Actividad 3 – Auditoría y Bitácora

Seguridad Informática II

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: Carlos Alberto Fuentes Mendoza

Fecha: 25-mayo-2023

Índice

Introducción

Un error durante el desarrollo de una aplicación puede causar graves consecuencias a las empresas que la utilizan, como por ejemplo, pérdida o robo de información, daños a la imagen corporativa o sanciones económicas. Por ello, es fundamental desarrollar y utilizar software lo más seguro posible. Debido a que los riesgos de ciberseguridad aumentan y evolucionan de una manera imparable, convirtiendo en imprescindibles los ciclos de vida de desarrollo de software y las metodologías que otorgan un papel protagonista a la seguridad de las aplicaciones.

¿Qué es el desarrollo seguro de software?

El desarrollo seguro de software es una metodología cuyo objetivo es considerar la seguridad de las aplicaciones durante todo su ciclo de vida, empezando desde la propia definición de requisitos de las mismas. El propósito de esta filosofía es determinar cuanto antes las necesidades de seguridad y las posibles vulnerabilidades que puede tener la aplicación, sin esperar a fases o iteraciones posteriores. Tradicionalmente era habitual que el desarrollo de aplicaciones estuviera enfocado principalmente a cumplir con las funcionalidades exigidas por el cliente. Otras cuestiones, como la seguridad, se tenían en cuenta de una manera más liviana al final del proyecto. Este enfoque provocaba que, al igual que con cualquier tipo de fallo, si se encontraba una vulnerabilidad durante la fase de pruebas o tras entregar la aplicación al cliente, el coste de solucionarla podía ser enorme. En otras palabras, podríamos decir que el desarrollo seguro de software es un modelo de trabajo que se basa en la realización de chequeos de seguridad continuos del proyecto en construcción, incluso desde sus fases iniciales y antes de que se escriba una sola línea de código. Estas pruebas se centran en descubrir y corregir cualquier error en una etapa temprana, y comprenden tests de autentificación, autorización, confidencialidad, no repudio, integridad, estabilidad, disponibilidad o resiliencia.

El Desarrollo de Software consta de varios pasos que deben seguirse y cumplirse para crear programas de computación que sean eficientes, seguros y útiles para los usuarios. Esto implica planificar, realizar y gestionar eficientemente un proyecto para ejecutarlo con éxito y lograr que cumpla con el objetivo para el cual fue diseñado.

Planificación

Esta primera etapa es esencial porque en ella se determina el ámbito del proyecto, el análisis de los riesgos, el estudio de viabilidad, la duración, la estimación del costo y la asignación de recursos a cada fase. Una planificación bien realizada, permite establecer las bases para un desarrollo orientado al éxito.

Análisis

A través de esta fase se descubre todo lo que se espera del software. Por ello, se realiza una exhaustiva investigación para llegar a una comprensión precisa de los requerimientos o características que debe poseer el programa. De este modo, se elige o crea la arquitectura o estructura en donde operará.

Diseño

Se exploran las posibles alternativas, algo que requiere de mucha atención. Se consideran todos los aspectos de la implementación tecnológica, como el hardware, el lenguaje y la red. Todo esto sirve para presentar algunos modelos de proceso, guiones gráficos, prototipos e, incluso, una simulación del diseño.

Programación

Es la etapa medular del desarrollo, ya que implica crear el código con el lenguaje de programación indicado para producir el software. Para ello, se deben identificar correctamente las variables y su alcance, crear algoritmos y estructuras de datos adecuadas, garantizar una lógica de aplicación sencilla y documentar el código.

Pruebas

Esta fase es crucial porque, antes de llegar al usuario, hay que comprobar que el programa ejecute las tareas especificadas. Además, sirve para detectar fallas y analizar el rendimiento del software. Aunque el desarrollador hace sus propias pruebas, se recomienda que también sean realizadas por alguien más.

Implementación

Se trata de habilitar el software para que el usuario lo utilice y así resolver cualquier problema o duda que se le presente. Previamente, se debe planificar el entorno considerando las dependencias entre los diferentes elementos que conforman el programa. Para ello, se analiza que no existan problemas de compatibilidad.

Mantenimiento

Aunque se crea que al poner en práctica el software se acaba el trabajo, esto no es así. Y es que es esencial mantener, optimizar y mejorar el programa para eliminar los errores detectados, adaptar nuevas necesidades o añadir nuevas funcionalidades. Esto significa que se requiere hacer actualizaciones frecuentes.

Documentación

Se debe dejar registro documentado de todo el proceso y cada una de las etapas del proyecto, considerando las modelaciones, los diagramas, las pruebas, el objetivo de las eventuales correcciones, la usabilidad y las posibles adecuaciones al sistema. También, deben realizarse el manual de usuario y el manual técnico.

Descripción

Dando continuidad a las actividades anteriores, en este proyecto final vamos a realizar una auditoria desde el equipo de cómputo o utilizando una herramienta especializada que nos permita identificar las licencias de los recursos instalados y obtener información precisa de los recursos del equipo de cómputo.

Recordando que las auditorias y bitácoras proporcionan un escenario de 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.

Por tal motivo, como ya lo mencionamos, vamos a realizar una auditoría de nuestro equipo utilizando las herramientas administrativas que se encuentran en el panel de control, en donde validaremos las licencias de sus recursos por cuestiones de los aspectos legales y regulatorios, del sistema, hardware, software, licencias y red. Adicional a esto, se tendrá que revisar y guardar la bitácora que son los registros de seguridad, para posteriormente eliminar dichos registros e iniciar una auditoria limpia.

Justificación

La importancia del desarrollo seguro del software al realizar aplicaciones, nos permite proteger no solo la información del usuario final, además cuidamos la reputación de la empresa prestadora del servicio. Con lo anterior, podremos evitar implicaciones legales, judiciales y los impactos financieros que esto conlleva.

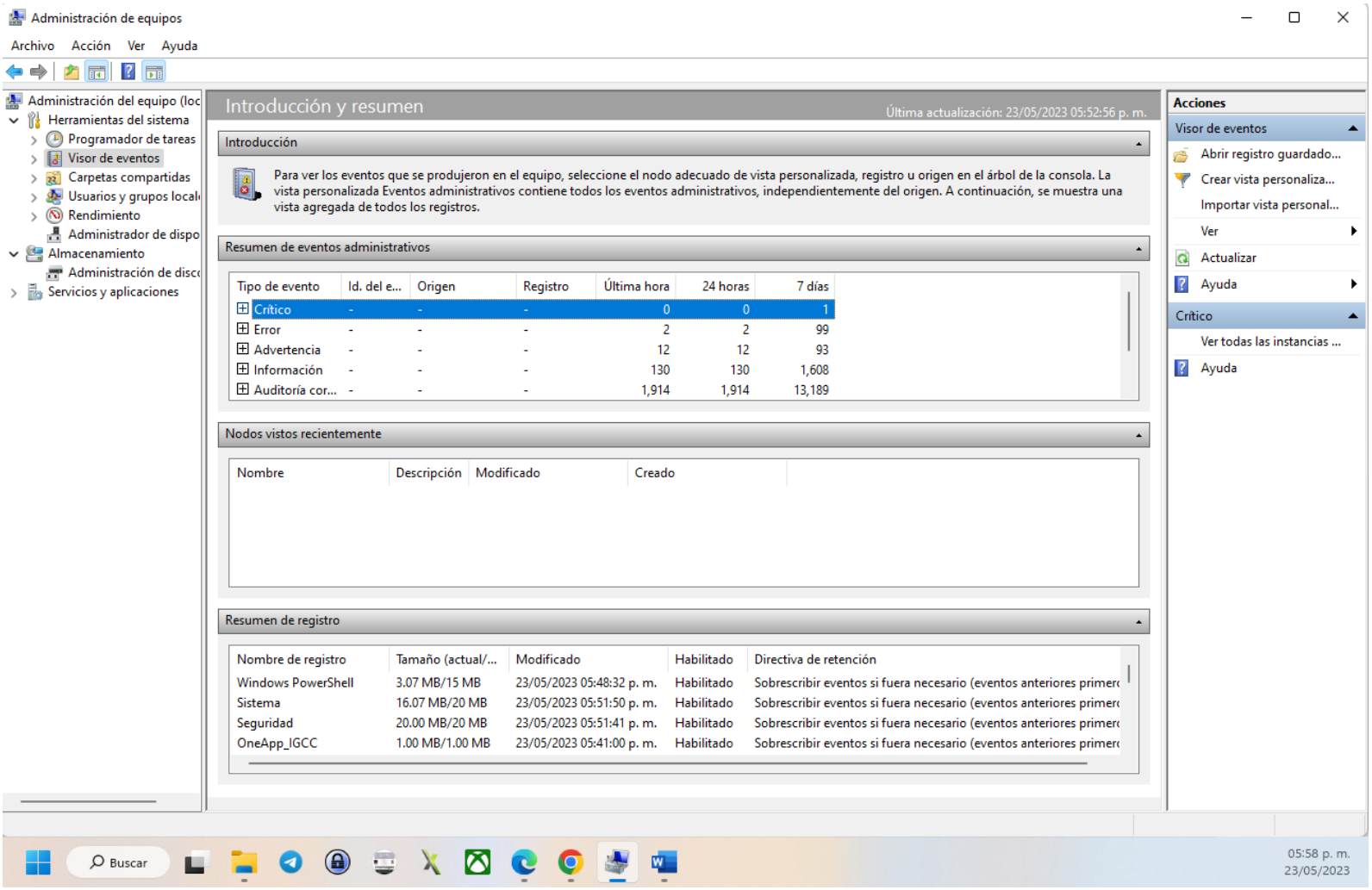
Los beneficios son evidentes, tanto para la empresa que desarrolla la aplicación como para sus clientes que la utilizan. Siguiendo el enfoque del desarrollo seguro de software, las aplicaciones serán diseñadas, implementadas y probadas pensando en su seguridad, facilitando conseguir lo siguiente:

- Aplicaciones más seguras. El número de vulnerabilidades que tendrán las aplicaciones será menor, al igual que su criticidad. Esto es fundamental puesto que el número de ataques que se aprovechan de vulnerabilidades en las aplicaciones es cada vez mayor y las consecuencias para las empresas y las personas son cada vez más severas.
- Optimización de tiempos y costes de ejecución en los proyectos. Los resultados de los proyectos serán mejores, puesto que la corrección de los fallos de seguridad requerirá menores tiempos de desarrollo al detectarse en fases más tempranas, y se evitarán imprevistos de última hora que puedan causar incumplimientos de plazo.
- Mayor satisfacción de los clientes. Las dos anteriores se traducirán en una mayor confianza de los clientes en las aplicaciones.

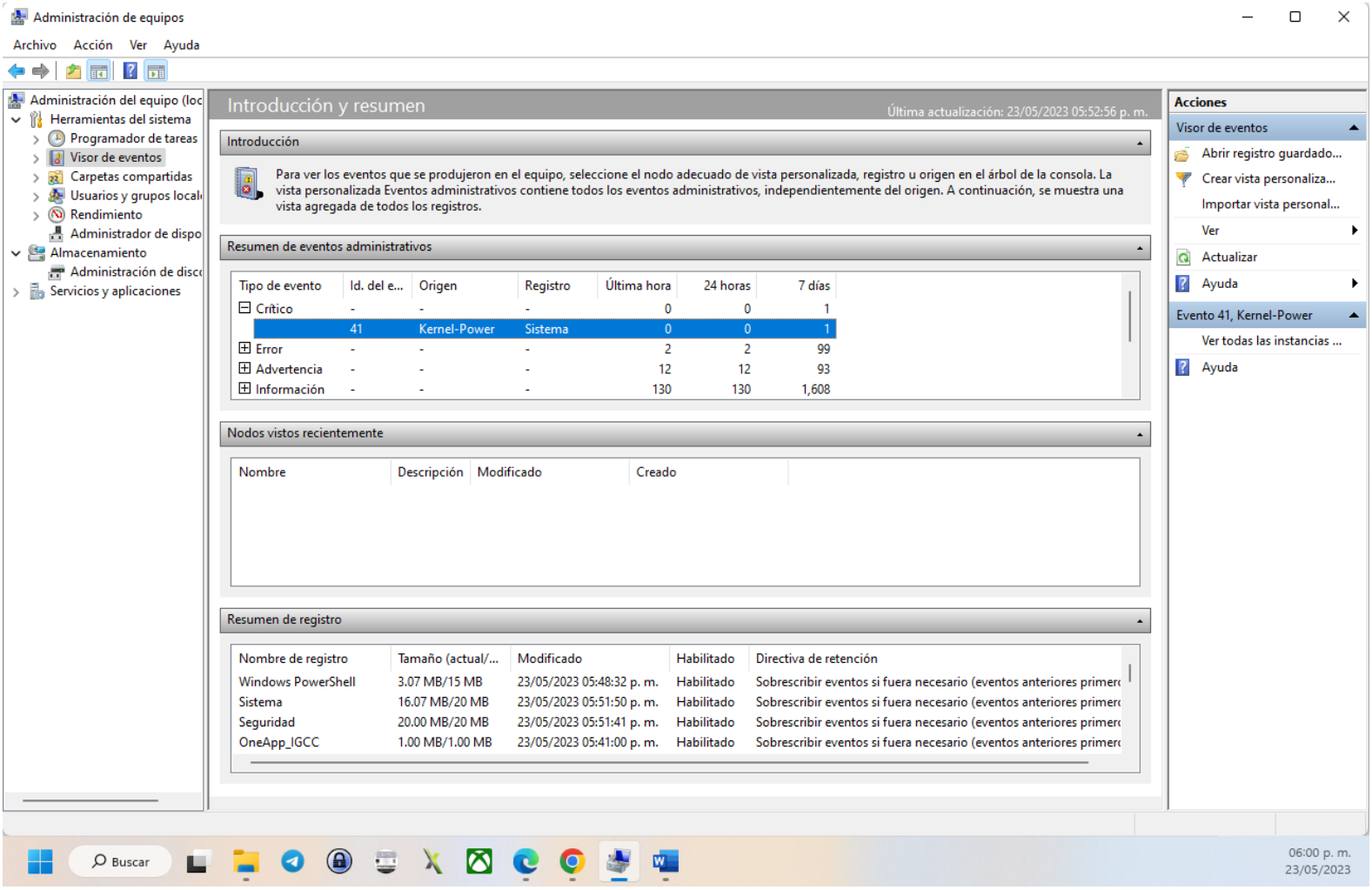
Desarrollo (Auditoría y Bitácora)

Auditoría de equipo

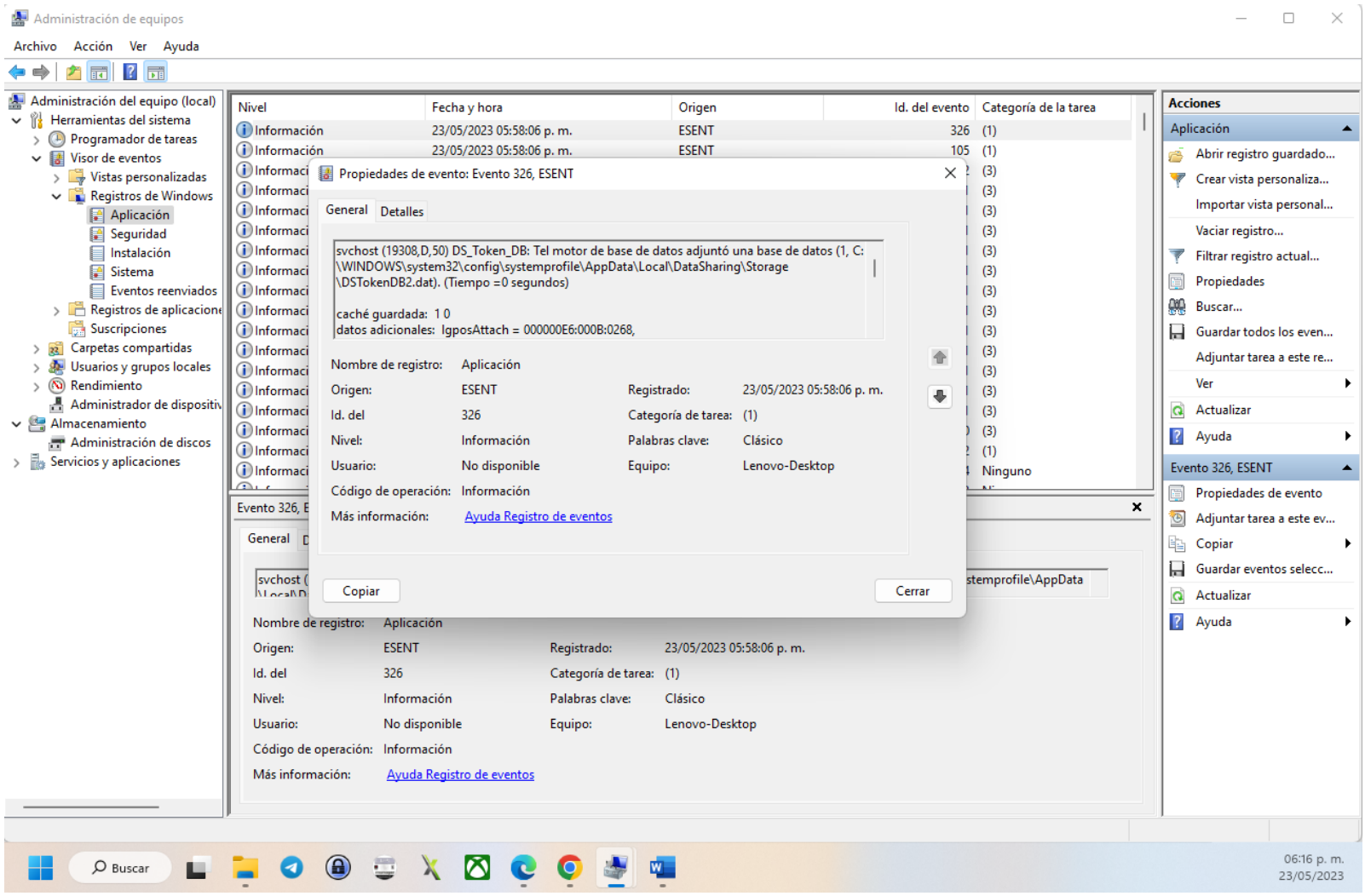
En la siguiente captura se observan los eventos de la auditoria que se realizo el día 23-05-2023 a las 05:52 pm.



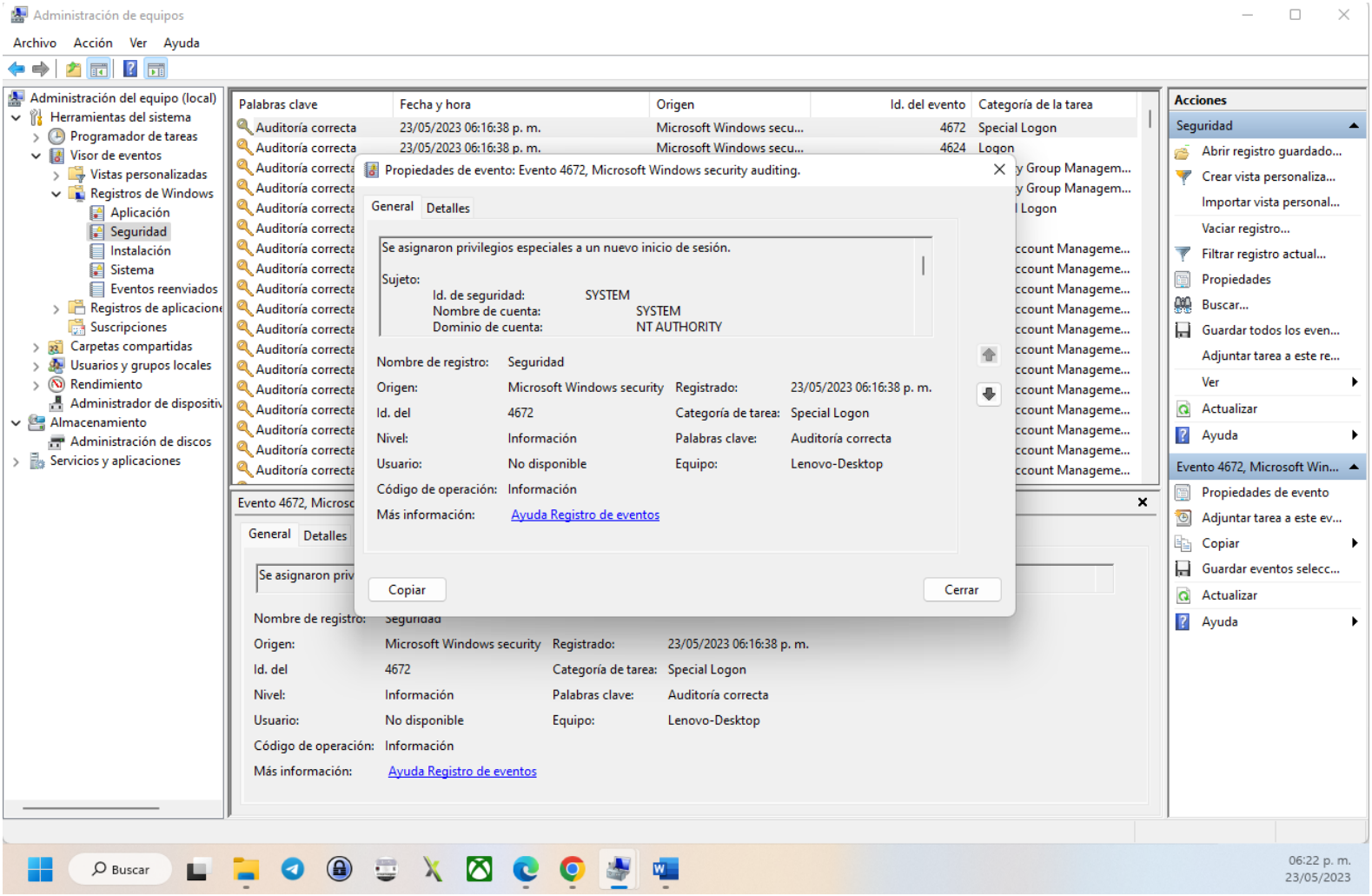
En la siguiente captura se observa el evento critico que arrojo la auditoria.



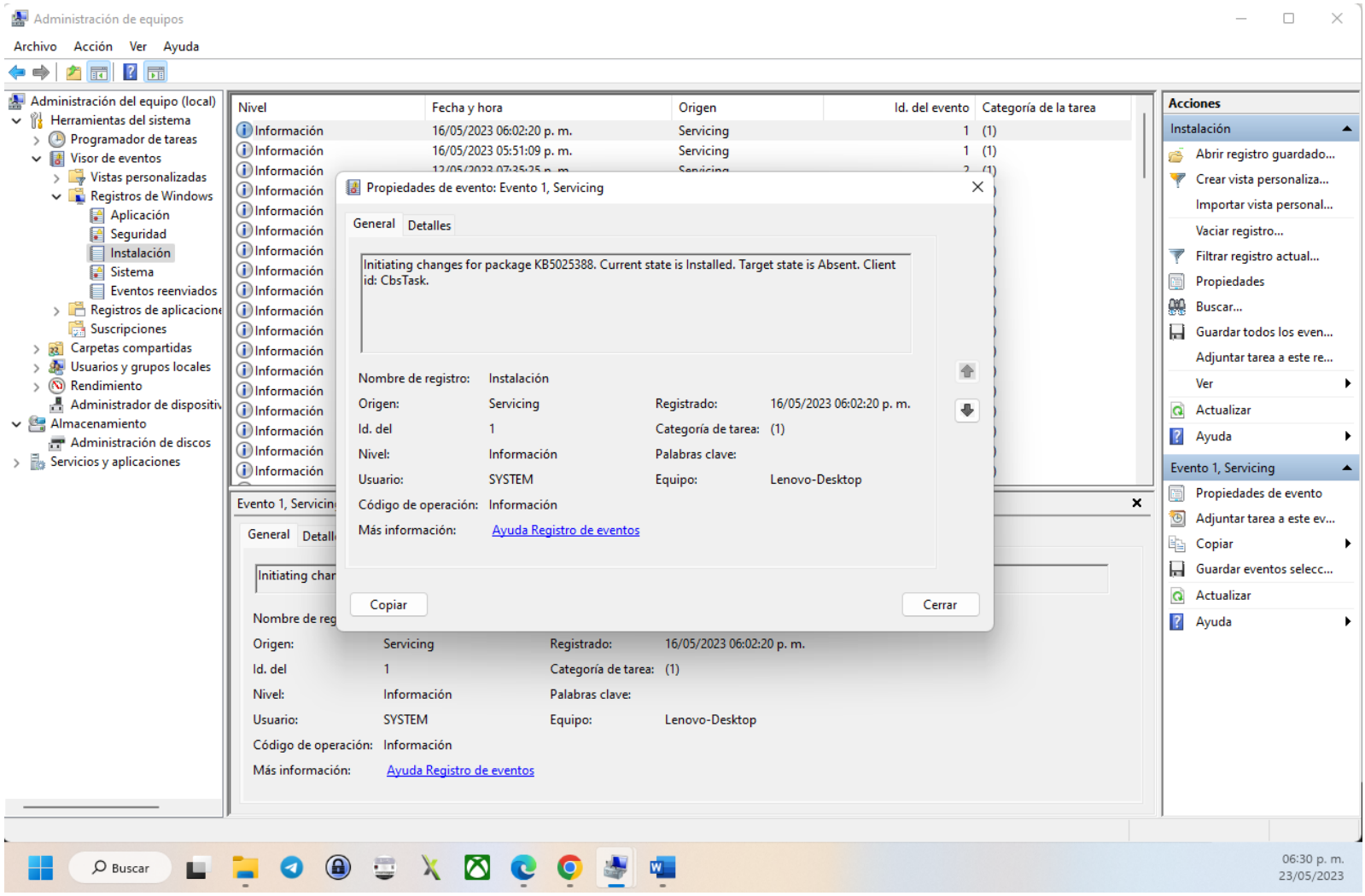
En la siguiente captura se observan los detalles de un evento de información de Esent.



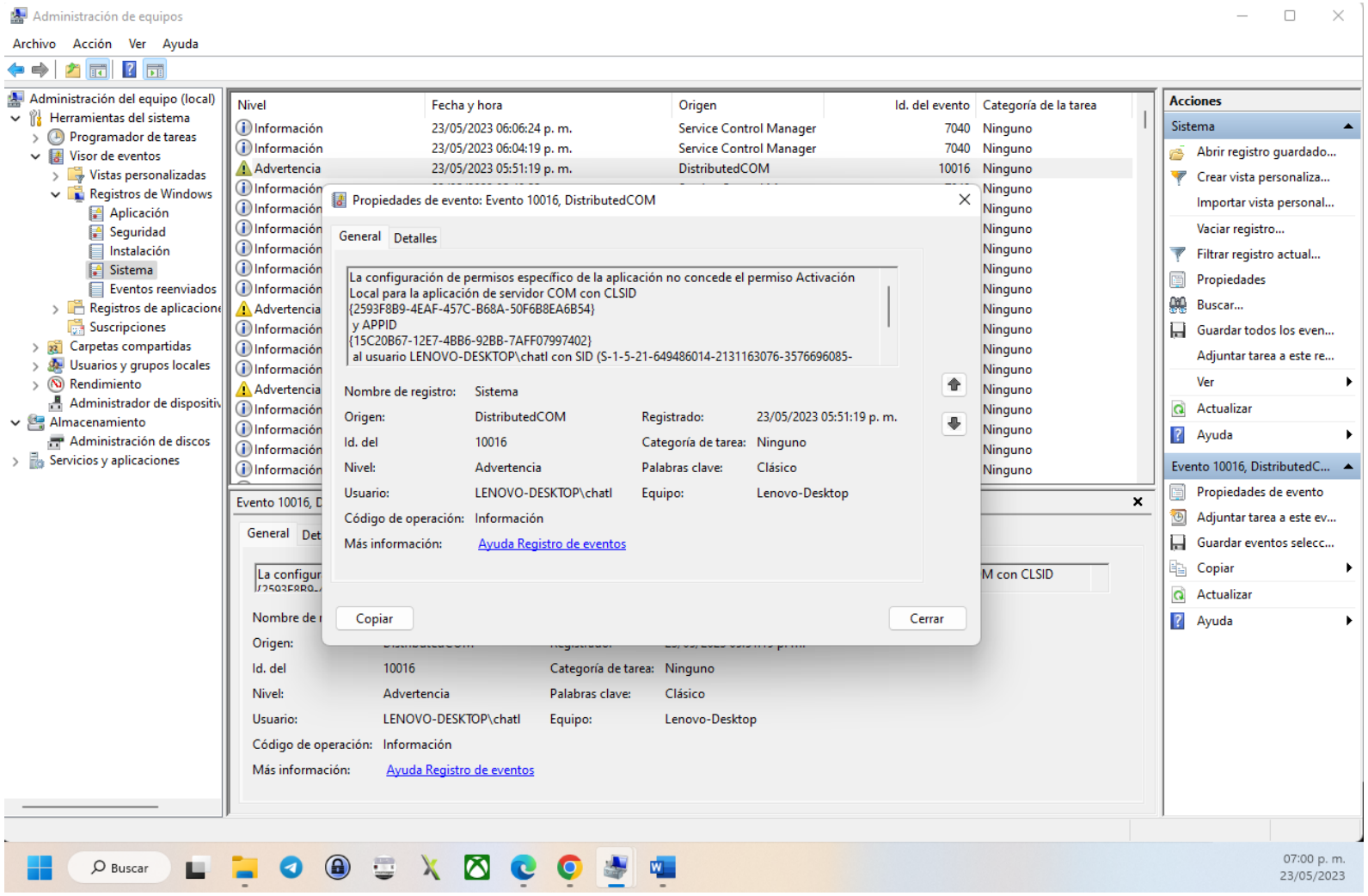
En la siguiente captura, se observa del rubro de Seguridad, los detalles de un evento de seguridad a Logon inicio de sesión.



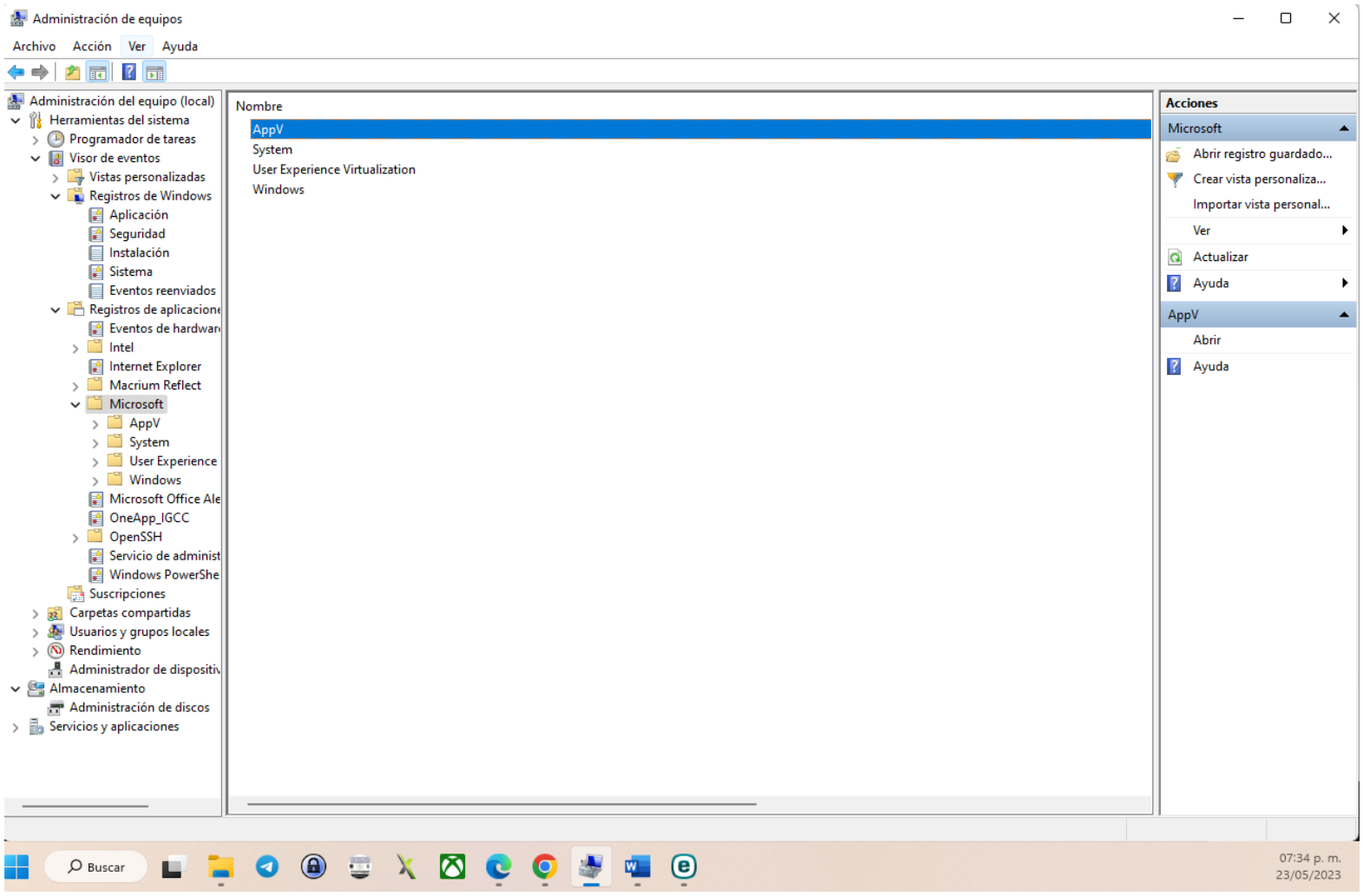
En la siguiente captura, se observa del rubro de Instalación, los detalles de un evento de instalación de una actualización de Windows.



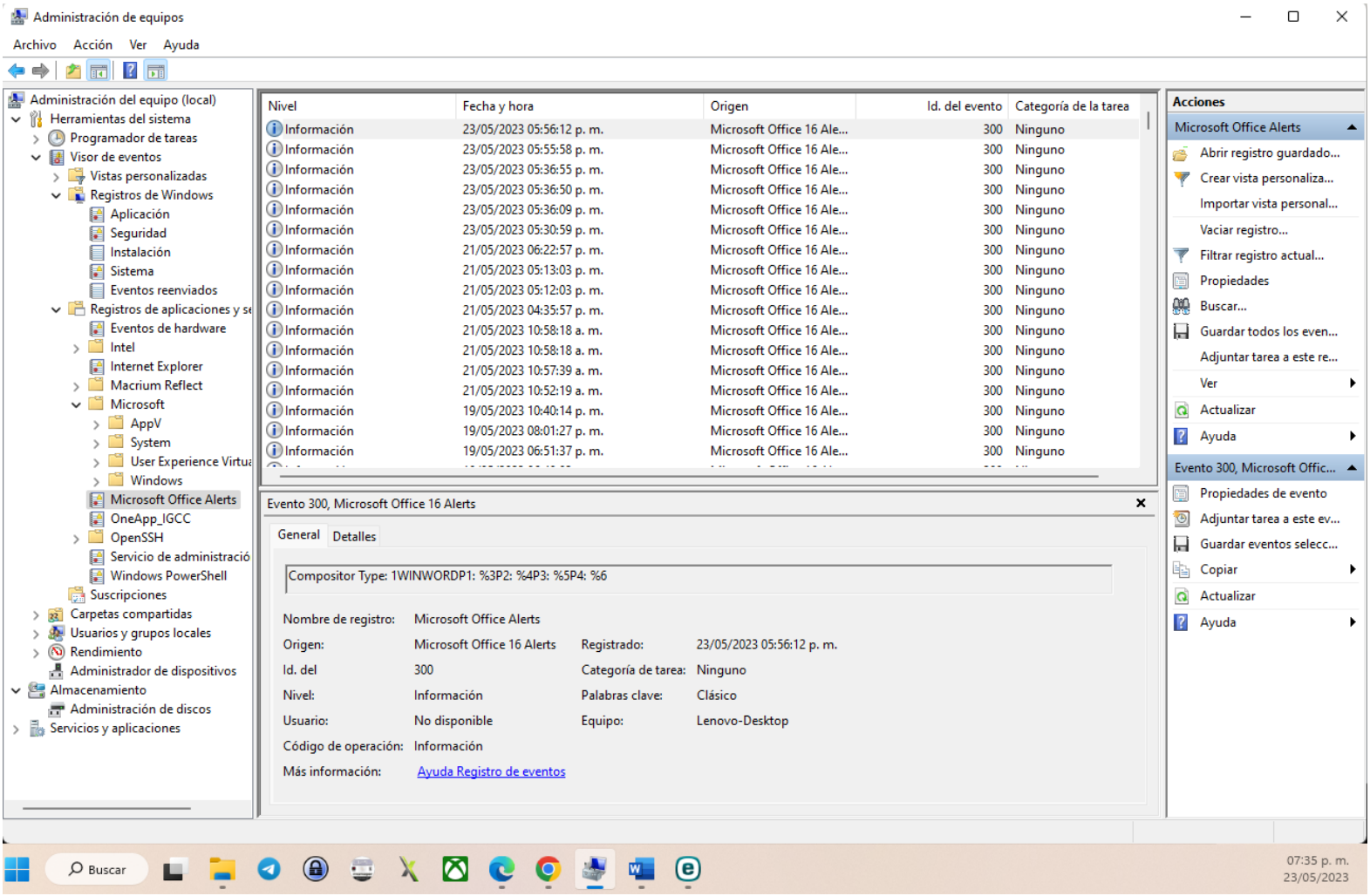
En la siguiente captura, se observa del rubro de Sistema, los detalles de un evento de activación.



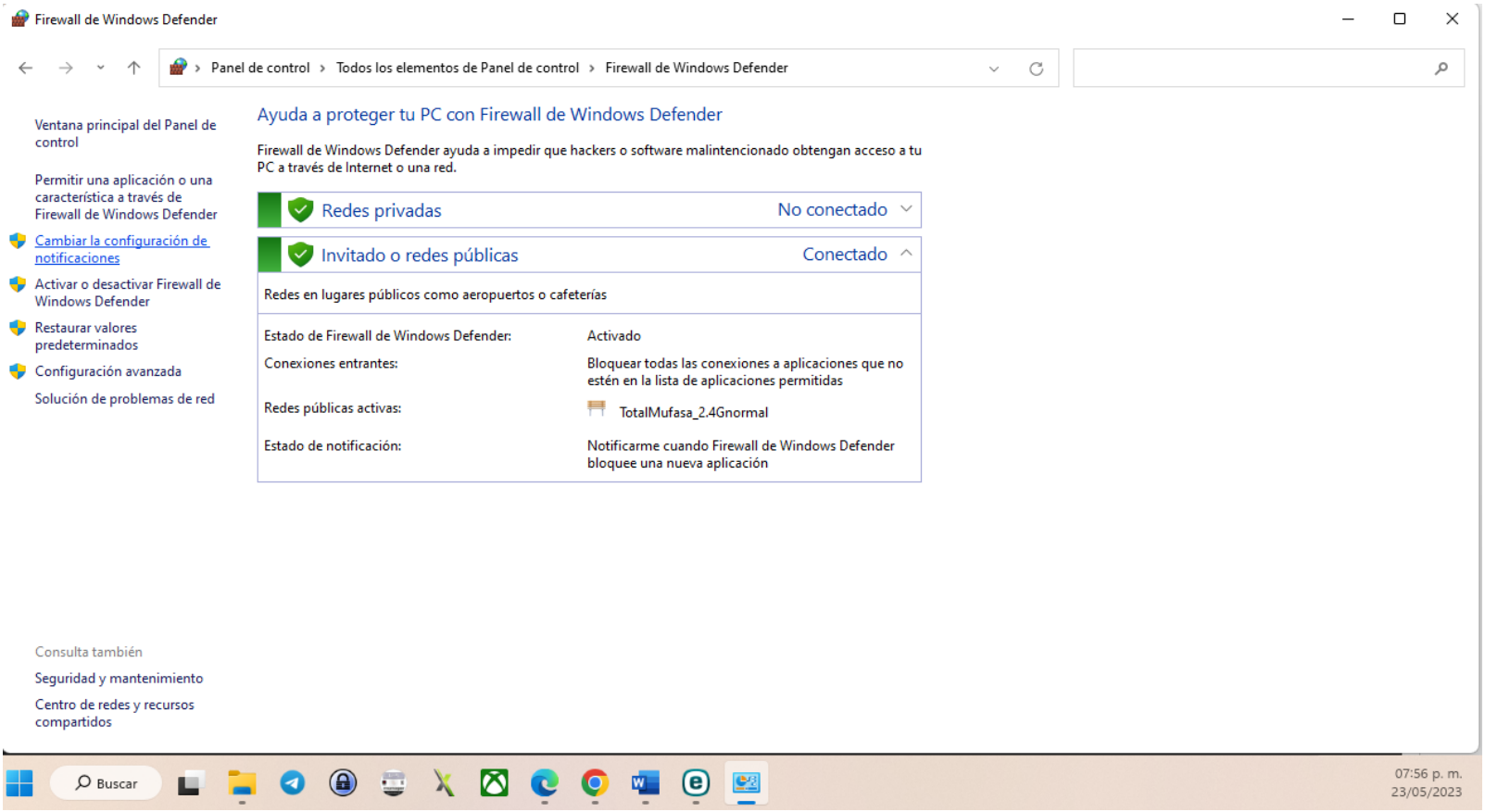
En la siguiente captura, se observa del rubro Registro de aplicaciones, en la pestaña Microsoft, en donde la auditoria no detecta ningún comportamiento extraño.



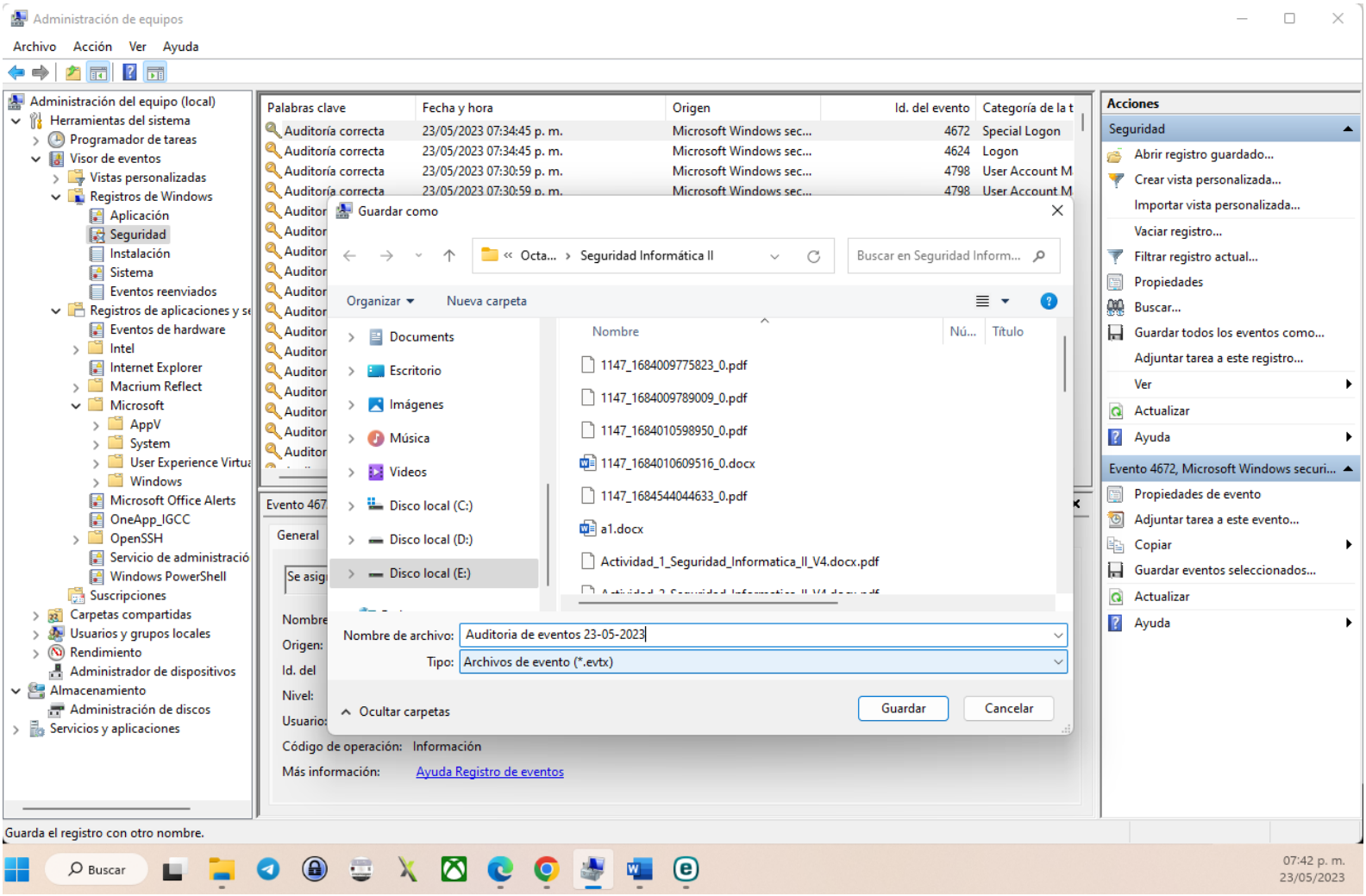
En la siguiente captura, se observa del rubro Registro de aplicaciones, en la pestaña Microsoft office Alerts, en donde la auditoria no detecta ningún comportamiento extraño.



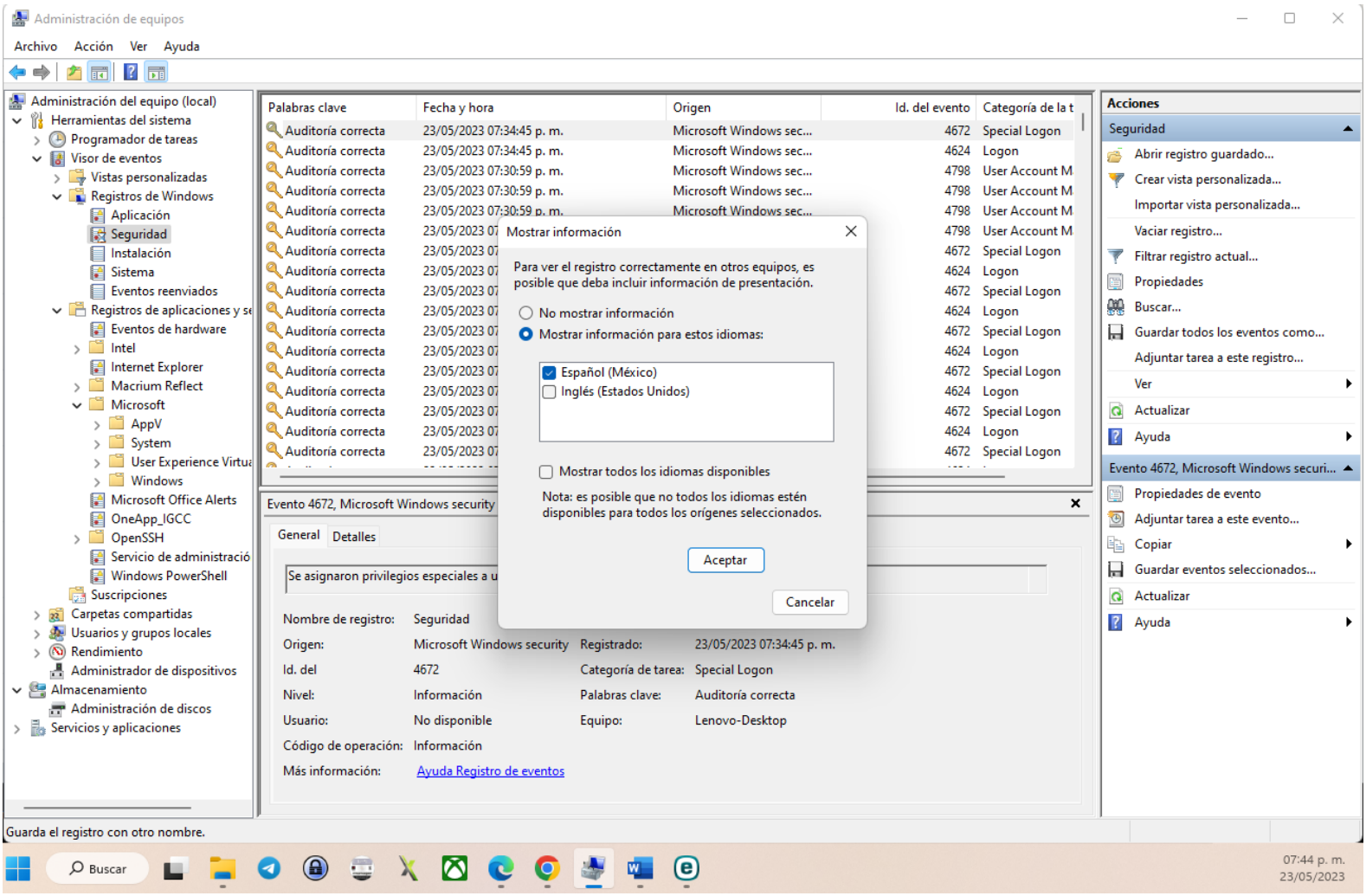
En la siguiente captura, se observa el firewall de Windows, como se puede observar, se encuentra activado y no se detecta ningún comportamiento extraño.



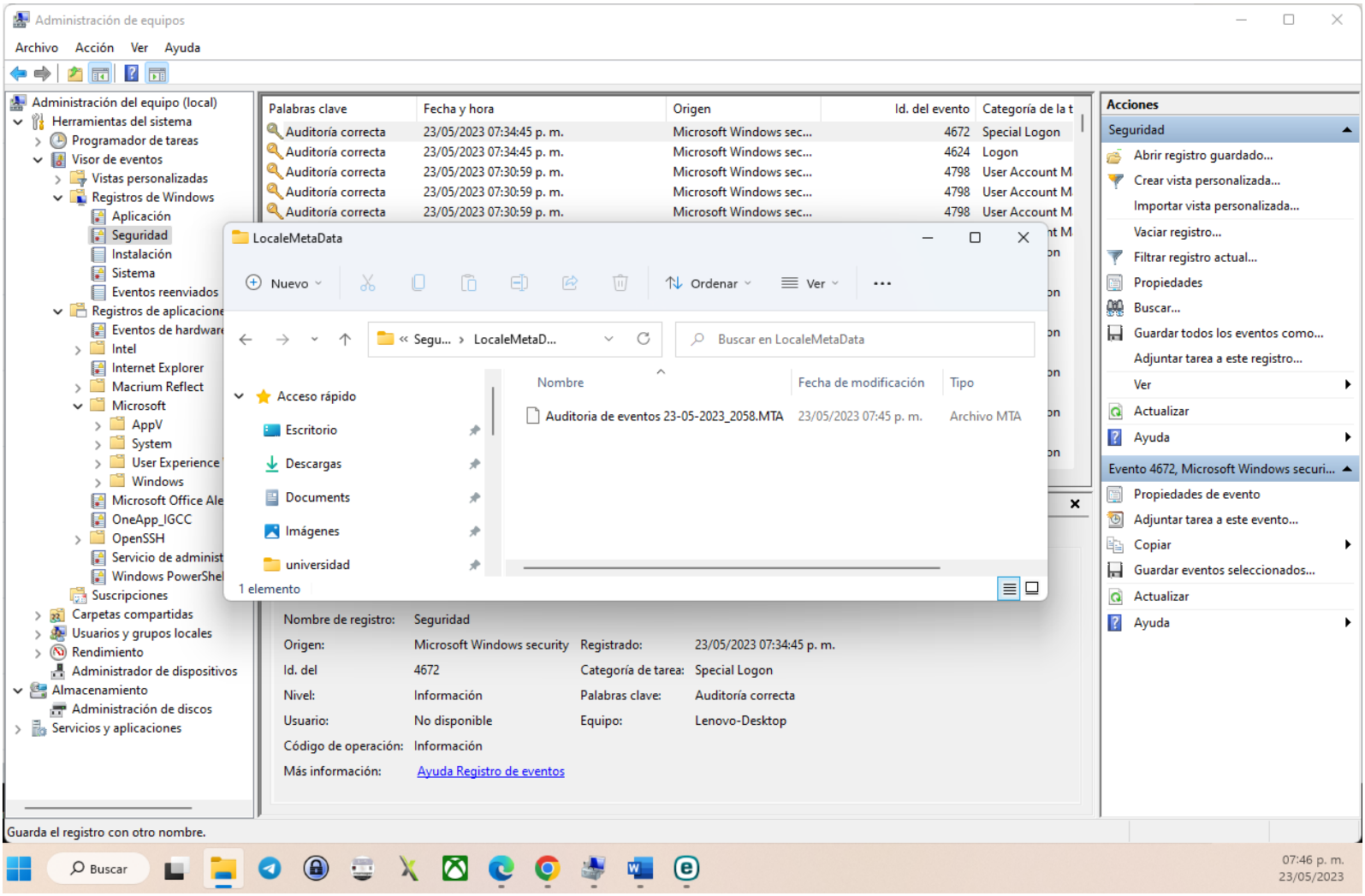
En la siguiente pantalla se observa cuando se guarda la información del registro de todos los eventos encontrados en la auditoria.



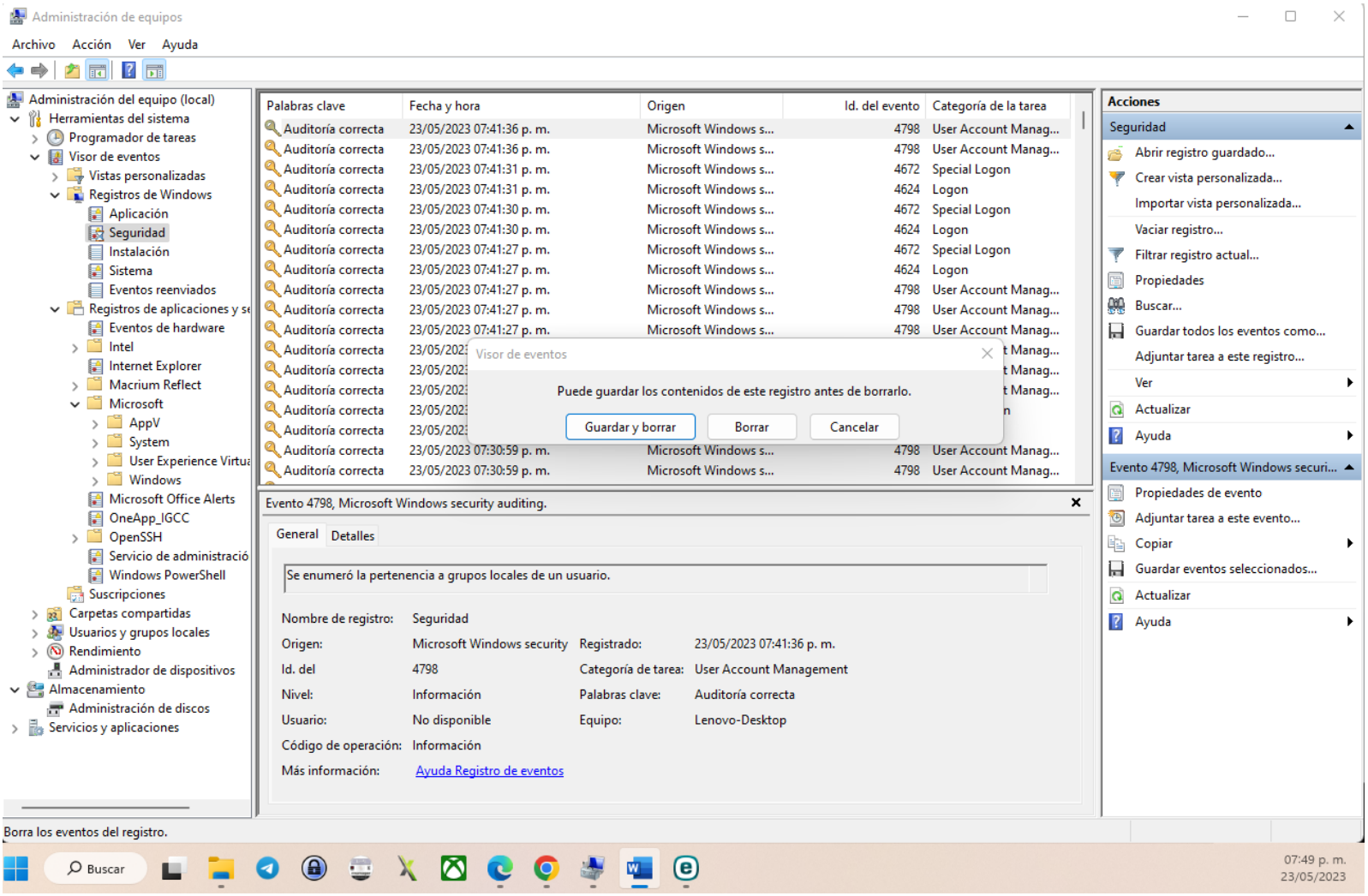
En la siguiente pantalla se observa que se solicita agregar información para el idioma español.



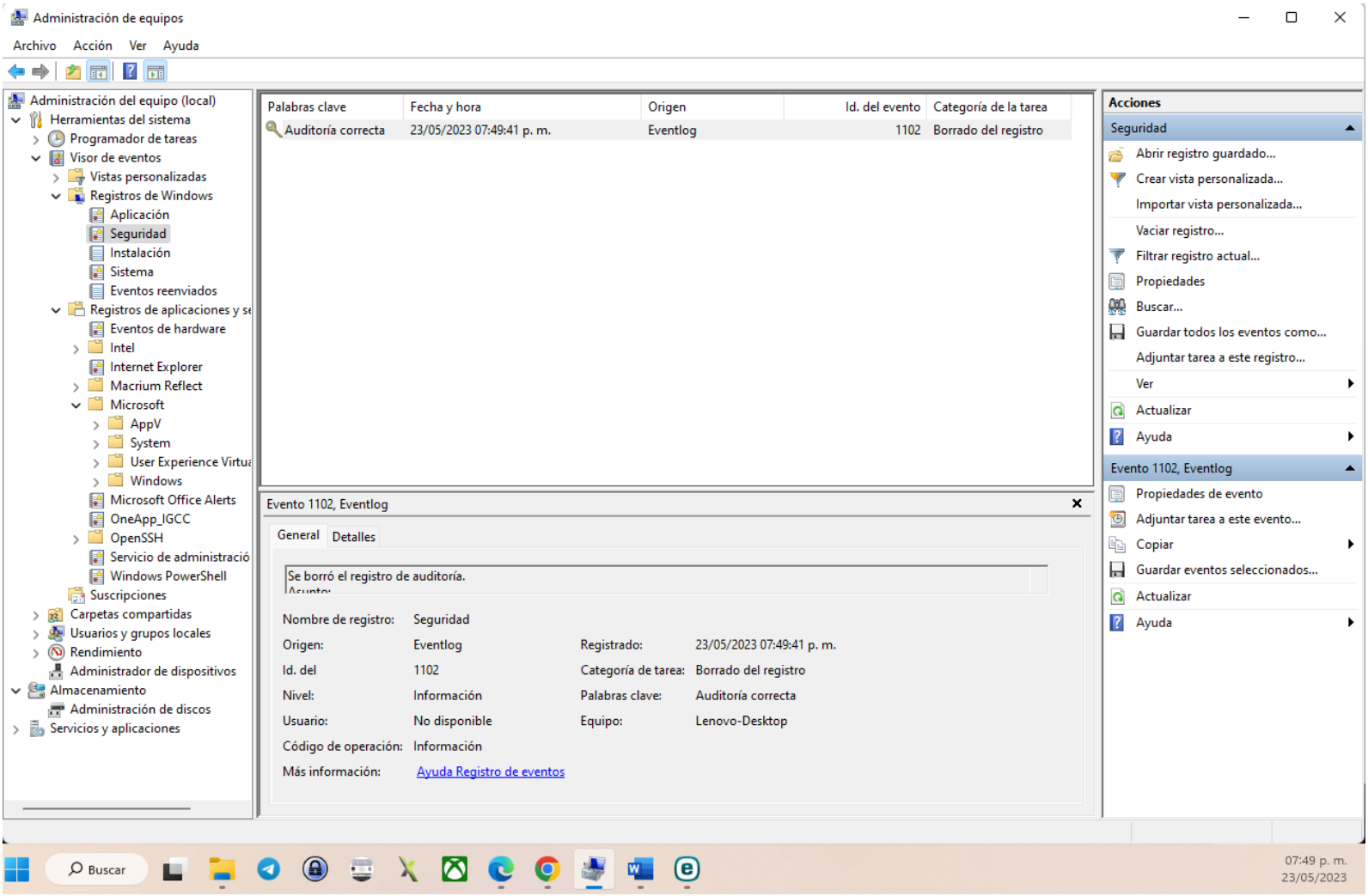
En la siguiente captura se puede observar el archivo guardado en el que contiene toda la información de los eventos de la auditoría realizada a mi equipo



En la captura siguiente se procede a limpiar el registro de la bitácora para poder realizar una nueva auditoria limpia.



En la siguiente captura, se puede observar que al realizar una nueva auditoria, la bitácora se encuentra vacía de registros, solo aparecen los eventos encontrados en la nueva auditoria que se acaba de realizar.



Importancia de seguridad (prevención, monitoreo, auditoría)

De acuerdo a lo que hemos aprendido a lo largo de esta materia, podemos decir que la ciberseguridad es una herramienta que permite tener la infraestructura electrónica de una empresa libre de robos en la base de datos de los usuarios y contraseñas y que este tipo de seguridad mantiene en confidencialidad los documentos, contratos, datos de personal, así como los procesos que lleva a cabo una compañía para aumentar su productividad de forma eficaz. Por lo tanto, la importancia de la seguridad informática radica en la prevención, puesto que se quiere evitar el robo de información en las distintas áreas de la empresa. Además, ayuda a identificar cuando existen amenazas de virus y riesgos en los sistemas de información internos. Algunas de las recomendaciones para prevenir ataques de acceso son:

- Crear contraseñas largas. Deben contener signos y números.
- Verificar que el sistema operativo y las diversas herramientas tecnológicas se encuentren protegidas.
- Actualizar el sistema operativo de las computadoras, así como su antivirus.
- Evita acceder a hipervínculos o archivos adjuntos desconocidos.

Por otra parte, nos damos cuenta que hoy en día las redes están más dinámicas que nunca. Los administradores de redes todos los días encuentran nuevos desafíos y complejidades, especialmente por la velocidad en la que llegan las nuevas tecnologías, herramientas, aplicaciones y posibilidades. El monitoreo de la red es parte fundamental de este proceso, ya que recoge los datos que se generan, los analiza y expone esa información al administrador, generalmente en formato de informes y sistemas de administración de alarmas que le ayudan a mantener el proceso en funcionamiento.
Ese monitoreo permite obtener información necesaria sobre los equipos de modo rápido, sintético, preciso y confiable, lo que facilita que el administrador tome determinadas decisiones al momento

de planear, adecuar y expandir la red. La verificación, el desempeño de servicios y resolución de diversos problemas como el de la conectividad e integración de plataformas, también suceden más fácilmente. Algunas de las ventajas que nos brinda el monitoreo de red son:

- Reduce las interrupciones de la red
- Brinda mayor protección contra posibles ciberataques
- Impacto positivo en la rentabilidad de la empresa
- Permite optimizar la productividad y los flujos de trabajo

Por último, después de realizar análisis para descubrir amenazas de seguridad, realizar monitoreos en la red, queda realizar auditorías. Comenzamos recordando que una auditoría informática nos permite detectar los problemas en los que incurre una empresa a nivel informático, su principal objetivo es, validar la integridad de la información y datos almacenados en las bases de datos de los sistemas de información y su procesamiento.

Gracias a este modo, podremos determinar situaciones como las siguientes:

- Uso indebido de los dispositivos tecnológicos de la empresa.
- Falta de políticas o estrategias de ciberseguridad que permitan enfrentar las amenazas digitales.
- Peligros que amenazan a una web o sistema.
- Problemas de optimización en la red informática.
- Carencia de medidas de seguridad y prevención digital.

Como se puede observar, esto es solo un ejemplo de lo que una auditoría puede descubrir, ya que cada área o empresa se enfrenta a distintas situaciones que una revisión exhaustiva puede descubrir.

Conclusión

En esta actividad continuamos reforzando las auditorias en nuestro equipo, esta vez me tocó aprender a realizar auditorías con las mismas herramientas administrativas de Windows, en esta ocasión nos centramos en utilizar la herramienta “Administración del equipo” para tal fin.

Esta aplicación cuenta con varias aplicaciones, sin embargo, vamos a centrarnos en” Herramientas de sistema”, aquí encontré varias herramientas como son: programador de tareas, visor de eventos, carpetas compartidas, Usuarios y grupos locales, rendimiento y administrador de dispositivos.

De todas estas herramientas mencionadas, conocí la herramienta de auditoria llamada Visor de eventos, con esta herramienta aprendí a realizar auditorías y a identificar algunos eventos que arrojo la auditoria, principalmente los críticos, junto con la información de los eventos que suceden en los demás rubros de “Aplicación”, “Seguridad”, “Instalación”, “Sistema”, así como también los registros de aplicaciones.

También aprendí a filtrar la información de dichos eventos por diferentes categorías, como son: Critico, Advertencia, Detallado, Error e Información.

Por último, aprendí a salvar la información de la Bitácora, que es la información detallada de estos eventos que surgieron del resultado de las auditorías realizadas, así como también a vaciarla para poder realizar una nueva auditoria en limpio.

Referencias

López, Á. (2022). Desarrollo seguro de software. ITCL. https://itcl.es/blog/desarrollo-seguro-de-software/#:~:text=El%20desarrollo%20seguro%20de%20software%20es%20una%20metodolog%C3%ADa%20cuyo%20objetivo,de%20requisitos%20de%20las%20mismas.

Vinaypamnani-Msft. (2023, 18 marzo). Auditoría de seguridad (Windows 10). Microsoft Learn. https://learn.microsoft.com/es-es/windows/security/threat-protection/auditing/security-auditing-overview.

De Between, I. S. (s. f.). Metodologías de desarrollo seguro de software | BETWEEN Technology. https://impulsate.between.tech/tecnicas-desarrollo-seguro-software.

Acevedo, E. (2022). ¿Por qué es importante el desarrollo de software seguro? InterGrupo. https://intergrupo.com/por-que-es-importante-el-desarrollo-de-software-seguro/

¿Cuáles son las etapas del Desarrollo de Software? (s. f.). https://global.tiffin.edu/noticias/cuales-son-las-etapas-del-desarrollo-de-software

Ciclo de vida del software: todo lo que necesitas saber. (s. f.). Intelequia. https://intelequia.com/blog/post/ciclo-de-vida-del-software-todo-lo-que-necesitas-saber

Westcon-Comstor, E. S. (2016, 21 septiembre). La importancia del monitoreo de la red y Analytics

avanzado. https://blog-es.lac.tdsynnex.com/la-importancia-del-monitoreo-de-la-red-y-analytics-avanzado.

Seguridad, P. (2022). La importancia de monitorear las redes de datos en una empresa. Protek. https://www.protek.com.py/novedades/monitorear-las-redes-de-datos/

Un1l@3sCh0. (2022, 18 julio). ¿Por qué es importante la seguridad informática? | UNILA. Unila. https://www.unila.edu.mx/por-que-es-importante-seguridad-informatica/#:~:text=La%20importancia%20de%20la%20seguridad,los%20sistemas%20de%20informaci%C3%B3n%20internos.