Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad [3] - [Auditoría y Bitácora]

[Seguridad Informática II]

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: Carlos Fco Estrada Salazar

Fecha: 03/Feb/2025

INDICE

GitHub Link:

INTRODUCCIÓN

En el ámbito de la seguridad informática, la auditoría de sistemas y la gestión de bitácoras son prácticas esenciales para garantizar la integridad, disponibilidad y confidencialidad de los recursos tecnológicos. Estas actividades permiten identificar vulnerabilidades, verificar el cumplimiento de normativas legales y regulatorias, así como mantener un control riguroso sobre los activos de hardware, software y redes. La correcta implementación de auditorías periódicas contribuye a la prevención de incidentes de seguridad y facilita la detección temprana de anomalías que podrían comprometer la infraestructura tecnológica de una organización.

El objetivo principal de esta actividad es realizar una auditoría exhaustiva de un equipo de cómputo utilizando herramientas especializadas, como Total Network Inventory, o bien, a través del Panel de Control en la sección de Herramientas Administrativas del sistema operativo. Esta auditoría permitirá obtener información detallada sobre las licencias de software instaladas, el estado de los recursos de hardware, configuraciones de red y otros aspectos críticos para la seguridad del sistema.

Además, se llevará a cabo la gestión de la bitácora, que consiste en registrar de manera sistemática todas las actividades y cambios detectados durante la auditoría. Este registro es fundamental para mantener un historial de eventos que facilite el análisis de seguridad a lo largo del tiempo. Como parte del proceso, se guardará la bitácora actual y se iniciará una nueva, permitiendo así una comparación efectiva de los cambios desde el día uno.

A lo largo de este informe, se presentarán los resultados obtenidos durante la auditoría, acompañados de capturas de pantalla que evidencian los procedimientos realizados. Este enfoque no solo proporciona una visión clara del estado actual del equipo auditado, sino que también establece una base sólida para futuras evaluaciones de seguridad.

DESCRIPCIÓN

El contexto presentado en esta actividad destaca la importancia de llevar a cabo auditorías de seguridad informática de manera regular. Las auditorías permiten identificar no solo las licencias de software instaladas en los equipos, sino también posibles vulnerabilidades en el sistema, el hardware y la red. Esto es fundamental para asegurar el cumplimiento de normativas legales y regulatorias, ya que tener licencias de software actualizadas y legales evita problemas legales y mejora la seguridad del entorno informático.

La actividad solicita realizar una auditoría utilizando herramientas como Total Network Inventory o las Herramientas Administrativas del Panel de Control. Esto permitirá obtener información precisa sobre los recursos del equipo, incluyendo el estado del hardware, el software instalado y la configuración de la red. Posteriormente, se debe gestionar una bitácora, lo que implica guardar el registro actual y crear uno nuevo. Esta práctica es crucial para detectar cambios significativos en el sistema desde el primer día, lo que facilita la identificación de anomalías y posibles incidentes de seguridad.

Realizar auditorías semanales, como se indica en el contexto, permite mantener un control continuo sobre los sistemas, identificar rápidamente cualquier irregularidad y tomar medidas preventivas o correctivas de manera oportuna. En resumen, esta actividad busca fortalecer la capacidad de análisis y gestión de la seguridad informática, promoviendo buenas prácticas que contribuyan a la protección de los recursos tecnológicos de la organización.

JUSTIFICACIÓN

El uso de herramientas especializadas como Total Network Inventory para la auditoría de sistemas y la gestión de bitácoras es altamente recomendable debido a su capacidad para ofrecer un análisis detallado y preciso de los recursos tecnológicos de una organización. Este tipo de software permite identificar rápidamente las licencias de software instaladas, verificar su legalidad y detectar posibles incumplimientos normativos, lo cual es fundamental para evitar problemas legales y garantizar el cumplimiento de las regulaciones vigentes.

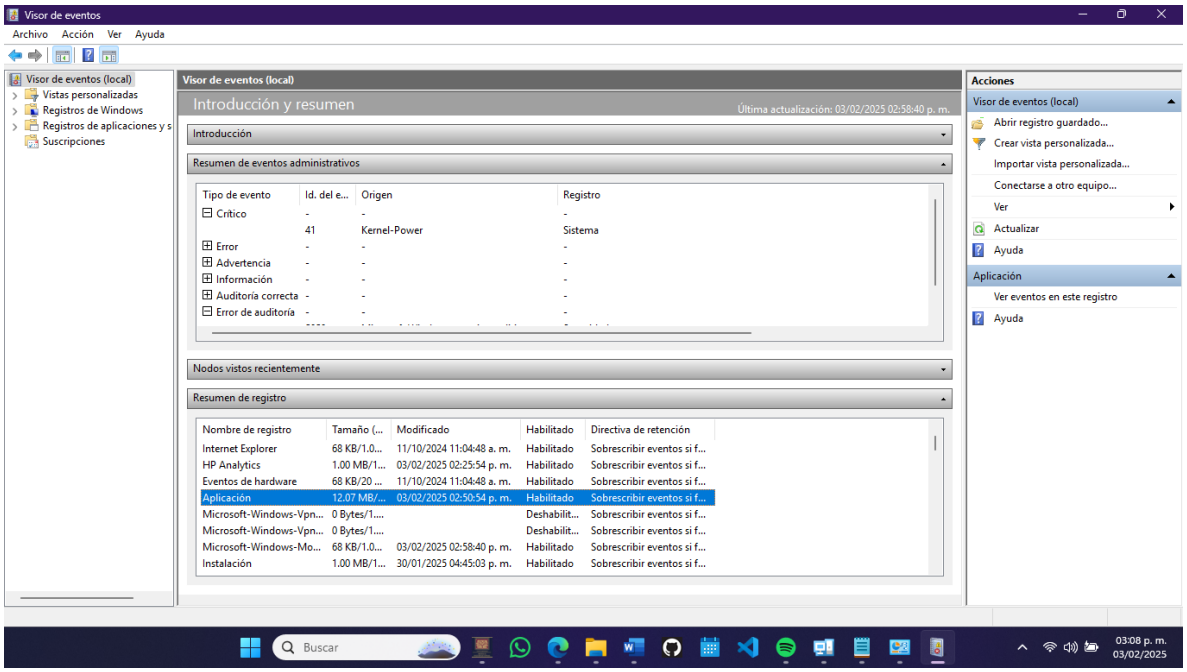
Además, Total Network Inventory proporciona una visión integral del estado del hardware, software y la red, facilitando la identificación de vulnerabilidades que podrían ser explotadas por atacantes. La capacidad de generar informes detallados y visualizaciones gráficas permite a los administradores de sistemas tomar decisiones informadas sobre las medidas de seguridad a implementar.

La gestión de bitácoras es otro aspecto crítico que se ve optimizado con el uso de estas herramientas. Registrar de manera sistemática todos los cambios y eventos relevantes en el sistema ayuda a mantener un historial completo que puede ser invaluable para la investigación de incidentes de seguridad y la auditoría interna. La posibilidad de iniciar nuevas bitácoras regularmente permite detectar rápidamente cualquier alteración en la configuración del sistema, mejorando así la capacidad de respuesta ante posibles amenazas.

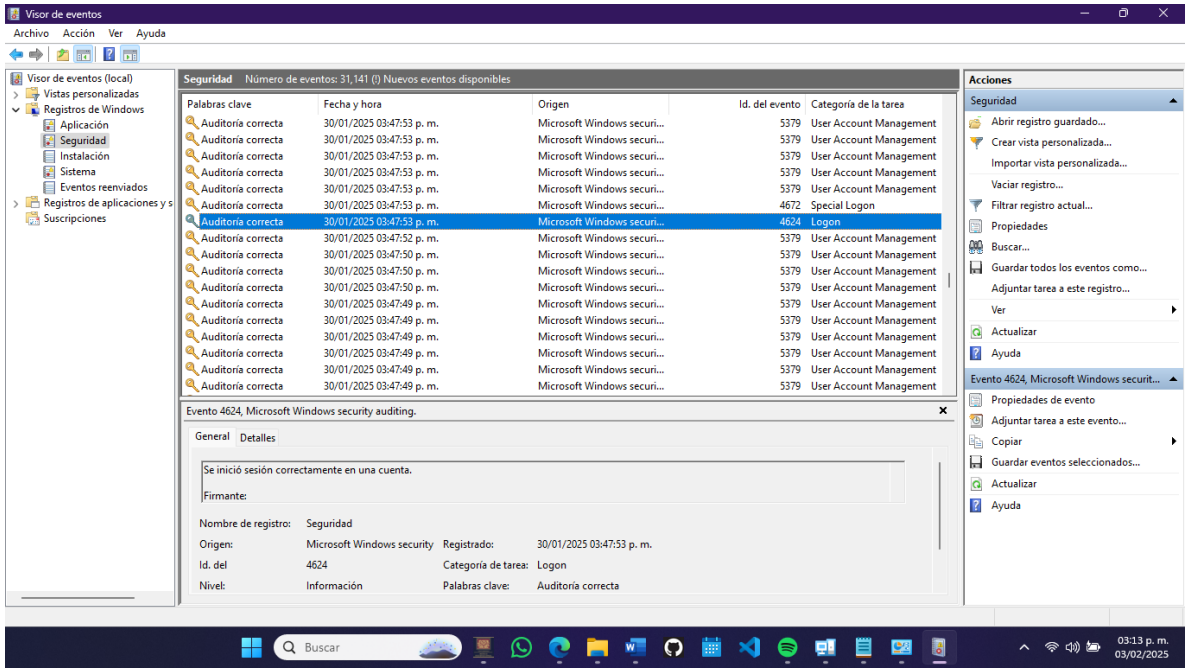
En resumen, el uso de soluciones especializadas para la auditoría y gestión de bitácoras no solo mejora la eficiencia del proceso, sino que también fortalece la postura de seguridad de la organización, contribuyendo a la protección de sus recursos tecnológicos más valiosos.

DESARROLLO

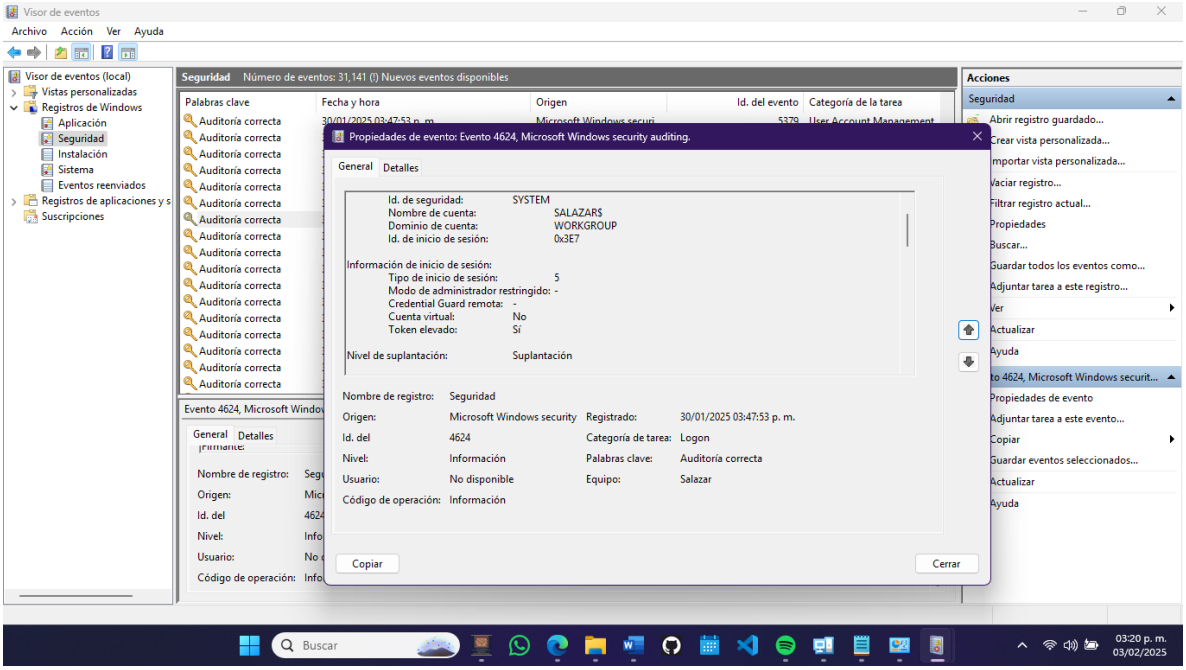
Auditoria del equipo



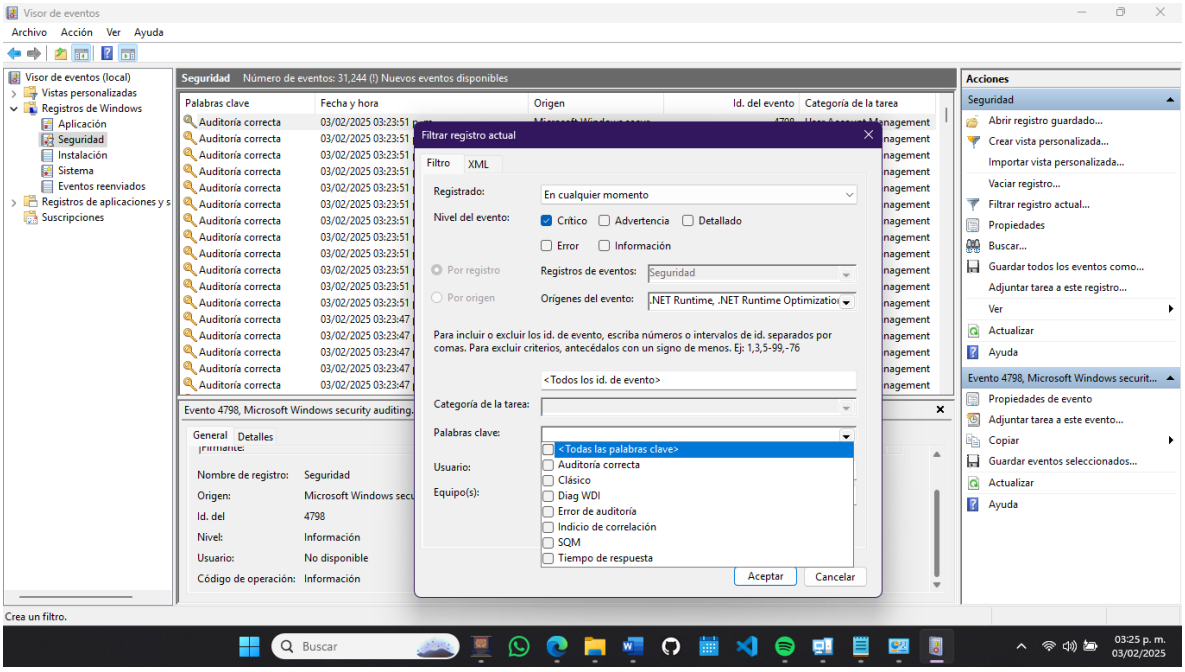
Información del visor de eventos



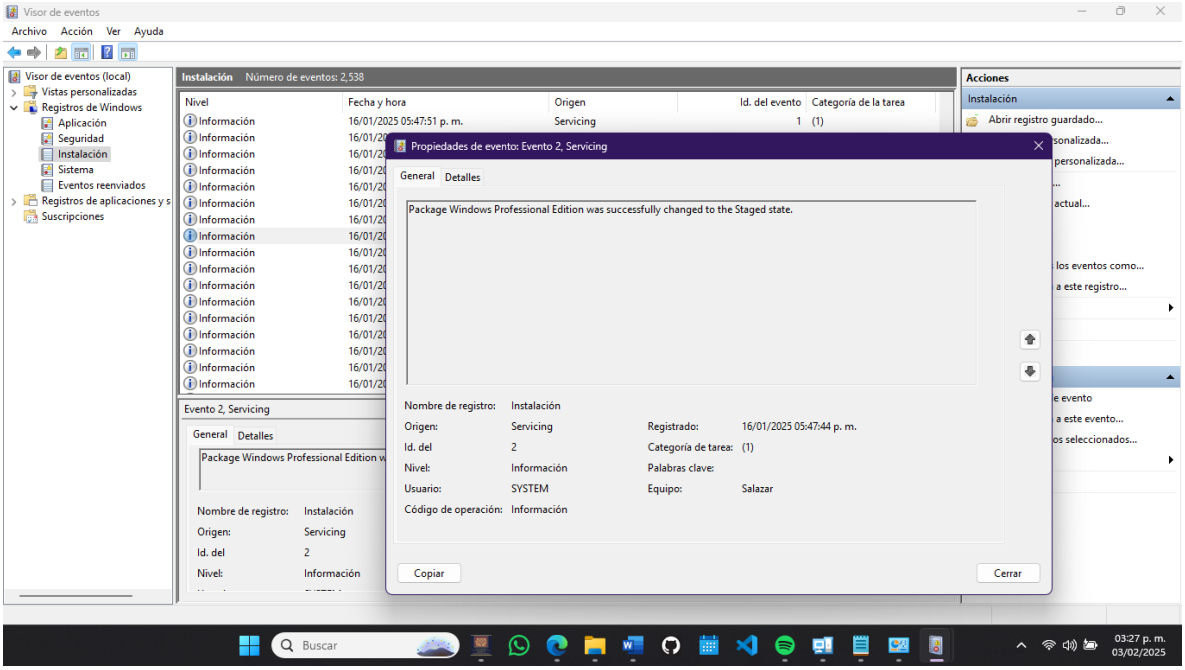
Reporte de auditorías de seguridad



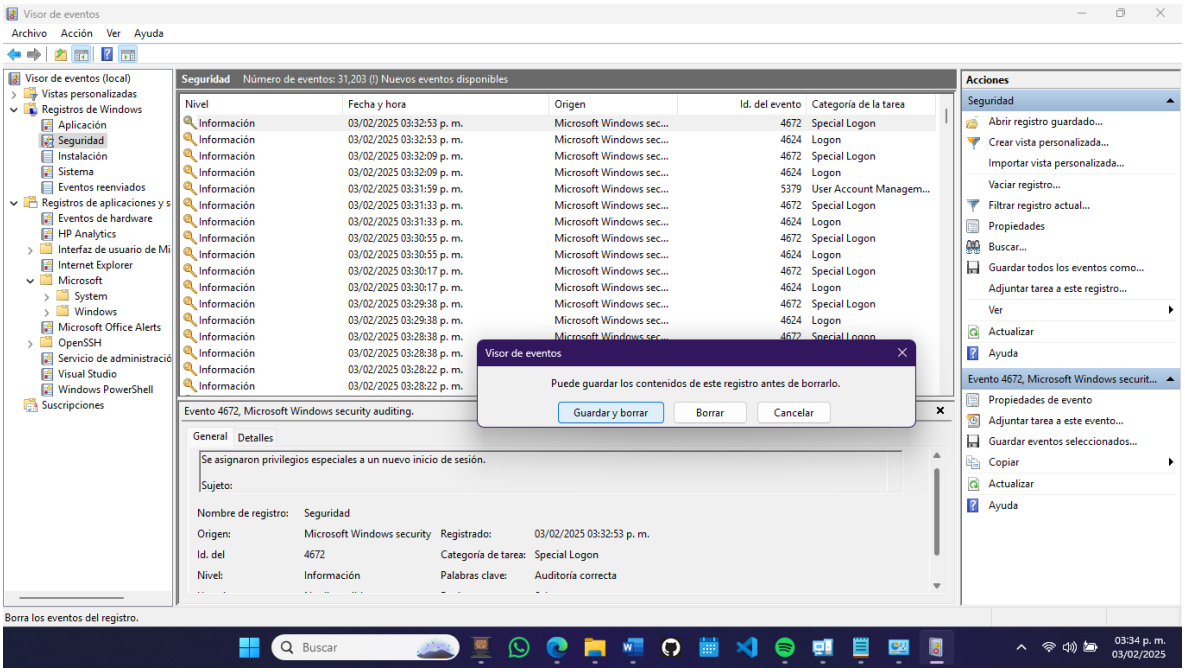
Detalles de auditoria



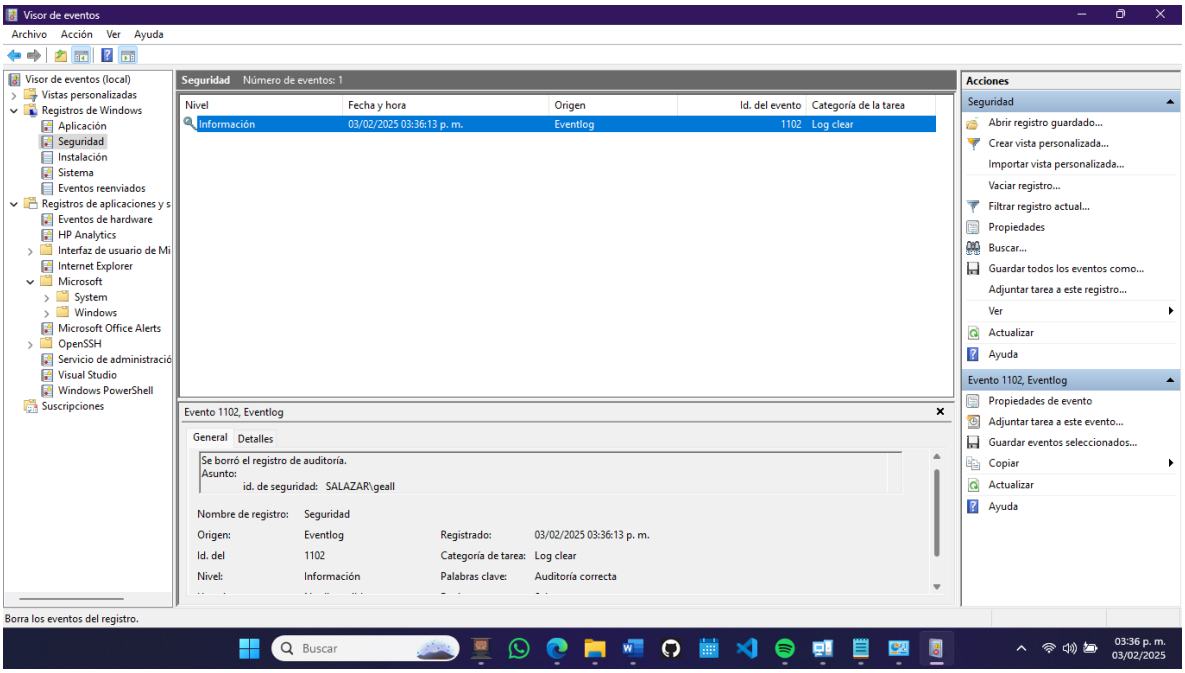
Utilizando los filtros de búsqueda



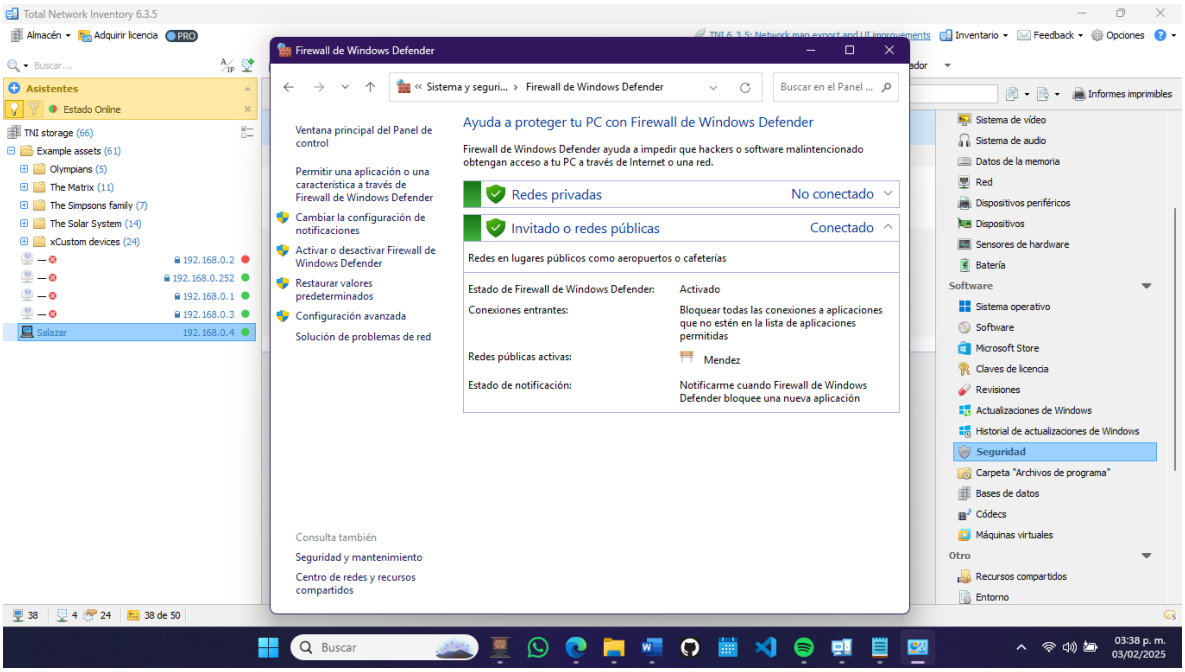
Detalles de eventos de Instalación



Vaciando el registro de eventos



Eventos borrados, y se creó el nuevo evento de borrado de eventos



Firewall activo

CONCLUSIÓN

La realización de auditorías y la gestión de bitácoras son prácticas fundamentales en el ámbito de la seguridad informática, tanto en el entorno laboral como en la vida cotidiana. Esta actividad ha permitido comprender la importancia de llevar un control riguroso sobre los recursos tecnológicos, incluyendo hardware, software, licencias y configuraciones de red. La auditoría regular de estos elementos no solo contribuye a la detección temprana de vulnerabilidades y amenazas, sino que también garantiza el cumplimiento de normativas legales y regulatorias, lo cual es esencial para evitar sanciones y mantener la integridad de la infraestructura tecnológica.

El uso de herramientas especializadas como Total Network Inventory facilita este proceso, proporcionando informes detallados que permiten identificar rápidamente cualquier anomalía o irregularidad. La gestión de bitácoras, por su parte, ofrece un registro histórico invaluable que ayuda a analizar la evolución de la seguridad del sistema a lo largo del tiempo. Esta práctica es crucial para detectar patrones de comportamiento inusuales, identificar posibles brechas de seguridad y tomar decisiones informadas para mitigar riesgos.

En el contexto laboral, estas actividades fortalecen la capacidad de respuesta ante incidentes de seguridad, mejoran la eficiencia en la gestión de recursos tecnológicos y contribuyen a la creación de un entorno más seguro y confiable. En la vida cotidiana, aplicar estos principios permite proteger dispositivos personales, asegurar la privacidad de la información y fomentar una cultura de seguridad digital. En conclusión, la auditoría y la gestión de bitácoras son herramientas clave para mantener la seguridad y el control en cualquier entorno tecnológico.