Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad |3| Auditoria y Bitácora.

Seguridad informática II.

Ingeniería en Desarrollo de Sofwtare.

academia global

TUTOR: Jessica Hernández

ALUMNO: Carlos Ariel Nicolini

FECHA: 6/06/2025

Índice

Introducción

Uno de los asuntos que más preocupa a las empresas hoy en día es la ciberseguridad. La gran dependencia de los negocios de la tecnología, las redes y las comunicaciones han puesto como prioridad la seguridad para poder garantizar la continuidad del negocio.

La auditoría de seguridad informática es la herramienta principal para poder conocer el estado de seguridad en que se encuentra una empresa en relación con sus sistemas informáticos, de comunicación y acceso a internet. Estas auditorias permiten mejorar los sistemas e incrementar la ciberseguridad. Siendo fundamentales para poder garantizar el funcionamiento del negocio y proteger la integridad de la información que manejan.

Una auditoria de seguridad informática es un procedimiento que evalúa el nivel de seguridad de una empresa o entidad, analizando sus procesos y comprobando si sus políticas de seguridad se cumplen.

El principal objetivo de una auditoria de seguridad es el de detectar las vulnerabilidades y debilidades de seguridad que pueden ser utilizadas por terceros malintencionados para robar información, impedir el funcionamiento de sistemas, o en general, causar daños a la empresa.

Dependiendo de quien realice la auditoria se denominan internas, cuando son realizadas por personal de la propia empresa (aunque pueden tener apoyo o asesoramiento externo) o externas, cuando se realizan por empresas externas que son independientes de la empresa.

Descripción

Contextualización:

A continuación, se procederá a realizar una auditoria 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 auditorias 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 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 auditoria 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:

Auditoria y bitácora:

- Realizar una auditoria 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.

Justificación

En esta actividad final de la materia de seguridad informática 2, realizaremos una auditoría y una bitácora en el equipo que hemos estado trabajando en los dos trabajos anteriores.

Con esto aprenderemos no solo la finalidad de dichos procesos, sino como realizarlos. A través de la explicación en la clase de la profesora, la cual no me fue posible asistir (pido disculpas), pero en el video se explica de manera muy completa todo el proceso de manera muy completa.

Es muy importante entender que para la seguridad informática es necesario contar con las herramientas y los conocimientos, pero, además, se debe tener especial atención a las alertas y demás alarmas que nos pueden surgir y saber cómo atenderlas.

En este trabajo realizaremos la auditoria con las herramientas del sistema operativo, revisaremos logs en busca de posibles intentos de intrusión, además de revisar las configuraciones básicas del equipo que estén configuradas de manera correcta y como indican las mejoras prácticas, ya sea antivirus activo y actualizado, firewall habilitado y con sus reglas configuradas, sistema operativo actualizado con sus parches de seguridad, aplicaciones actualizadas a la versión más estable y segura o con sus parches de seguridad.

El tema de la seguridad y las buenas prácticas es algo que nunca se termina, siempre hay que tener los sistemas actualizados mes con mes, los programas o sistemas escanearlos en busca de vulnerabilidades y remediarlas antes de que sean explotadas.

Este trabajo fue subido al siguiente enlace de GitHub

https://github.com/CarlosNico/ServiciosenlaNube

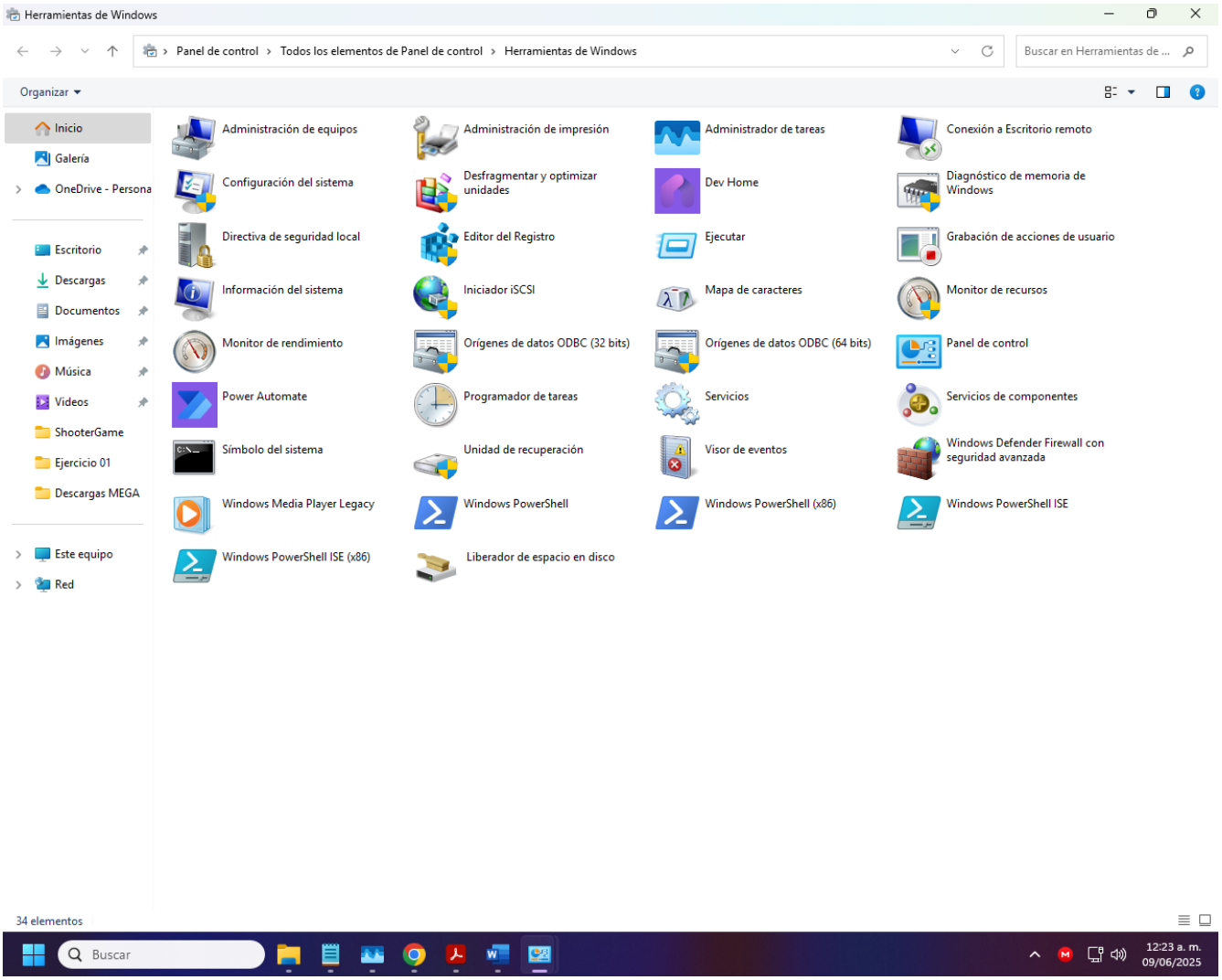
Desarrollo

Auditoria y Bitácora

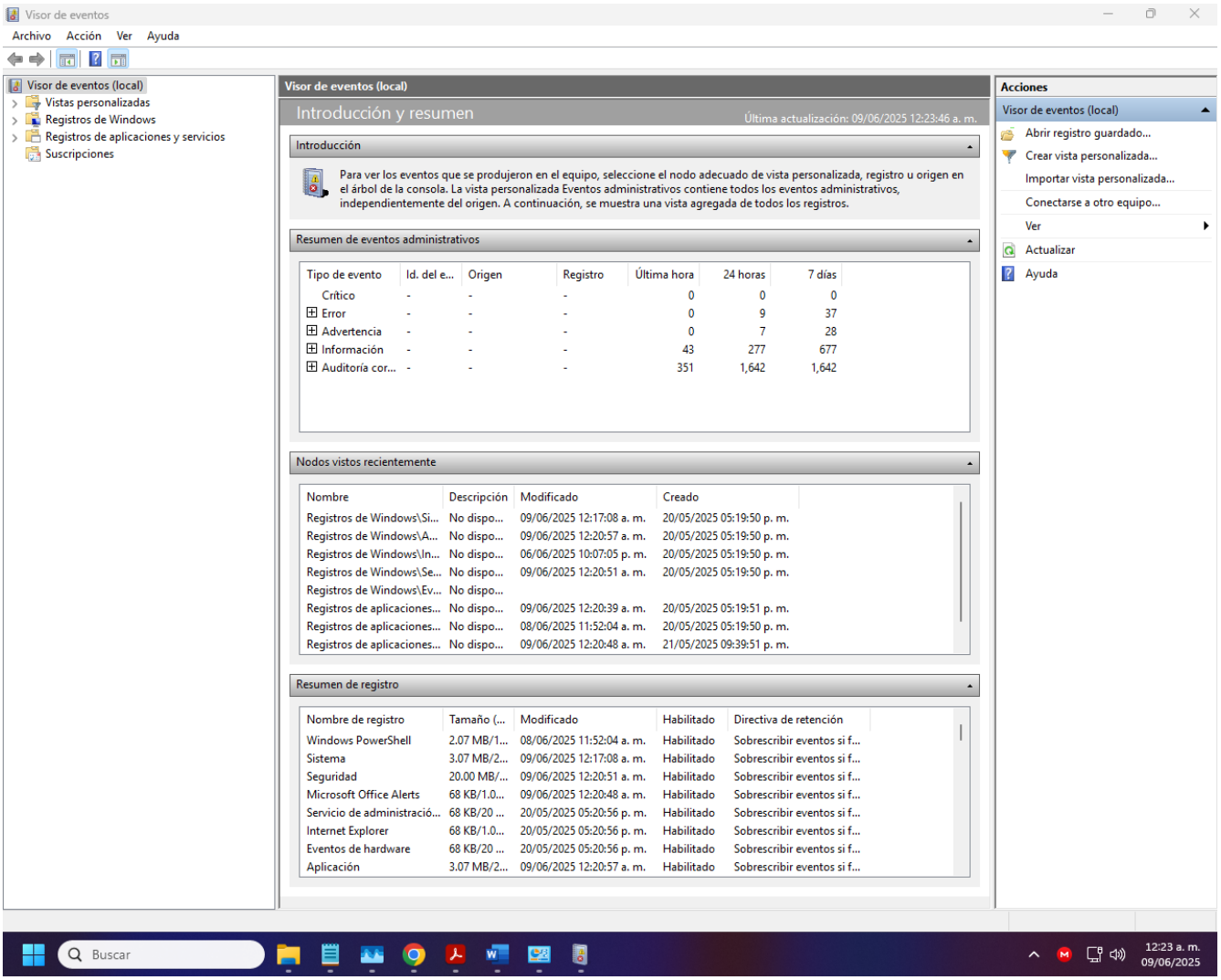
Auditoria de equipo

En esta parte del ejercicio realizaremos una auditoria sobre los logs de Windows del equipo que estamos utilizando en los anteriores ejercicios para este fin.

Para tal fin, nos dirigiremos al panel de control y seleccionaremos la opción Herramientas de Windows (en Windows 11 se llama así).

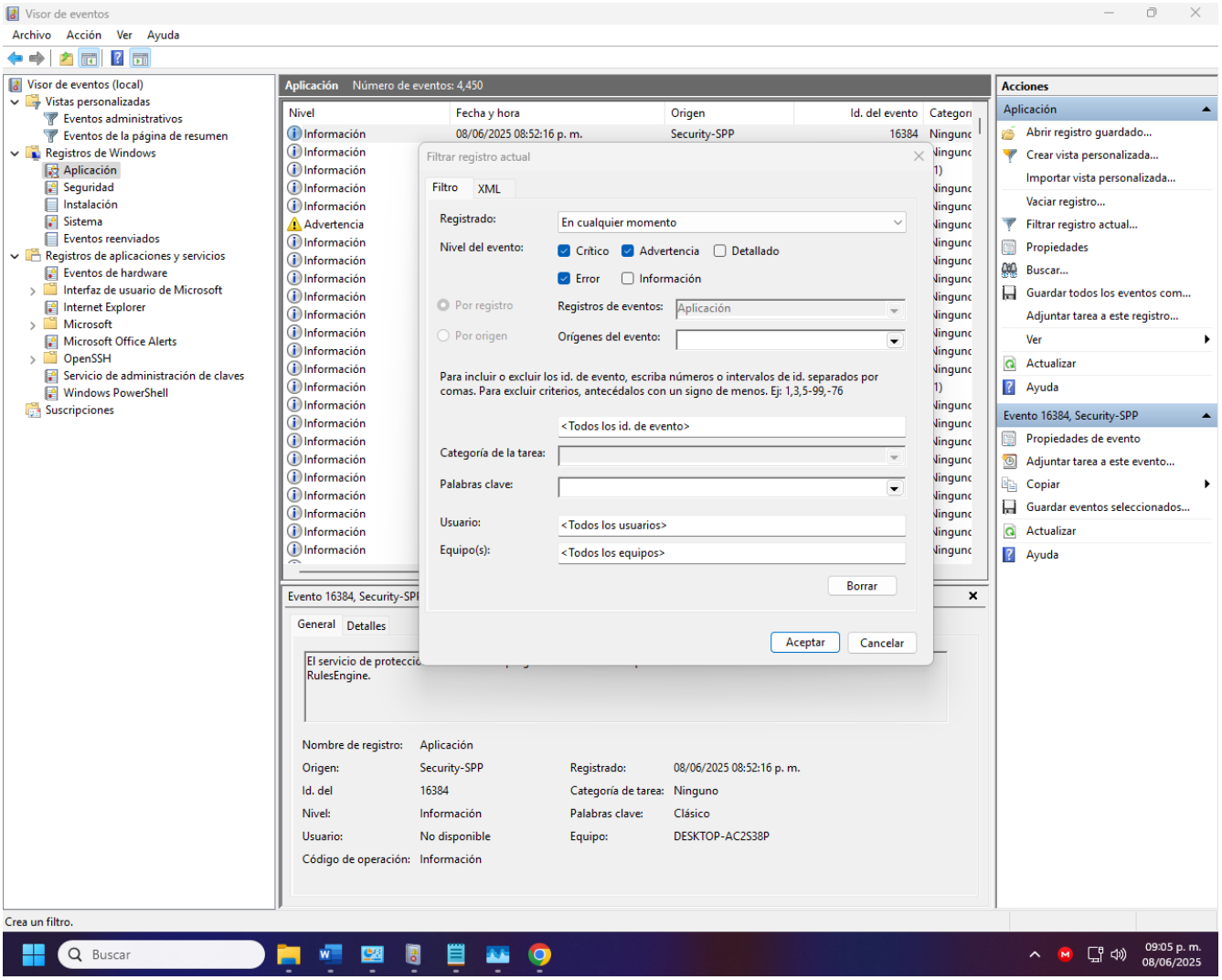


En esta sección elegiremos el visor de eventos de Windows, donde vemos que no contamos con eventos críticos, pero si hay unos errores y advertencias.



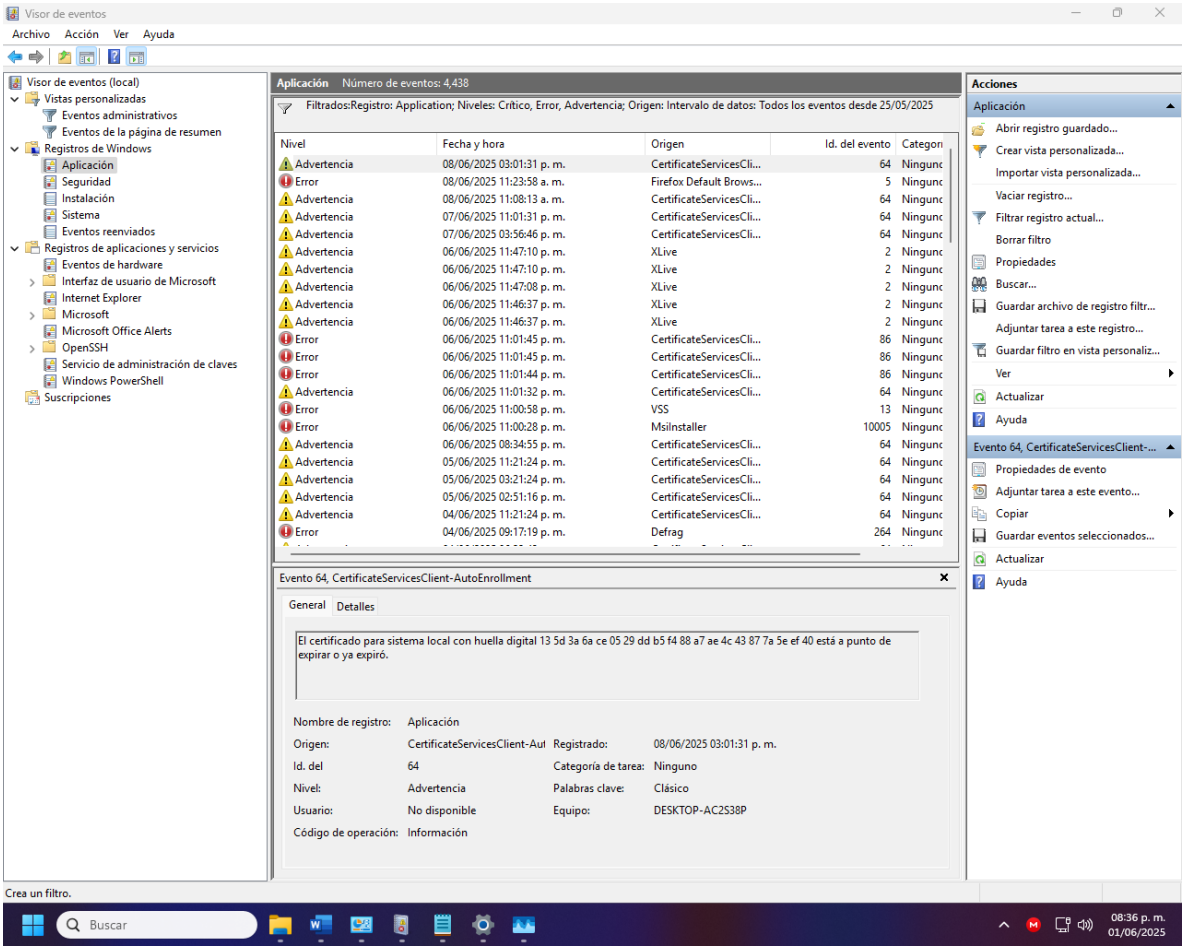
Bitácora

En esta parte del ejercicio realizaremos una bitácora sobre los logs de Windows del equipo que estamos utilizando en los anteriores ejercicios para este fin. Se realizo una revisión de logs en el intervalo desde el día 25-05-2025 hasta el día 01-06-2025. Para tal acción realizamos un filtrado de logs eligiendo las opciones de crítico, advertencia y error como se muestra en la imagen siguiente.



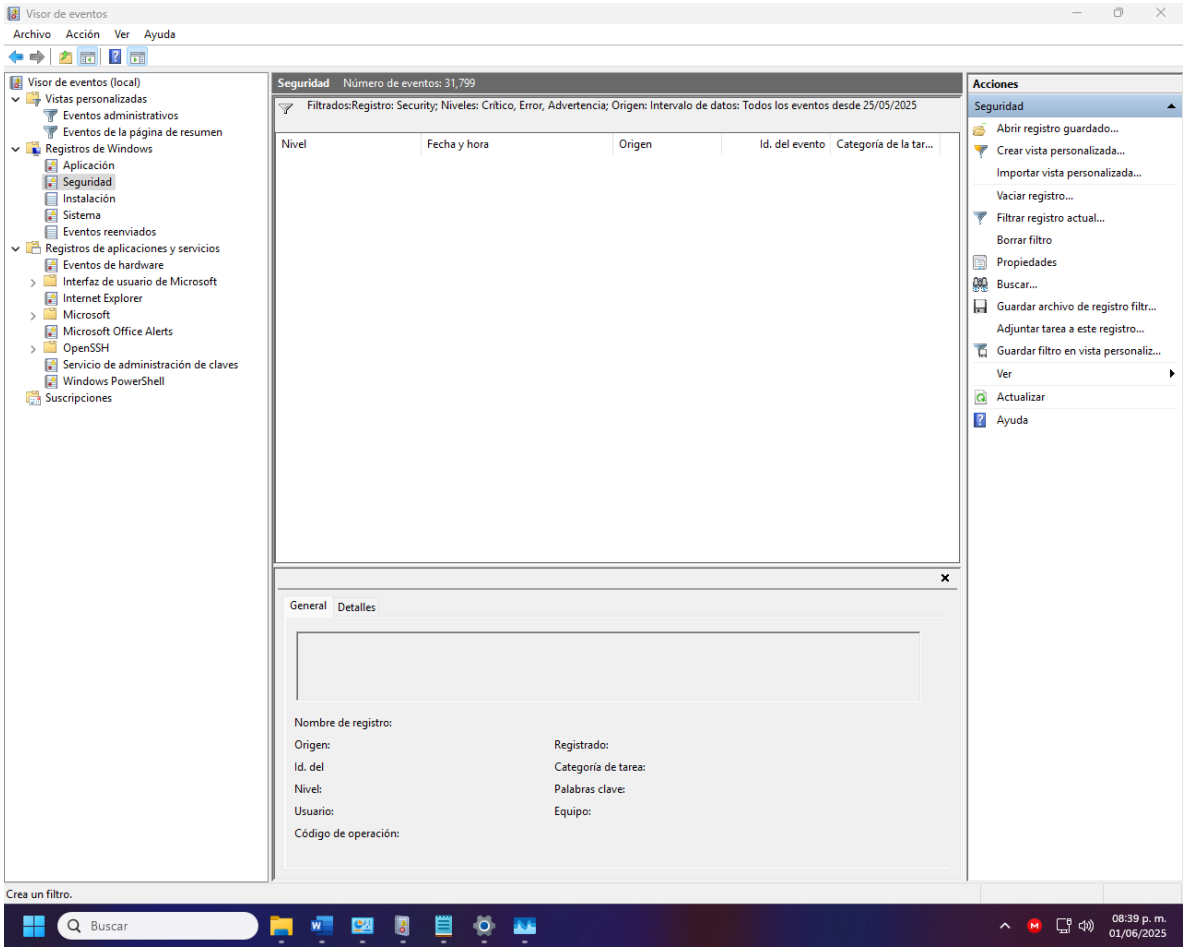
En la revisión encontramos lo siguiente en cada categoría como explicaremos a continuación:

- Logs de aplicación: Se encontraron los siguientes logs.

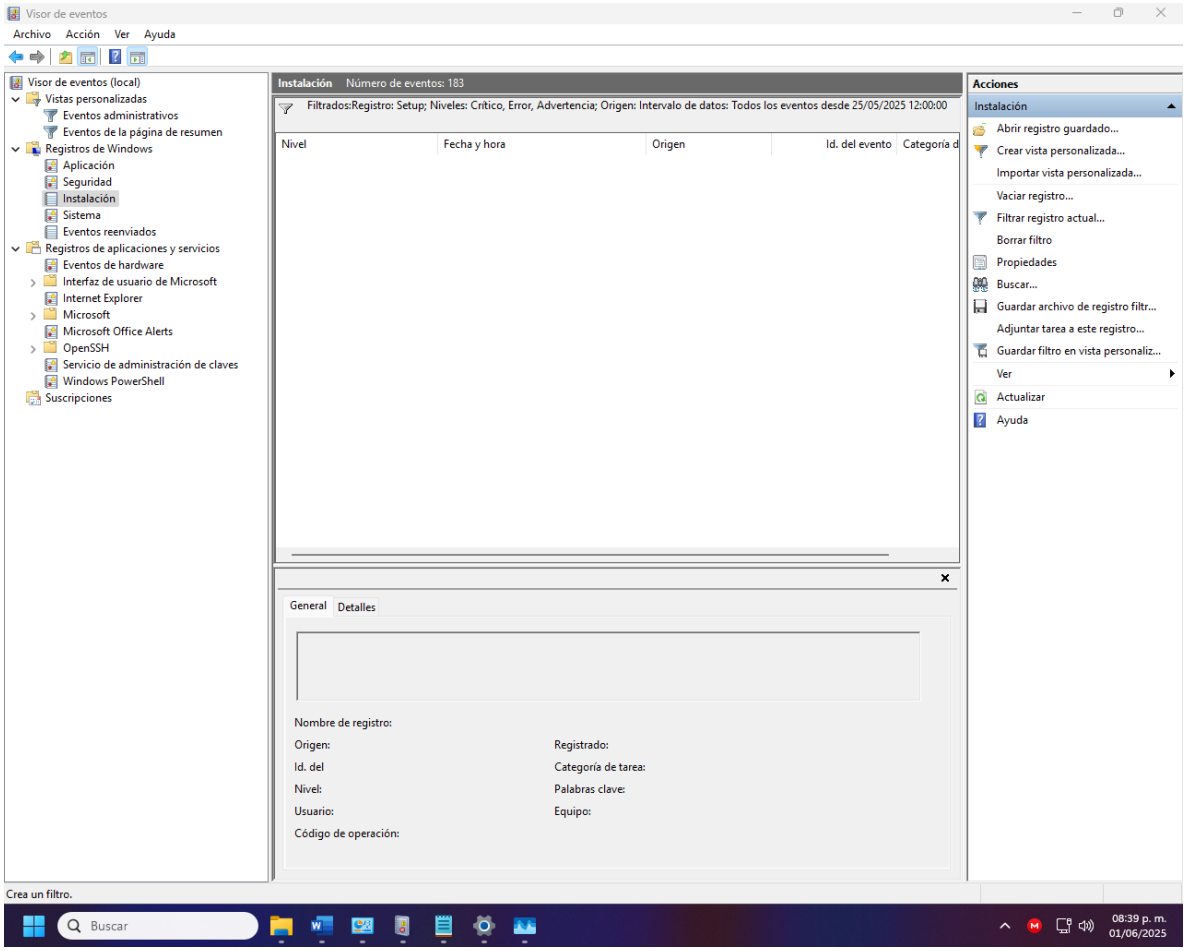


- Advertencia: El certificado con Huella digital 13 5d 3a 6a ce 05 29 dd b5 f4 88 a7 ae 4c 43 87 7a 5e ef 40 está a punto de expirar o expiro.
- Advertencia: El servicio de XLive (Windows live) no pudo logearse de manera correcta.
- Error: Error en inicialización de la inscripción de certificado de SCEP.
- Error: No puede iniciarse el servicio de CEventSystem.
- Error: Product Gear of war no pudo crear archivo en carpeta installer.
- Error: El optimizador de almacenamiento no pudo completar la defragmentacion de disco.
- Error: Error al llamar la rutina CoCreatelInstance del servicio de instantáneas de volumen.

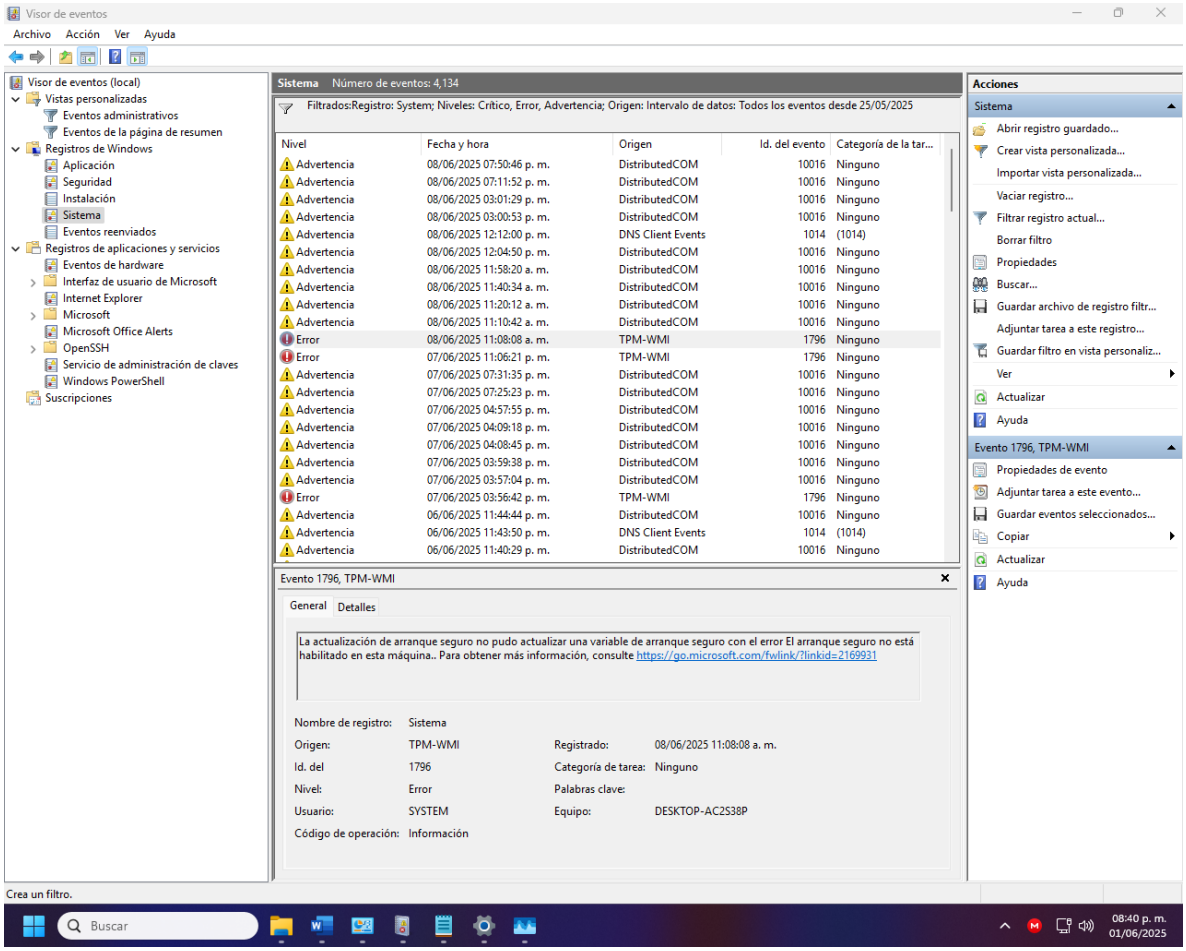
- Logs seguridad: No se encontraron detalles.



- Logs instalación: No se encontraron detalles.



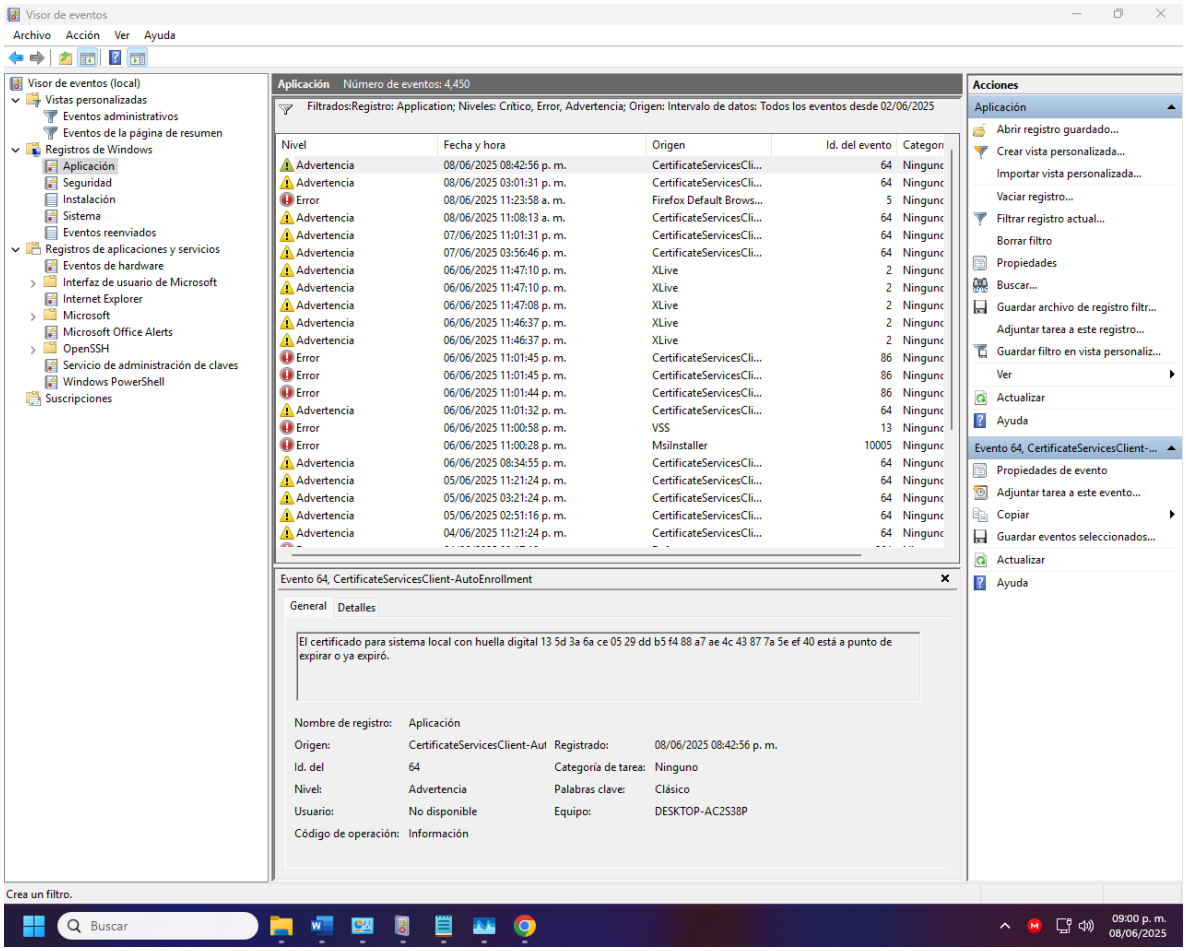
- Logs sistemas:



- Advertencia: APPID con identificar especifico no tiene permisos suficientes para una activación local.
- Advertencia: Se agoto el tiempo para la resolución de nombres t-ring-fdv2.msedge.net.
- Error: Actualización de arranque seguro no puede actualizar una variable. El arranque seguro no está habilitado en esta máquina.

Se realizo un nuevo seguimiento a la auditoría realizada, pero esta vez se utilizo el rango de fecha desde el día 02-06-2025 hasta el día 08-06-2025 con los siguientes resultados.

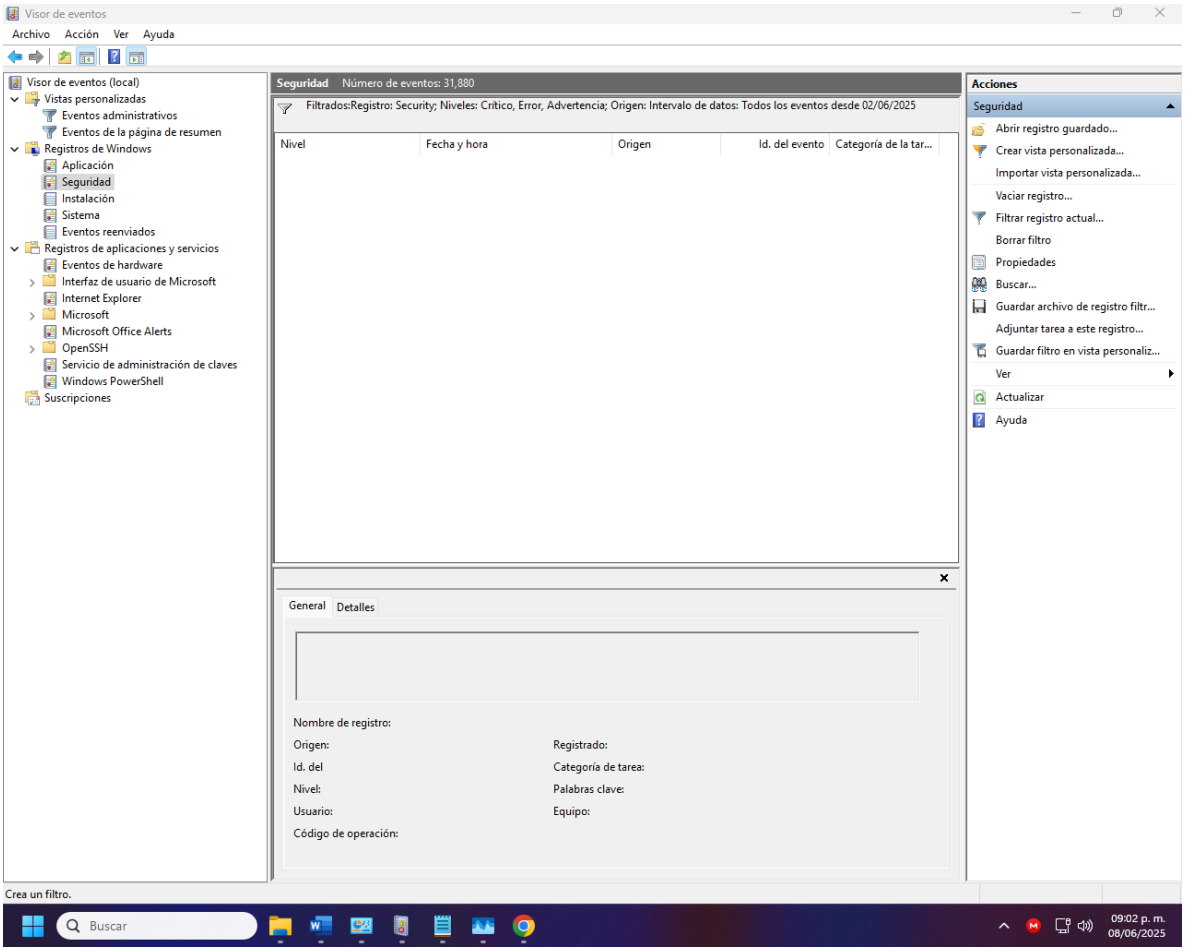
- Logs de aplicación:



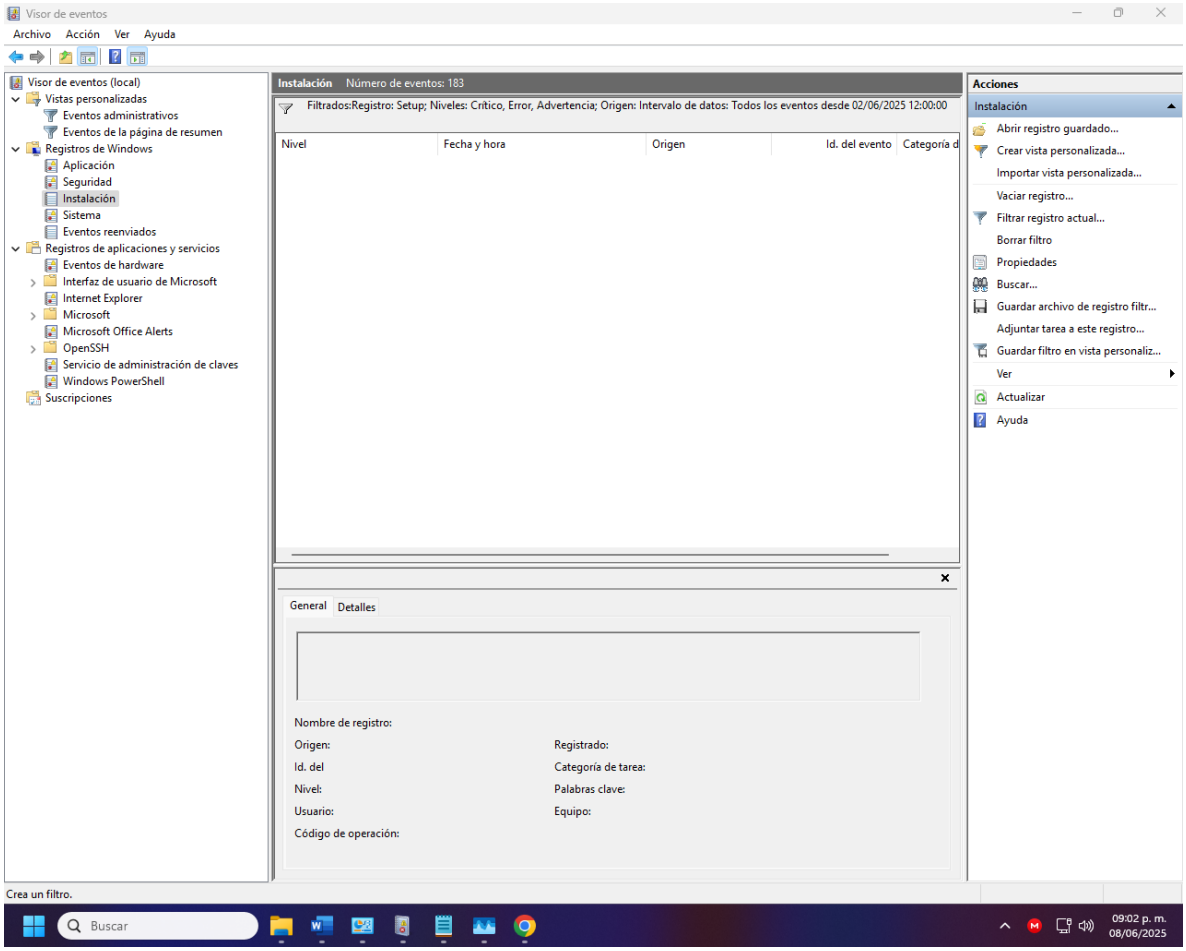
- Advertencia: El certificado con Huella digital 13 5d 3a 6a ce 05 29 dd b5 f4 88 a7 ae 4c 43 87 7a 5e ef 40 está a punto de expirar o expiro.
- Advertencia: El servicio de XLive (Windows live) no pudo logearse de manera correcta.
- Error: Error en inicialización de la inscripción de certificado de SCEP.
- Error: No puede iniciarse el servicio de CEventSystem.
- Error: Product Gear of war no pudo crear archivo en carpeta installer.

- Error: El optimizador de almacenamiento no pudo completar la defragmentacion de disco.
- Error: Acceso denegado Firefox default browser Agent.
- Error: Error al llamar la rutina CoCreatelInstance del servicio de instantáneas de volumen.

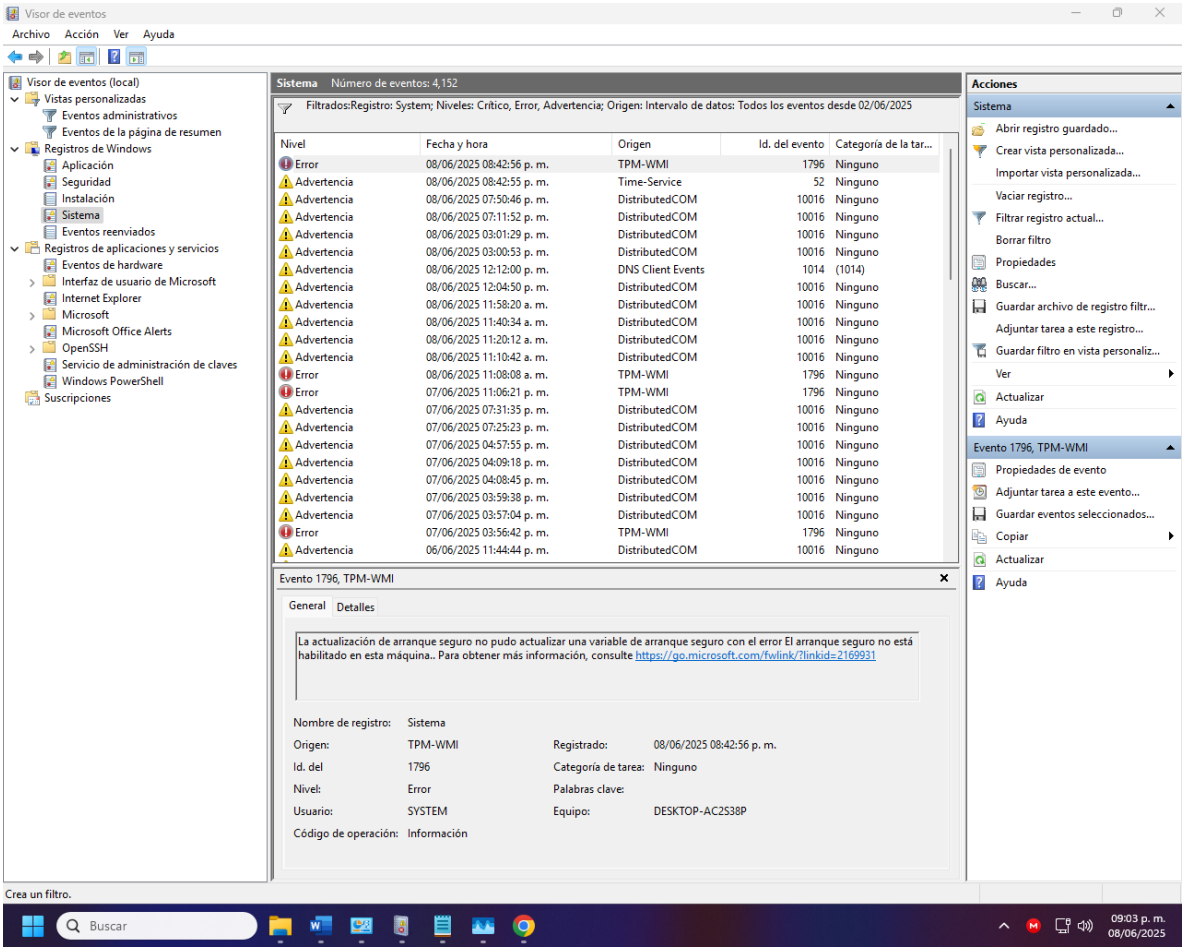
- Logs de seguridad: No se encontraron detalles.



- Logs de instalación: No se encontraron detalles.



- Logs de sistema:



- Advertencia: APPID con identificar especifico no tiene permisos suficientes para una activación local.
- Advertencia: Se agoto el tiempo para la resolución de nombres t-ring-fdv2.msedge.net.
- Error: Actualización de arranque seguro no puede actualizar una variable. El arranque seguro no está habilitado en esta máquina.

Sobre los errores y advertencias encontradas los importantes, se revisó el tema y no se encontró por el momento una solución especifica, por tal motivo la recomendación es crear un folio a Microsoft para la recolecta de esos logs y nos apoyen a remediar esos detalles.

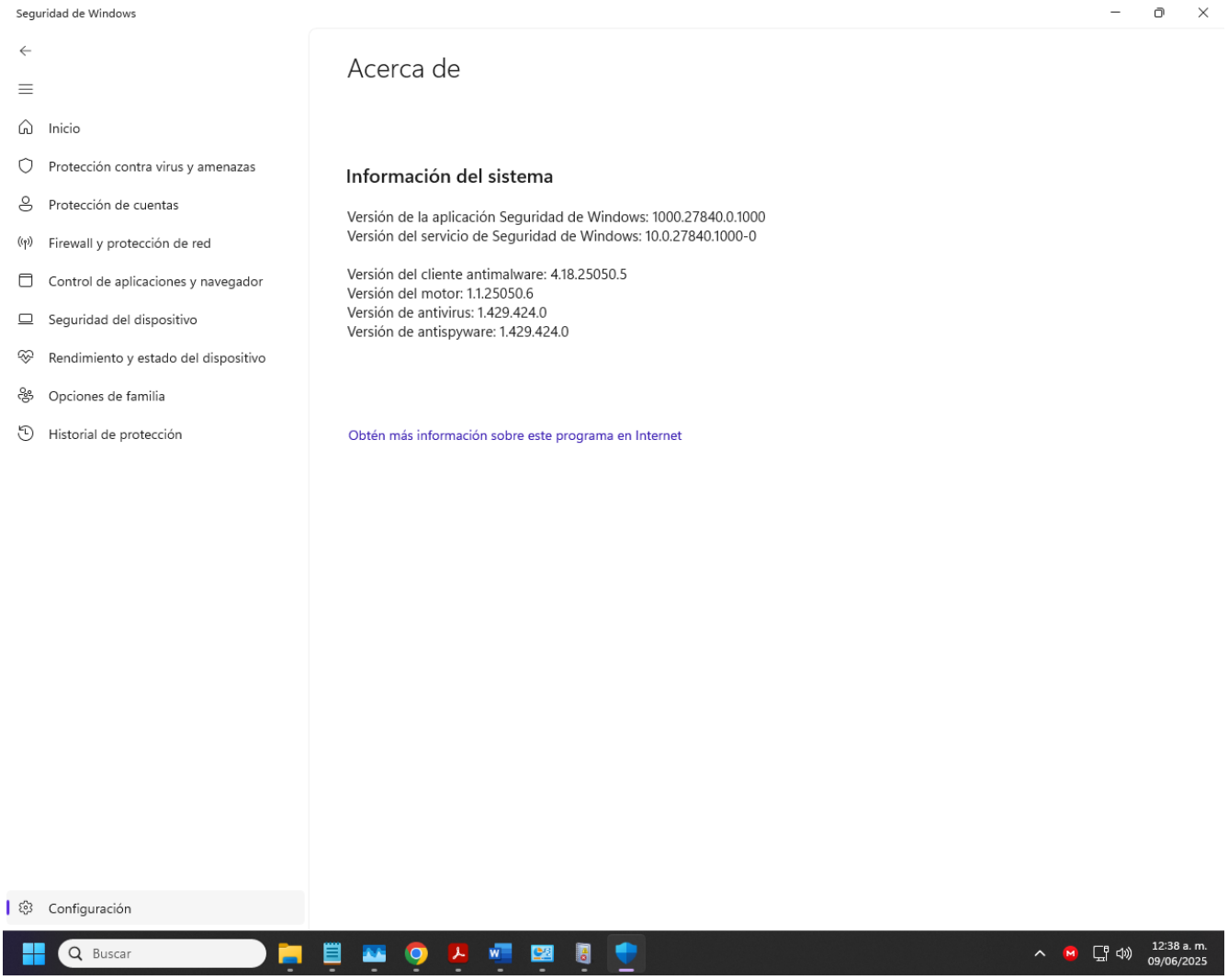
Sobre instalaciones incompletas como en el caso de software gear of war, se necesita terminar la instalación o en caso contrario su eliminación.

En el caso del XLive, es un servicio deprecado de Microsoft, el cual se está intentando hacer funcionar, caso contrario se desinstalará.

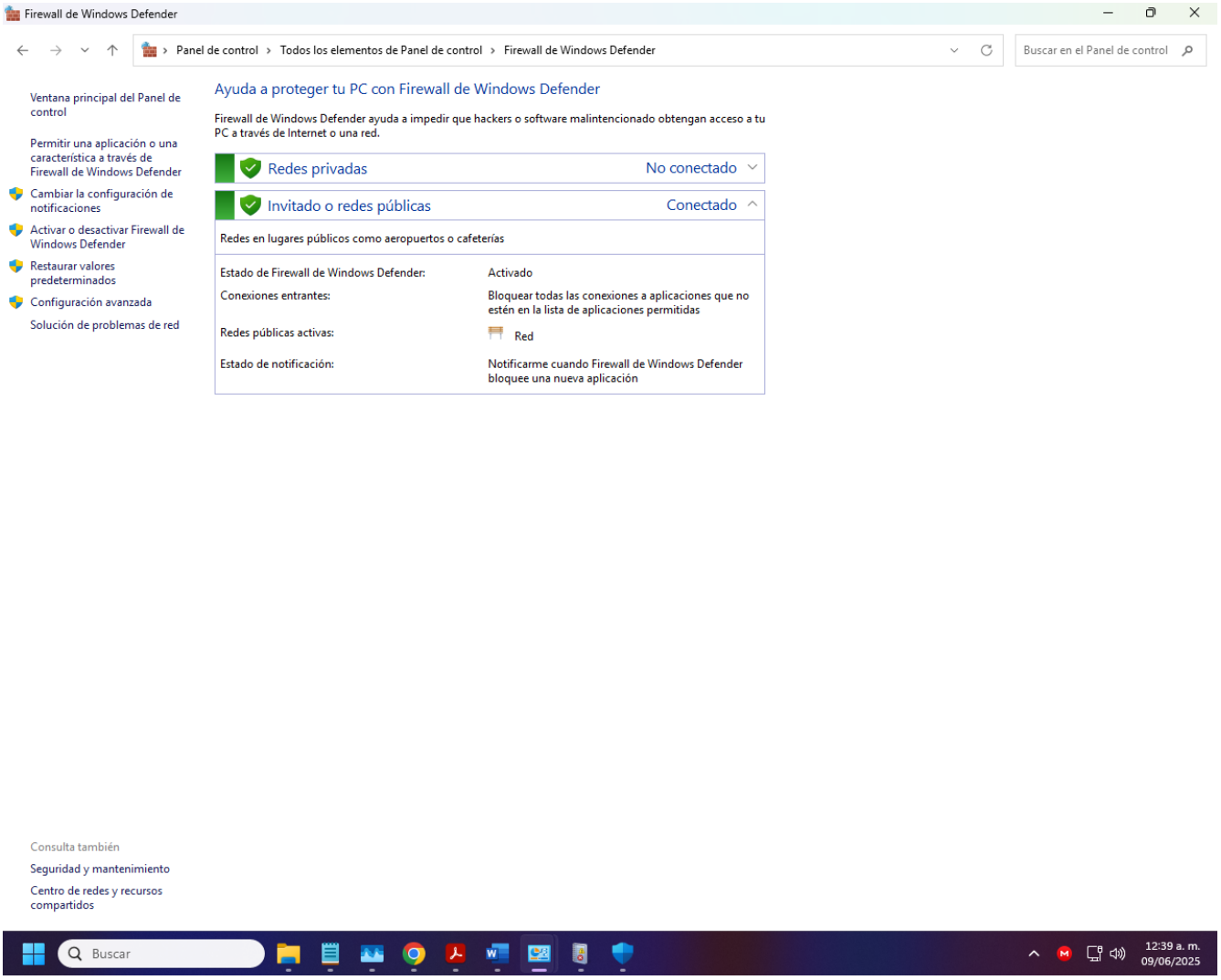
Importancia de seguridad (prevención, monitoreo, auditoria)

La seguridad es fundamental para proteger los sistemas, datos y operaciones de la organización. Para lo cual es necesario cumplir con ciertos factores y herramientas. Para evitar que ocurran incidentes de seguridad es muy importante la utilización de antivirus, firewall y sistemas de prevención de intrusos, tener las configuraciones seguras del sistema y los servicios.Ademas de tener políticas de contraseñas robustas y actualización y parcheo regular de software entre otras.

Windows defender activado y actualizado.



Firewall de Windows habilitado y con sus reglas activadas



El monitoreo es una pieza esencial en la seguridad, ya que su objetivo es detectar amenazas o actividades anómalas en tiempo real antes de que se materialicen en una afectación. Lo cual nos va a permitir tener respuestas rápidas ante incidentes y minimizar el impacto en la operación, identificar comportamientos inusuales que pueden significar ataques internos o externos y nos va a facilitar la continuidad operativa al detectar fallos o errores antes de que se escalen.

Para monitoreo se pueden utilizar sistemas de detección de intrusos, el SIEM y tener una monitorización de trafico de red, usuarios y accesos.

Las auditorias sirven para evaluar la eficacia de las medidas de seguridad que se implementaron, su importancia radica en detectar vulnerabilidades o incumplimiento de políticas, nos proporciona evidencia para procesos regulatorios o legales y nos ayuda a identificar áreas de mejoras.

Se pueden realizar mediante la revisión de logs y eventos de seguridad, revisión de accesos, roles y políticas de uso, pruebas de penetración y análisis de vulnerabilidades entre otras.

Cabe mencionar que las 3 practicas son muy importantes y se complementan entre ellas, para una buena salud de seguridad informática es necesario que las 3 estén implementadas.

Conclusión

Como hemos visto en esta materia, la seguridad cibernética es algo muy importante para una empresa si quiere tener seguro su información e infraestructura. Las auditorias de seguridad informática son una herramienta muy importante en este aspecto, ya que nos permitirá evaluar las políticas de seguridad implementadas y el estado de su implementación, con ellas podremos detectar vulnerabilidades o puntos débiles en los sistemas, ya sea contraseñas inseguras o con una configuración no recomendable, vulnerabilidades en códigos fuente de sistemas o malas prácticas, configuraciones inseguras en la infraestructura de la red. Además, también pueden servir para simular ataques reales y encontrar vulnerabilidades antes que los ciberdelincuentes.

Me han tocado casos donde se realizaron auditorias externas simulando ataques para ver la seguridad de la infraestructura completa, detalle que debe ser comunicado a tosas las áreas necesarias, pero en ese caso no fue así, por tal motivo se activaron alarmas de seguridad en los distintos departamentos y se realizó una revisión de un posible ataque, se llego al equipo en cuestión, con el usuario que había realizado dicho ataque y resulto que era una auditora programada por un área en específico. pero no comunicada de manera correcta, que, si el equipo de seguridad respondió bien a la alarma, se tardo en encontrar al personal responsable para una respuesta rápida.

Este trabajo fue subido al siguiente enlace de GitHub

https://github.com/CarlosNico/ServiciosenlaNube

Referencias

Auditoría de ciberseguridad: qué es, para qué sirve y cómo formarte en este campo. (n.d.). Incibe.es. Retrieved June 9, 2025, from https://www.incibe.es/index.php/ed2026/talento-hacker/blog/auditoria-de-ciberseguridad-que-es-para-que-sirve-y-como-formarte-en-este-campo

¿Qué es una auditoría de seguridad informática? Tipos y Fases. (n.d.). Ambit-iberia.com. Retrieved June 9, 2025, from https://www.ambit-iberia.com/blog/qu%C3%A9-es-una-auditor%C3%ADa-de-seguridad-inform%C3%A1tica-tipos-y-fases