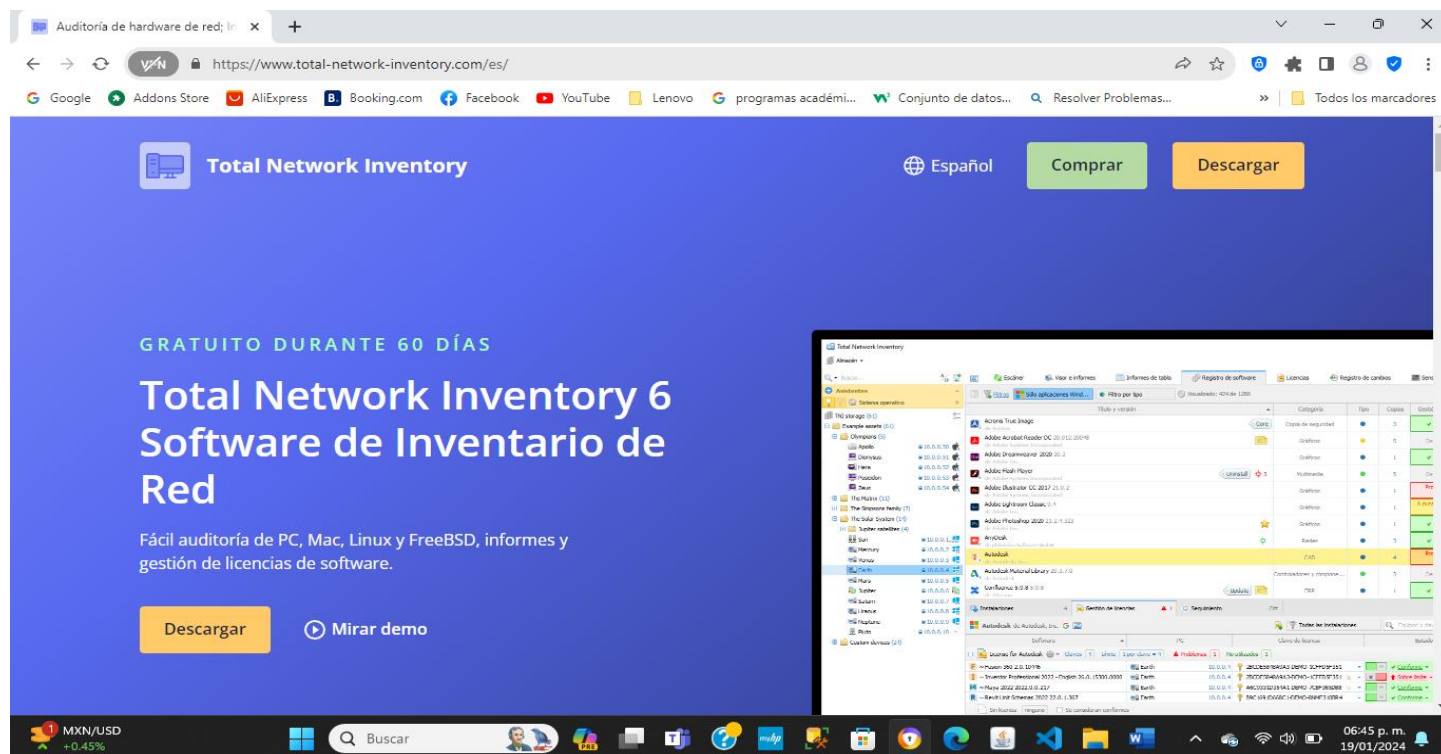
La implementación de un sistema de monitoreo de red se presenta como una solución estratégica para la actividad propuesta. En la era digital actual, donde la ciberseguridad es esencial, este enfoque proporciona una defensa proactiva y constante contra posibles amenazas y ataques informáticos. La capacidad de nuestro "amigo cercano", el monitoreo de red, para alertar y prevenir problemas antes de que escalen a desafíos mayores, garantiza la integridad y disponibilidad de nuestros sistemas.

Este tipo de solución es esencial para mantener la seguridad en tiempo real, permitiéndonos no solo reaccionar a eventos inesperados con rapidez y conocimiento, sino también anticiparnos a posibles contratiempos. Al aprovechar técnicas avanzadas y herramientas especializadas, el monitoreo de red se convierte en un guardián confiable que opera las 24 horas del día, los 7 días de la semana, asegurando una vigilancia constante.

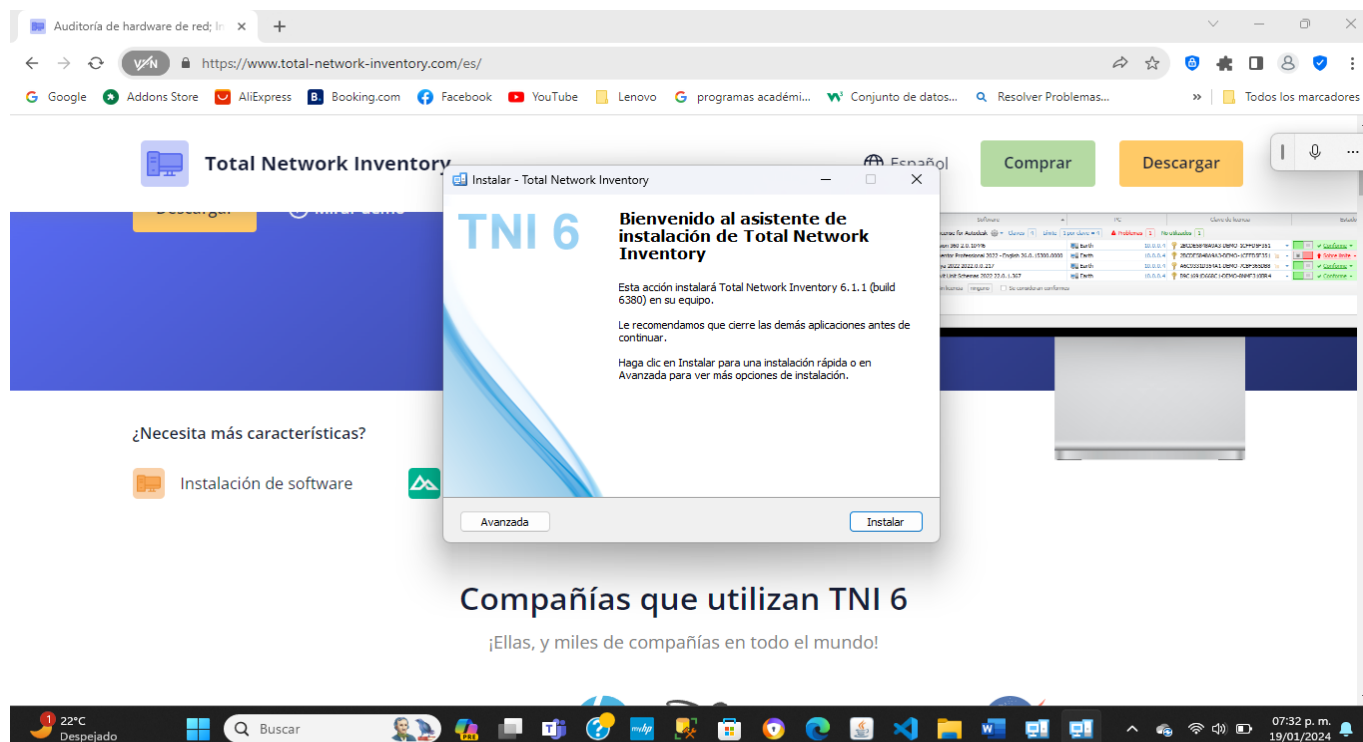
La exploración de métricas estratégicas no solo contribuye a evaluar el rendimiento, sino que también actúa como un instinto protector, previniendo y mitigando riesgos potenciales. El emplear esta solución es una inversión crucial para fortalecer la seguridad, eficiencia y resiliencia de nuestros sistemas en el entorno digital dinámico y siempre cambiante.

## Desarrollo: Resultado del escaneo.

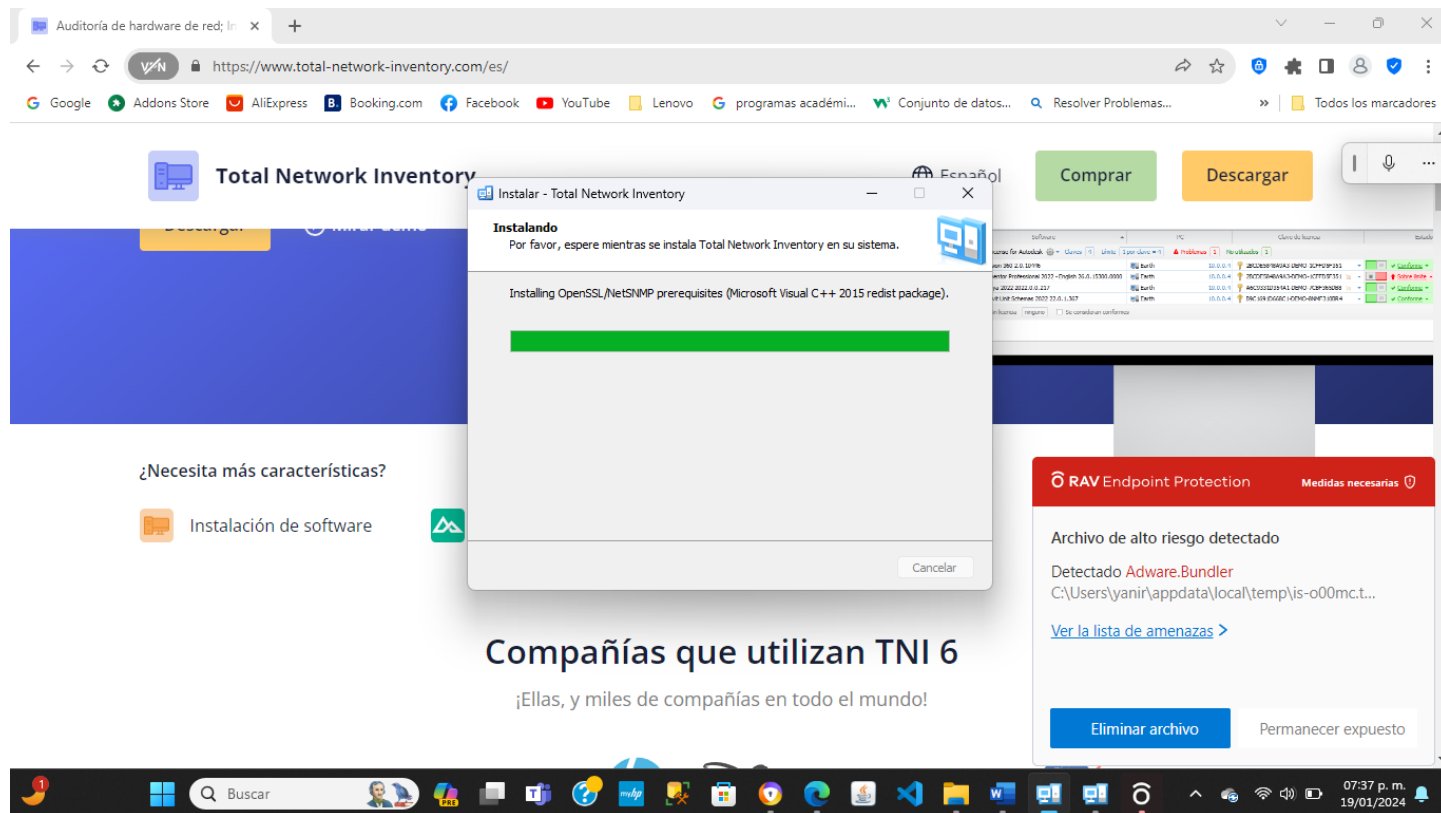
En la siguiente imagen podemos observar el inicio de la página de Network Inventory en la cual la podremos descargar la herramienta solicitada en la actividad.



Una vez se realizó la descarga podemos observar cómo se procede con la instalación.



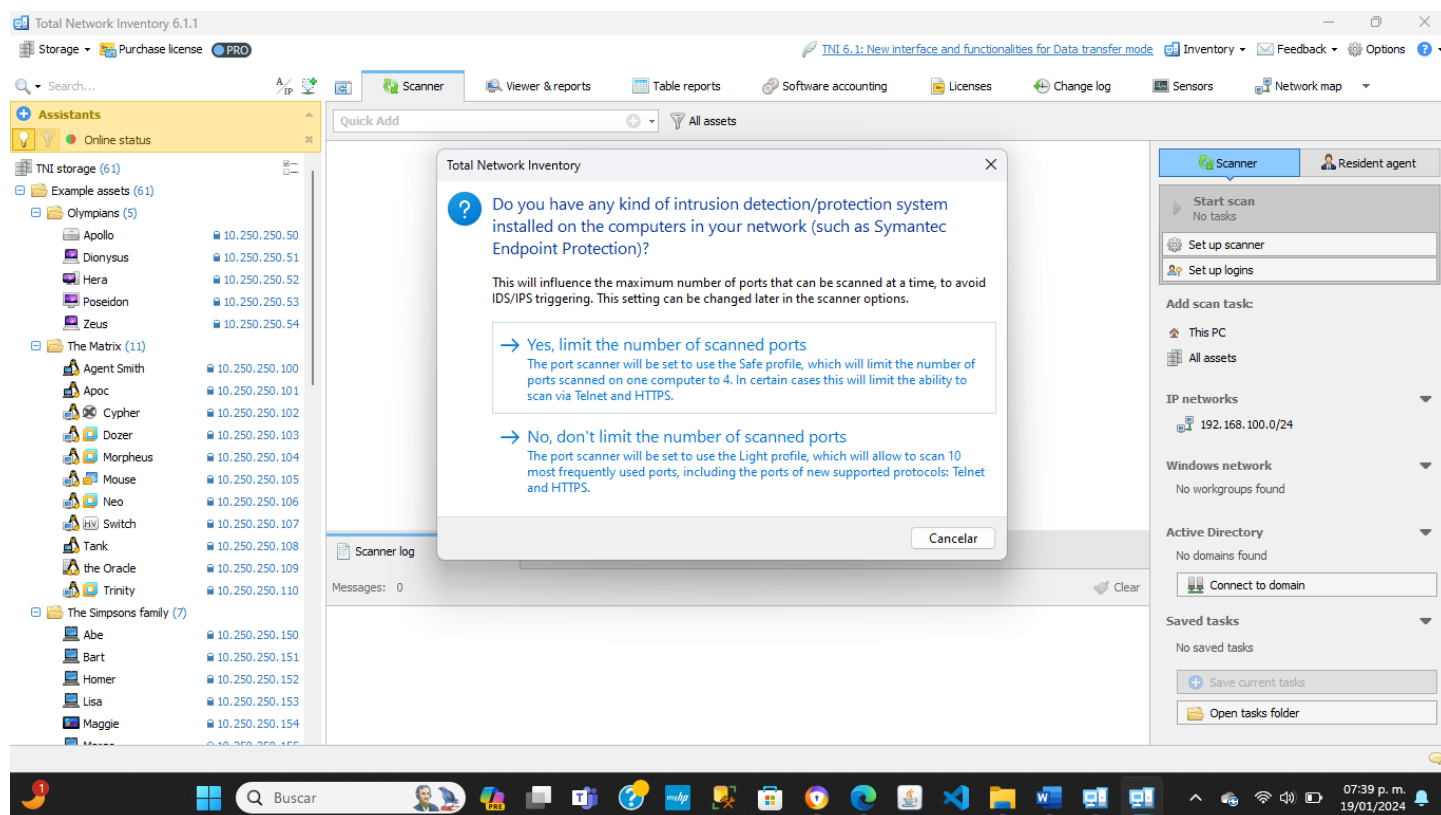
En la siguiente imagen se muestra la instalación de la herramienta Network Inventory.



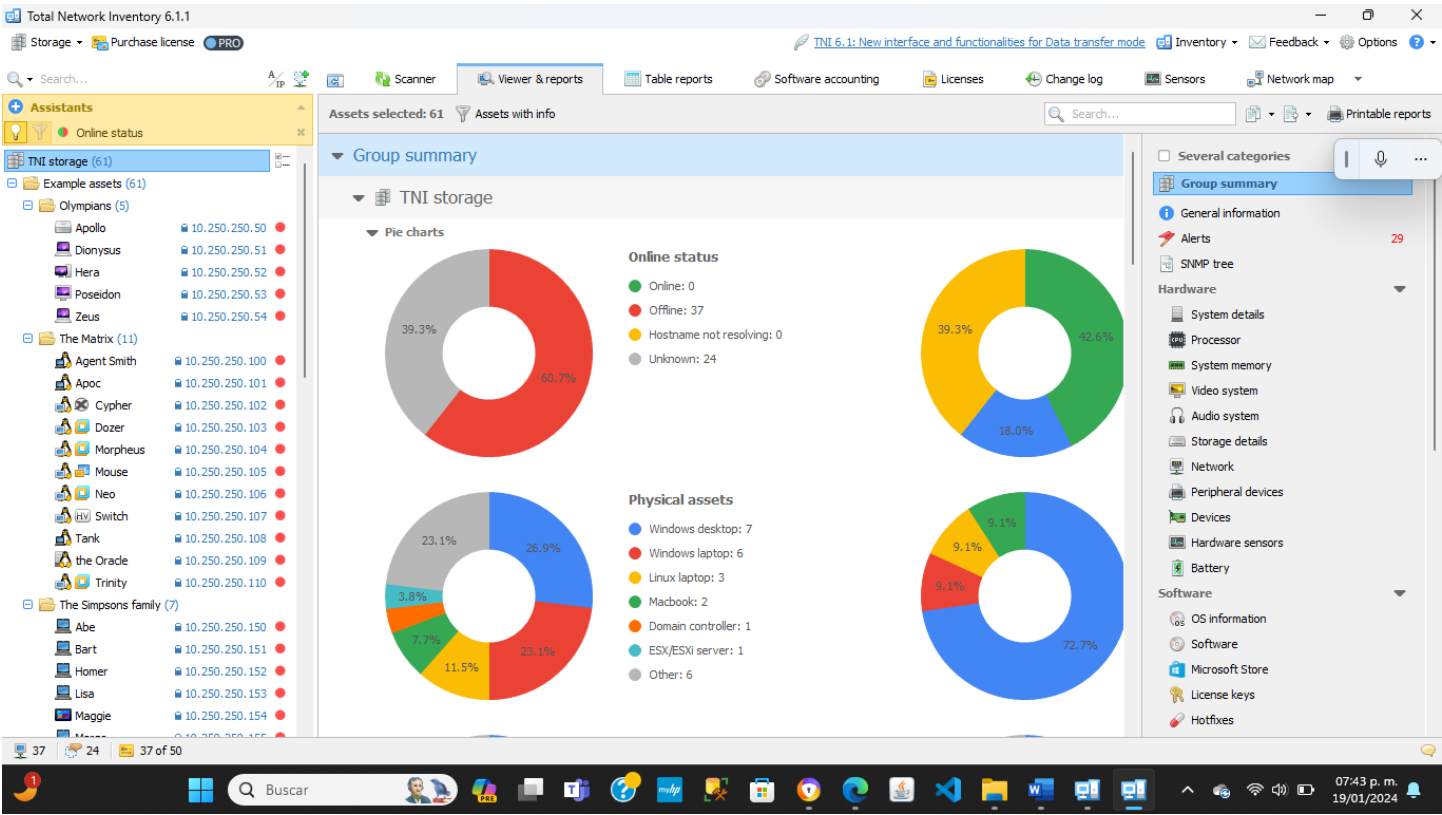
## Compañías que utilizan TNI 6

¡Ellas, y miles de compañías en todo el mundo!

Unas que nuestra herramienta fue instalada nos arroja el siguiente mensaje, en el cual debemos seleccionar no limitar el número de puertos a escanear.



Una vez realizada la configuración anterior nos arroja la siguiente imagen en la cual se muestra algunas ip conectadas a red.



En seguida realizamos una consulta en el CMD que nos permita conocer la ip de mi equipo, así como las mascara, las cual necesitare al momento de pedir el escaneo de mi equipo.

The screenshot shows a Windows desktop with a Command Prompt window open. The window displays the output of the 'ipconfig' command, showing network configuration details for the system.

```
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . . . :

Adaptador desconocido Conexión de área local 2:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . . . :

Adaptador de LAN inalámbrica Conexión de área local* 1:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . . . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . . . :

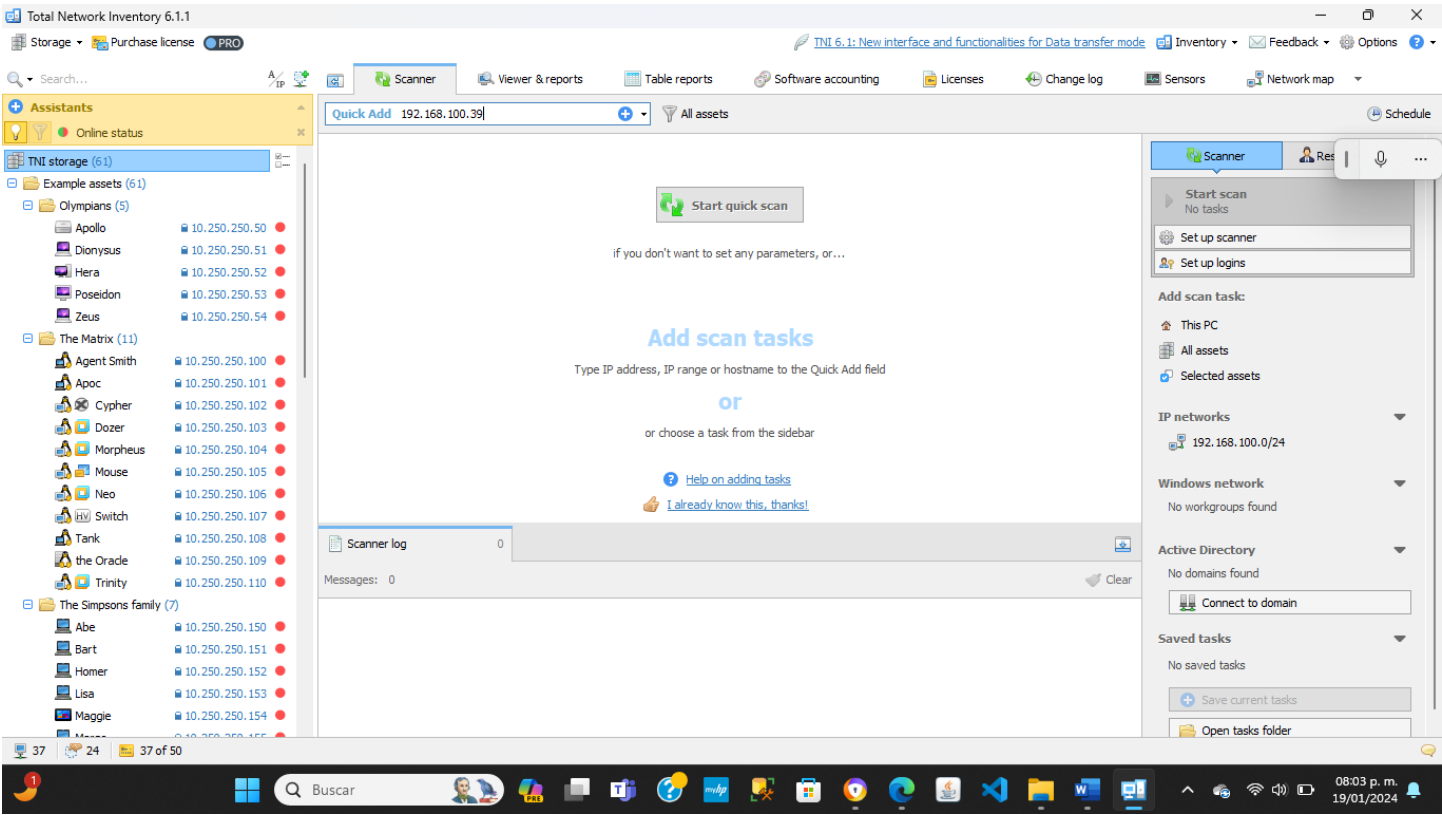
Adaptador de LAN inalámbrica Wi-Fi:

Sufijo DNS específico para la conexión. . . . . :
Dirección IPv6 . . . . . : 2806:2f0:2041:f420:2e1:54cc:50b0:d447
Dirección IPv6 temporal. . . . . : 2806:2f0:2041:f420:8400:5414:7b50:f802
Vínculo: dirección IPv6 local. . . . . : fe80::7c6d:d89c:38be:cb2f%18
Dirección IPv4. . . . . : 192.168.100.39
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : fe80::1%18
192.168.100.1

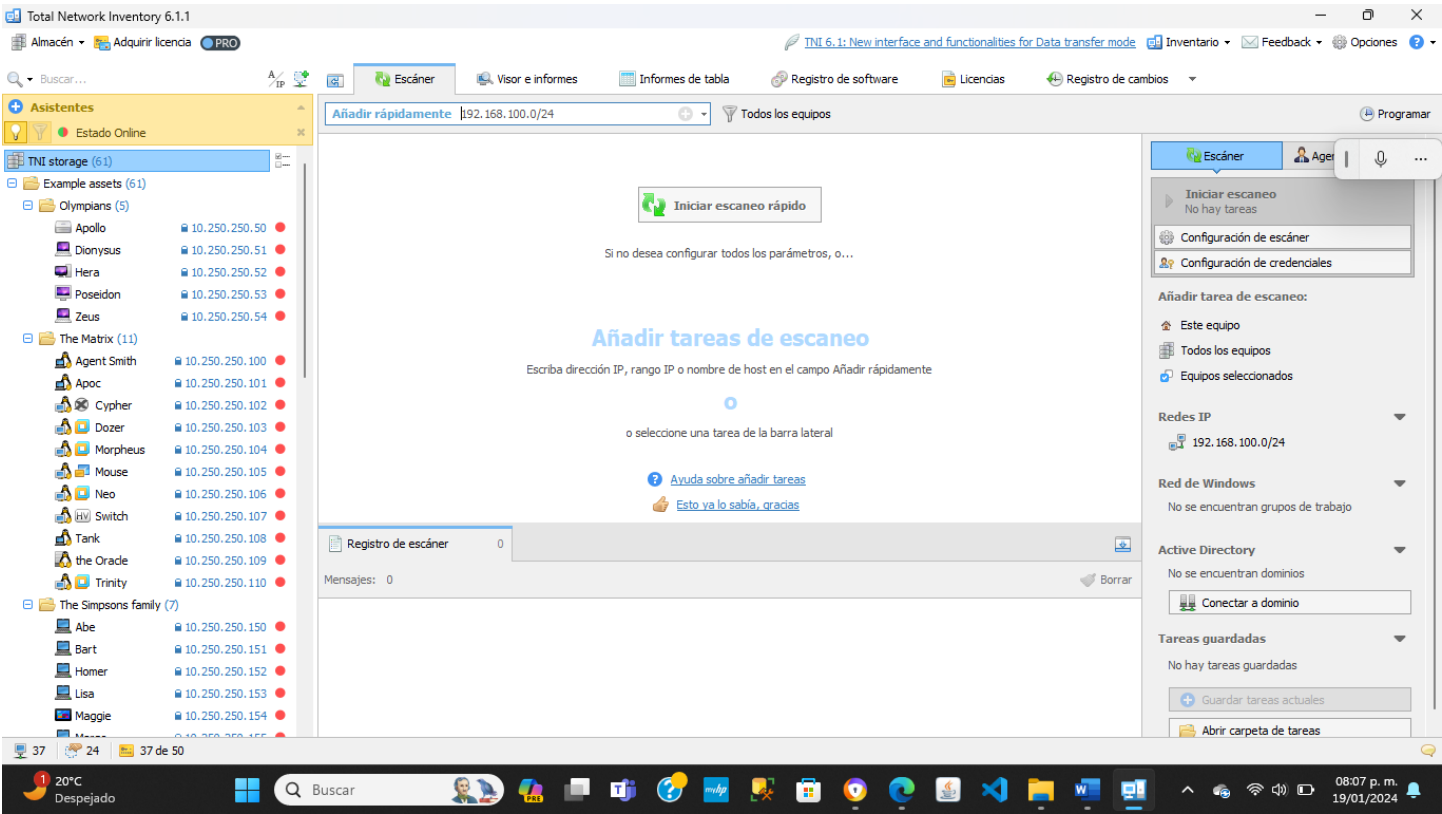
C:\Users\yanir|
```



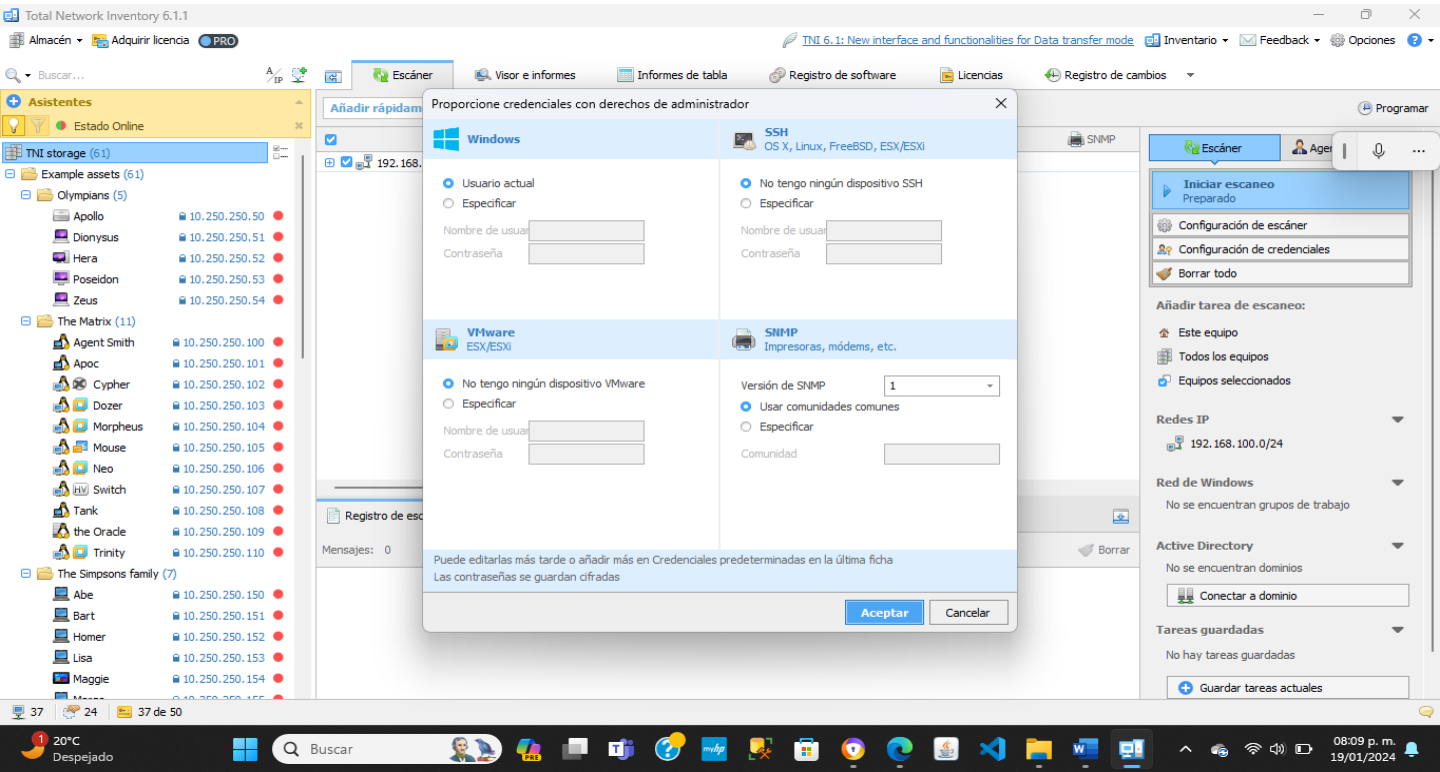
En la siguiente imagen podemos observar la pantalla que nos permite ingresar el numero de la ip. de mi equipo, la cual es 192.168.100.39 la cual es la que se muestra en el renglón de Quick Add.



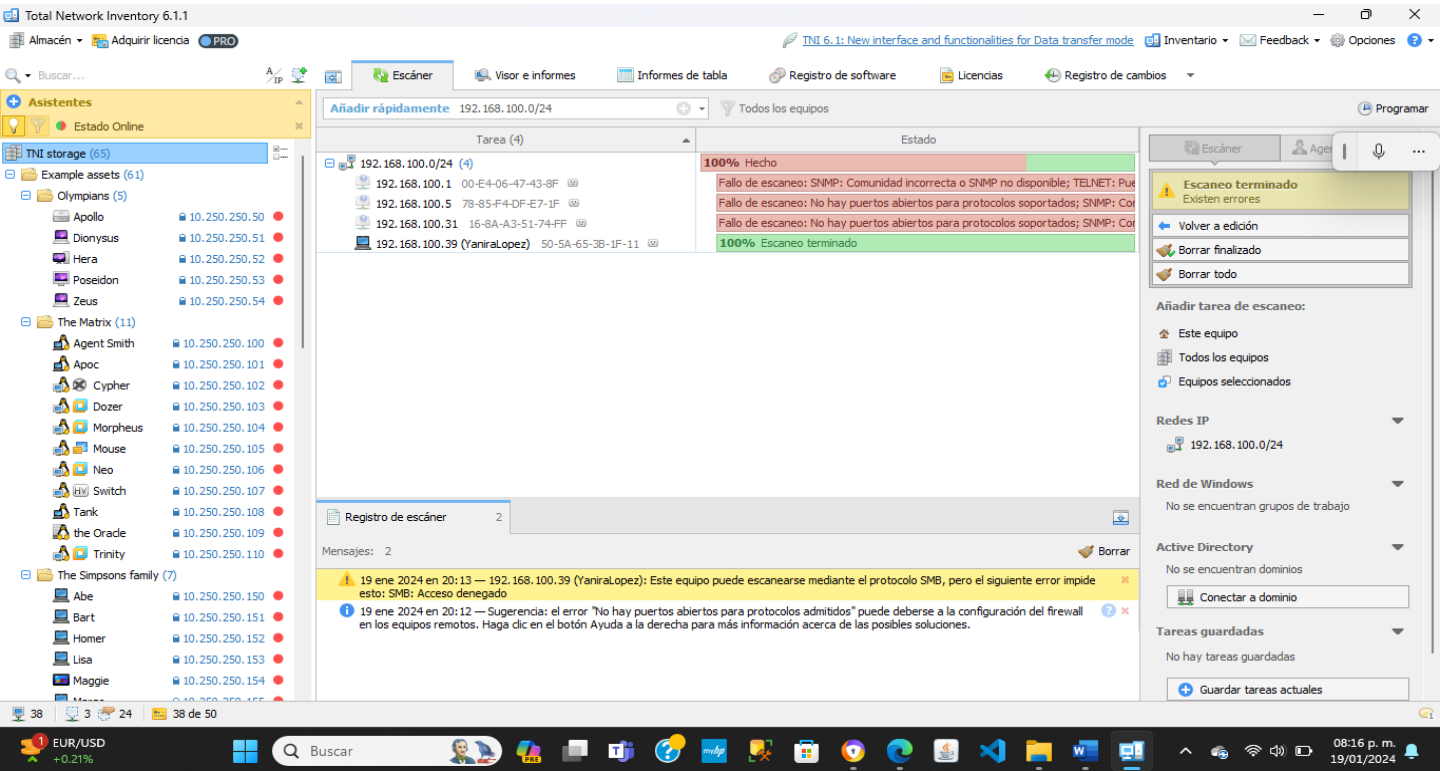
En seguida procedemos la indicación de iniciar escaneo rápido.



Una vez que se ejecutó la indicación de realizar el escaneo nos arroja la siguiente pantalla, en la cual solo decidimos seleccionar aceptar.

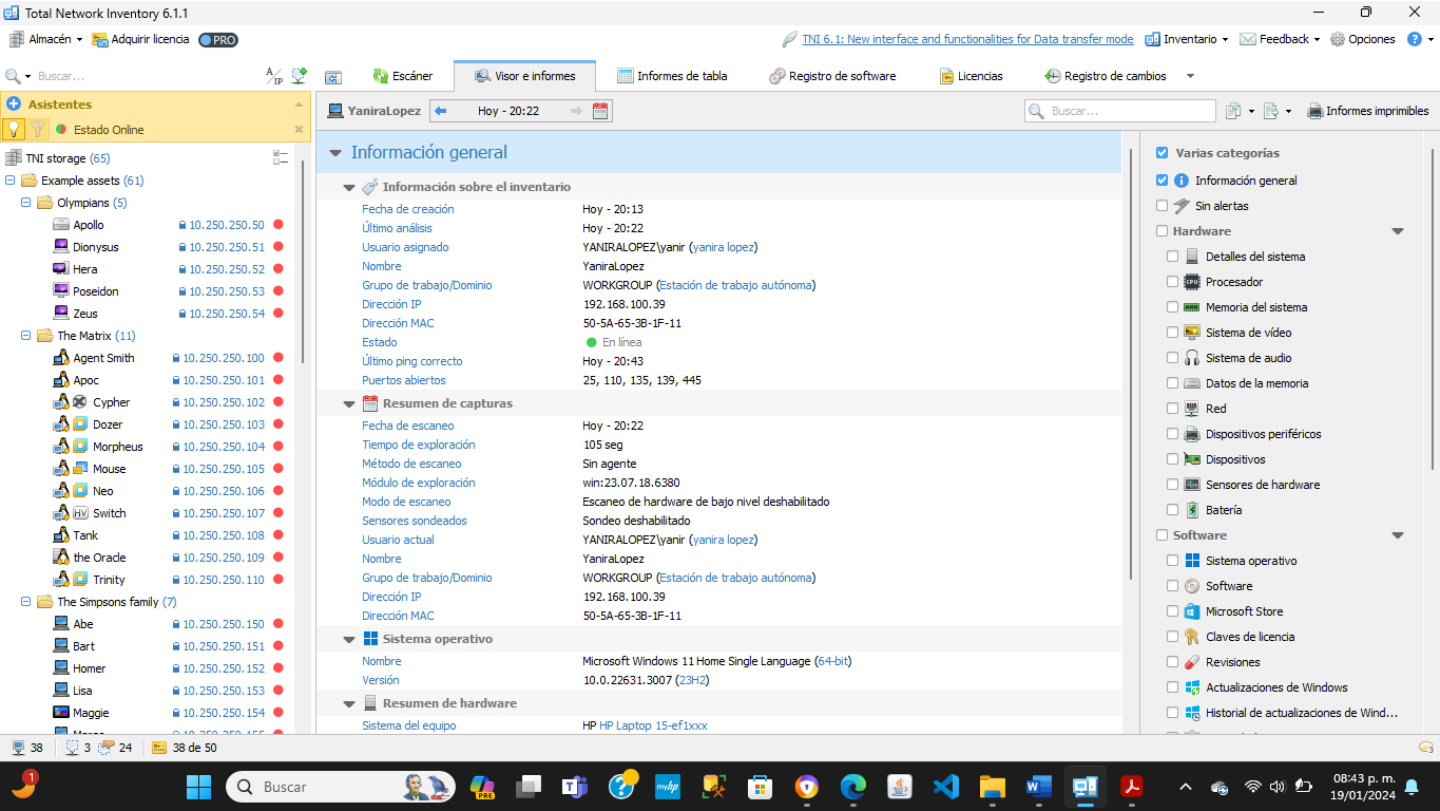


Una vez finalizado el escaneo del equipo nos arroja la siguiente pantalla en la cual podemos observar que en la ip de mi equipo la cual se le proporcionó si se completó el escaneo al 100% en cambio para el resto de las ip que se muestran nos arroja un error.

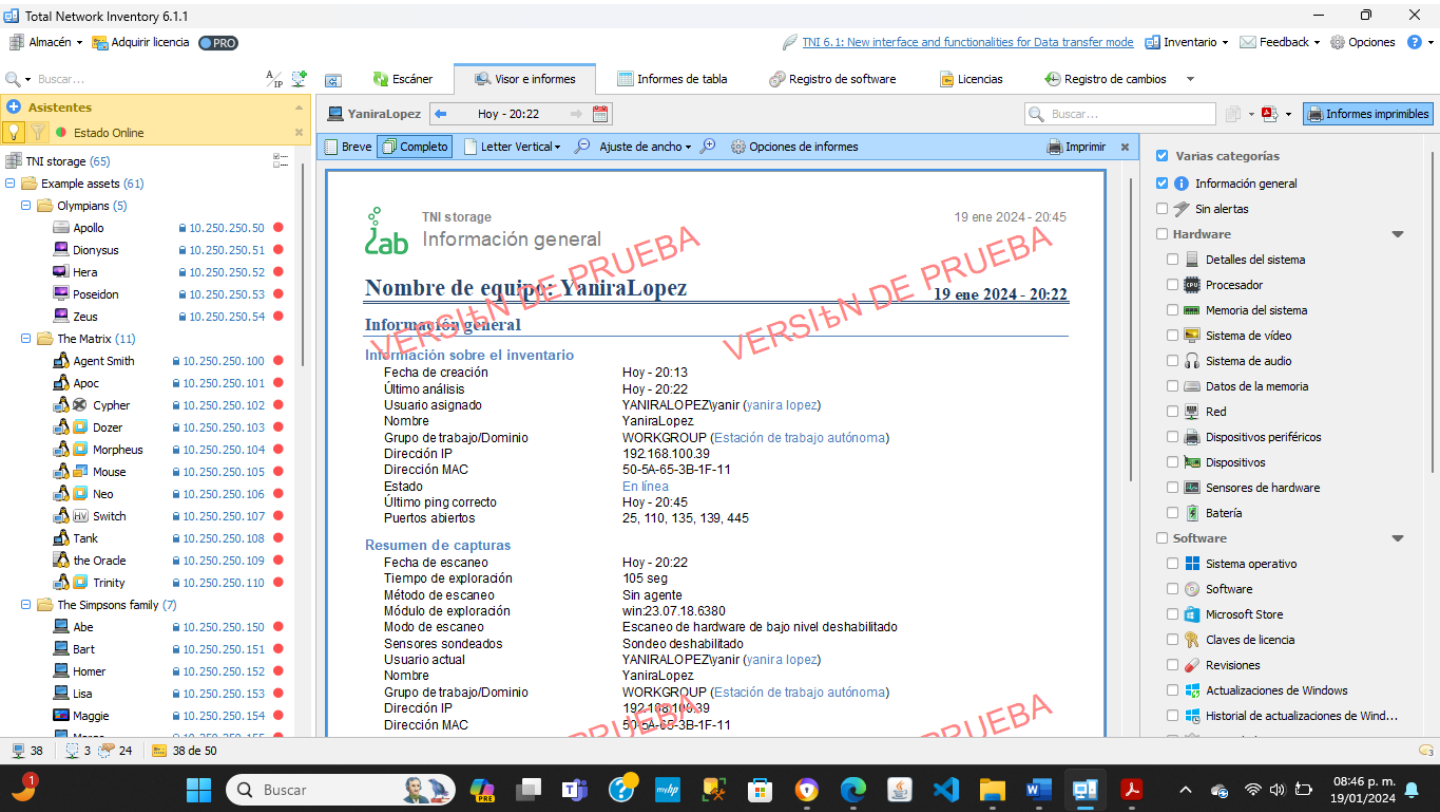


# Reporte

En seguida podemos observar el reporte generado por el escaneo solicitado hace un momento.



A continuación, nos muestra esta pantalla una vez de solicitar la exportación del reporte.



Una vez que el reporte fue exportado así nos lo muestra.

The screenshot displays a web browser window with a top navigation bar containing menu icons and labels like "Actividad", "Reporte generado p...", "+ Create", and "Iniciar sesión". Below the navigation bar is a search bar labeled "Buscar texto o herramientas" and several utility icons.

The main content area shows a report titled "Informe general" for "Nombre de equipo: YaniraLopez". The report date is "19 ene 2024 - 20:45".

**Información sobre el inventario:**

|                          |  |
|--------------------------|--|
| Fecha de creación        | Hoy - 20:13                              |
| Último análisis          | Hoy - 20:22                              |
| Usuario asignado         | YANIRALOPEZ,yanir (yanira lopez)         |
| Nombre                   | YaniraLopez                              |
| Grupo de trabajo/Dominio | WORKGROUP (Estación de trabajo autónoma) |
| Dirección IP             | 192.168.100.39                           |
| Dirección MAC            | 50-5A-65-3B-1F-11<br>(nueva)             |
| Estatus                  | Hoy - 20:45                              |
| Último ping correcto     | Hoy - 20:45                              |
| Puertos abiertos         | 25, 110, 135, 139, 445                   |

**Resumen de capturas:**

|                          |   |
|--------------------------|---|
| Fecha de escaneo         | Hoy - 20:22                                     |
| Tiempo de exploración    | 105 seg   |
| Método de escaneo        | Sin agente                                      |
| Módulo de exploración    | wmi:23.07.18.6360                               |
| Modo de escaneo          | Escaneo de hardware de bajo nivel deshabilitado |
| Sensores conectados      | Código desahabilitado                           |
| Usuario actual           | YANIRALOPEZ,yanir (yanira lopez)                |
| Nombre                   | YaniraLopez                                     |
| Grupo de trabajo/Dominio | WORKGROUP (Estación de trabajo autónoma)        |
| Dirección IP             | 192.168.100.39                                  |
| Dirección MAC            | 50-5A-65-3B-1F-11                               |

**Sistema operativo:**

|         |   |
|---------|---|
| Nombre  | Microsoft Windows 11 Home Single Language (x64-bit) |
| Versión | 10.0.22H1.3007 (23H2)                               |

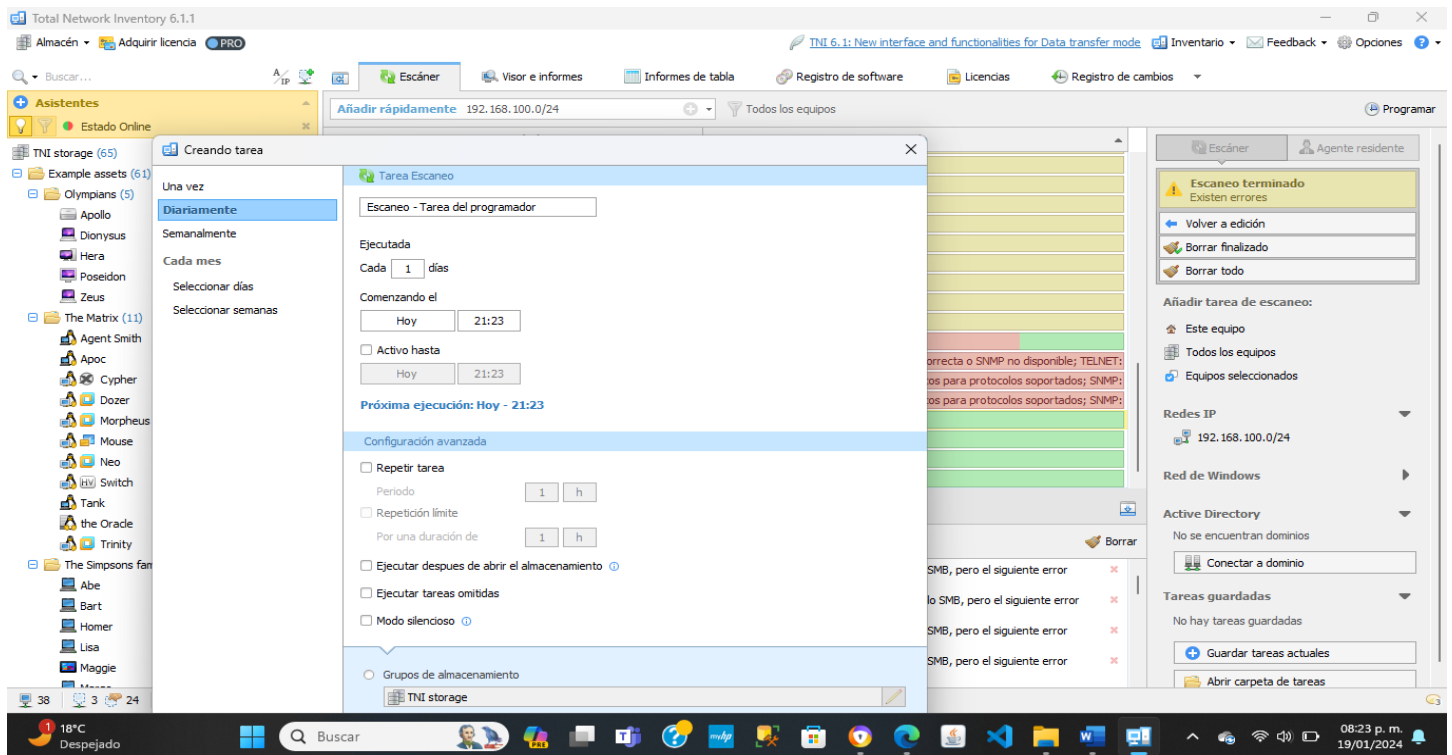
**Referencias de hardware:**

|                               |   |
|-------------------------------|---|
| Sistema del equipo            | HP HP Laptop 14-e2000t                                      |
| Número de serie               | SCD0113L35  |
| Procesador                    | 1 x AMD Athlon Silver 3050U with Radeon Graphics (2300 MHz) |
| Placa base                    | HP (n/a)  |
| Memoria del sistema           | 8 GB  |
| Adaptador de video            | AMD Radeon Graphics   |
| Monitor                       | AUC0191 (15.3")   |
| Dispositivo de almacenamiento | SK hynix BC711 HFM256GDJUXD13N (256 GB)                     |
| Dispositivo de sonido         | Realtek High Definition Audio                               |
| Impresora                     | Microsoft Print to PDF (Predefinida), PORTPROMPT,           |
| Impresora                     | OneNote (Desktop) (n/a)                                     |

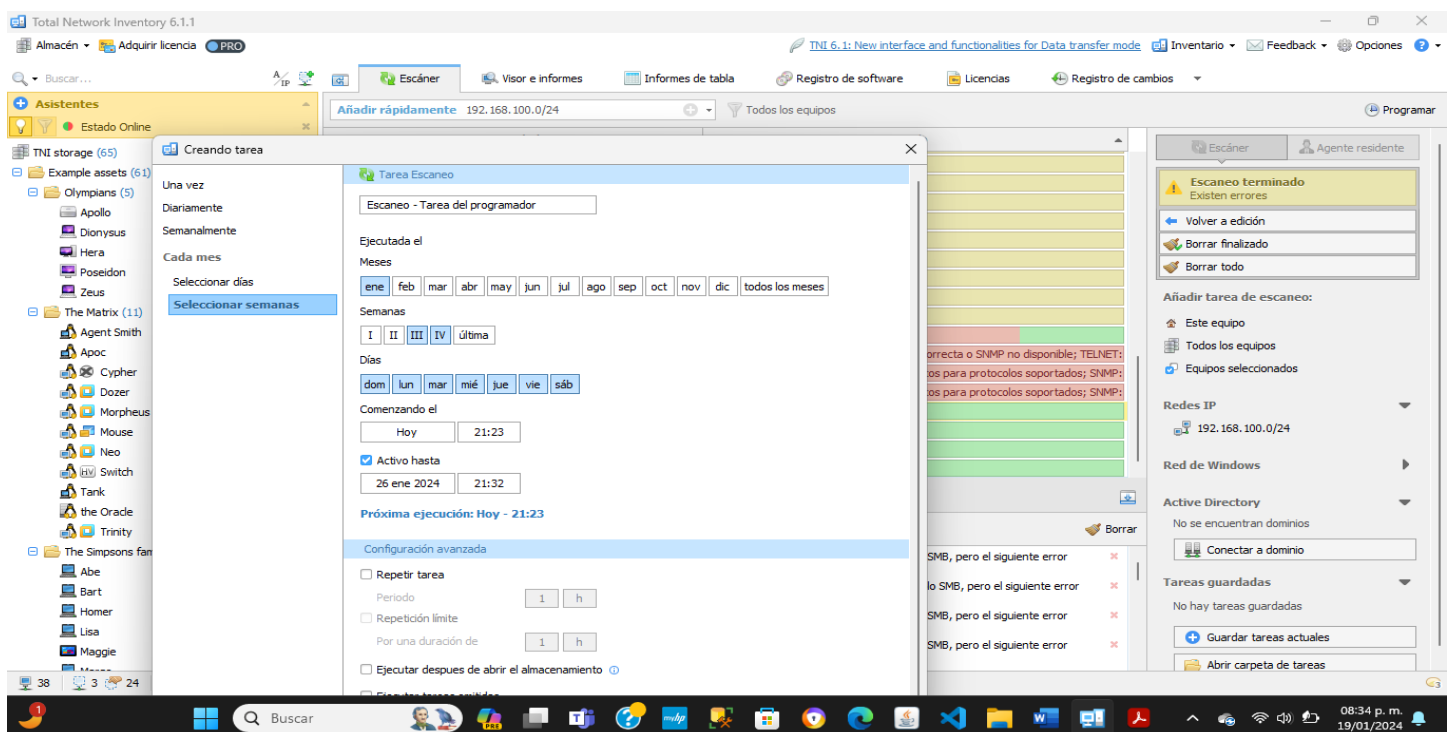
The bottom of the browser window shows a taskbar with various application icons and a system tray on the right displaying the time as 09:03 p.m. on 19/01/2024.

# Auditoría semanal y reporte

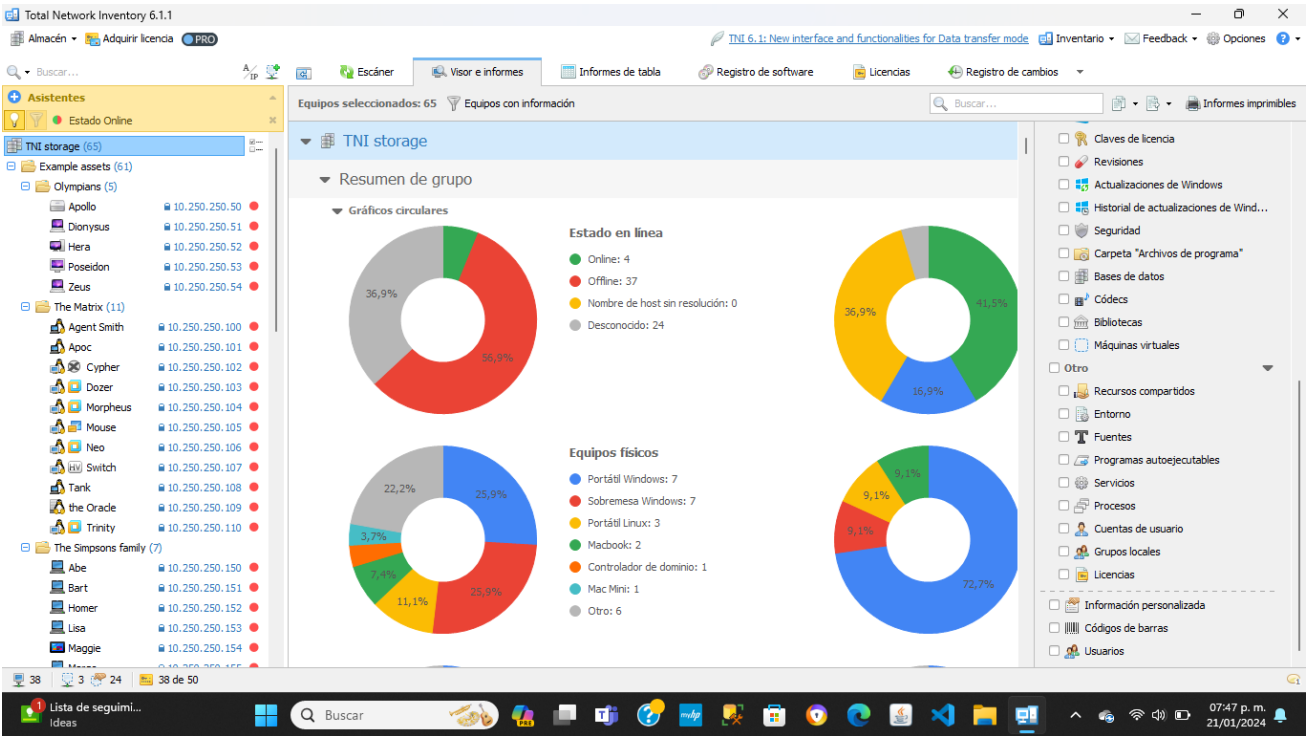
En la siguiente imagen podemos observar la pantalla en la cual nos permite realizar algunas de las configuraciones indicadas en la actividad como por ejemplo 1 día como se muestra en la imagen.



A continuación, modificamos la configuración anterior ya que en la actividad se solicita que sea durante 1 semana, la cual inicia hoy y termina el día 26 de enero de 2024.



A continuación, se muestra el reporte generado después de 2 días de haber realizado las configuraciones indicadas en el material de estudio.



## Conclusión

En conclusión, la actividad dedicada al monitoreo de red emerge con impacto directo en el ámbito laboral y en la vida cotidiana. La implementación de estas estrategias y herramientas avanzadas no solo se traduce en la defensa activa de la integridad de los sistemas, sino que también marca la diferencia en la eficiencia operativa diaria.

En el contexto laboral, la importancia radica en la capacidad de anticiparse y prevenir posibles amenazas, garantizando la continuidad de las operaciones y protegiendo la información sensible. La respuesta ágil a eventos inesperados se convierte en un diferenciador clave para minimizar impactos negativos y mantener la productividad.

A nivel personal, la conciencia constante proporcionada por el monitoreo de red se traduce en una mayor seguridad en nuestras interacciones digitales. La prevención de intrusiones y la detección temprana de posibles problemas se alinean con la necesidad de salvaguardar la privacidad y la confidencialidad en la vida cotidiana.

La actividad realizada no solo fortalece la postura de seguridad en el entorno laboral, sino que también brinda un sentido de tranquilidad en el ámbito personal al proporcionar las herramientas necesarias para enfrentar los desafíos en el mundo digital actual.



## Referencias

Ingeniería en desarrollo de software. Universidad México Internacional. Recuperado el día 16 de enero de 2024, <https://umi.edu.mx/coppel/IDS/mod/scorm/player.php>

Global, A. (2024, 9 enero). *Video 1 DynaTrace Synthetic Monitoring Monitorización de disponibilidad y rendimiento de las aplicaciones web.mp4* [Vídeo]. Vimeo.

<https://vimeo.com/660530504/e6e2591340>

Global, A. (2024b, enero 14). *Video 2 Auditoría de vulnerabilidades en la red con Nessus* [Vídeo].

Vimeo. <https://vimeo.com/660530360/ad1982a98c>

*Video conferencing, web conferencing, webinars, screen sharing.* (s. f.). Zoom.

<https://academiaglobal->

[mx.zoom.us/rec/play/gWzPS3uYC39mKO2DO6BHcGnawsHGU83ki1Xsu6lJ7MS0vD3MrHy\\_d4MBD3kgKjQVanvSStiv6ga4JbA1.MOQCG88rlfVAnI5U?canPlayFromShare=true&from=share\\_recording\\_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2F3fhpzQYPUaAHyt7CQTM1mS8E4G52cYmQOnHLLtPq9XcM5f7Pnnbu8scnVAY1MbSq.fVGa69AQ\\_I\\_VhXXw](https://mx.zoom.us/rec/play/gWzPS3uYC39mKO2DO6BHcGnawsHGU83ki1Xsu6lJ7MS0vD3MrHy_d4MBD3kgKjQVanvSStiv6ga4JbA1.MOQCG88rlfVAnI5U?canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2F3fhpzQYPUaAHyt7CQTM1mS8E4G52cYmQOnHLLtPq9XcM5f7Pnnbu8scnVAY1MbSq.fVGa69AQ_I_VhXXw)