Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Etapa | # 3 Proyecto Final: Auditoría y Bitácora

Seguridad Informática II

Ingeniería en Desarrollo de Software

academia global

TUTOR: Jessica Hernández Romero

ALUMNO: Sarahi Jaqueline Gomez Juárez

FECHA: martes 02 de febrero de 2026

Índice

Introducción:

La seguridad informática se construye a partir de un proceso continuo que integra la prevención de riesgos, el monitoreo constante de los sistemas y la realización de auditorías que permitan evaluar el estado real de protección de los equipos de cómputo; En las etapas anteriores del proyecto se abordó la detección y prevención de ataques de acceso mediante el uso de herramientas especializadas como Tenable Nessus Essentials, lo que permitió identificar vulnerabilidades técnicas, servicios expuestos y posibles riesgos dentro del sistema, este análisis inicial evidenció la importancia de aplicar mecanismos de seguridad preventiva para reducir la superficie de ataque y fortalecer la protección de la información.

Posteriormente, se reforzó el enfoque de seguridad mediante la observación del comportamiento del sistema a través del monitoreo de eventos y registros, permitiendo identificar errores, procesos internos y actividades relevantes que podrían representar amenazas o fallas de funcionamiento, este seguimiento continuo demostró que la seguridad no depende únicamente de la detección de vulnerabilidades, sino también de la supervisión constante de los recursos tecnológicos.

En esta nueva etapa, el proyecto avanza hacia la auditoría del equipo a través de herramientas propias del sistema operativo, como el Panel de control y las Herramientas administrativas de Windows, complementadas con el uso de bitácoras de acceso, este proceso permite evaluar de manera más amplia el estado del sistema, validar aspectos legales como las licencias de los recursos utilizados y analizar los registros de eventos que documentan el comportamiento del equipo, de esta forma, se integra una visión más completa de la seguridad informática, donde la prevención, el monitoreo y la auditoría trabajan de manera conjunta para

fortalecer la protección del sistema.

Asimismo, la implementación de bitácoras representa un elemento clave en la gestión de la seguridad, ya que permite conservar evidencia de los eventos ocurridos, facilitar futuras auditorías y mejorar la toma de decisiones en materia de protección informática, en conjunto, esta etapa consolida el aprendizaje práctico del proyecto, demostrando que una estrategia de seguridad efectiva requiere no solo identificar vulnerabilidades, sino también supervisar continuamente el sistema y evaluar periódicamente su estado mediante auditorías estructuradas.

Descripción:

El desarrollo del proyecto se centra en la realización de una **auditoría** técnica del equipo de cómputo mediante el uso de las herramientas administrativas de Windows, específicamente desde el Panel de control y el Visor de eventos, este proceso permitió analizar de manera detallada el estado del sistema, los recursos instalados y los eventos generados por el propio sistema operativo, con el fin de identificar posibles vulnerabilidades, errores operativos y comportamientos relevantes para la seguridad informática, contribuyendo tanto a la **prevención** de ataques de acceso como al **monitoreo** constante del sistema.

En primera instancia, se accedió al Panel de control en vista general para identificar las principales opciones de configuración del sistema, lo cual permitió ubicar las Herramientas de Windows, a través de estas herramientas se ingresó al Visor de eventos, donde se visualizó el resumen administrativo que clasifica los eventos en críticos, errores, advertencias, información y auditorías correctas, este resumen ofreció una visión general del estado del sistema y facilitó el **monitoreo** inicial de incidentes relevantes dentro del proceso de **auditoría**.

Posteriormente, se revisaron los distintos registros del sistema, tales como Seguridad, Aplicación, Sistema e Instalación, en el registro de Seguridad se analizaron eventos de auditoría correcta relacionados con conexiones permitidas por el firewall, así como detalles técnicos de procesos, direcciones IP y puertos utilizados, lo que permitió evaluar el comportamiento de la red y fortalecer la **prevención** de accesos no autorizados, para optimizar el análisis, se aplicaron filtros que mostraron únicamente eventos críticos y de error, concentrando el **monitoreo** en aquellos incidentes con mayor impacto en la estabilidad y seguridad del sistema.

En el registro de Aplicación se identificaron errores generados por distintos servicios, lo

que evidenció posibles fallas de configuración o rendimiento, al seleccionar eventos específicos, se desplegó información técnica detallada que facilitó la comprensión de cada problema detectado, de igual manera, en el registro de Instalación se revisaron eventos informativos relacionados con procesos de actualización del sistema operativo, confirmando instalaciones exitosas de componentes y parches de seguridad, lo cual resulta fundamental para la **prevención** de vulnerabilidades dentro del proceso de **auditoría**.

Asimismo, se analizaron los eventos del registro de Sistema, donde se observaron errores y procesos internos que reflejan el comportamiento general del sistema operativo, contribuyendo al **monitoreo** integral del equipo, también se revisó la sección de eventos reenviados, constatando su estado deshabilitado y aplicando filtros para verificar la ausencia de registros externos, lo cual permitió comprender el funcionamiento de esta característica dentro de la **auditoría** realizada.

Como parte de la gestión de la bitácora, se accedió a la opción para guardar o borrar los eventos del registro de seguridad, cumpliendo con el requisito de iniciar una nueva bitácora para el seguimiento de cambios posteriores, esta acción fortalece tanto el **monitoreo** continuo como la capacidad de **auditoría**, al permitir mantener registros actualizados para futuras revisiones.

Finalmente, se accedió al Firewall de Windows Defender con seguridad avanzada para verificar el estado de los perfiles de red (dominio, privado y público), la visualización de estos perfiles activos confirmó que el sistema cuenta con medidas de **prevención** para bloquear conexiones no autorizadas, reforzando la protección del equipo frente a posibles amenazas.

En conjunto, el desarrollo del proyecto permitió integrar de manera práctica los principios de **prevención**, **monitoreo** y **auditoría**, mediante el análisis detallado de bitácoras de eventos y la verificación de medidas de seguridad del sistema, evidenciando asi la importancia

de aplicar estas estrategias de forma continua para fortalecer la seguridad informática y reducir riesgos operativos.

Justificación:

El objetivo principal de este proyecto fue fortalecer el conocimiento práctico en el área de la seguridad informática mediante la aplicación de procesos reales de auditoría de sistemas, monitoreo de eventos y gestión de bitácoras de acceso, utilizando herramientas administrativas del sistema operativo Windows, a través de estas etapas, se buscó comprender de manera integral cómo se protegen los equipos de cómputo frente a amenazas digitales, errores técnicos y accesos no autorizados, integrando conceptos fundamentales como la prevención de ataques, la supervisión constante y la evaluación periódica del estado del sistema.

Asimismo, una de las metas del proyecto consistió en analizar los recursos del equipo, validar procesos de actualización, identificar posibles vulnerabilidades y confirmar la correcta configuración de los mecanismos de seguridad, como el Firewall de Windows Defender y los registros del Visor de eventos, este enfoque permitió desarrollar una visión crítica sobre la importancia de mantener sistemas actualizados, configurados adecuadamente y monitoreados de forma continua para garantizar la protección de la información y la estabilidad operativa.

Dentro del servicio de monitoreo implementado se destacaron características como la supervisión continua del sistema en tiempo real, el registro automático de eventos críticos, informativos y de error, la aplicación de filtros para concentrar el análisis en incidentes relevantes, y la generación de reportes a partir de los registros del sistema, estas características permiten detectar anomalías de manera temprana, optimizar la respuesta ante fallas y mantener un control constante del comportamiento del equipo.

Por su parte, el servicio de auditoría presentó características esenciales como la revisión sistemática de los recursos del sistema, la evaluación de configuraciones de seguridad, la

verificación de actualizaciones y parches de protección, el análisis de eventos técnicos específicos y la validación de mecanismos de control como el firewall, estas acciones facilitan la identificación de vulnerabilidades, errores operativos y áreas de mejora dentro del sistema.

Otro propósito relevante fue aplicar el uso de bitácoras como herramienta clave para documentar actividades del sistema, detectar anomalías y conservar evidencia para futuras auditorías, mediante el guardado y reinicio de los registros, ayudando a comprender cómo se realiza un control histórico de eventos, fortaleciendo la capacidad de análisis y prevención de incidentes de seguridad.

Además, el proyecto vincula los conocimientos adquiridos en las etapas anteriores con prácticas reales de auditoría y monitoreo, consolidando habilidades técnicas esenciales dentro del campo de la ciberseguridad, esta integración contribuye a la formación profesional, preparándonos para enfrentar escenarios reales en entornos laborales donde la seguridad de la información es un elemento crítico.

En conjunto, el desarrollo de esta etapa permitió alcanzar una comprensión completa de cómo la prevención, el monitoreo, la auditoría y el manejo adecuado de bitácoras trabajan de manera complementaria para proteger los sistemas de cómputo, de esta forma, el proyecto no solo fortaleció el aprendizaje técnico, sino que también fomentó una cultura de seguridad digital orientada a la protección responsable de los recursos tecnológicos tanto en contextos profesionales como cotidianos.

Desarrollo:

Proyecto Final - Etapa 3 - Auditoría y Bitácora

Contextualización:

A continuación se procederá a realizar una auditoría desde el equipo de cómputo o utilizando una herramienta especializada, esto permitirá identificar las licencias de los recursos instalados y obtener información precisa de los recursos del equipo de cómputo. Las auditorías y bitácoras proporcionan un escenario de los posibles ataques que se pueden presentar y a su vez poder prevenirlos, de igual manera otorga información legal respecto a las licencias obtenidas y faltantes, mantener un control total del equipo apertura una mayor seguridad en los mecanismos que se implementen para salvaguardar los recursos valiosos como es la información.

●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.

● Es importante que se guarde la bitácora, eliminarla e iniciar una nueva para detectar los cambios desde el día 1.

Actividad: tomando en cuenta las actividades 1 y 2, realiza lo siguiente:

Auditoría y bitácora:

● Realizar una auditoría de un equipo desde el Panel de control > Herramientas administrativas; o desde una herramienta digital.

● Guardar la bitácora e iniciar una nueva.

● Adjuntar capturas de pantalla.

Software propuesto: Total Network Inventory. O bien, desde el **Panel de Control del Equipo.**

Enlace de la Auditoría en Drive Google:

https://drive.google.com/file/d/1M9nuxc-bxOHVroKoVhMgs-8p8mE5UFeG/view?usp=sharing

Nota: Es fundamental que se descargue el archivo para interactuar con la auditoría, no permite la visualización previa en Drive Google para este tipo de archivos.

Enlace de la Etapa 1 - Detección y Prevención de Ataques de Acceso en Drive Google:

https://drive.google.com/file/d/1TxzQMW8o3b87fEvb553iCJ6nemVTqEFK/view?usp=sharing

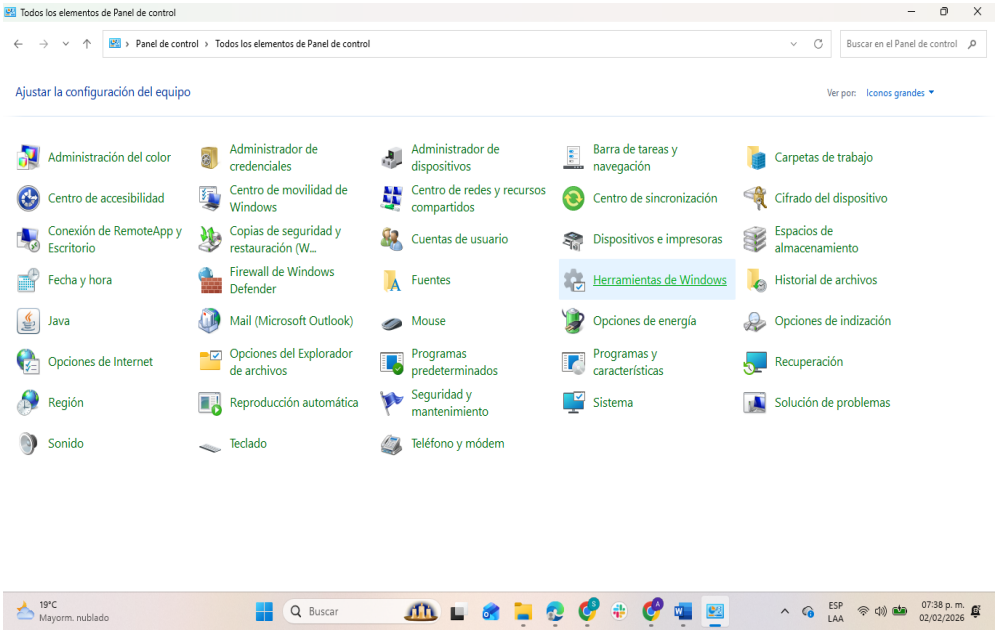
Enlace de la Etapa 2 - Monitoreo de Red en Drive Google:

https://drive.google.com/file/d/1dpM7GT5eZD2KOVT3SdNMMclO8dEuo1JL/view?usp=sharing

Auditoría de Equipo:

Figura 1

Visualización General de los Elementos del Panel de Control de Windows

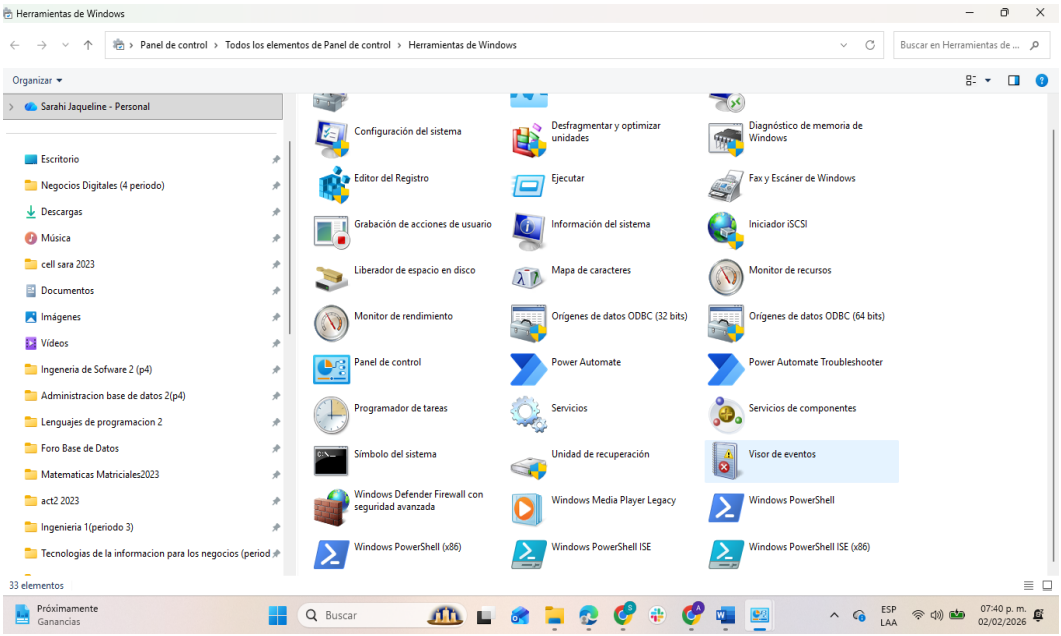


Nota: Se accedió al Panel de control de Windows en vista de iconos grandes, donde se muestran las principales herramientas de configuración del sistema, incluyendo opciones de seguridad, red, cuentas de usuario y administración, esta acción permitió identificar de forma centralizada los componentes que intervienen en la protección y gestión del equipo.

El resultado fue la visualización completa de las funciones disponibles para el control del sistema, desde el enfoque de la ciberseguridad, este acceso facilita la supervisión de configuraciones críticas como firewall, cifrado y cuentas de usuario, se recomienda revisar periódicamente estas opciones para asegurar que los mecanismos de seguridad estén correctamente habilitados.

Figura 2

Acceso a las Herramientas Administrativas desde la Carpeta Herramientas de Windows

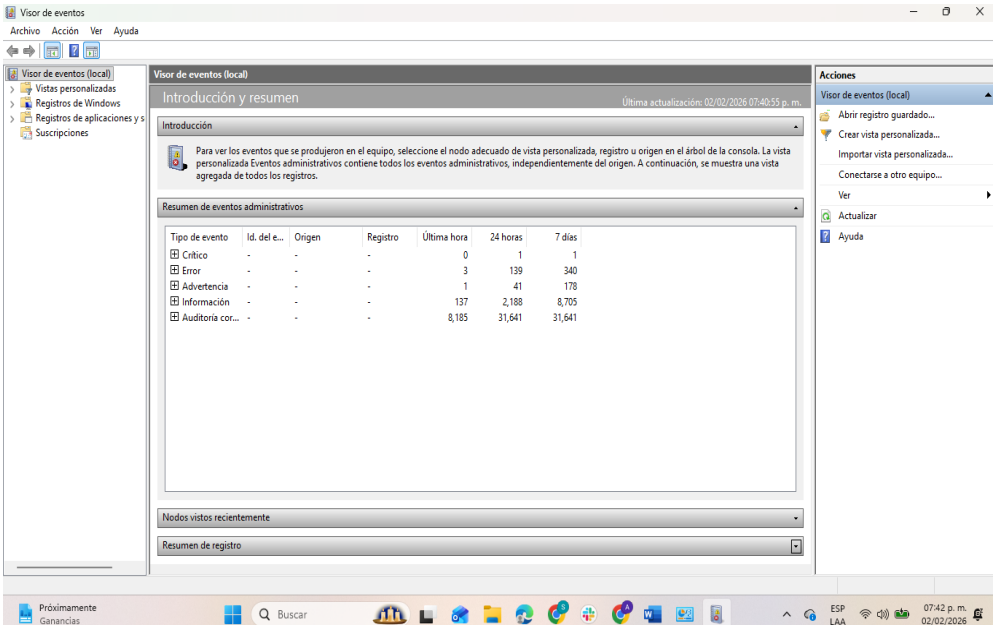


Nota: Se seleccionó la opción “Herramientas de Windows” dentro del Panel de control, desplegándose una carpeta con diversas utilidades administrativas como Visor de eventos, Servicios, Programador de tareas y Monitor de recursos, esta acción permitió acceder a las herramientas encargadas del monitoreo interno del sistema.

El resultado fue la visualización de los módulos de administración avanzada de Windows, desde el enfoque de la ciberseguridad, estas herramientas son fundamentales para el control de procesos, registros y configuraciones críticas, se recomienda utilizarlas para realizar revisiones técnicas periódicas del sistema.

Figura 3

Interfaz Principal del Visor de Eventos Mostrando El Resumen Administrativo

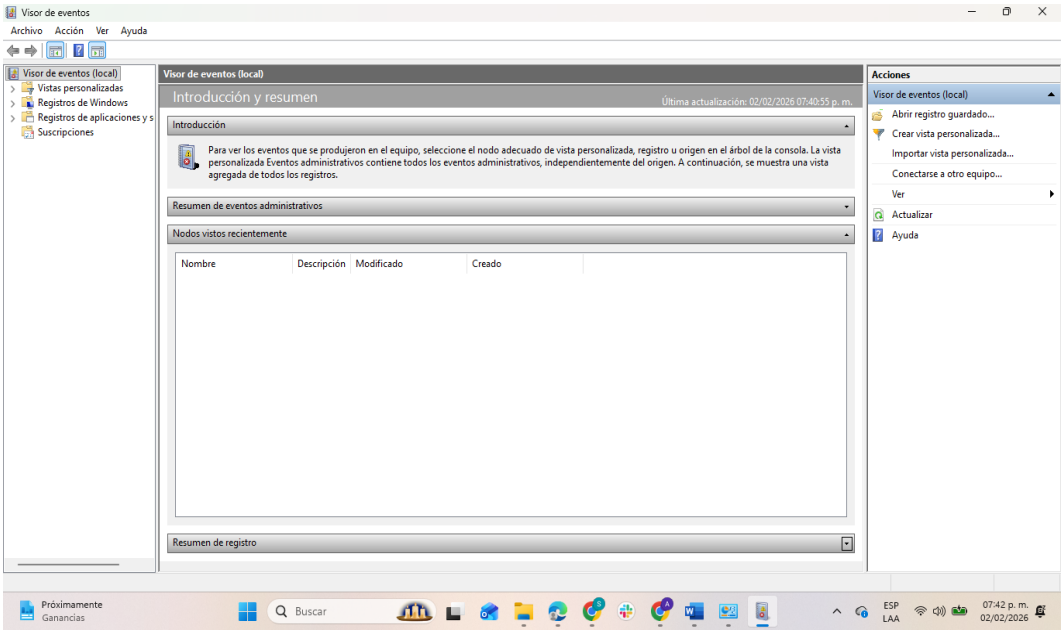


Nota: Se ingresó al Visor de eventos seleccionando su icono dentro de las Herramientas de Windows, esta acción permitió visualizar el resumen administrativo que clasifica los eventos en críticos, errores, advertencias, información y auditorías correctas.

El resultado fue la presentación general del estado del sistema mediante registros acumulados, desde el enfoque de la ciberseguridad, este resumen permite identificar rápidamente fallos graves o comportamientos anómalos, se recomienda analizar con frecuencia esta sección para detectar incidentes tempranos.

Figura 4

Visualización de la Sección de Nodos Vistos Recientemente



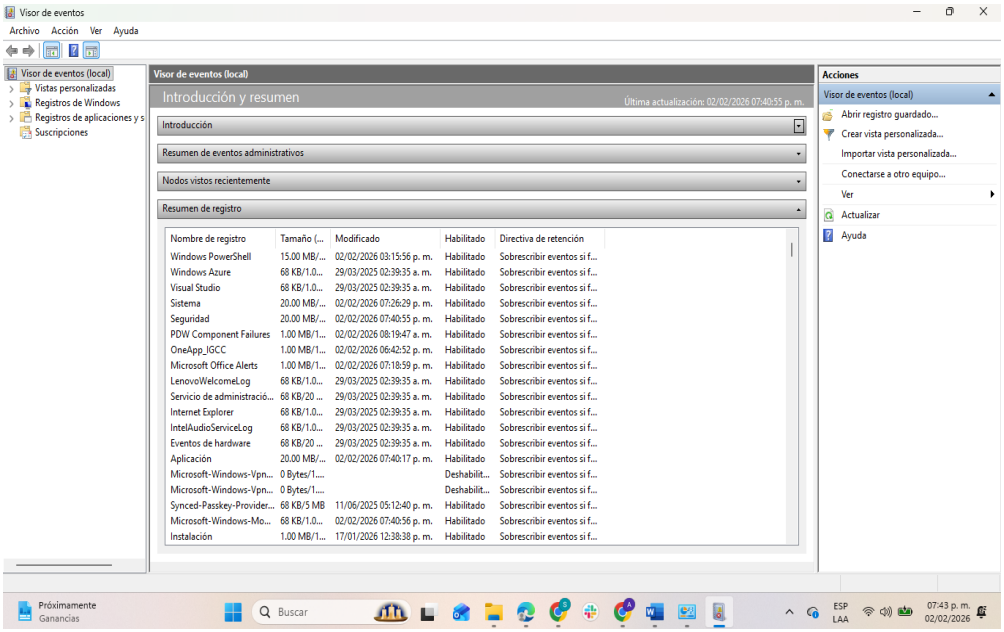
Nota: Dentro del Visor de eventos se observó la sección de nodos vistos recientemente, la cual muestra accesos previos a diferentes registros o vistas del sistema, esta acción permitió confirmar las áreas que han sido consultadas durante el monitoreo.

El resultado fue la visualización de accesos recientes dentro del visor, desde el enfoque de la ciberseguridad, esta función facilita el seguimiento continuo de registros importantes.

Se recomienda utilizar esta sección para agilizar revisiones periódicas de eventos críticos.

Figura 5

Resumen General de Registros del Sistema

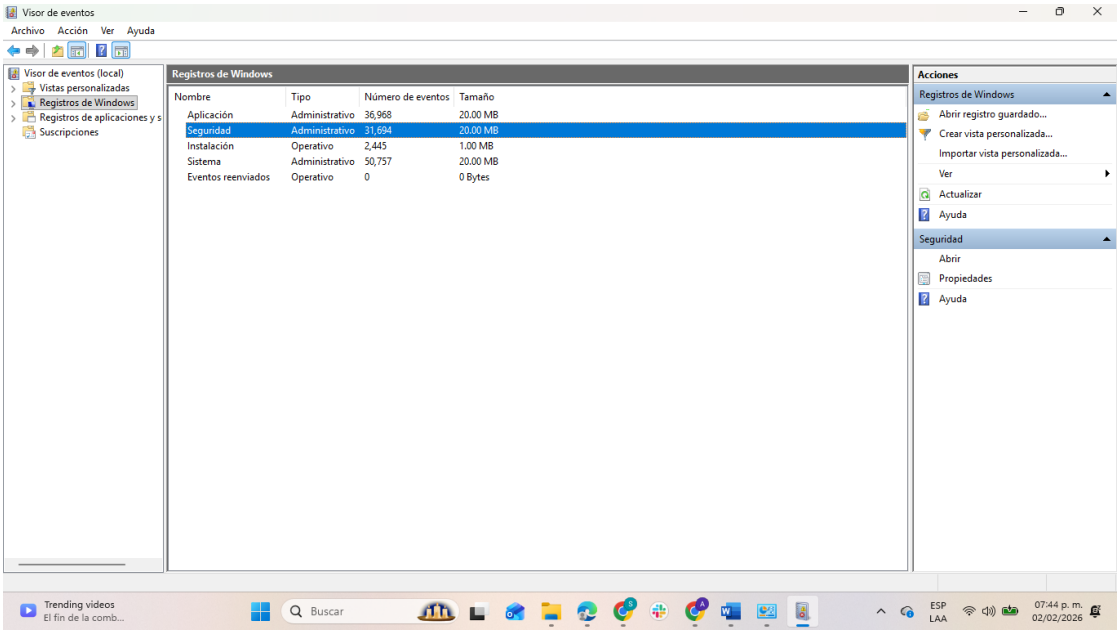


Nota: Se visualizó el apartado de resumen de registros, donde se listan diferentes bitácoras del sistema como Seguridad, Sistema, Aplicación e Instalación, junto con información de tamaño y estado de habilitación, esta acción permitió verificar que los registros se encuentran activos y funcionando correctamente.

El resultado fue la confirmación del almacenamiento continuo de eventos, desde el enfoque de la ciberseguridad, mantener estos registros habilitados es esencial para auditorías y análisis de incidentes. Se recomienda no deshabilitar ninguna bitácora crítica.

Figura 6

Selección del Registro de Seguridad Dentro de los Registros de Windows

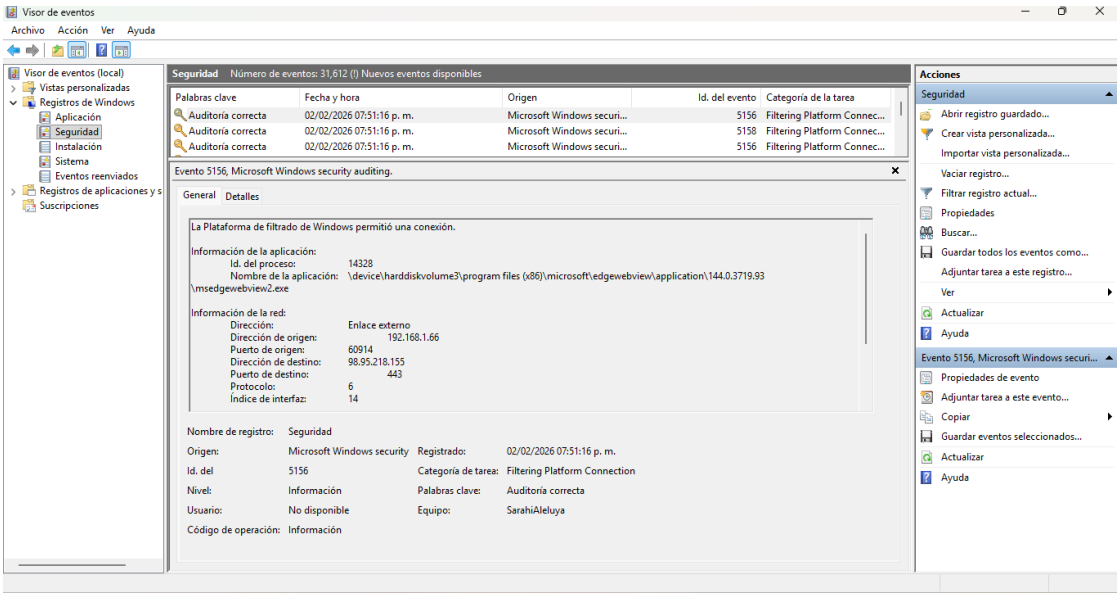


Nota: Se ingresó al apartado **"Registros de Windows"** y se seleccionó específicamente el registro de Seguridad, esta acción permitió acceder a los eventos relacionados con auditorías, accesos y conexiones del sistema.

El resultado fue la visualización del conjunto de eventos de seguridad registrados por Windows, desde el enfoque de la ciberseguridad, este registro es uno de los más importantes para detectar accesos no autorizados o actividad sospechosa, se recomienda revisarlo constantemente como parte del monitoreo de seguridad.

Figura 7

Listado de Eventos de Auditoría Correcta en el Registro de Seguridad



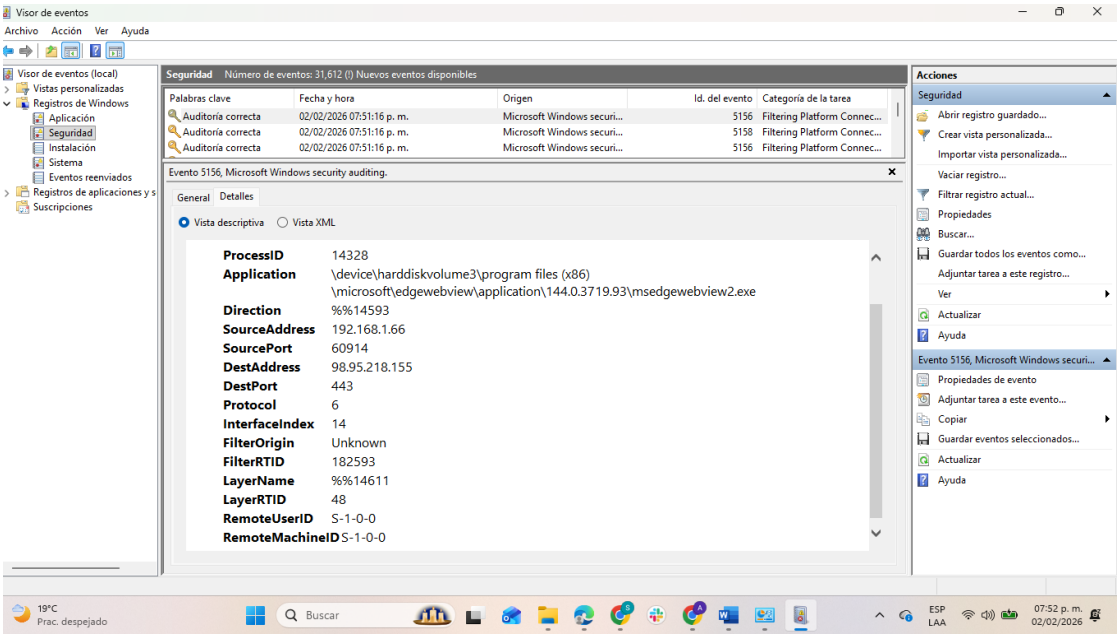
Nota: Se observaron múltiples eventos marcados como “Auditoría correcta”, generados por Microsoft Windows Security Auditing, relacionados con conexiones permitidas por la plataforma de filtrado, esta acción permitió analizar la actividad normal del sistema y del firewall.

El resultado fue la visualización continua de conexiones autorizadas, desde el enfoque de la ciberseguridad, estos eventos confirman el funcionamiento del control de tráfico de red.

Se recomienda revisar patrones inusuales que puedan indicar intentos de intrusión.

Figura 8

Detalle Técnico de un Evento de Seguridad con Conexión Permitida

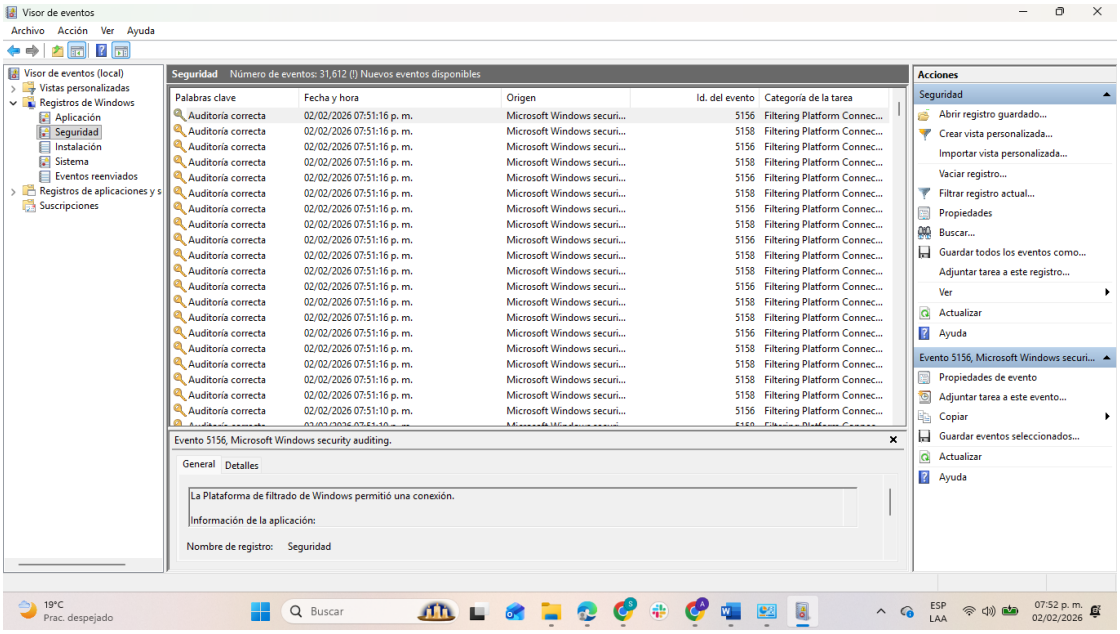


Nota: Se seleccionó un evento específico dentro del registro de Seguridad, desplegándose su información detallada como ID del proceso, aplicación involucrada, direcciones IP, puertos y protocolo utilizado, esta acción permitió analizar una conexión autorizada por el sistema.

El resultado fue la visualización completa de los datos técnicos de red, desde el enfoque de la ciberseguridad, este nivel de detalle es clave para rastrear tráfico legítimo y detectar posibles conexiones sospechosas. Se recomienda monitorear estas conexiones regularmente.

Figura 9

Visualización Masiva de Eventos Registrados en el Apartado de Seguridad



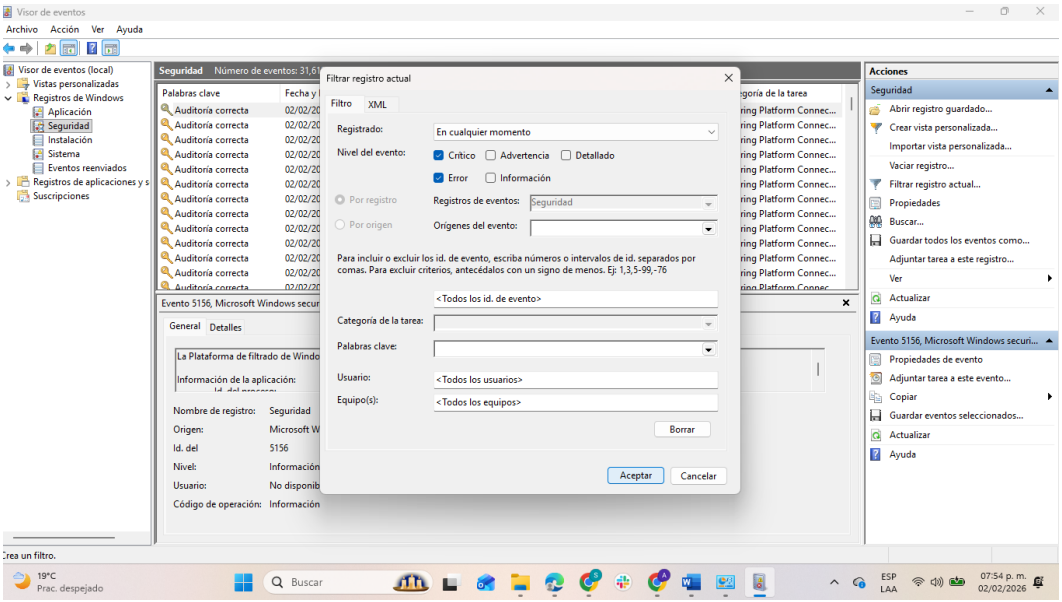
Nota: Se observó una extensa lista de eventos de auditoría correcta acumulados dentro del registro de Seguridad, evidenciando la alta actividad de monitoreo del sistema, esta acción permitió confirmar el registro continuo de eventos de seguridad.

El resultado fue la visualización de múltiples conexiones y procesos supervisados, desde el enfoque de la ciberseguridad, esta acumulación refleja el funcionamiento activo de los mecanismos de control.

Se recomienda analizar periódicamente estos eventos para detectar comportamientos anormales.

Figura 10

Aplicación de Filtros en el Registro de Seguridad del Visor de Eventos

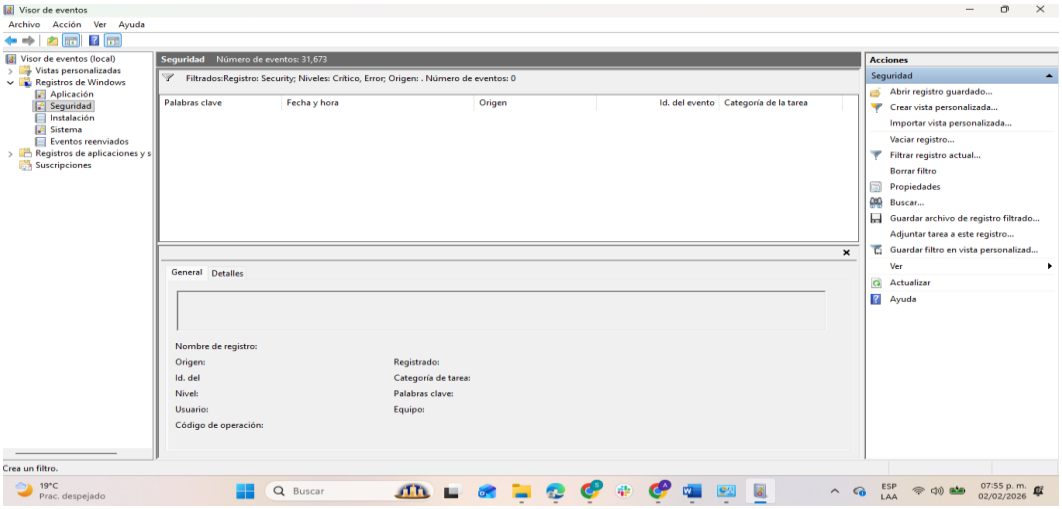


Nota: Se aplicó un filtro de eventos seleccionando niveles críticos y de error dentro del registro de Seguridad, esta acción permitió depurar los eventos relevantes para el análisis.

El resultado fue una vista filtrada que facilita la identificación de incidentes importantes, desde la ciberseguridad, este filtrado permite concentrarse en amenazas potenciales y errores graves, se recomienda emplear filtros para auditorías periódicas.

Figura 11

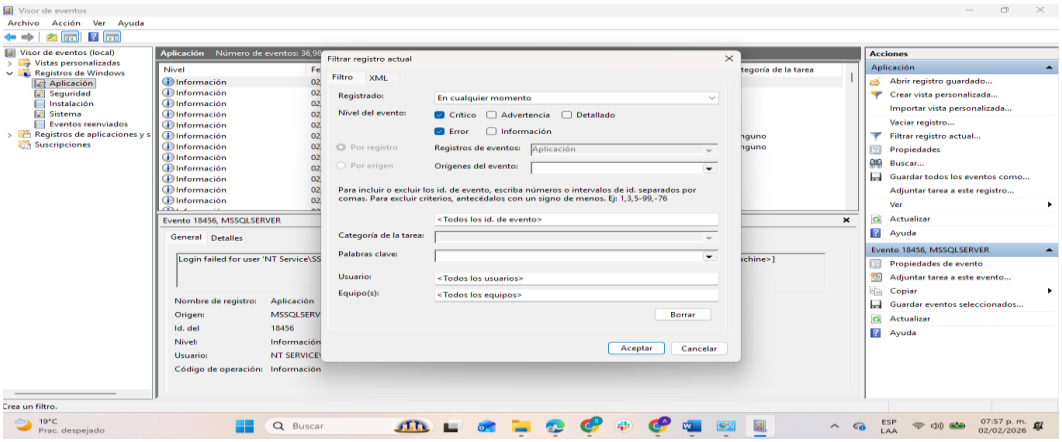
Resultado del Filtrado de Eventos Críticos en el Registro de Seguridad



Nota: Se observó que no existían eventos críticos o de error tras aplicar el filtro en Seguridad, esto confirmó la estabilidad del sistema en ese periodo, desde el enfoque de seguridad, la ausencia de errores indica funcionamiento adecuado del firewall y auditorías, se recomienda continuar con monitoreo constante.

Figura 12

Configuración de Filtros en el Registro de Aplicación

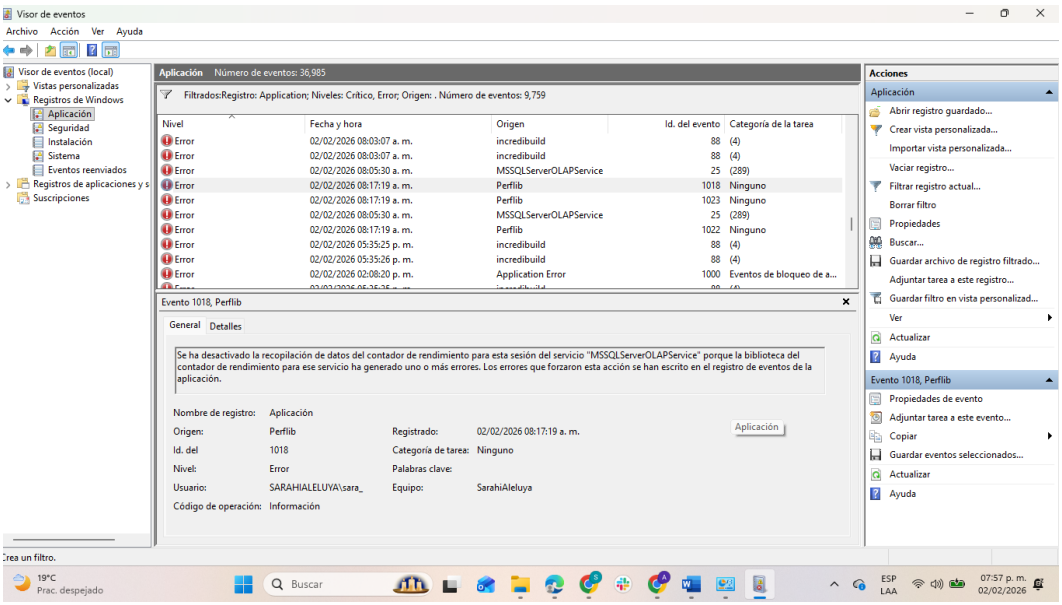


Nota: Se configuraron filtros en el registro de Aplicación para mostrar errores críticos relacionados con software, esta acción permitió detectar fallos de servicios.

El resultado fue una lista depurada de errores relevantes, desde la ciberseguridad, estos errores pueden representar vulnerabilidades del sistema, se recomienda revisar eventos de aplicaciones con frecuencia.

Figura 13

Visualización de Errores Detectados en el Registro de Aplicación

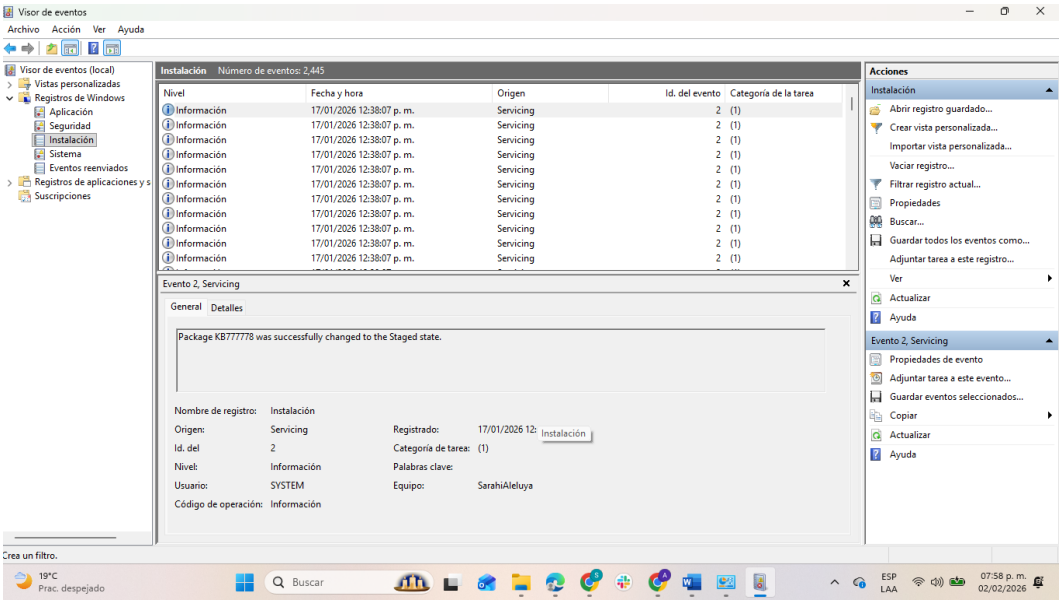


Nota: Se mostró una lista de eventos de error provenientes de distintos servicios del sistema, esto permitió analizar problemas recurrentes, desde el enfoque de seguridad, múltiples errores pueden indicar configuraciones incorrectas o riesgos operativos.

Se recomienda corregir servicios con fallas constantes.

Figura 14

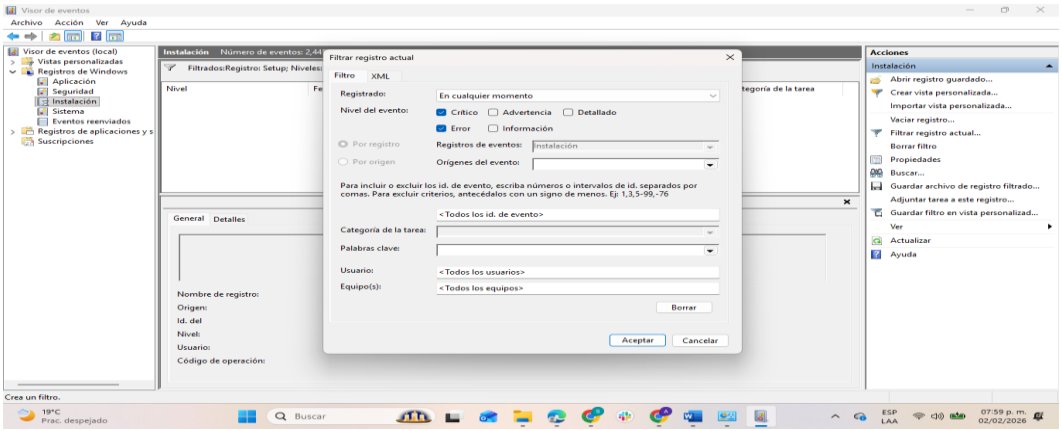
Detalle de Evento de Error Específico en Aplicación



Nota: Se seleccionó un evento detallado mostrando fallos de recopilación de datos de rendimiento, esto permitió identificar problemas técnicos, desde la ciberseguridad, estos errores pueden afectar la estabilidad del monitoreo, se recomienda reparar servicios afectados.

Figura 15

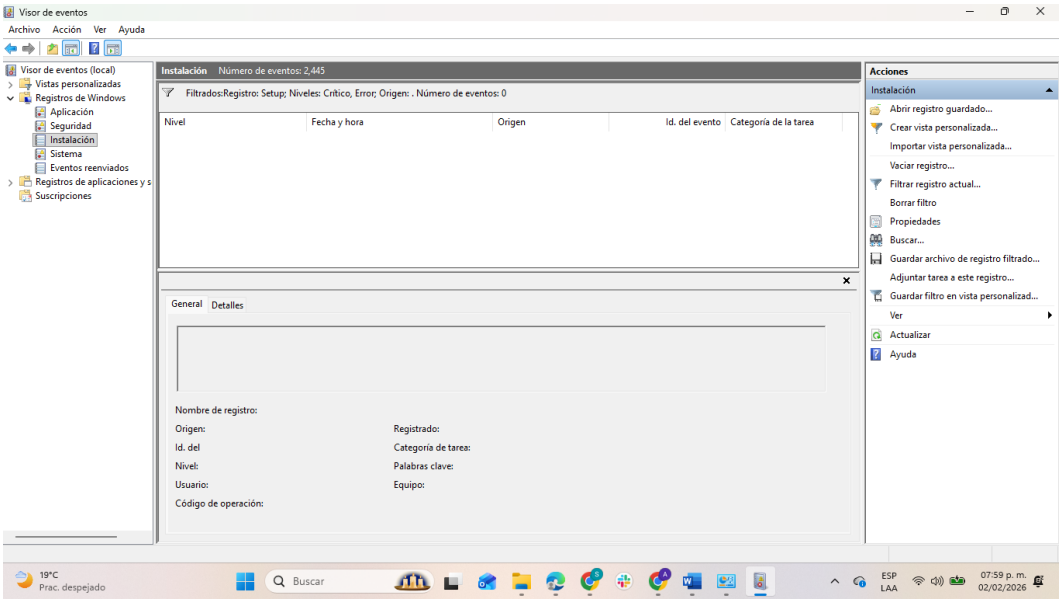
Listado de Eventos del Registro de Instalación



Nota: Se visualizó el registro de Instalación aplicando el filtro correspondiente para mostrar únicamente eventos críticos y de error, junto con eventos informativos sobre procesos de actualización del sistema, esto permitió confirmar cambios exitosos y descartar fallos relevantes durante las instalaciones, desde el enfoque de la ciberseguridad, mantener las actualizaciones correctamente ejecutadas es fundamental para la corrección de vulnerabilidades y el fortalecimiento del sistema, se recomienda revisar periódicamente estos registros filtrados para asegurar que todas las instalaciones se realicen correctamente.

Figura 16

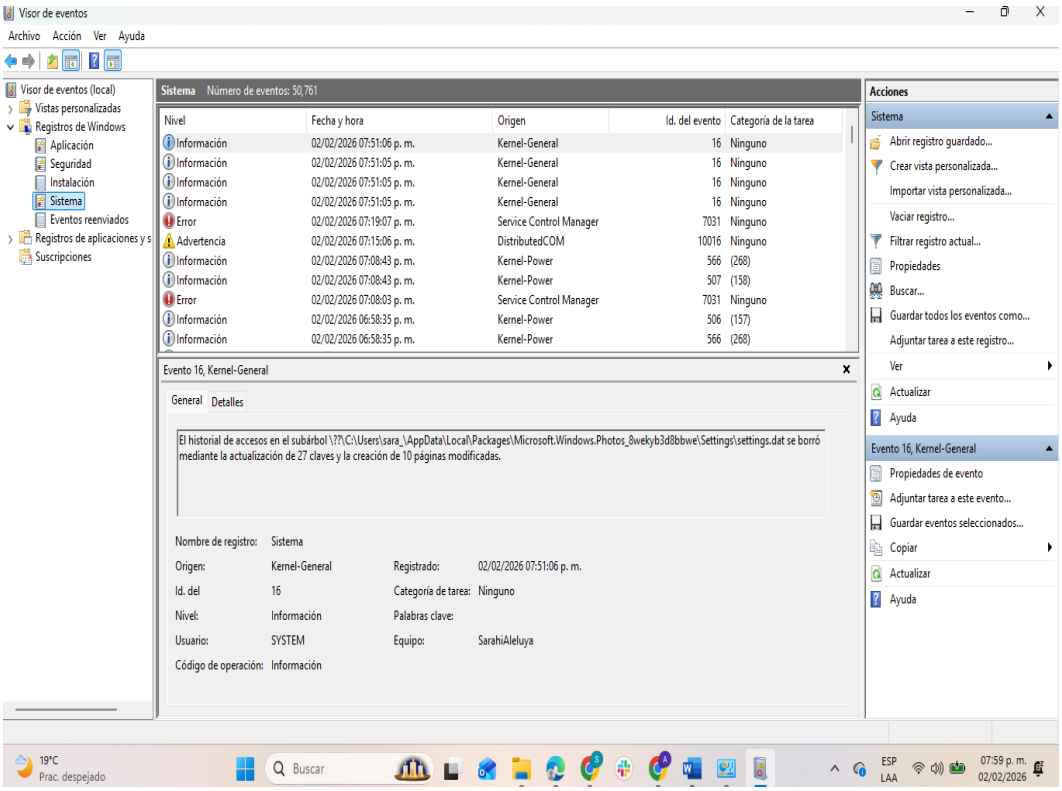
Detalle de Evento de Instalación Exitosa



Nota: Se observó un evento que confirma la actualización correcta de un paquete del sistema, esto permitió validar la integridad de procesos de instalación, desde el enfoque de seguridad, las actualizaciones previenen vulnerabilidades, se recomienda mantener el sistema actualizado.

Figura 17

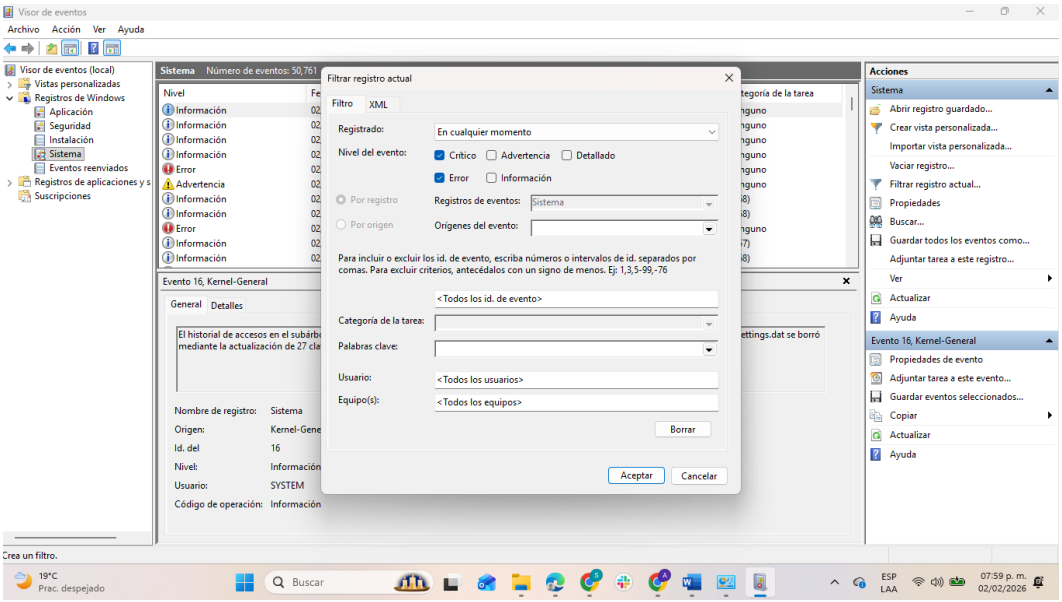
Configuración de Filtros en el Registro de Sistema



Nota: Se aplicaron filtros en el registro de Sistema para visualizar errores críticos. Esto permitió depurar eventos relevantes. Desde la ciberseguridad, este filtrado facilita identificar fallas graves del sistema operativo. Se recomienda aplicar filtros regularmente.

Figura 18

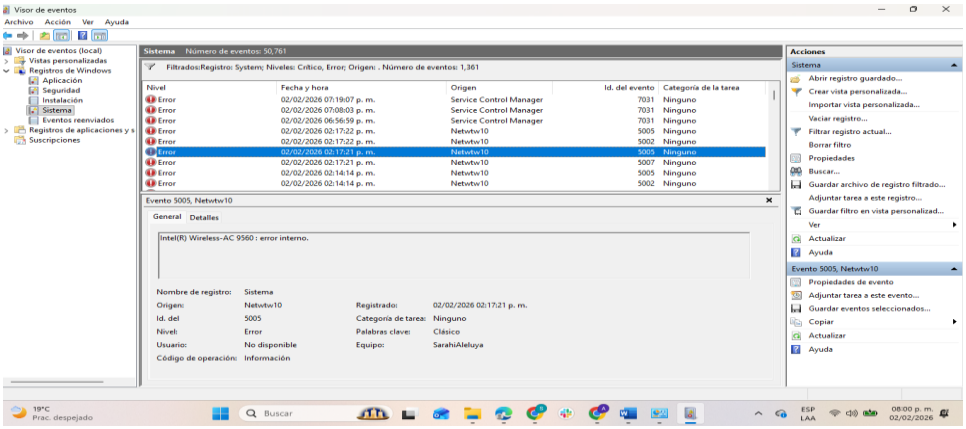
Visualización de eventos informativos y errores del sistema



Nota: Se mostró una lista de eventos del sistema relacionados con procesos internos, esto permitió analizar el comportamiento del sistema operativo, desde el enfoque de seguridad, estos eventos ayudan a detectar anomalías. Se recomienda monitorear continuamente estos registros.

Figura 19

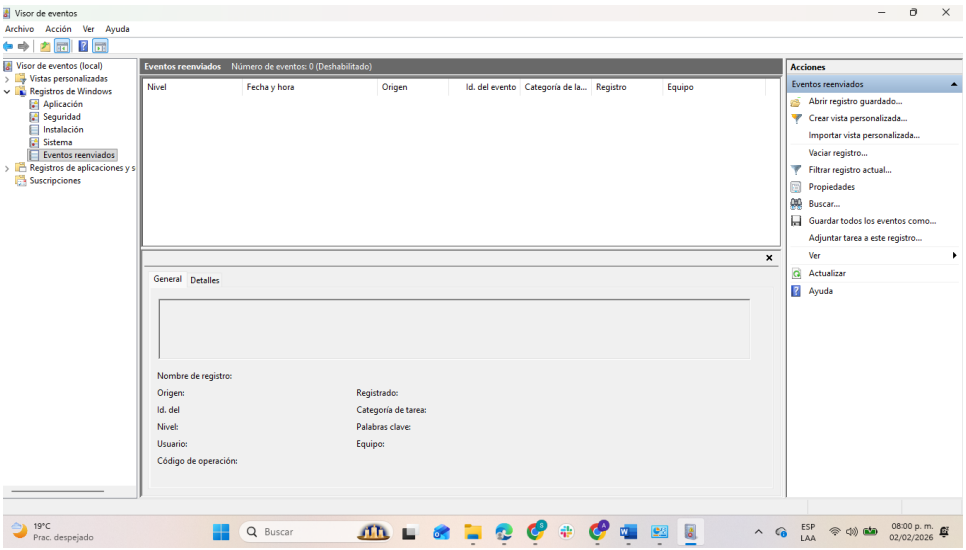
Error de Red Detectado en el Registro del Sistema



Nota: Se seleccionó un evento de error relacionado con el controlador de red Intel Wireless dentro del registro del sistema, esto permitió identificar fallas internas en la conectividad, desde el enfoque de la ciberseguridad, estos errores pueden afectar la disponibilidad del servicio y abrir vulnerabilidades, se recomienda actualizar controladores de red y monitorear fallos recurrentes.

Figura 20

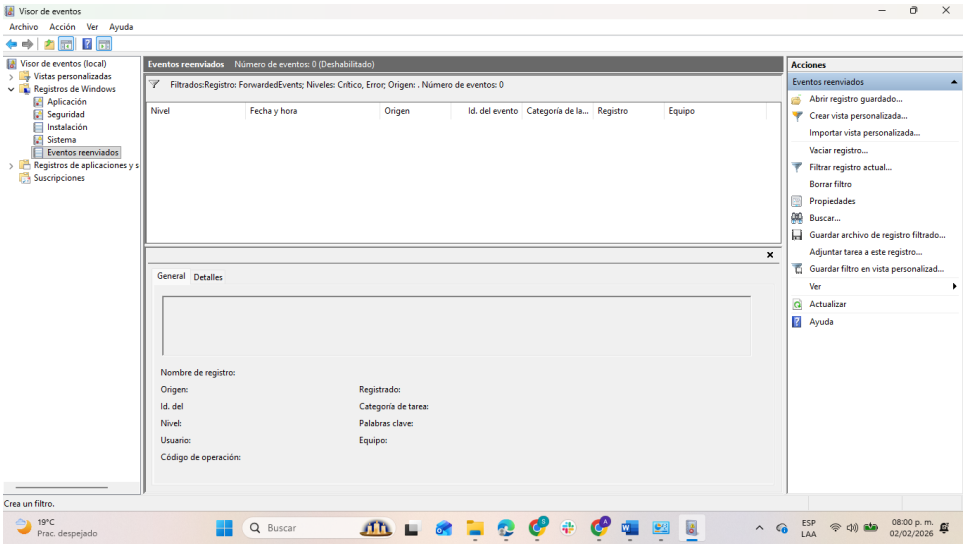
Sección de Eventos Reenviados Deshabilitada



Nota: Se ingresó al apartado de eventos reenviados observando que se encuentra deshabilitado, esto indica que no se están recibiendo registros externos, desde la ciberseguridad, habilitar esta función puede permitir monitoreo centralizado, se recomienda activarla en redes empresariales.

Figura 21

Filtro Aplicado en Eventos Reenviados

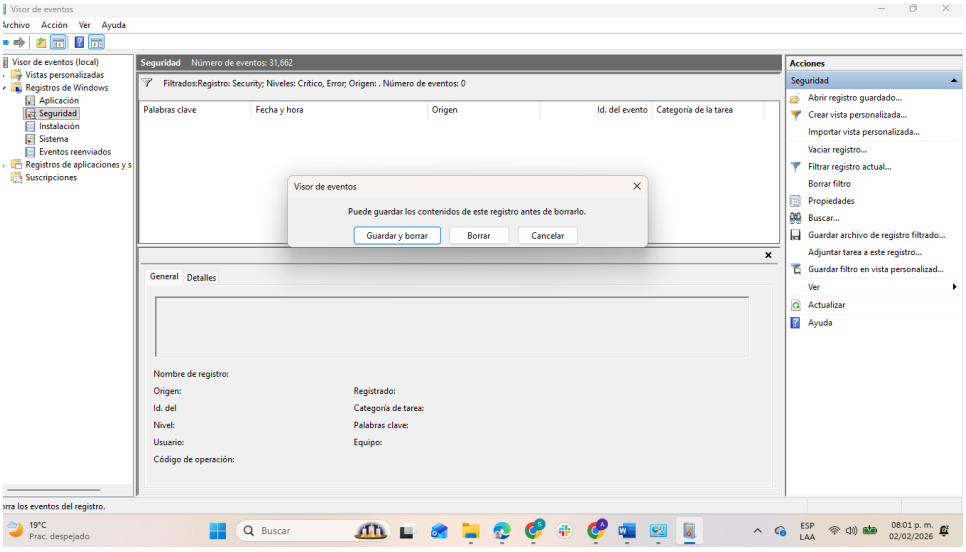


Nota: Se aplicó un filtro en eventos reenviados configurando niveles críticos y de error. El resultado fue la ausencia de eventos filtrados. Desde el enfoque de seguridad, esto confirma que no existen registros reenviados activos. Se recomienda configurar fuentes de eventos externos.

Bitácora de Eventos

Figura 22

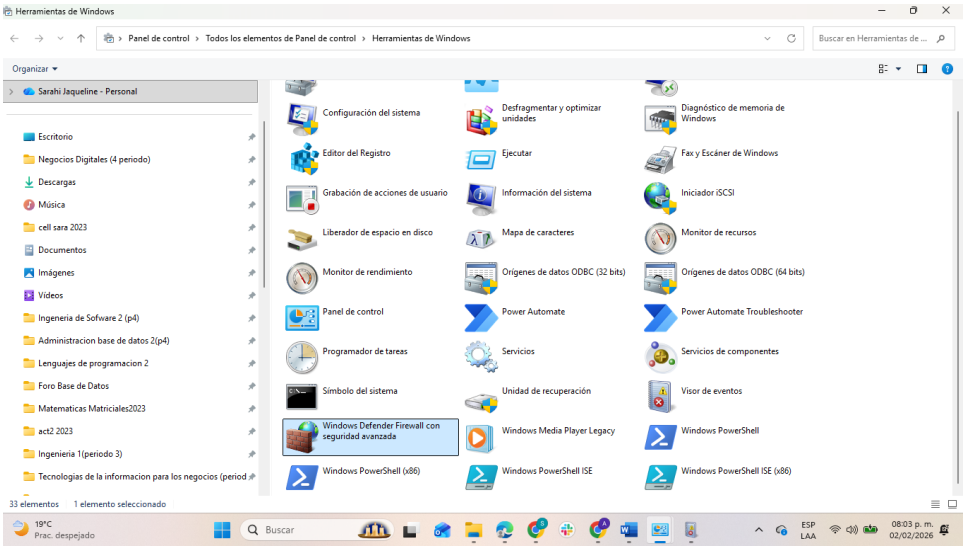
Confirmación para Borrar Eventos del Registro de Seguridad



Nota: Se mostró la ventana de confirmación para guardar o borrar eventos del registro de seguridad, esta acción permite administrar bitácoras del sistema, desde la ciberseguridad, es fundamental respaldar registros antes de eliminarlos, se recomienda conservar evidencias para auditorías.

Figura 23

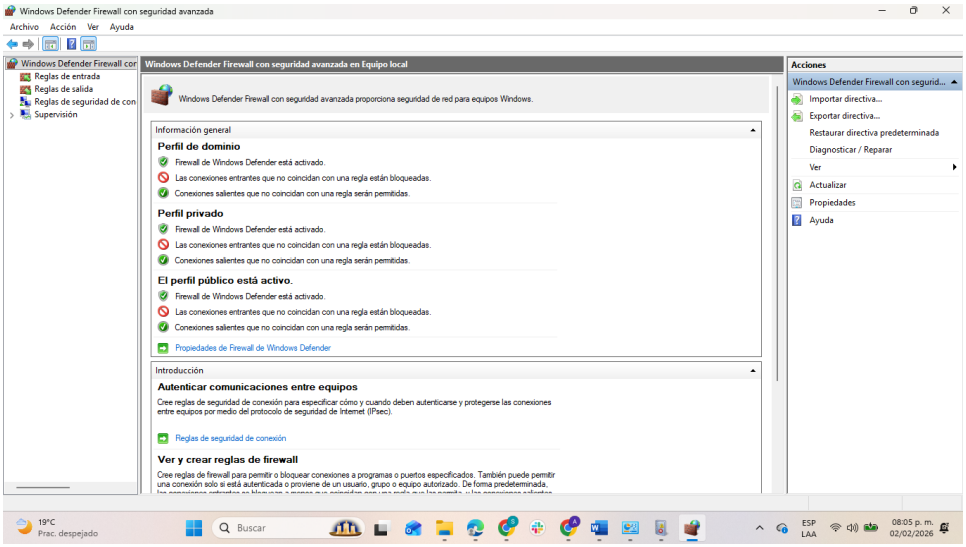
Acceso al Firewall de Windows Defender desde Herramientas de Windows



Nota: Se seleccionó el acceso al Firewall de Windows Defender con seguridad avanzada desde Herramientas de Windows, esto permitió abrir el módulo de protección de red, desde la ciberseguridad, este firewall es clave para bloquear accesos no autorizados, se recomienda revisar reglas periódicamente.

Figura 24

Panel principal del Firewall de Windows Defender con Perfiles Activos



Nota: Se visualizó el panel principal del Firewall mostrando perfiles de dominio, privado y público activos, esto confirma que la protección de red está habilitada, desde la ciberseguridad, mantener perfiles activos reduce riesgos de intrusión, se recomienda no desactivar ninguno.

Importancia de la Seguridad Informática:

Prevención, Monitoreo, Auditoría y Bitácoras de Acceso

Prevención de ataques de acceso:

• La prevención de ataques de acceso se logra mediante mecanismos de protección como firewalls, configuraciones de seguridad y actualizaciones constantes del sistema.

• La implementación de controles de acceso reduce la posibilidad de intrusiones no autorizadas.

• El uso de perfiles de red seguros fortalece la protección del equipo.

• La corrección de vulnerabilidades técnicas minimiza riesgos informáticos.

• La aplicación de políticas de seguridad adecuadas protege la información.

La prevención de ataques de acceso constituye una de las bases más importantes de la seguridad informática, ya que busca evitar que usuarios o procesos no autorizados ingresen al sistema, en términos generales, esta prevención se logra mediante el uso de firewalls, configuraciones adecuadas del sistema, controles de acceso y actualizaciones constantes del software, estas medidas permiten reducir significativamente las vulnerabilidades que pueden ser aprovechadas por atacantes.

Un ejemplo de esta práctica se observó en la auditoría realizada, donde se accedió al Firewall de Windows Defender desde las Herramientas administrativas para verificar que los perfiles de red se encontraban activos, esto permitió confirmar que las conexiones sospechosas son bloqueadas automáticamente, fortaleciendo la protección del sistema y reduciendo el riesgo de accesos no autorizados.

Monitoreo de Red y del Sistema:

• El monitoreo de red y del sistema permite supervisar continuamente actividades y detectar anomalías.

• La revisión constante de registros de eventos facilita la identificación de errores críticos.

• El análisis de procesos internos ayuda a prevenir incidentes de seguridad.

• El uso de filtros optimiza la detección de eventos relevantes.

• La supervisión en tiempo real mejora la respuesta ante fallas del sistema.

El monitoreo continuo es una práctica esencial dentro de la seguridad informática, ya que permite observar el comportamiento del sistema y la red en tiempo real, de manera general, este proceso se apoya en herramientas que registran eventos relacionados con accesos, errores y procesos internos, lo que facilita la detección temprana de anomalías.

En el trabajo desarrollado, el monitoreo se llevó a cabo mediante el Visor de eventos de Windows, donde se analizaron los registros de seguridad, sistema, aplicación e instalación. Además, se aplicaron filtros para visualizar únicamente eventos críticos y de error, lo cual permitió concentrar el análisis en incidentes relevantes, este procedimiento demuestra cómo el monitoreo constante contribuye a mantener la estabilidad del sistema y prevenir posibles fallas de seguridad.

Auditoría Informática:

• La auditoría informática evalúa el estado de seguridad de los equipos.

• Permite identificar vulnerabilidades y errores de configuración.

• Facilita la revisión de actualizaciones del sistema.

• Ayuda a mejorar las políticas de seguridad existentes.

• Contribuye al control general del sistema.

La auditoría informática consiste en una revisión sistemática de los recursos tecnológicos con el objetivo de evaluar su nivel de seguridad y funcionamiento, de forma general, este proceso permite detectar vulnerabilidades, errores técnicos y áreas de mejora que podrían

comprometer la protección del sistema.

En la auditoría realizada se analizaron distintos registros del sistema, como seguridad, aplicación, sistema e instalación, así como eventos específicos relacionados con errores de software, procesos de actualización exitosa y fallas de red, este análisis evidenció la importancia de realizar auditorías periódicas, ya que permiten verificar que el sistema se encuentre actualizado, protegido y funcionando correctamente.

Bitácoras de Acceso:

• Las bitácoras de acceso registran eventos importantes del sistema.

• Permiten rastrear accesos autorizados y actividades sospechosas.

• Facilitan la detección de errores y fallas técnicas.

• Sirven como evidencia en auditorías de seguridad.

• Ayudan en la toma de decisiones preventivas.

Las bitácoras de acceso son registros que almacenan información detallada sobre las actividades que ocurren dentro del sistema, como accesos, conexiones de red, errores y procesos internos, de forma general, estas bitácoras permiten rastrear incidentes y analizar su origen, convirtiéndose en una herramienta fundamental para la seguridad informática.

En el trabajo desarrollado, las bitácoras se visualizaron a través del Visor de eventos de Windows, donde se documentaron conexiones permitidas, errores del sistema y eventos críticos, este uso práctico demuestra cómo las bitácoras permiten llevar un control completo de las operaciones del sistema, facilitando la identificación de anomalías y apoyando la implementación de medidas correctivas.

Conclusión:

El desarrollo de la Etapa 3 del proyecto permitió consolidar de manera práctica los fundamentos de la seguridad informática mediante la aplicación de auditorías técnicas y el uso de bitácoras de eventos como herramientas esenciales para la prevención, el monitoreo y el control del sistema, a lo largo de esta etapa se evidenció que la seguridad no depende únicamente de mecanismos aislados, sino de un proceso continuo que integra la supervisión constante, la evaluación periódica y la correcta gestión de los registros del sistema.

La auditoría realizada desde el Panel de control y las Herramientas administrativas de Windows permitió analizar de forma detallada los recursos del equipo, los eventos generados por el sistema operativo y el estado de las configuraciones de seguridad, lo cual facilitó la identificación de errores técnicos, procesos internos, actualizaciones exitosas y posibles riesgos operativos, este análisis demostró la importancia de realizar auditorías frecuentes para asegurar que el sistema se encuentre actualizado, protegido y funcionando correctamente.

Por otra parte, el monitoreo mediante el Visor de eventos permitió supervisar continuamente los registros de seguridad, aplicación, sistema e instalación, así como aplicar filtros para concentrarse en eventos críticos y de error, esta práctica evidenció cómo el monitoreo constante contribuye a la detección temprana de anomalías, fortaleciendo la estabilidad del sistema y reduciendo la posibilidad de incidentes de seguridad.

Asimismo, la Gestión de Las Bitácoras de Acceso permitió documentar de manera precisa las actividades relevantes del sistema, incluyendo conexiones permitidas, errores internos y procesos de actualización, el guardado y reinicio de la bitácora fortaleció el control histórico de eventos, facilitando futuras auditorías y la toma de decisiones preventivas en materia de

seguridad informática.

Finalmente, la verificación del Firewall de Windows Defender con perfiles de red activos confirmó la implementación de mecanismos de prevención para bloquear accesos no autorizados, reforzando la protección del equipo frente a posibles amenazas externas.

Además de los resultados técnicos obtenidos, la realización de este proyecto permitió desarrollar diversas habilidades fundamentales en el ámbito de la ciberseguridad, tales como el análisis de sistemas, la interpretación de registros de eventos, la aplicación de filtros de seguridad, la identificación de vulnerabilidades, la gestión de bitácoras y el uso de herramientas administrativas para auditorías técnicas. Estas competencias son ampliamente utilizadas en el entorno laboral, especialmente en áreas como soporte técnico, administración de sistemas, seguridad informática y auditoría tecnológica, donde se requiere supervisar constantemente equipos, detectar fallas, responder a incidentes y garantizar el cumplimiento de medidas de seguridad.

En la vida cotidiana, estos conocimientos también resultan de gran utilidad, ya que permiten a los usuarios proteger sus propios dispositivos, verificar que el firewall se encuentre activo, identificar errores del sistema, mantener actualizaciones seguras y monitorear actividades sospechosas en sus equipos personales, por ejemplo, una persona con estas habilidades puede detectar intentos de acceso no autorizados en su computadora, corregir fallas del sistema antes de que generen problemas mayores o asegurarse de que su red doméstica se encuentre protegida.

En conclusión, la integración de la prevención, el monitoreo, la auditoría y el uso adecuado de bitácoras constituye una estrategia integral de seguridad informática que fortalece la protección de los sistemas de cómputo, al mismo tiempo, el desarrollo de estas habilidades técnicas aporta un valor significativo tanto en el ámbito profesional como en la vida diaria,

fomentando una cultura de seguridad digital y un uso responsable de la tecnología.

Referencias:

IBM i. (s. f.-a). https://www.ibm.com/docs/en/i/7.4.0?topic=journal-planning-security-auditing

IBM i. (s. f.-b). https://www.ibm.com/docs/en/i/7.4.0?topic=journal-planning-security-auditing

IBM i. (s. f.-c). https://www.ibm.com/docs/es/i/7.6.0?topic=reference-auditing-security-i

mportancia de seguridad (prevención, monitoreo, auditoría) en ciber seguridad - Resultados de búsqueda de - Videos. (s. f.-a). https://mx.video.search.yahoo.com/yhs/search?fr=yhs-fc-2461&ei=UTF-8&hsimp=yhs-2461&hspart=fc&param1=7&param2=eJwtj8tuwjAURH%2FFS5DscO3Yxo9VAvQDqq5qeEkBqy8EAEF9esr02o2o7nnSjOX1DnrP48UgCmQDvvJWa%2B1Vg77fII9SFY67Nu%2F3GGfbs76TBsmleFKGy0CNfuOciM14%2BasRGPOsmEO%2B0ucnfXjy2H%2FDNnNP2kYwk4UgDZrmrp5XdD0QBQKsGhNk%2BQWvSTfonC7DXGNTZ8eO1Hui1KiTX99jANGQ%2BojusS2n7eovd7nMe4o5wVkoSWcwz39v%2BS6y3tjLrDE%2B9srAFnVJyDVQWtC6QeQStaMCHrUFT8caF2dMt9mmAEThAKh%2BgtKQ5kRrJCl%2Bv4FSiZZiA%3D%3D&p=mportancia+de+seguridad+%28prevenci%C3%B3n%2C+monitoreo%2C+auditor%C3%ADa%29+en+ciber+seguridad&type=fc_AC934C13286_s58_g_e_d070623_n9998_c999#id=6&vid=57fcde893c6a6b2765fc007e4206e36f&action=click

mportancia de seguridad (prevención, monitoreo, auditoría) en ciber seguridad - Resultados de búsqueda de - Videos. (s. f.-b). https://mx.video.search.yahoo.com/yhs/search?fr=yhs-fc-2461&ei=UTF-8&hsimp=yhs-

2461&hspart=fc&param1=7&param2=eJwtj8tuwjAURH%2FFS5DscO3Yxo9VAvQDqq5qeeEk
Bqy8EAEF9esr02o2o7nnSjOX1DnrP48UgCmQDvvJWa%2B1Vg77fII9SFY67Nu%2F3GGfbs7
6TBsmleFKGy0CNfuOciM14%2BasRGPOsmEO%2B0ucnfXjy2H%2FDNnNP2kYwk4UgDZr
mrp5XdD0QBQKsGhNk%2BQWvSTfonC7DXGNTZ8eO1Hui1KiTX99jANGQ%2BojusS2n7e
ovd7nMe4o5wVkoSWcwz39v%2BS6y3tjLrDE%2B9srAFnVJyDVQWtC6QeQStaMCHrUFT8
caF2dMt9mmAEThAKh%2BgtKQ5kRrJCl%2Bv4FSiZZiA%3D%3D&p=mportancia+de+segur
idad+%28prevenci%C3%B3n%2C+monitoreo%2C+auditor%C3%ADa%29+en+ciber+segurida
d&type=fc_AC934C13286_s58_g_e_d070623_n9998_c999#id=1&vid=469e1686f7c8fbab9185
349df80af0ac&action=view

mportancia de seguridad (prevención, monitoreo, auditoría) en ciber seguridad - Resultados de búsqueda de - Videos. (s. f.-c). https://mx.video.search.yahoo.com/yhs/search?fr=yhs-fc-2461&ei=UTF-8&hsimp=yhs-2461&hspart=fc&param1=7&param2=eJwtj8tuwjAURH%2FFS5DscO3Yxo9VAvQDqq5qeeEkBqy8EAEF9esr02o2o7nnSjOX1DnrP48UgCmQDvvJWa%2B1Vg77fII9SFY67Nu%2F3GGfbs76TBsmleFKGy0CNfuOciM14%2BasRGPOsmEO%2B0ucnfXjy2H%2FDNnNP2kYwk4UgDZrmrp5XdD0QBQKsGhNk%2BQWvSTfonC7DXGNTZ8eO1Hui1KiTX99jANGQ%2BojusS2n7eovd7nMe4o5wVkoSWcwz39v%2BS6y3tjLrDE%2B9srAFnVJyDVQWtC6QeQStaMCHrUFT8caF2dMt9mmAEThAKh%2BgtKQ5kRrJCl%2Bv4FSiZZiA%3D%3D&p=mportancia+de+seguridad+%28prevenci%C3%B3n%2C+monitoreo%2C+auditor%C3%ADa%29+en+ciber+seguridad&type=fc_AC934C13286_s58_g_e_d070623_n9998_c999#id=26&vid=6a665ade731ef34f9fb432078a2db4a6&action=view

mportancia de seguridad (prevención, monitoreo, auditoría) en ciber seguridad - Resultados de búsqueda de - Videos. (s. f.-d).

https://mx.video.search.yahoo.com/yhs/search?fr=yhs-fc-2461&ei=UTF-8&hsimp=yhs-2461&hspart=fc&param1=7&param2=eJwtj8tuwjAURH%2FFS5DscO3Yxo9VAvQDqq5qeEkBqy8EAEF9esr02o2o7nnSjOX1DnrP48UgCmQDvvJWa%2B1Vg77fII9SFY67Nu%2F3GGfbs76TBsmleFKGy0CNfuOciM14%2BasRGPOsmEO%2B0ucnfXjy2H%2FDNnNP2kYwk4UgDZrmrp5XdD0QBQKsGhNk%2BQWvSTfonC7DXGNTZ8eO1Hui1KiTX99jANGQ%2BojusS2n7eovd7nMe4o5wVkoSWcwz39v%2BS6y3tjLrDE%2B9srAFnVJyDVQWtC6QeQStaMCHrUFT8caF2dMt9mmAEThAKh%2BgtKQ5kRrJCl%2Bv4FSiZZiA%3D%3D&p=mportancia+de+seguridad+%28prevenci%C3%B3n%2C+monitoreo%2C+auditor%C3%ADa%29+en+ciber+seguridad&type=fc_AC934C13286_s58_g_e_d070623_n9998_c999#action=view&id=35&vid=dc33581c3b18a3c37f24f085403dd386

¿Necesitas más información? Utiliza tu registro de log. (s. f.). Empresas | INCIBE. https://www.incibe.es/empresas/blog/necesitas-mas-informacion-utiliza-tu-registro-log

Otero, E. (2024, 15 agosto). *Panel de control en Windows 11: qué es, cómo acceder y qué opciones tiene*. Profesional Review. https://www.profesionalreview.com/2024/08/15/panel-de-control-windows-11/

Sec, T. (2025, 17 junio). *Auditoría de Ciberseguridad: Qué es, Por Qué es Vital y Cómo Protege a tu Empresa*. Trinity Sec | Consultoría de Ciberseguridad. https://trinitysec.mx/auditoria-de-ciberseguridad/

Seguridad Cultura de prevencion TI -Herramientas de deteccion (1.a ed.). (s. f.). https://revista.seguridad.unam.mx/sites/default/files/revistas/pdf/23_RevistaSeguridad-HerramientasDeDeteccion.pdf

Susana, C. E. (2025, 1 octubre). *Guía Completa sobre la Bitácora de Auditoría: Importancia y Mejores Prácticas | Actualizado febrero 2026*. CARMELITA.

https://carmelita.com.mx/ingenieria/bitacora-de-auditoria/