



Etapa | # 2|Monitoreo de Red

Seguridad Informática II

Ingeniería en Desarrollo de
Software



TUTOR: Jessica Hernández Romero

ALUMNO: Sarahi Jaqueline Gomez Juárez

FECHA: martes 02 de febrero de 2026

Índice

Índice	2
Introducción:	5
Descripción:	7
Justificación:.....	10
Desarrollo:	13
Etapa 2 - Monitoreo de Red	13
Contextualización:	13
<i>Página Oficial de Descarga de Total Network Inventory:</i>	<i>14</i>
<i>Archivo Ejecutable Descargado del Instalador del Sistema.....</i>	<i>14</i>
<i>Pantalla de Bienvenida del Asistente de Instalación de Total Network Inventory</i>	<i>15</i>
<i>Proceso de Instalación y Extracción de Archivos del Sistema.....</i>	<i>15</i>
<i>Selección del Tipo de Almacenamiento del Sistema de inventario.....</i>	<i>16</i>
<i>Interfaz Principal del Sistema Lista para Añadir Tareas de Escaneo.....</i>	<i>17</i>
<i>Configuración de Tareas de Escaneo con Dirección IP de la Red Local.....</i>	<i>18</i>
<i>Configuración de Credenciales Administrativas para el Escaneo.....</i>	<i>18</i>
Resultado del Escaneo	19
<i>Ejecución del Escaneo de Red en Progreso</i>	<i>19</i>
<i>Resultados del Escaneo con Detección de Dispositivos y Errores</i>	<i>20</i>
<i>Ejecución del escaneo de red en el rango 192.168.1.0/24.....</i>	<i>20</i>
<i>Progreso Del Análisis de Hardware del Equipo Sarahialeluya</i>	<i>22</i>
<i>Finalización del Escaneo con Errores Detectados</i>	<i>22</i>

Reporte:	23
<i>Información General del Sistema Inventariado</i>	<i>23</i>
<i>Detalles Ampliados del Hardware y Sistema Operativo</i>	<i>24</i>
<i>Alerta de Poco Espacio Libre en Disco</i>	<i>24</i>
<i>Información Detallada del Sistema Base y BIOS.....</i>	<i>25</i>
<i>Ranuras de sistema y puertos detectados</i>	<i>26</i>
<i>Estado del Módulo TPM para Seguridad.....</i>	<i>26</i>
<i>Detalles del Procesador Intel Core i5 Detectado</i>	<i>27</i>
<i>Estado y Uso de la Memoria del Sistema</i>	<i>28</i>
<i>Información del Sistema de Video.....</i>	<i>28</i>
<i>Dispositivos del Sistema de Audio</i>	<i>29</i>
<i>Visualización del Uso de Almacenamiento</i>	<i>29</i>
<i>Adaptadores de Red Detectados.....</i>	<i>30</i>
<i>Redes Inalámbricas Disponibles</i>	<i>30</i>
<i>Historial de Redes Guardadas</i>	<i>31</i>
<i>Generación de Informe General del Sistema.....</i>	<i>31</i>
<i>Vista Previa del Informe Imprimible de Software Instalado (Inventario del Equipo)</i>	<i>32</i>
<i>Revisión del Estado de Seguridad del Equipo (Antivirus y Firewall).....</i>	<i>33</i>
Auditoría Semanal y Reporte:	34
<i>Configuración de una Tarea Programada para Generar el Informe del Registro de Cambios (Ajustes Avanzados).....</i>	<i>34</i>
<i>Definición de Periodicidad Semanal (Día y Hora) para la Ejecución</i>	

<i>Automática del Informe</i>	35
<i>Validación en el Programador: Tarea Creada y Próxima Ejecución Registrada</i>	36
Conclusión:	38
Referencias:	41

Introducción:

En el presente proyecto que trata el contexto actual de la seguridad informática, donde las amenazas ciberneticas evolucionan constantemente y los sistemas tecnológicos se encuentran cada vez más interconectados, resulta indispensable adoptar estrategias integrales que no solo permitan detectar vulnerabilidades, sino también supervisar de manera continua el estado de los equipos y la red, la protección efectiva de la información requiere una combinación de auditorías técnicas periódicas y mecanismos de monitoreo constante que aseguren el control de activos, configuraciones y cambios dentro de la infraestructura informática.

En la Etapa 1 del proyecto se desarrolló una auditoría de vulnerabilidades mediante la herramienta Tenable Nessus Essentials, la cual permitió identificar riesgos asociados a servicios activos, configuraciones inseguras y componentes críticos como OpenSSL, Apache HTTP y el protocolo SMB, a través de este análisis se evidenció que, aunque no se detectaron amenazas críticas inmediatas, el sistema presentaba múltiples exposiciones informativas y vulnerabilidades de nivel medio que podían ser aprovechadas por atacantes, esta fase resultó fundamental para comprender la postura de seguridad del equipo y establecer medidas de mitigación orientadas a la prevención de ataques de acceso no autorizado.

Sin embargo, la detección de vulnerabilidades representa únicamente una parte del proceso de seguridad informática, para lograr una protección efectiva y sostenible en el tiempo, es necesario complementar las auditorías con sistemas de monitoreo que permitan supervisar continuamente la red, los dispositivos conectados, el hardware, el software instalado y los cambios que se producen en la infraestructura tecnológica, de esta manera, se pueden identificar alteraciones no autorizadas, fallos de configuración, consumo excesivo de recursos y posibles

indicadores de incidentes de seguridad antes de que se conviertan en amenazas graves.

En este sentido, la Etapa 2 del proyecto se enfoca en el monitoreo de red mediante la implementación de la herramienta Total Network Inventory, la cual permite realizar inventarios detallados de dispositivos, analizar componentes de hardware, supervisar aplicaciones instaladas, validar el estado de controles de seguridad y automatizar reportes de cambios del sistema, esta etapa complementa directamente la auditoría realizada con Nessus, ya que proporciona una visión continua y estructurada del entorno tecnológico, fortaleciendo la gestión de activos y la detección temprana de riesgos.

La integración de ambas etapas: auditoría de vulnerabilidades y monitoreo de red, conforma un enfoque preventivo e integral de la seguridad informática, donde no solo se identifican fallos técnicos, sino que también se mantiene un control constante sobre la infraestructura, este modelo permite reducir la superficie de ataque, mejorar la respuesta ante posibles incidentes y promover buenas prácticas de protección de la información tanto en entornos académicos como profesionales.

Descripción:

El presente proyecto desarrolla un proceso integral de monitoreo y auditoría de red mediante la implementación de la herramienta Total Network Inventory, con el objetivo de fortalecer la seguridad informática a través del control de dispositivos, análisis de hardware, supervisión de software y automatización de reportes de cambios en el sistema, a lo largo del documento se evidencia la importancia de contar con un sistema de monitoreo continuo que permita identificar activos tecnológicos, detectar configuraciones inseguras y prevenir accesos no autorizados dentro de una infraestructura de red.

El trabajo inicia con la descarga e instalación del software desde su sitio oficial, garantizando la procedencia confiable de la herramienta y reduciendo riesgos asociados a programas maliciosos, posteriormente, se configura el entorno de inventario seleccionando un almacenamiento local de un solo usuario, lo cual permite centralizar la información de los dispositivos monitoreados sin necesidad de bases de datos externas, disminuyendo la exposición de datos sensibles, desde la interfaz principal del sistema se establecen tareas de escaneo utilizando el rango de direcciones IP de la red local (192.168.1.0/24), lo que posibilita la detección automática de computadoras, equipos de red y otros dispositivos conectados.

Durante el proceso de escaneo se emplean credenciales administrativas y protocolos como SNMP, SSH y SMB para obtener información detallada de los sistemas analizados, incluyendo datos de hardware, sistema operativo, puertos abiertos y servicios activos, los resultados evidencian tanto dispositivos detectados correctamente como errores de comunicación ocasionados por configuraciones de firewall y restricciones de red, lo cual refleja la presencia de medidas defensivas parciales que limitan el acceso no autorizado, desde el enfoque de

ciberseguridad, estas barreras son positivas, aunque se destaca la necesidad de permitir accesos controlados durante auditorías internas para obtener análisis completos.

Uno de los aspectos más relevantes del proyecto es el análisis profundo del hardware del equipo inventariado, donde se recopilan datos sobre el procesador, memoria, almacenamiento, BIOS, adaptadores de red, módulos de seguridad como TPM y dispositivos periféricos, esta información resulta fundamental para la gestión de activos tecnológicos, ya que permite identificar componentes obsoletos, configuraciones inseguras y posibles vulnerabilidades asociadas a firmware desactualizado o controladores antiguos, asimismo, se detectan alertas críticas como el bajo espacio en disco y el alto consumo de memoria, factores que pueden afectar el funcionamiento del sistema y comprometer la correcta generación de registros de seguridad.

El sistema también permite visualizar redes inalámbricas disponibles e historial de conexiones previas, proporcionando información clave para auditorías de seguridad, ya que facilita identificar conexiones a redes potencialmente inseguras o no autorizadas, de igual manera, se genera un informe detallado del software instalado en el equipo, lo cual es esencial para el control de aplicaciones, detección de programas no autorizados y verificación de versiones vulnerables que podrían incrementar la superficie de ataque.

Como parte del enfoque de monitoreo continuo, se revisa el estado de controles básicos de seguridad, como el antivirus y el firewall, confirmando que se encuentren habilitados y operativos, esta verificación representa una medida mínima de protección que contribuye a la mitigación de amenazas comunes como malware y accesos indebidos, sin embargo, el proyecto enfatiza que estas herramientas deben complementarse con políticas de actualización, configuraciones de red adecuadas y supervisión constante.

Finalmente, se configura una tarea programada para la generación automática de

informes del registro de cambios del sistema, estableciendo una periodicidad semanal con día y hora específicos, esta automatización permite mantener una bitácora continua de modificaciones en hardware, software y configuraciones, facilitando la detección temprana de alteraciones no autorizadas o comportamientos anómalos, la validación de la tarea en el programador confirma que el monitoreo quedó correctamente configurado, cerrando el ciclo de auditoría continua.

En conjunto, el proyecto demuestra la importancia del monitoreo de red como una estrategia preventiva dentro de la seguridad informática, ya que no solo permite identificar dispositivos conectados y vulnerabilidades técnicas, sino también mantener un control detallado de los cambios en la infraestructura tecnológica. La integración de inventarios de hardware, supervisión de software, revisión de controles de seguridad y automatización de reportes contribuye significativamente a fortalecer la postura de seguridad del sistema, reducir riesgos de accesos no autorizados y promover una gestión eficiente de los recursos tecnológicos.

Justificación:

La realización del presente proyecto se ha realizado por la creciente necesidad de fortalecer la seguridad informática en un entorno donde los sistemas tecnológicos se encuentran cada vez más expuestos a amenazas ciberneticas, en la actualidad, los ataques de acceso no autorizado, la explotación de vulnerabilidades y la manipulación de información representan riesgos constantes tanto para organizaciones como para usuarios individuales, lo que hace indispensable la implementación de estrategias preventivas basadas en auditorías técnicas y monitoreo continuo de redes y sistemas.

Hay que recordar que en la Etapa 1 del proyecto se llevó a cabo una auditoría de vulnerabilidades mediante la herramienta Nessus Essentials, la cual permitió identificar fallos técnicos, servicios expuestos y configuraciones inseguras que podían ser aprovechadas por atacantes, no obstante, la detección puntual de vulnerabilidades resulta insuficiente si no se acompaña de mecanismos que permitan supervisar de forma constante el estado de los equipos y la red, por esta razón, la Etapa 2 se enfoca en el monitoreo de red utilizando Total Network Inventory, herramienta que complementa la auditoría inicial al proporcionar un control permanente de dispositivos conectados, hardware, software y cambios en la infraestructura tecnológica.

El monitoreo continuo se justifica como una práctica fundamental dentro de la ciberseguridad moderna, ya que permite identificar de manera temprana alteraciones no autorizadas, consumo anormal de recursos, instalaciones de software desconocido y configuraciones que pueden comprometer la seguridad del sistema, a través de inventarios detallados de activos tecnológicos, se facilita la gestión de recursos y se reducen riesgos

asociados a dispositivos obsoletos, firmware desactualizado y controladores vulnerables, asimismo, la supervisión de redes inalámbricas y adaptadores de red contribuye a detectar posibles accesos indebidos o conexiones inseguras.

Otro de sus objetivos clave es el desarrollo del proyecto, la automatización de auditorías mediante la programación de informes periódicos del registro de cambios del sistema, esta funcionalidad permite mantener una bitácora continua de modificaciones en hardware, software y configuraciones, fortaleciendo la trazabilidad y el control de la infraestructura informática, en términos de seguridad, contar con registros históricos facilita la identificación de incidentes, el análisis forense y la implementación de medidas correctivas oportunas.

Desde el punto de vista académico y profesional, la aplicación práctica de herramientas reales de monitoreo y auditoría de red contribuye significativamente al desarrollo de competencias técnicas en ciberseguridad. El uso de Total Network Inventory permite comprender cómo se gestionan activos tecnológicos, cómo se analizan sistemas y cómo se implementan mecanismos de supervisión continua en entornos reales, habilidades esenciales para el desempeño en áreas de tecnología de la información, redes y seguridad informática.

Finalmente, el proyecto tiene como meta identificar su impacto en la vida cotidiana , ya que fomenta una mayor conciencia sobre la protección de equipos personales y redes domésticas, conocer cómo funcionan los escaneos de red, la detección de dispositivos conectados y la supervisión de sistemas permite a los usuarios adoptar buenas prácticas de seguridad, mantener sus equipos actualizados y reducir la probabilidad de sufrir ataques comunes como intrusiones, robo de datos o infecciones de malware.

En conclusión, la implementación del monitoreo de red como complemento de la auditoría de vulnerabilidades representa una estrategia preventiva integral que fortalece la

postura de seguridad del sistema, mejora el control de recursos tecnológicos y promueve una cultura de seguridad informática responsable, este enfoque no solo permite detectar riesgos, sino también prevenir incidentes futuros mediante la supervisión constante y la aplicación de buenas prácticas, justificando plenamente la realización del proyecto en el ámbito académico, profesional y personal.

Desarrollo:**Etapa 2 - Monitoreo de Red****Contextualización:**

Se pretende utilizar algunas técnicas de protección ante ataques de explotación y obtención de acceso a sistemas auditando y monitoreando la red, en este sentido, deberás 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.
- 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.

Actividad: Instalar un software de monitoreo y analizar el equipo.

Software de monitoreo:

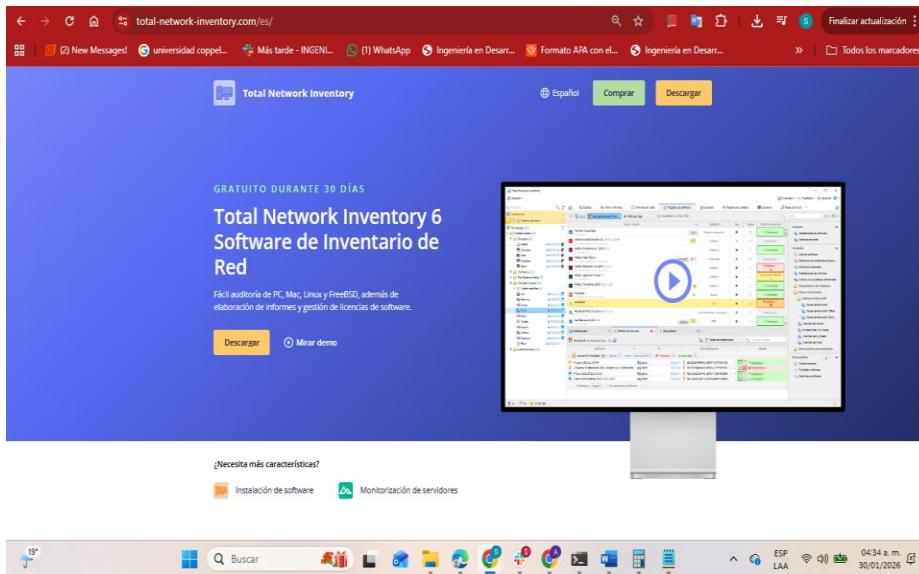
1. Seleccionar, instalar y analizar el equipo.

Escanear la red e identificar los dispositivos conectados a ella. Emitir un reporte que identifique cada uno de sus detalles.

2. Configurar una auditoría cada semana desde la opción Programación de auditoría.

Figura 1

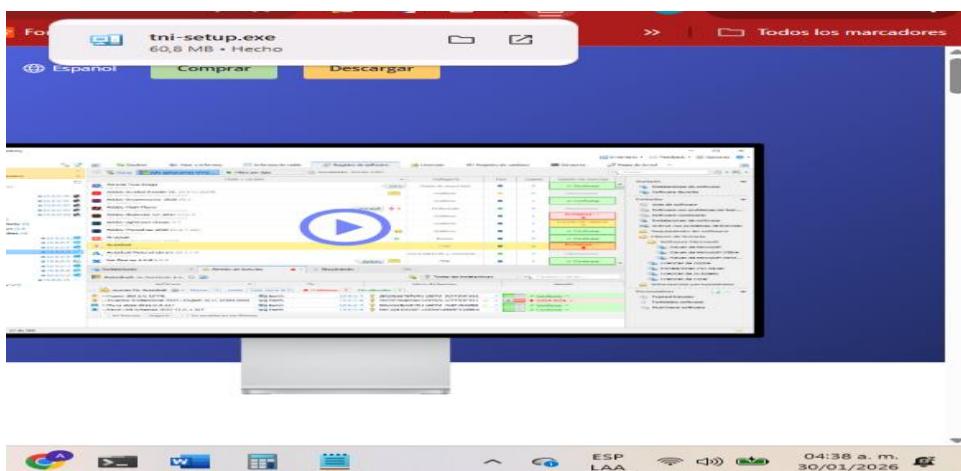
Página Oficial de Descarga de Total Network Inventory:



Nota: La imagen muestra el sitio oficial de Total Network Inventory, desde donde se obtiene el instalador del sistema, esta etapa es fundamental para garantizar que la herramienta provenga de una fuente confiable, evitando riesgos de malware o software modificado que pudiera comprometer la seguridad del equipo y de la red.

Figura 2

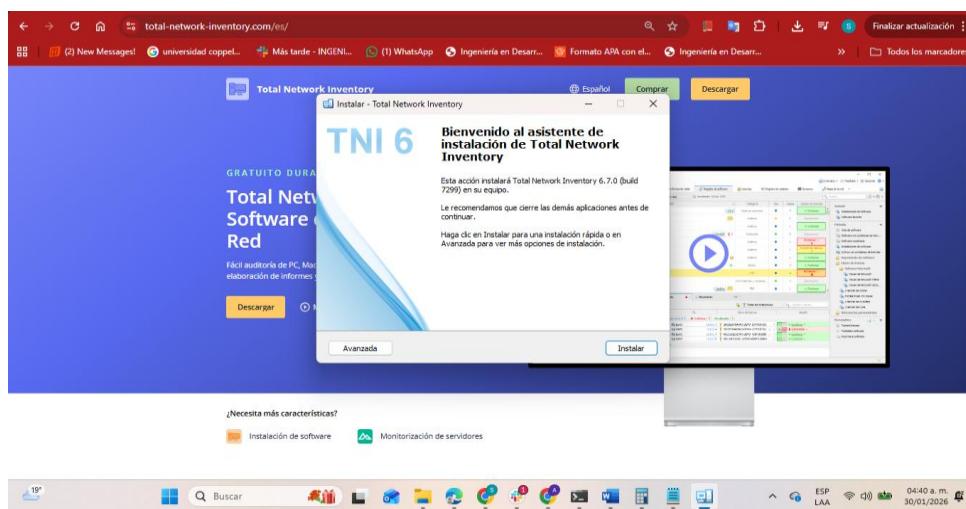
Archivo Ejecutable Descargado del Instalador del Sistema



Nota: Se observa el archivo ejecutable correspondiente al instalador del software, este archivo permite iniciar la instalación de la herramienta de inventario de red, paso esencial para implementar el sistema de monitoreo y auditoría de dispositivos dentro de la infraestructura informática.

Figura 3

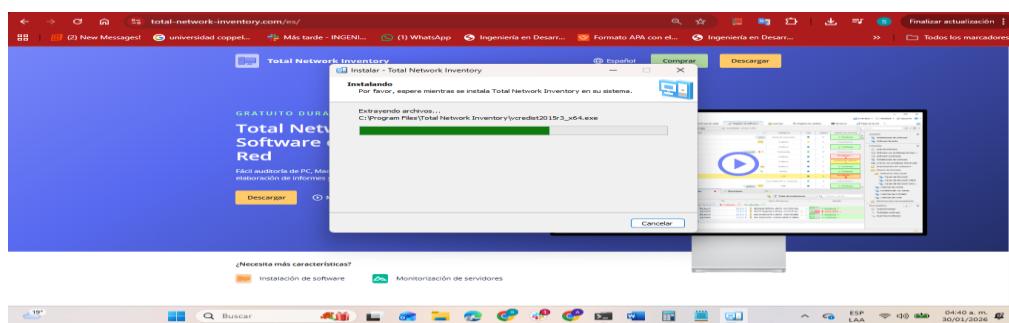
Pantalla de Bienvenida del Asistente de Instalación de Total Network Inventory



Nota: La imagen muestra el asistente de instalación del software, donde se informa la versión a instalar y se permite iniciar el proceso, esta fase asegura que el programa se configure correctamente en el sistema operativo antes de realizar cualquier análisis de red.

Figura 4

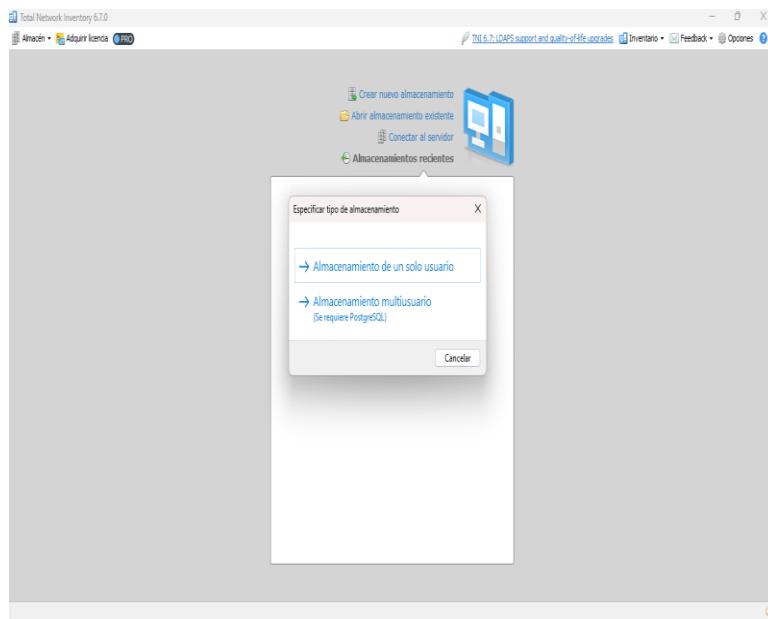
Proceso de Instalación y Extracción de Archivos del Sistema



Nota: Se visualiza el proceso automático de extracción e instalación de componentes necesarios para el funcionamiento de Total Network Inventory, este procedimiento instala librerías y servicios que permitirán la detección de dispositivos, recopilación de datos de hardware y monitoreo seguro.

Figura 5

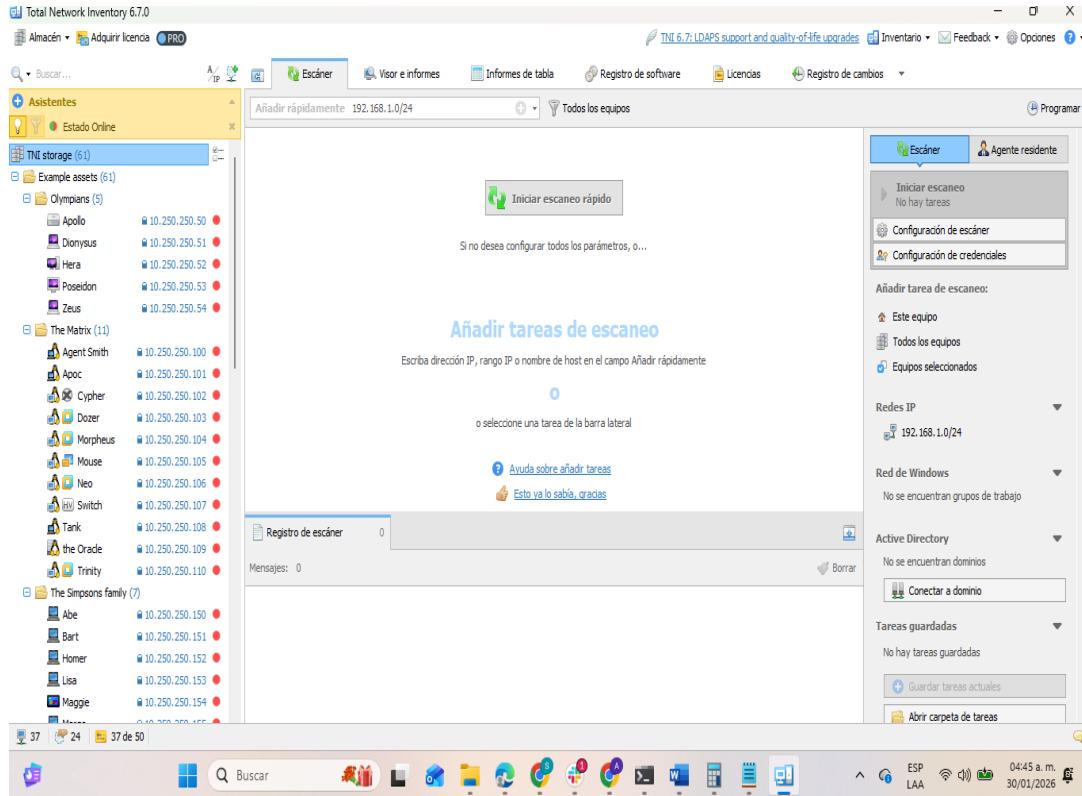
Selección del Tipo de Almacenamiento del Sistema de Inventario



Nota: La imagen muestra la opción para elegir entre almacenamiento de un solo usuario o multiusuario, en este caso, el almacenamiento de un solo usuario permite administrar la información de red localmente, facilitando auditorías individuales sin requerir bases de datos externas, lo cual reduce riesgos de exposición.

Figura 6

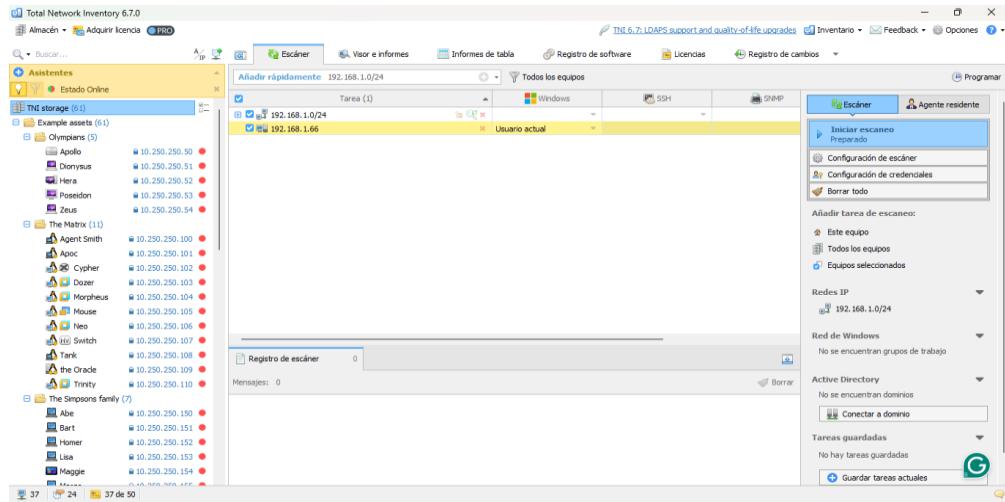
Interfaz Principal del Sistema Lista para Añadir Tareas de Escaneo



Nota: Se observa la interfaz principal de Total Network Inventory, desde donde se pueden agregar tareas de escaneo de red, esta sección centraliza el control del análisis de dispositivos conectados, permitiendo identificar activos tecnológicos y posibles puntos vulnerables.

Figura 7

Configuración de Tareas de Escaneo con Dirección IP de la Red Local

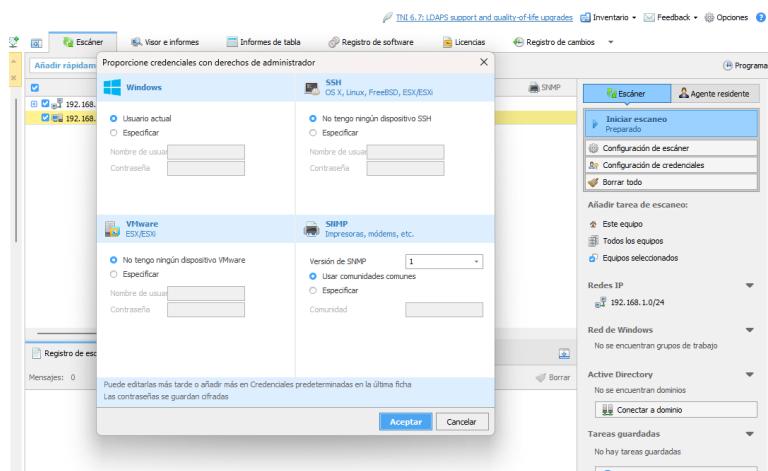


Nota: La imagen muestra la introducción del rango de direcciones IP (192.168.1.0/24)

para analizar todos los dispositivos de la red local, este procedimiento permite detectar computadoras, routers y otros equipos conectados, lo cual es esencial para el control de accesos y monitoreo de seguridad.

Figura 8

Configuración de Credenciales Administrativas para el Escaneo

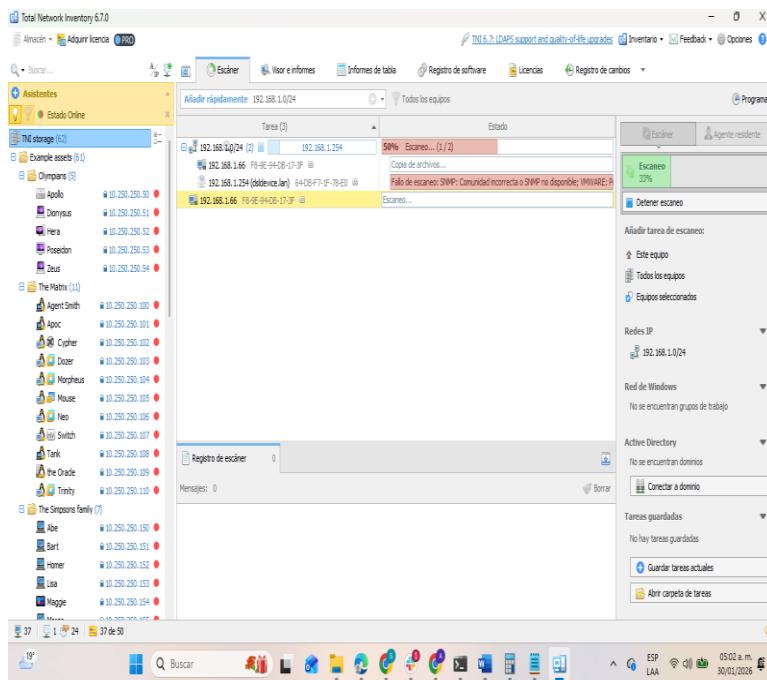


Nota: Se visualiza la sección donde se configuran credenciales de Windows, SSH y SNMP, estas credenciales permiten acceder a información más detallada de los dispositivos, como hardware, sistema operativo y servicios activos, fortaleciendo la auditoría de seguridad.

Resultado del Escaneo

Figura 9

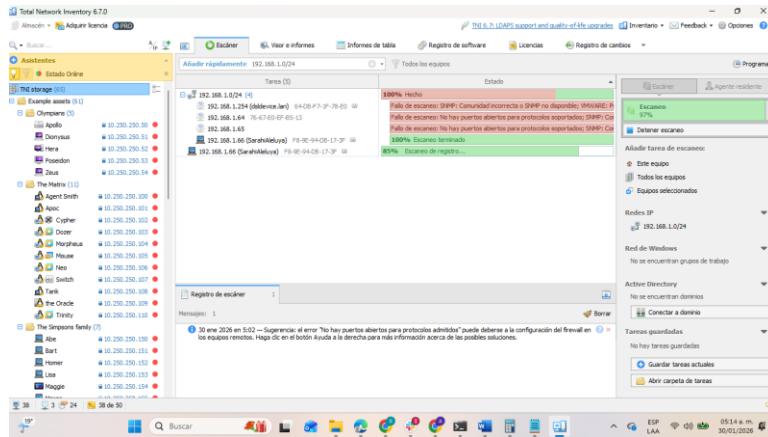
Ejecución del Escaneo de Red en Progreso



Nota: La imagen muestra el proceso de escaneo en tiempo real, donde el sistema analiza dispositivos conectados y recopila información técnica, este paso es clave para detectar equipos desconocidos, errores de configuración y posibles riesgos de seguridad en la red.

Figura 10

Resultados del Escaneo con Detección de Dispositivos y Errores

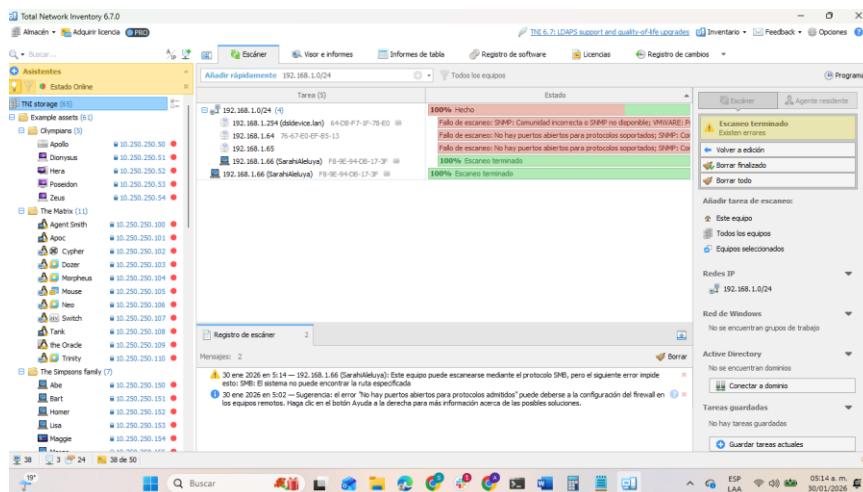


Nota: Se observan los dispositivos detectados junto con mensajes de error relacionados

con protocolos SNMP y puertos cerrados, estos avisos permiten identificar configuraciones restrictivas o problemas de comunicación que pueden afectar el monitoreo, además de señalar áreas donde podrían existir vulnerabilidades o bloqueos de seguridad.

Figura 11

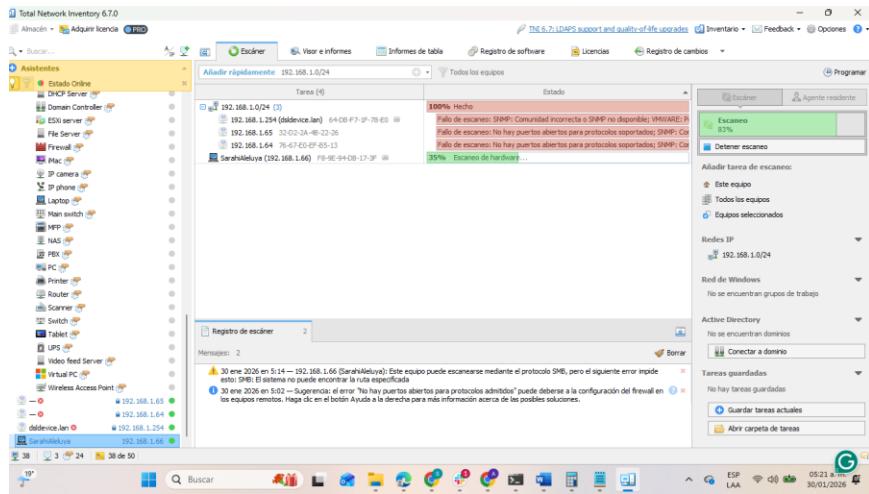
Ejecución del escaneo de red en el rango 192.168.1.0/24



Nota: Durante esta fase se utilizó el botón “Escáner” junto con la opción de agregar rápidamente la red IP para iniciar la auditoría, el sistema intentó emplear protocolos como SNMP y SMB, sin embargo se detectaron bloqueos por firewall y configuraciones incorrectas, lo cual refleja una superficie de ataque protegida parcialmente, desde el enfoque de ciberseguridad, esto demuestra la importancia de reglas de red bien configuradas para evitar accesos no autorizados, aunque se recomienda permitir temporalmente puertos controlados para auditorías internas.

Figura 12

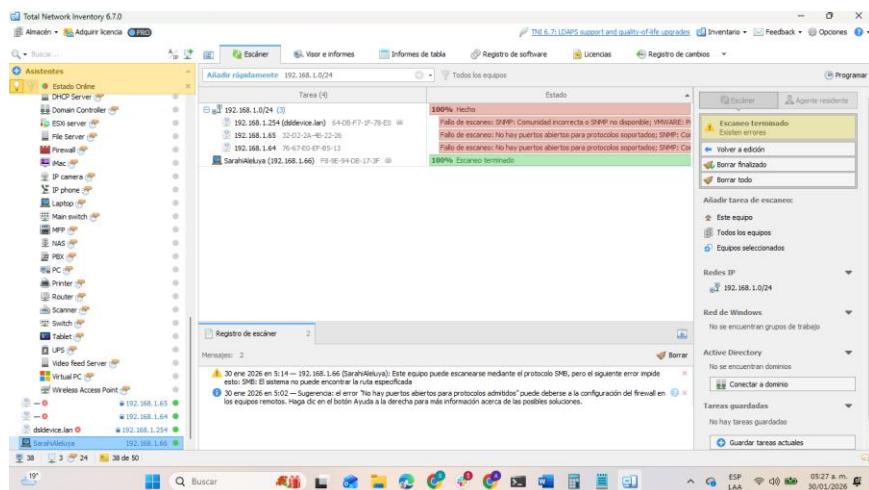
Progreso Del Análisis de Hardware del Equipo Sarahialeluya



Nota: Aquí se observa el análisis progresivo del hardware del equipo objetivo, activado mediante el botón de escaneo de equipos seleccionados, esta acción permitió recolectar información crítica de componentes físicos, en términos de seguridad, conocer el hardware facilita detectar vulnerabilidades asociadas a dispositivos obsoletos o configuraciones inseguras.

Figura 13

Finalización del Escaneo con Errores Detectados

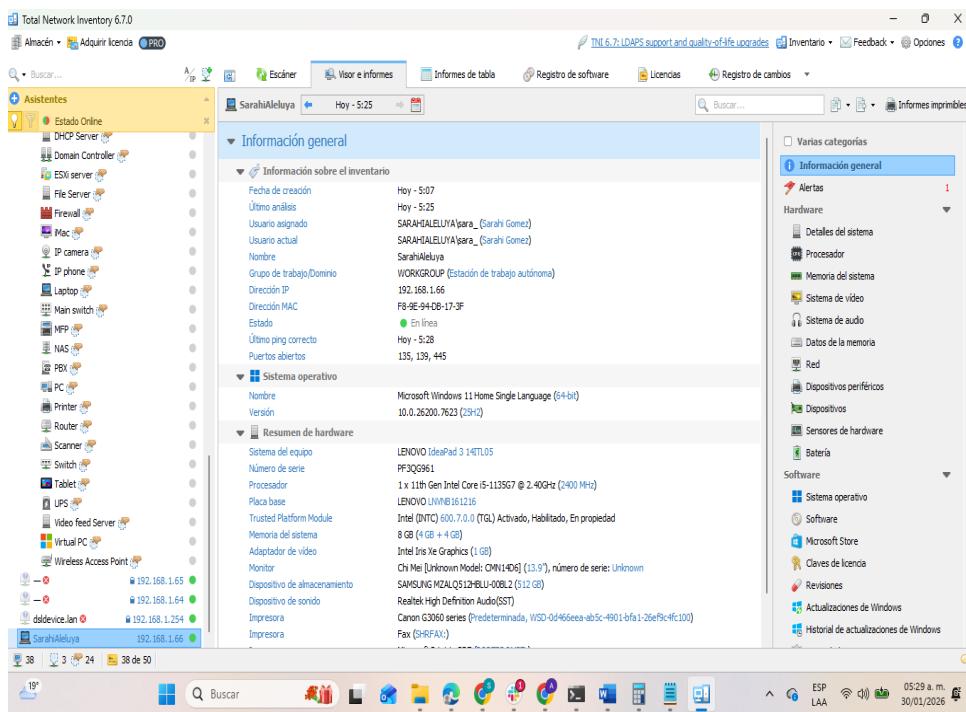


Nota: El sistema muestra el escaneo concluido con errores de comunicación, lo que evidencia restricciones de red, en la ciberseguridad, esto es positivo como barrera defensiva, aunque se recomienda documentar reglas de firewall para futuras auditorías completas.

Reporte:

Figura 14

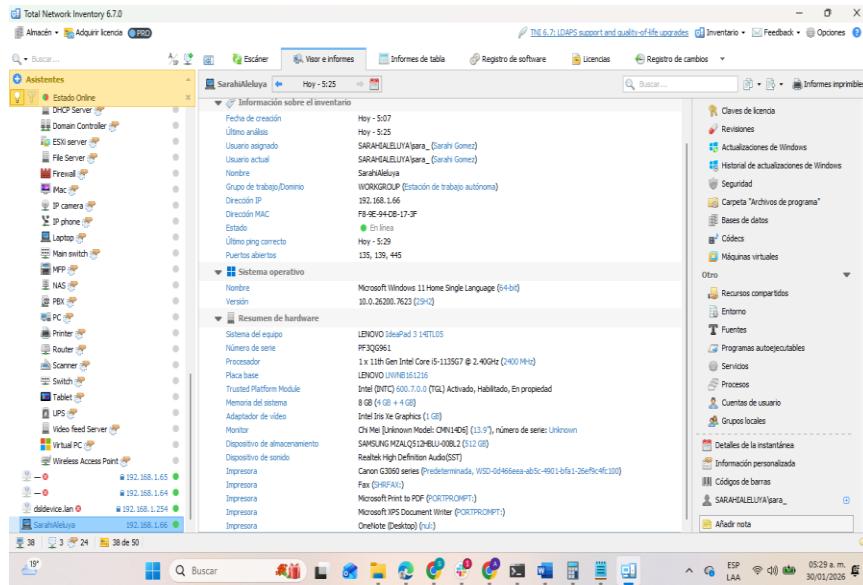
Información General del Sistema Inventariado



Nota: Se presenta la información general del activo inventariado, incluyendo IP, puertos abiertos y sistema operativo, mediante los botones de navegación del visor permitieron acceder a estas categorías, así mismo los puertos 135, 139 y 445 abiertos representan riesgos potenciales de ataques SMB, por lo que se recomienda restringirlos o protegerlos con firewall.

Figura 15

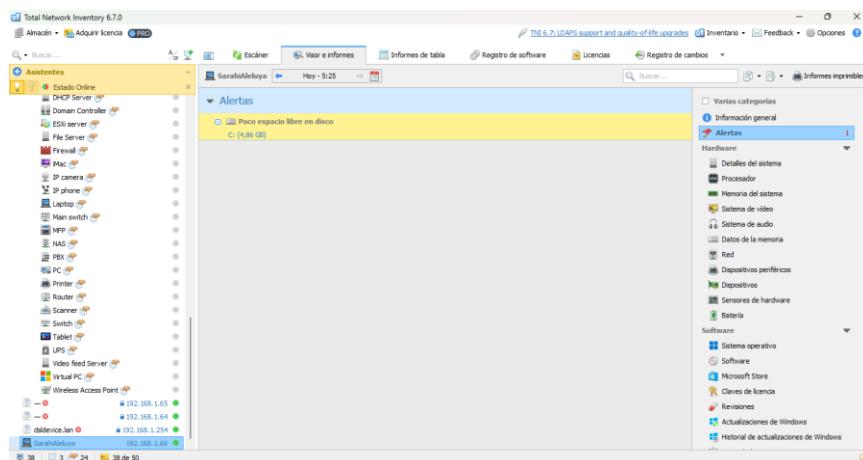
Detalles Ampliados del Hardware y Sistema Operativo



Nota: En esta captura se amplía la información del hardware detectado mediante opciones del panel lateral. Esto fortalece la gestión de activos, permitiendo identificar vulnerabilidades ligadas a versiones de sistema y controladores.

Figura 16

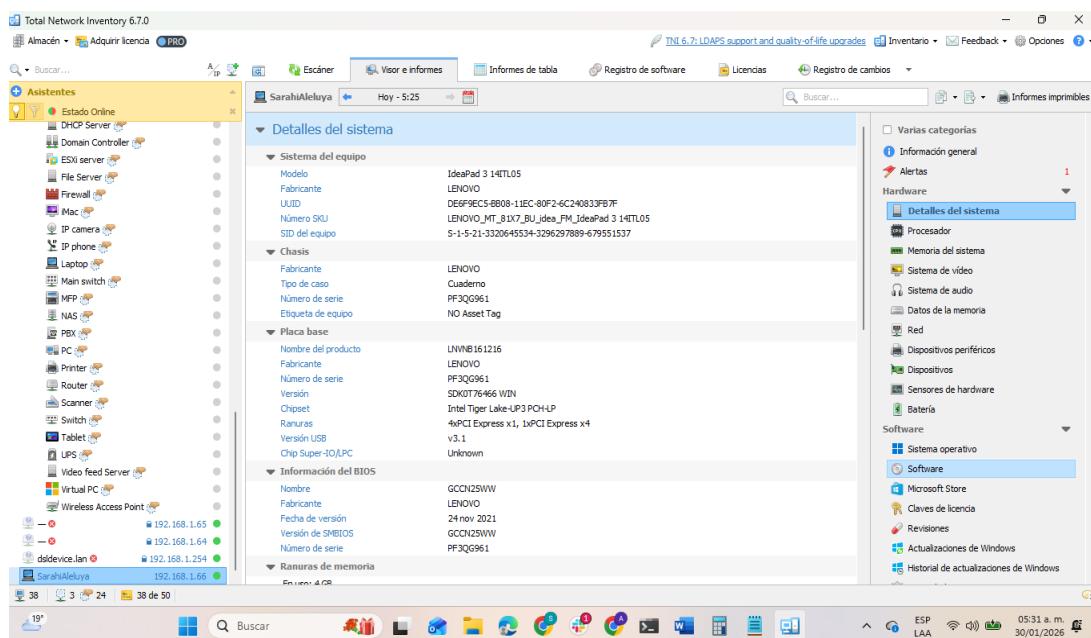
Alerta de Poco Espacio Libre en Disco



Nota: La alerta automática indica bajo espacio en disco, generada por el módulo de monitoreo, desde un enfoque de seguridad informática, esto es crítico ya que discos saturados pueden impedir registros de seguridad y actualizaciones, recomendándose limpieza o ampliación de almacenamiento.

Figura 17

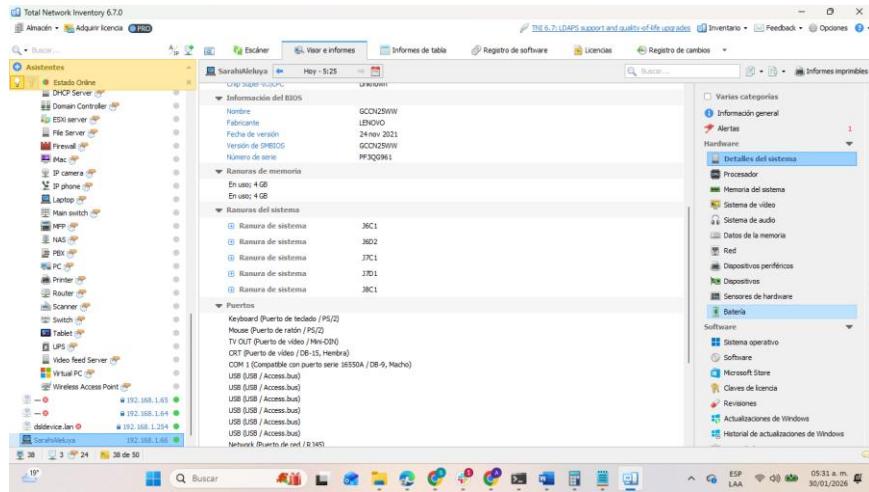
Información Detallada del Sistema Base y BIOS



Nota: Aquí se muestran datos del BIOS y placa base obtenidos mediante el escaneo de hardware, obtenidos mediante los botones de expansión permitieron visualizar cada componente, esto es clave en seguridad para detectar firmware desactualizado susceptible a exploits.

Figura 18

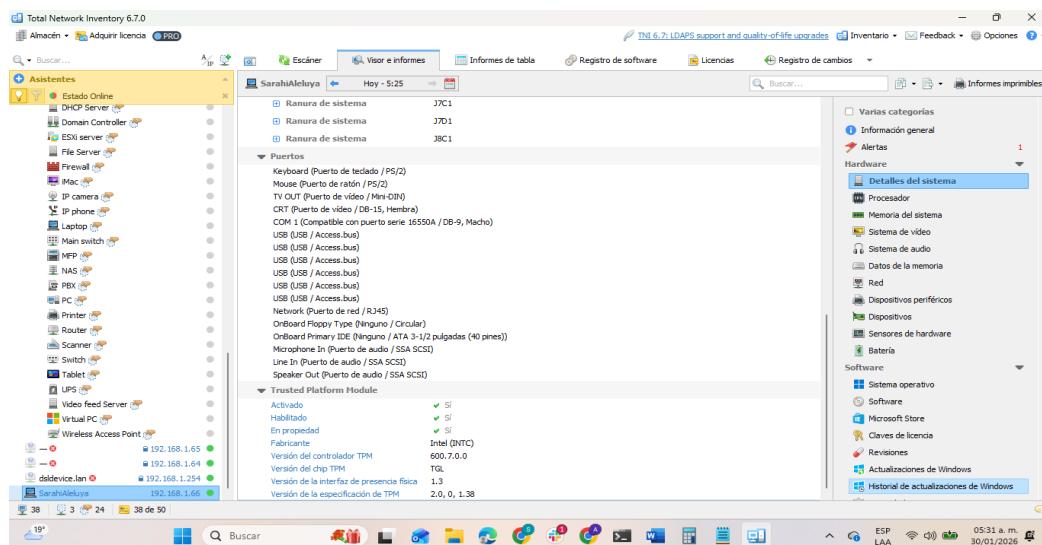
Ranuras de sistema y puertos detectados



Nota: Se identifican ranuras y puertos físicos del sistema, recopilados automáticamente, esta información ayuda a controlar accesos físicos no autorizados y evaluar riesgos de dispositivos externos.

Figura 19

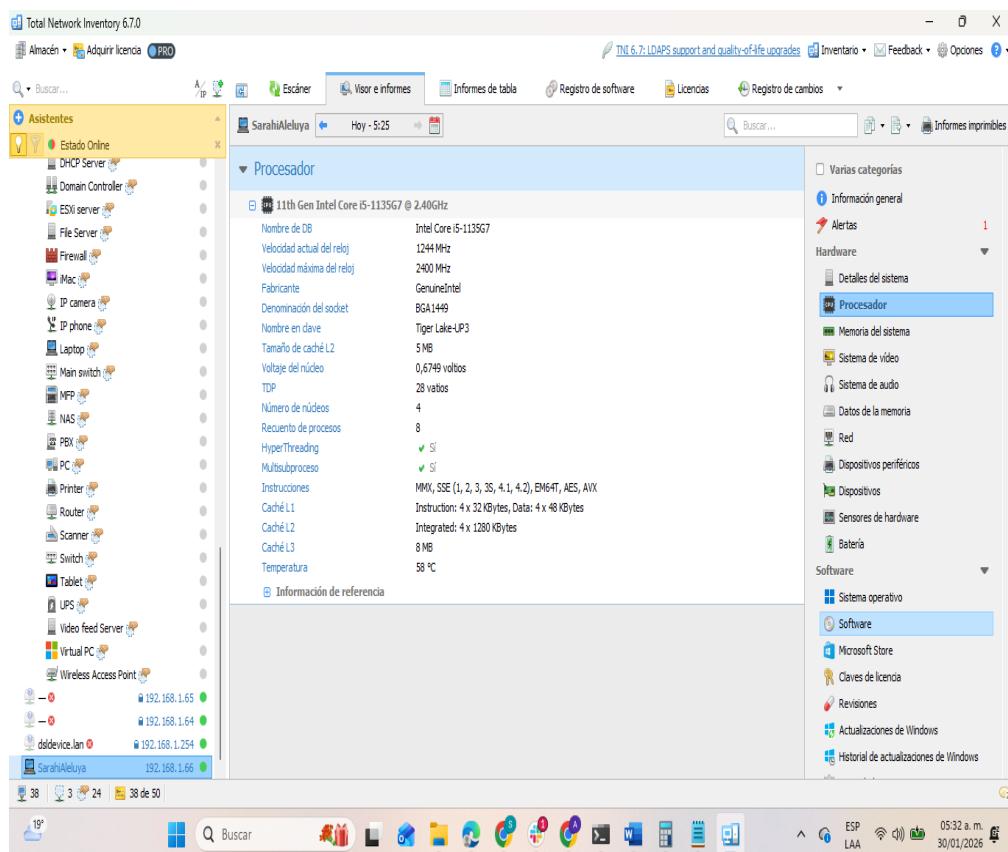
Estado del Módulo TPM para Seguridad



Nota: Se confirma que el módulo TPM está activo, habilitado y operativo, este componente fortalece la seguridad al proteger cifrado y credenciales, siendo altamente recomendable mantenerlo activo para prevenir accesos no autorizados.

Figura 20

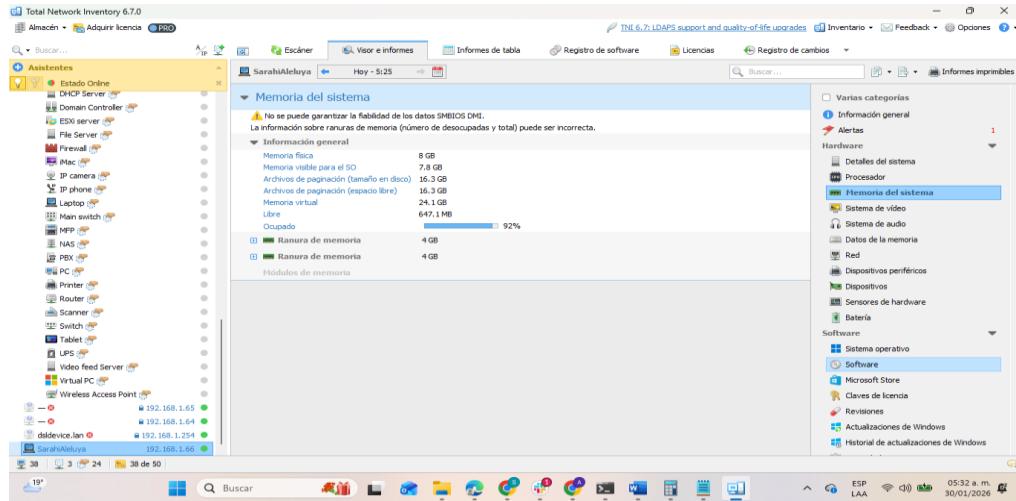
Detalles del Procesador Intel Core i5 Detectado



Nota: Se observa la información detallada del CPU obtenida mediante el módulo de hardware, esto se logró mediante el botón de expansión que permitió visualizar parámetros como núcleos, temperatura y tecnologías de seguridad como AES, en ciberseguridad, conocer estas capacidades permite implementar cifrado eficiente y monitorear sobrecalentamientos que puedan indicar procesos maliciosos.

Figura 21

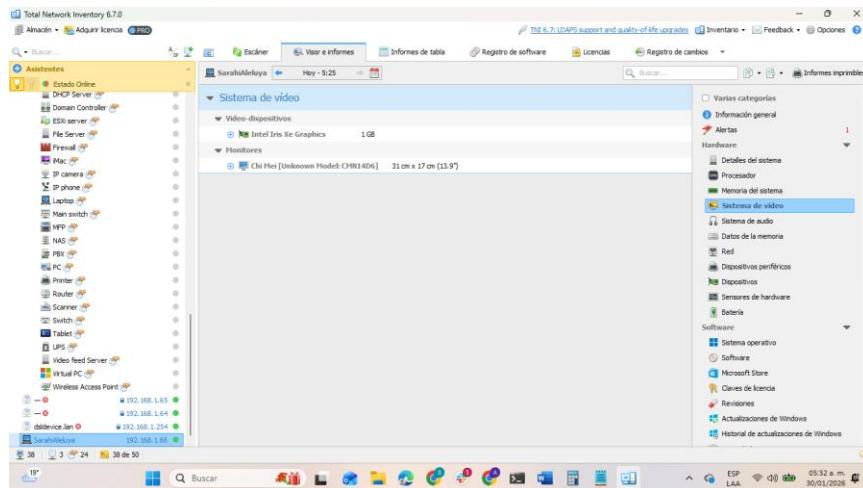
Estado y Uso de la Memoria del Sistema



Nota: Aquí se evidencia el alto consumo de memoria, detectado tras el escaneo, los controles de navegación permitieron acceder al apartado de memoria, desde la seguridad informática, una memoria saturada puede facilitar ataques de denegación de servicio o fallas de sistema, recomendándose monitoreo constante.

Figura 22

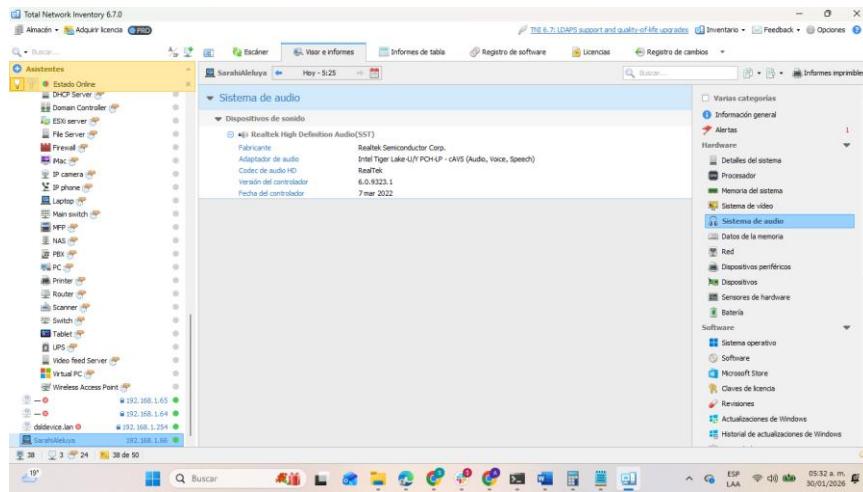
Información del Sistema de Video



Nota: La sección muestra la tarjeta gráfica y monitor detectados, esto ayuda a identificar controladores vulnerables que podrían ser explotados si no se actualizan correctamente.

Figura 23

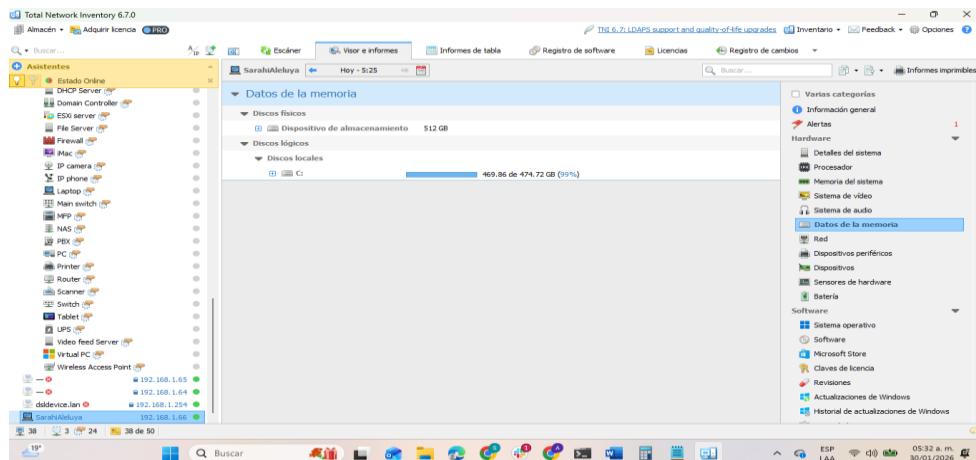
Dispositivos del Sistema de Audio



Nota: Se listan los dispositivos de audio con versiones de controladores, en ciberseguridad, drivers obsoletos pueden representar vulnerabilidades, por lo que se recomienda mantenerlos actualizados.

Figura 24

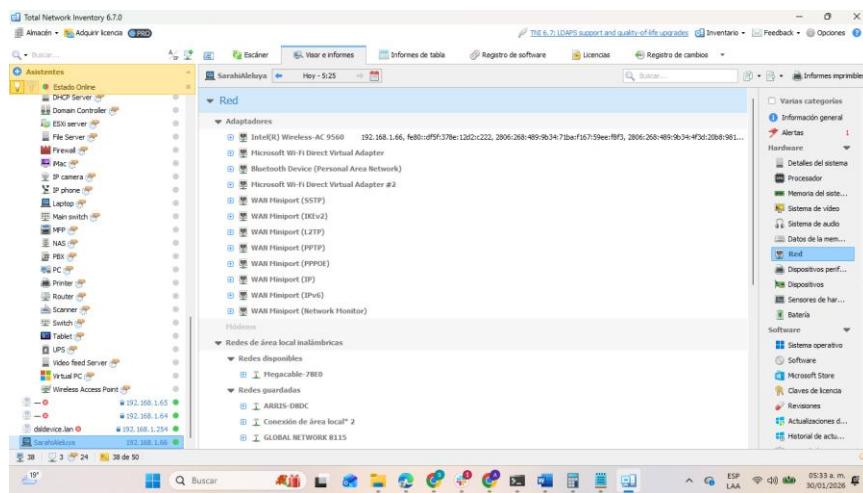
Visualización del Uso de Almacenamiento



Nota: Se observa el uso crítico del almacenamiento, identificado por la herramienta, esto puede afectar registros de auditoría y actualizaciones de seguridad, por lo que se sugiere liberar espacio o ampliar capacidad.

Figura 25

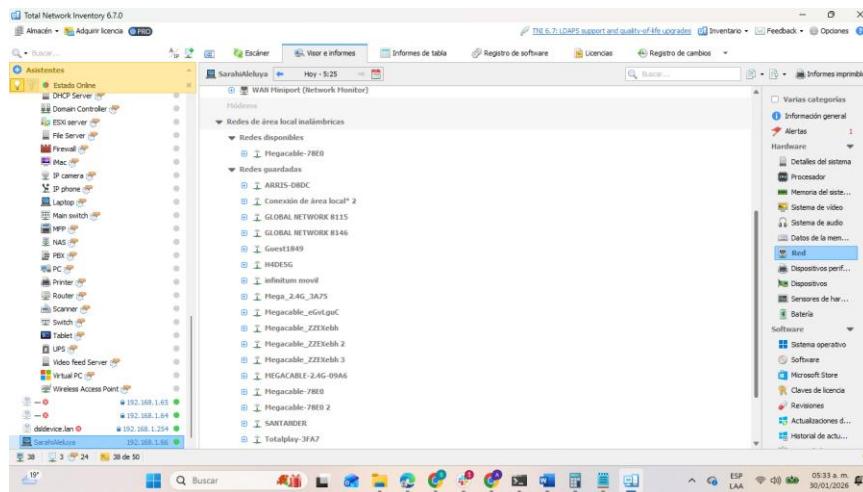
Adaptadores de Red Detectados



Nota: Se detallan adaptadores físicos y virtuales, esta información permite identificar interfaces potenciales de ataque, como adaptadores virtuales no autorizados.

Figura 26

Redes Inalámbricas Disponibles

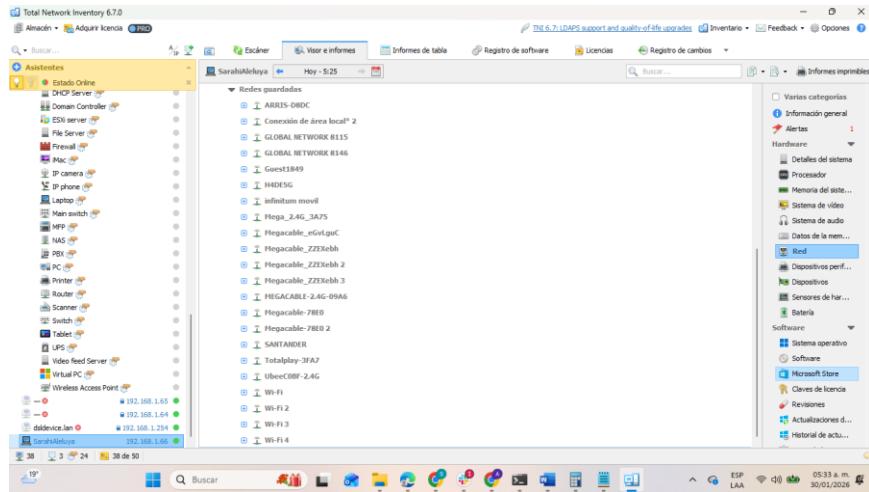


Nota: Aquí se muestran redes disponibles en el entorno, detectadas automáticamente.

Desde seguridad, es útil para identificar posibles redes inseguras o suplantadas.

Figura 27

Historial de Redes Guardadas

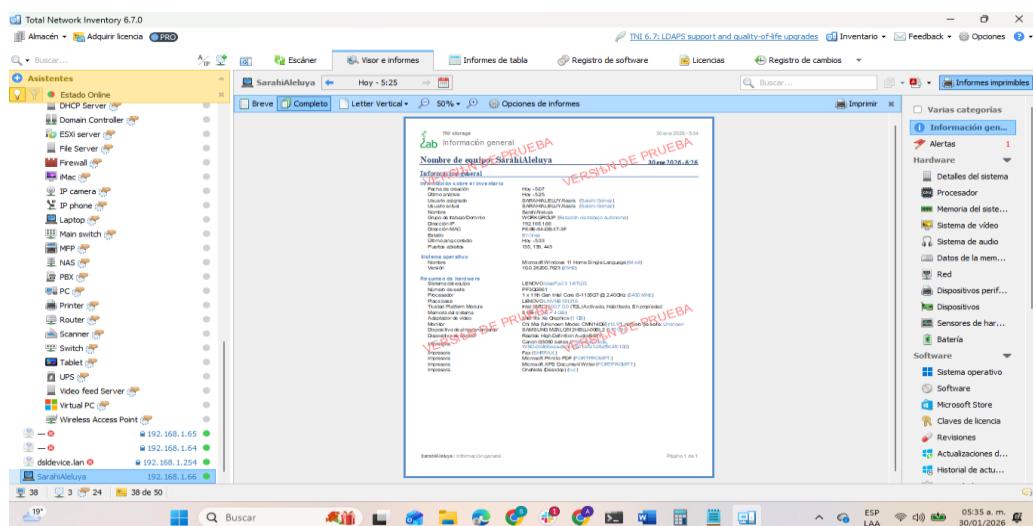


Nota: Se presenta el historial de redes conectadas, esto es clave para auditorías de

seguridad, ya que permite rastrear conexiones a redes potencialmente peligrosas.

Figura 28

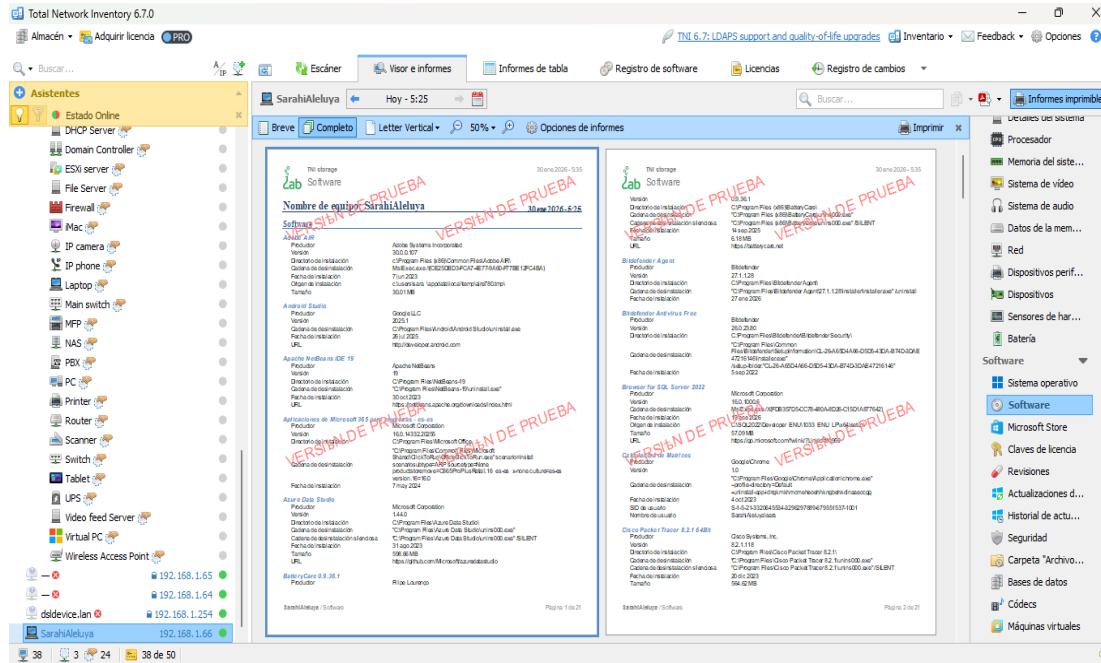
Generación de Informe General del Sistema



Nota: Finalmente se observa la generación del reporte general mediante el botón de informes imprimibles, permitiendo documentar evidencias técnicas para auditorías formales.

Figura 29

Vista Previa del Informe Imprimible de Software Instalado (Inventario del Equipo)

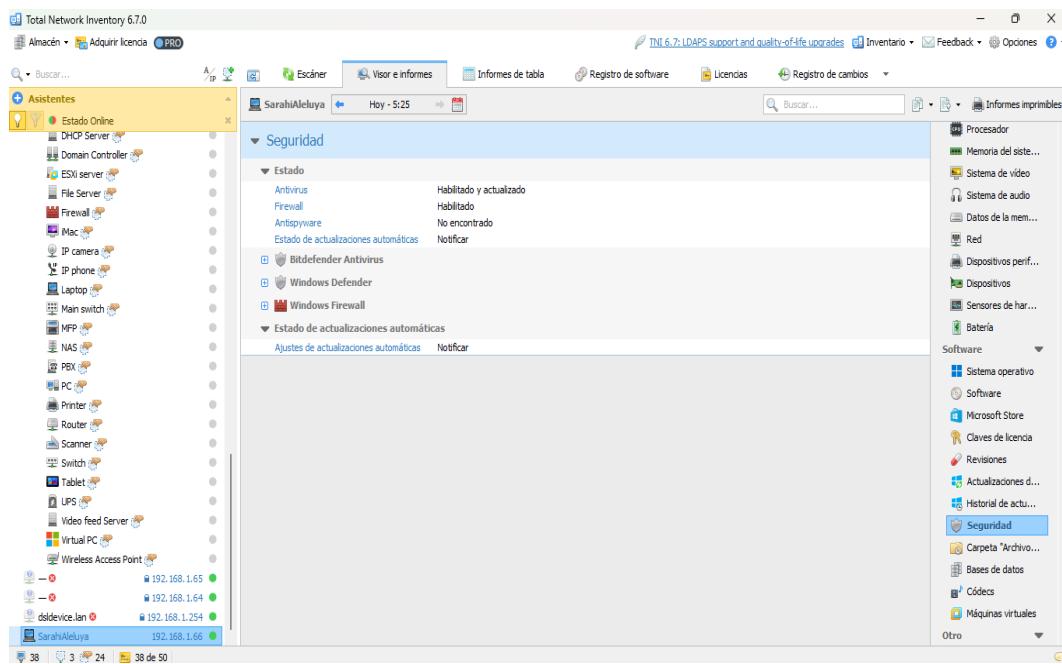


Nota: En esta evidencia se aprecia la opción **Informes imprimibles** mostrando la vista previa del reporte de Software del equipo, donde se listan aplicaciones instaladas (con nombre, versión, directorio de instalación y, en algunos casos, URL o fabricante), para obtener esta evidencia, se navega dentro del inventario del equipo y se selecciona el módulo “Software”, posteriormente se abre la sección de **Informes imprimibles** y se elige el formato de reporte (por ejemplo, **Completo**, con visualización tipo carta/vertical), desde el enfoque de ciberseguridad, este reporte es clave para la **gestión de activos y control de software**: permite detectar aplicaciones no autorizadas, versiones desactualizadas (potencialmente vulnerables) y huellas de herramientas que podrían incrementar la superficie de ataque, como recomendación práctica, se

debe contrastar este listado contra una base lineal aprobada, eliminar software innecesario, y mantener un ciclo de actualización/patching; además, conviene restringir instalaciones mediante políticas (principio de mínimo privilegio) para reducir el riesgo de ejecución de software malicioso.

Figura 30

Revisión del Estado de Seguridad del Equipo (Antivirus y Firewall)



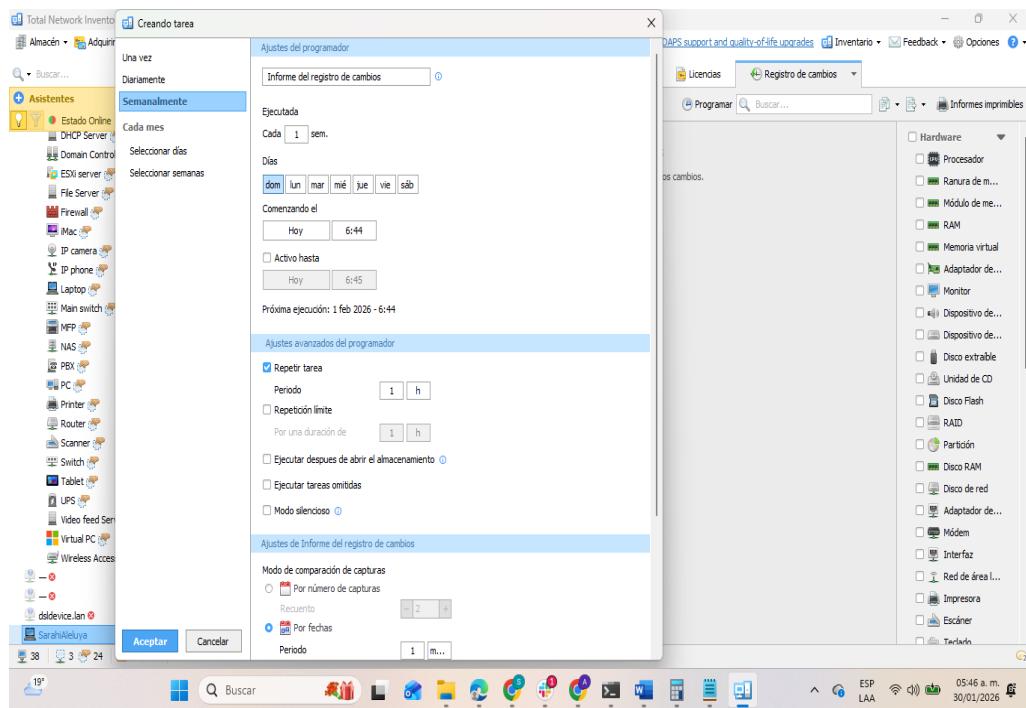
Nota: En la captura se observa el apartado denominado “**Seguridad**”, donde el sistema reporta el estado de controles esenciales: **Antivirus** (habilitado y actualizado) y **Firewall** (habilitado), para llegar a esta pantalla se selecciona la categoría **Seguridad** en el panel derecho del inventario del equipo, desde la perspectiva de ciberseguridad, esta verificación sirve para validar medidas mínimas de protección: un antivirus actualizado ayuda a mitigar malware común y un firewall reduce exposición al filtrar tráfico no deseado, como recomendación, además de confirmar que estén activos, se sugiere revisar que las reglas del firewall estén alineadas al uso

real (evitar puertos abiertos innecesarios), habilitar protección en tiempo real, y complementar con buenas prácticas como actualizaciones automáticas, copias de seguridad y cuentas de usuario sin privilegios administrativos para tareas cotidianas.

Auditoría Semanal y Reporte:

Figura 31

Configuración de una Tarea Programada para Generar el Informe del Registro de Cambios (Ajustes Avanzados)

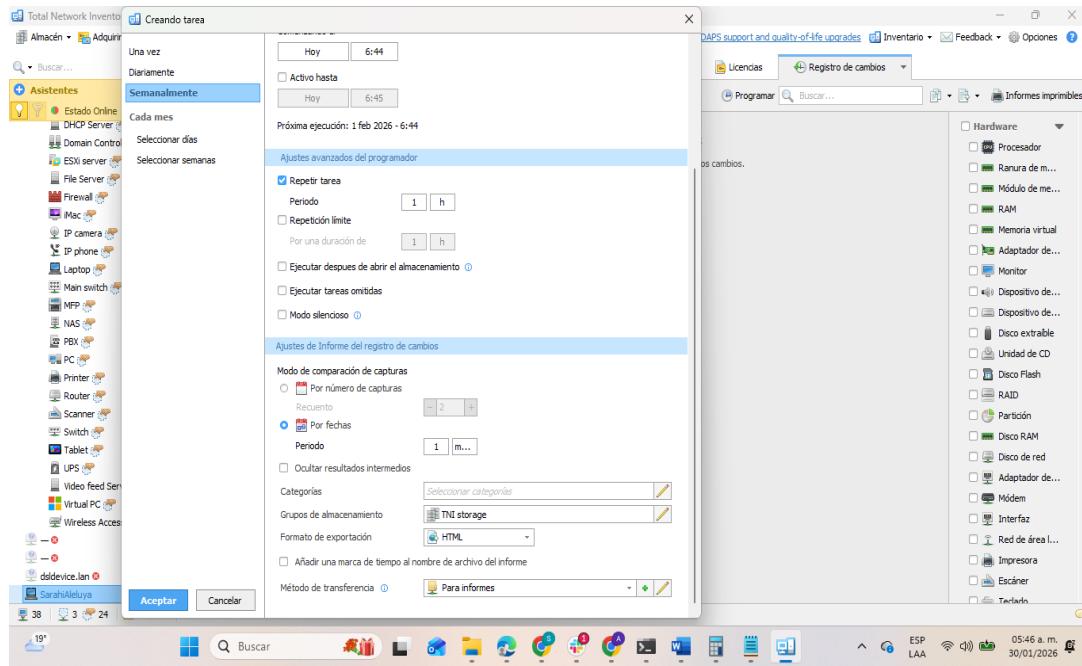


Nota: Aquí se muestra la ventana “**Creando tarea**”, con la opción “**Semanalmente**” seleccionada, donde se configuran parámetros avanzados para automatizar la generación del **Informe del registro de cambios**, se observa el uso de controles como **Repetir tarea**, definición de **Periodo**, y ajustes del informe (modo de comparación de capturas, periodo de comparación, grupo de almacenamiento y formato de exportación), para construir esta evidencia se accede al módulo **Programador** y se crea una nueva tarea; dentro de la ventana se selecciona la

periodicidad y se activan los parámetros requeridos antes de pulsar **Aceptar**, en ciberseguridad, la automatización del registro de cambios es fundamental para contar con trazabilidad: permite identificar variaciones en software, configuración o componentes que puedan indicar alteraciones no autorizadas, se recomienda definir una periodicidad acorde al riesgo (semanal o más frecuente), conservar historiales, y revisar alertas ante cambios críticos (instalación de software nuevo, desactivación de seguridad, cambios de red).

Figura 32

Definición de Periodicidad Semanal (Día y Hora) para la Ejecución Automática del Informe

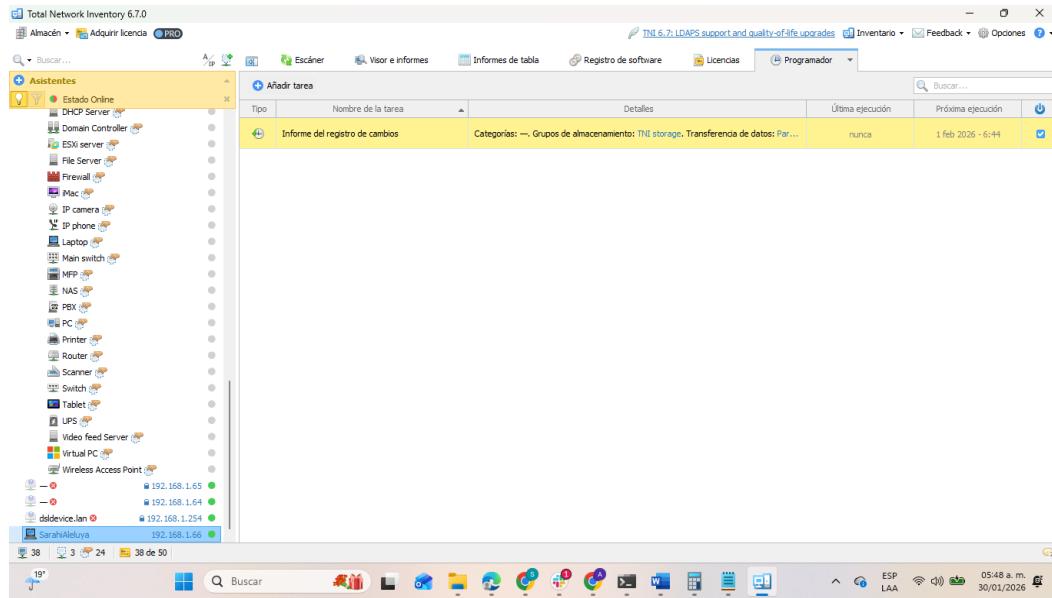


Nota: En esta evidencia se aprecia la sección de programación semanal donde se selecciona el **día** (por ejemplo, domingo) y **la hora** de ejecución (por ejemplo, 6:44), además de opciones como **Activo hasta** y confirmación de la **próxima ejecución**, también se mantiene activada la opción de **Repetir Tarea**, los botones y controles utilizados incluyen la selección del modo **Semanalmente**, la elección del día en la fila (domingo, lunes, martes ...), el ajuste de hora

y, finalmente, el botón **Aceptar** para guardar, desde el enfoque de ciberseguridad, esto materializa la auditoría continua: al ejecutar informes en horarios definidos se reduce el riesgo de no detectar cambios oportunamente, recomendación: programar la tarea en horarios de baja actividad para reducir impacto, asegurar que el almacenamiento de reportes esté protegido (permisos y respaldos), y establecer un procedimiento de revisión (quién valida los cambios y qué acciones se toman cuando algo no coincide con lo esperado).

Figura 33

Validación en el Programador: Tarea Creada y Próxima Ejecución Registrada



Nota: La pantalla muestra el **Programador** con la tarea ya registrada (por ejemplo, **Informe del Registro de Cambios**), indicando detalles como el alcance (**Grupo de Almacenamiento**), el estado, y la **próxima ejecución** (fecha y hora), para obtener esta evidencia se ingresa al módulo “**Programador**” y se verifica la fila de la tarea recién creada, confirmando que quedó activa, en términos de ciberseguridad, esta verificación cierra el ciclo de control: no basta con configurar, sino comprobar que la tarea quedó habilitada para garantizar continuidad

del monitoreo, por lo que es vital revisar periódicamente que las tareas no estén deshabilitadas, probar la generación del informe manualmente la primera vez, y establecer un mecanismo de notificación/seguimiento cuando el informe se genere (por ejemplo, revisión semanal del reporte o almacenamiento centralizado con control de acceso).

Conclusión:

El desarrollo de la Etapa 2 del proyecto permitió consolidar un enfoque integral de seguridad informática mediante la implementación de un sistema de monitoreo continuo de red utilizando la herramienta Total Network Inventory, complementando de manera efectiva la auditoría de vulnerabilidades realizada previamente con Nessus Essentials, mientras que la primera etapa se enfocó en identificar fallos técnicos y exposiciones de seguridad en el sistema, esta segunda fase fortaleció la gestión de activos tecnológicos y la supervisión constante de los dispositivos, configuraciones y cambios dentro de la infraestructura informática.

A través del escaneo de la red local y el análisis detallado de hardware, software y servicios activos, se logró obtener una visión completa del entorno tecnológico, evidenciando tanto aspectos positivos de protección, como restricciones de firewall y controles de seguridad activos, así como áreas de riesgo relacionadas con puertos abiertos, alto consumo de recursos y configuraciones que podrían ser aprovechadas por atacantes. La recopilación de información sobre componentes físicos, módulos de seguridad como el TPM, adaptadores de red y redes inalámbricas disponibles demostró la importancia de mantener un inventario actualizado para la prevención de accesos no autorizados y la detección temprana de vulnerabilidades.

Asimismo, la generación de reportes detallados del sistema y del software instalado fortaleció el control de aplicaciones y recursos, facilitando la identificación de programas no autorizados o versiones desactualizadas que incrementan la superficie de ataque, la revisión del estado de medidas básicas de protección, como el antivirus y el firewall, confirmó la existencia de barreras mínimas de seguridad, aunque se destacó la necesidad de complementarlas con políticas de actualización, configuraciones adecuadas de red y supervisión constante.

Uno de los aportes más relevantes de esta etapa fue la configuración de tareas programadas para la generación automática de informes del registro de cambios, estableciendo una auditoría continua que permite detectar modificaciones no autorizadas en el sistema de manera periódica, esta automatización representa una práctica fundamental en la ciberseguridad moderna, ya que proporciona trazabilidad, control y capacidad de respuesta ante posibles incidentes de seguridad.

En conjunto, el proyecto demuestra que la seguridad informática no debe limitarse únicamente a la detección puntual de vulnerabilidades, sino que requiere un monitoreo permanente que garantice el control de los recursos tecnológicos y la prevención de riesgos a largo plazo; La integración de la auditoría técnica con Nessus y el monitoreo continuo con Total Network Inventory conforma una estrategia preventiva sólida que permite reducir la superficie de ataque, mejorar la postura de seguridad del sistema y promover buenas prácticas de protección de la información.

Además, la adquisición de estos conocimientos y el desarrollo de habilidades en auditoría de vulnerabilidades, monitoreo de red, análisis de sistemas y automatización de reportes resulta de gran importancia tanto en la vida cotidiana como en el ámbito laboral, en el entorno profesional, estas competencias son altamente demandadas en áreas de tecnología de la información, redes y ciberseguridad, ya que permiten desempeñar funciones relacionadas con la protección de sistemas, gestión de activos tecnológicos, detección de riesgos, análisis de incidentes y aplicación de medidas preventivas, las organizaciones requieren personal capacitado para mantener la seguridad de sus infraestructuras frente a amenazas cada vez más sofisticadas, por lo que contar con experiencia práctica en herramientas profesionales fortalece el perfil técnico del estudiante.

En la vida cotidiana, estos conocimientos contribuyen a una mayor conciencia sobre la importancia de proteger equipos personales, redes domésticas y datos sensibles, comprender cómo funcionan los escaneos de red, el monitoreo de dispositivos y las configuraciones de seguridad permite a los usuarios identificar riesgos comunes, mantener sus sistemas actualizados, evitar conexiones inseguras y reducir la posibilidad de sufrir ataques como robo de información, intrusiones o infecciones de malware.

Finalmente, este proyecto no solo permitió comprender el funcionamiento de herramientas reales de seguridad informática, sino que también fomentó una visión preventiva y analítica frente a los riesgos tecnológicos, la correcta interpretación de resultados, la propuesta de mejoras y la implementación de monitoreo continuo fortalecen una cultura de seguridad informática responsable, preparando al estudiante para enfrentar retos reales en el ámbito académico, profesional y personal, y promoviendo prácticas que contribuyen a la protección de la información en un mundo cada vez más digitalizado.

Referencias:

Amenazas. (s. f.). Kaspersky. <https://www.fortinet.com/resources/cyberglossary/wireless-security>

Amenazas a la seguridad en Internet / Consejos de seguridad en línea / Kaspersky Latam. (s. f.). <https://latam.kaspersky.com/resource-center/threats>

Cyberglossary. (s. f.). Fortinet Home.

<https://www.fortinet.com/resources/cyberglossary/wireless-security>

Dempsey, K. L., Chawla, N. S., Johnson, L. A., Johnston, R., Jones, A. C., Orebaugh, A. D., Scholl, M. A., & Stine, K. M. (2011). *Information Security Continuous Monitoring (ISCM) for federal information systems and organizations.* <https://doi.org/10.6028/nist.sp.800-137>

ISO 30435:2023. (s. f.). ISO. <https://www.iso.org/standard/68712.html>

Novaltti. (2025, 30 mayo). *¿Qué es el TPM y por qué es importante?* Novaltti.

<https://novaltti.com/que-es-el-tpm-y-por-que-es-importante/>

Officedocspr. (s. f.-a). *Información general sobre la tecnología del Módulo de plataforma segura.* Microsoft Learn. <https://learn.microsoft.com/es-es/windows/security/hardware-security/tpm/trusted-platform-module-overview>

Officedocspr. (s. f.-b). *Información general sobre la tecnología del Módulo de plataforma segura.* Microsoft Learn. <https://learn.microsoft.com/es-es/windows/security/hardware-security/tpm/trusted-platform-module-overview>

Security / Wi-Fi alliance. (s. f.). <https://www.wi-fi.org/security>

Tenable Nessus Documentation / TenableTM. (s. f.). <https://docs.tenable.com/Nessus.htm>

Total network inventory. (s. f.). Total Network Inventory. <https://www.total-network-inventory.com/es/>