Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

# Actividad | 3 |

Auditoría y Bitácora

## Seguridad Informática II

Ingeniería en Desarrollo de Software

academia global

TUTOR: Jessica Hernández

ALUMNO: Yanira Lizbeth Lopez Navarro

FECHA: 23/01/2024

# Índice

# Introducción

En la era actual, donde la información es un recurso de valor incalculable y la dependencia de la tecnología se ha vuelto omnipresente, la evaluación y preservación de la integridad de los sistemas informáticos se convierte en una prioridad estratégica tanto para organizaciones como para usuarios individuales. La presente actividad se adentra en un análisis detallado sobre la importancia de las auditorías y la gestión de bitácoras en la seguridad y eficiencia de los entornos digitales.

La actividad nos sumergirá en la comprensión de cómo las auditorías, ya sea a través del Panel de control o mediante herramientas especializadas, desempeñan un papel fundamental al identificar vulnerabilidades y validar licencias. Estas prácticas no solo contribuyen a fortalecer la seguridad de los sistemas.

Exploraremos el papel vital de las bitácoras como testigos digitales que no solo registran cambios en el sistema a lo largo del tiempo, sino que también se convierten en herramientas esenciales para la detección temprana de incidentes y la garantía de un historial detallado para cumplir con requerimientos legales. Esta actividad ofrece una inmersión integral en la importancia y aplicación de auditorías y bitácoras en la salvaguarda de entornos informáticos en la actualidad.

## Descripción

El contexto presentado implica la realización de una auditoría en un equipo de cómputo con el objetivo de identificar las licencias de los recursos instalados y obtener información detallada sobre el sistema, hardware, software y red. Se destaca la importancia de validar las licencias por razones legales y regulatorias, así como la necesidad de realizar auditorías periódicas para prevenir posibles ataques y mantener un control total del equipo, lo que contribuirá a fortalecer los mecanismos de seguridad implementados para proteger la información valiosa.

La actividad solicitada consiste en realizar una auditoría utilizando el Panel de control o una herramienta digital, guardar la bitácora actual y empezar una nueva para detectar cambios desde el inicio. Este proceso se realiza con el propósito de mantener un registro detallado de la configuración y licencias del equipo, facilitando la identificación de posibles alteraciones o vulnerabilidades.

Argumentando, se puede afirmar que estas prácticas son esenciales en entornos empresariales y de seguridad informática. La auditoría proporciona una visión clara del estado del sistema, asegurando el cumplimiento legal y la protección de activos digitales. Además, el mantenimiento de bitácoras permite rastrear cambios y establecer un historial que puede resultar crucial en la detección y respuesta ante posibles amenazas cibernéticas. La realización de auditorías y la gestión adecuada de bitácoras son componentes fundamentales en la estrategia de seguridad de la información.

# Justificación

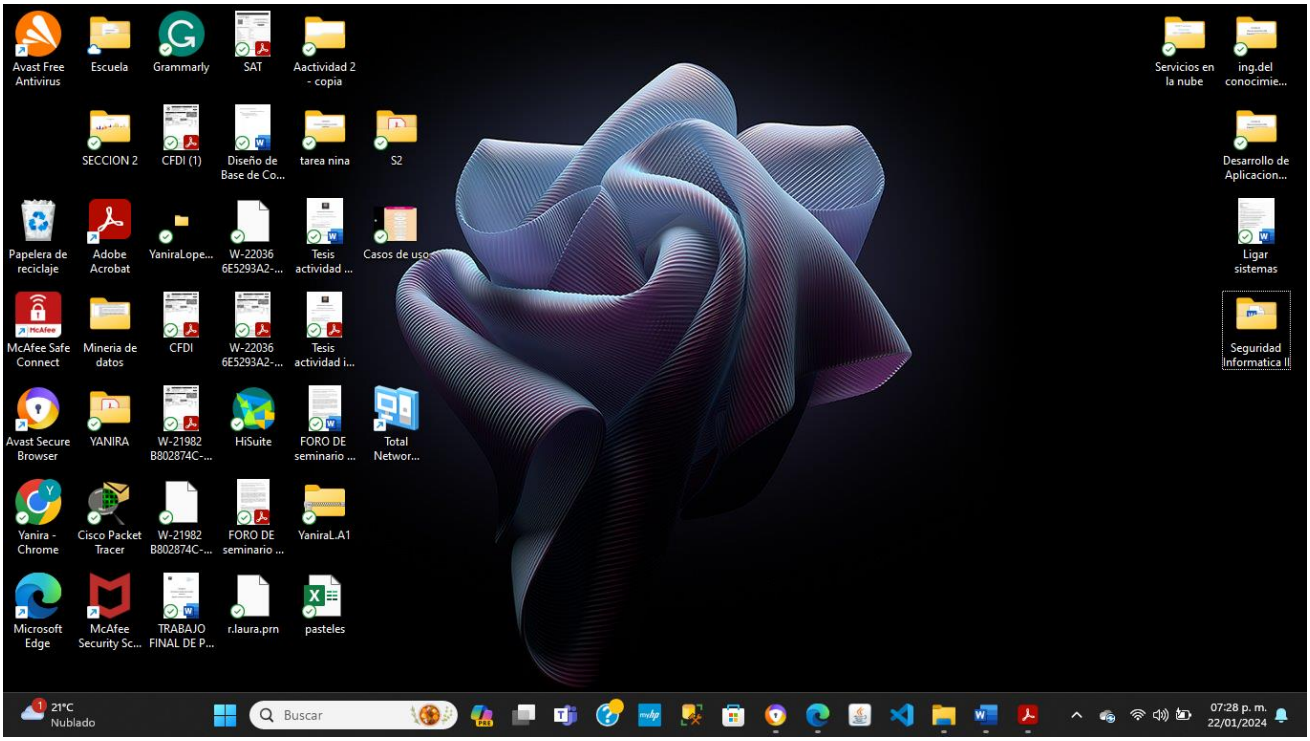
La implementación de auditorías periódicas y la gestión de bitácoras en la actividad propuesta son fundamentales debido a su contribución crucial a la seguridad y cumplimiento normativo en entornos informáticos. La realización de auditorías desde el Panel de control o utilizando herramientas especializadas permite una evaluación exhaustiva de la configuración del equipo, identificando posibles vulnerabilidades, asegurando la legalidad de las licencias

La justificación de emplear este tipo de solución radica en la capacidad para prevenir potenciales ataques, ya que la auditoría proporciona un panorama detallado de los recursos y posibles puntos de vulnerabilidad. Además, la validación regular de licencias garantiza el cumplimiento de requisitos legales y regulatorios, evitando posibles sanciones y pérdida de reputación. La gestión de bitácoras, al guardar registros detallados y establecer un historial de cambios, fácil

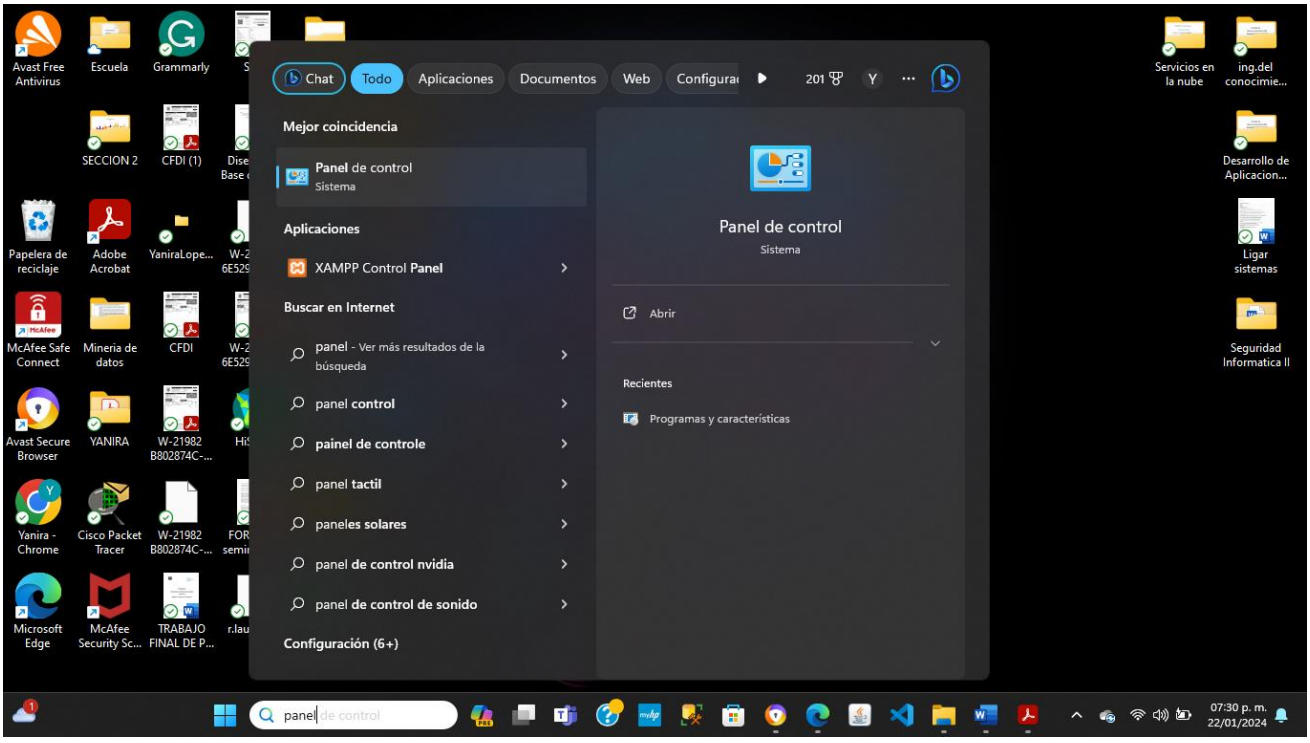
Esta solución se justifica por su capacidad para fortalecer la seguridad, mantener la conformidad legal y proporcionar una herramienta valiosa para la detección y mitigación de posibles amenazas en el entorno informático.

# Desarrollo:
# Auditoría y Bitácora

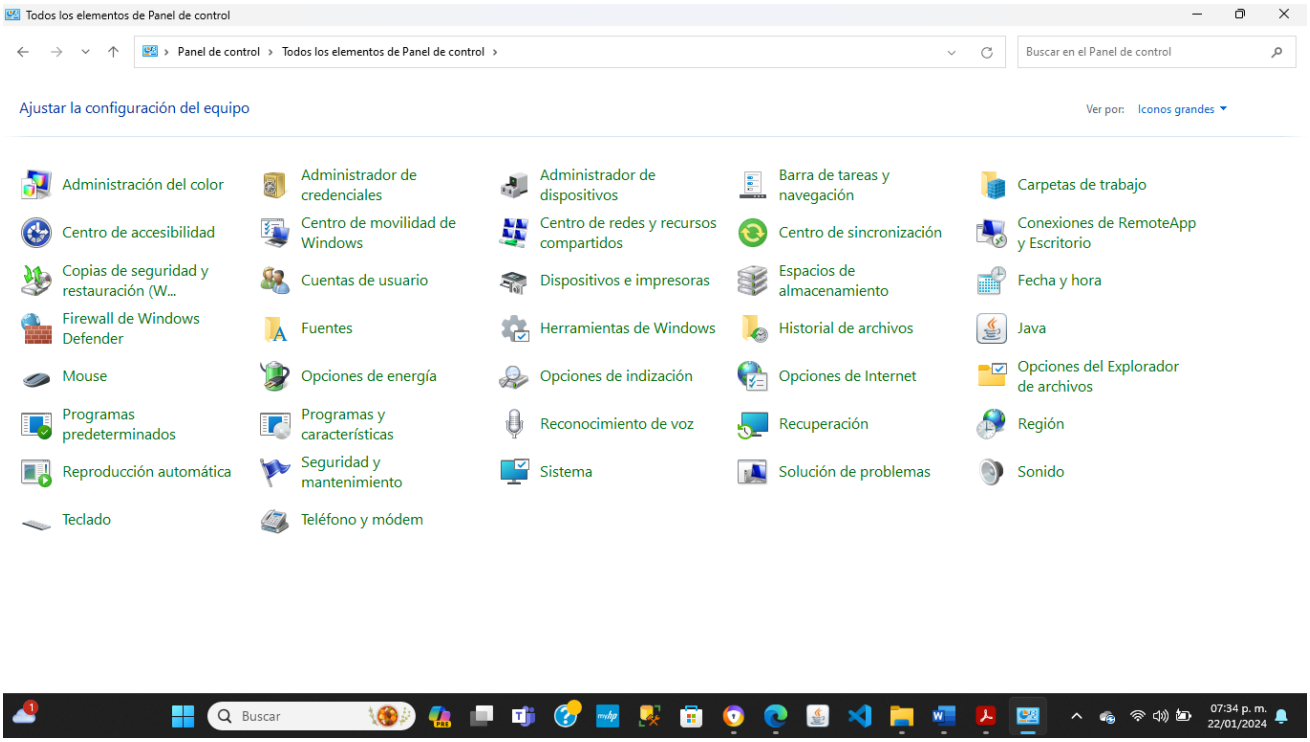
En la siguiente imagen nos muestra el inicio de la pantalla de mi equipo el cual vamos a analizar.



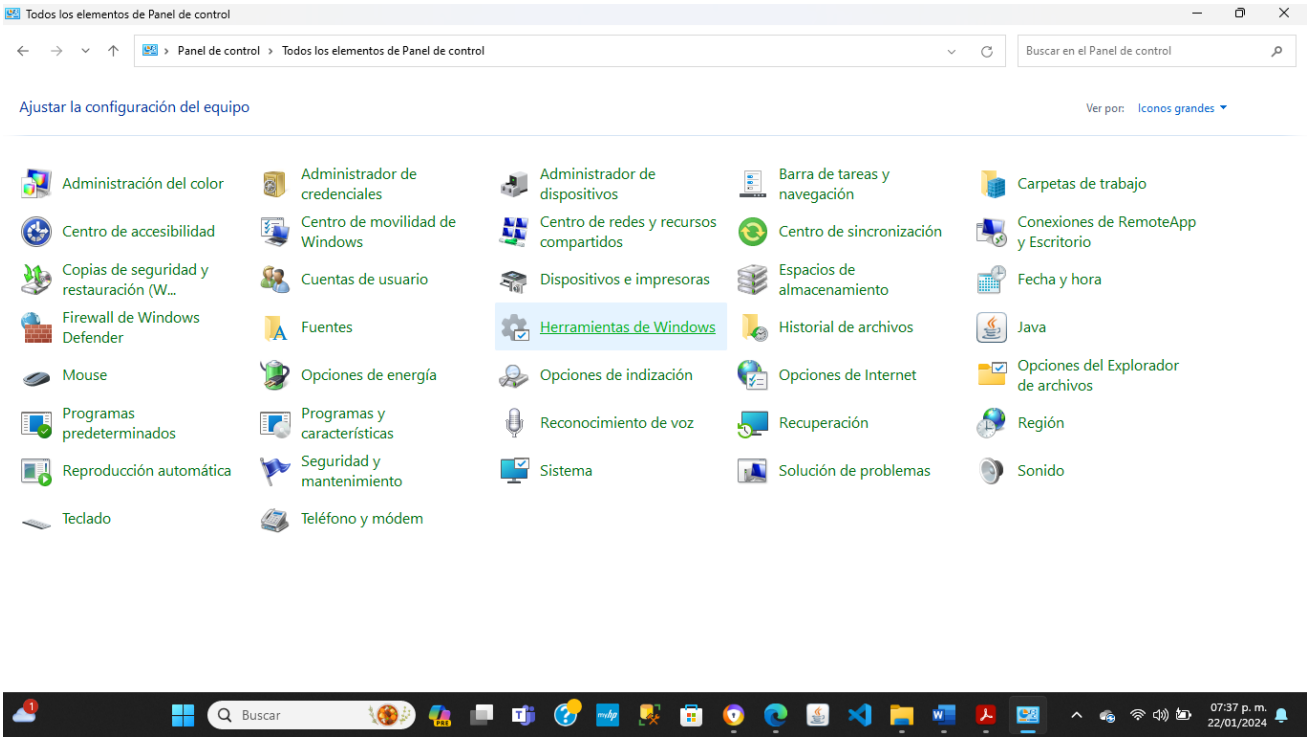

Enseguida se muestra el inicio a nuestro panel de control.



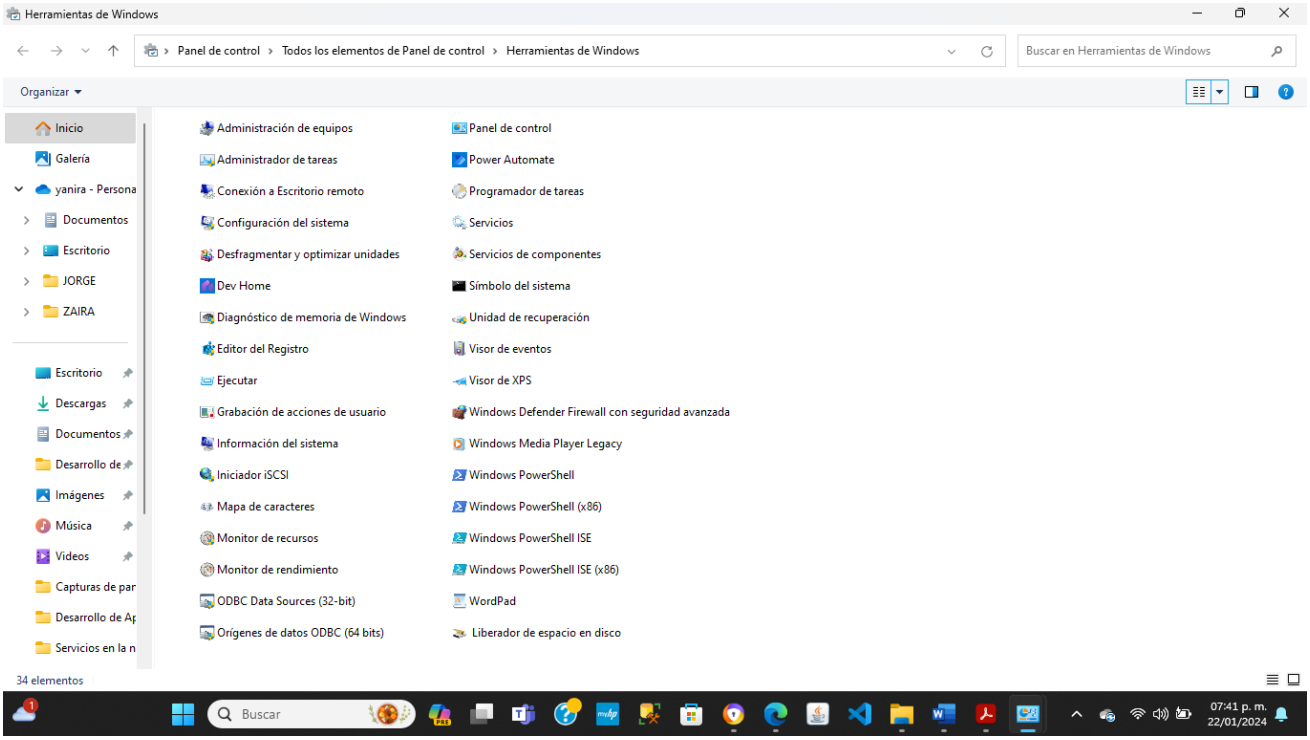
Una vez que se abrió el panel de control podemos observar el logo de todas las configuraciones que podemos realizar desde nuestro panel.



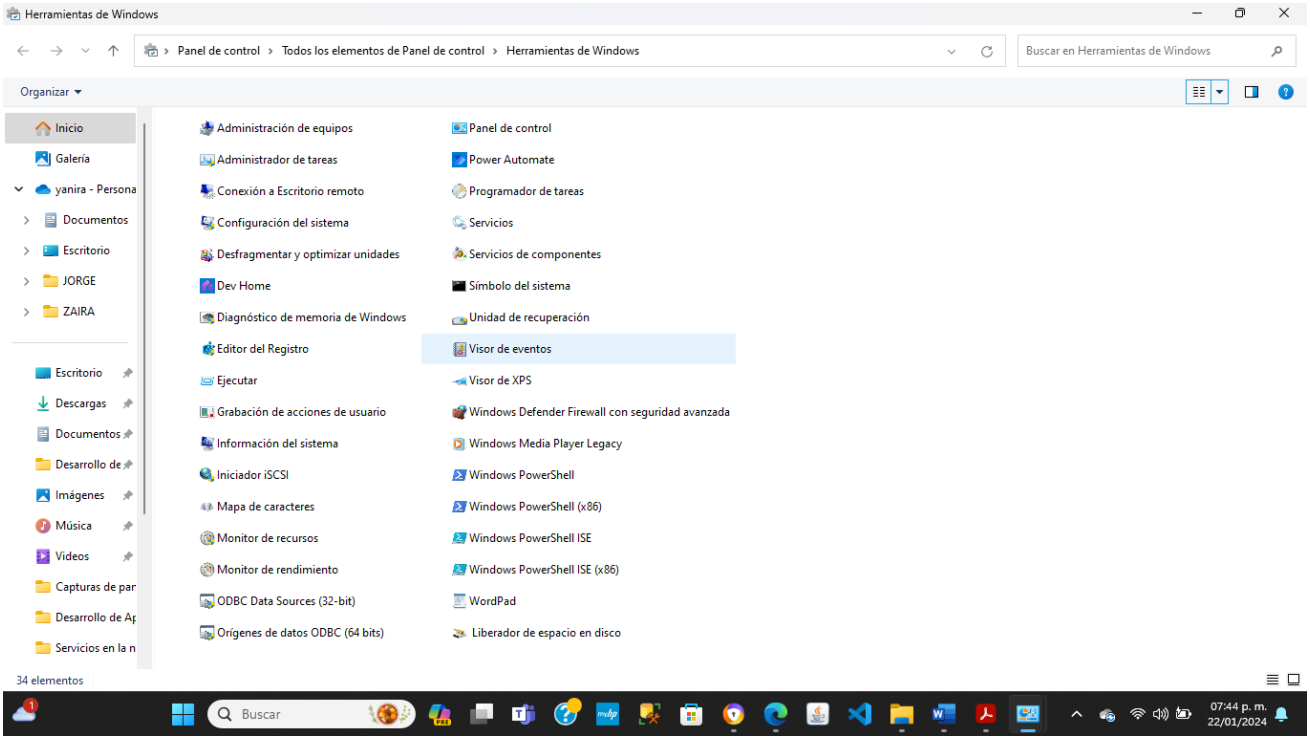

Procedemos a seleccionar Herramientas de Windows como bien lo menciono la maestra viaria de acuerdo a la versión Windows de cada equipo.



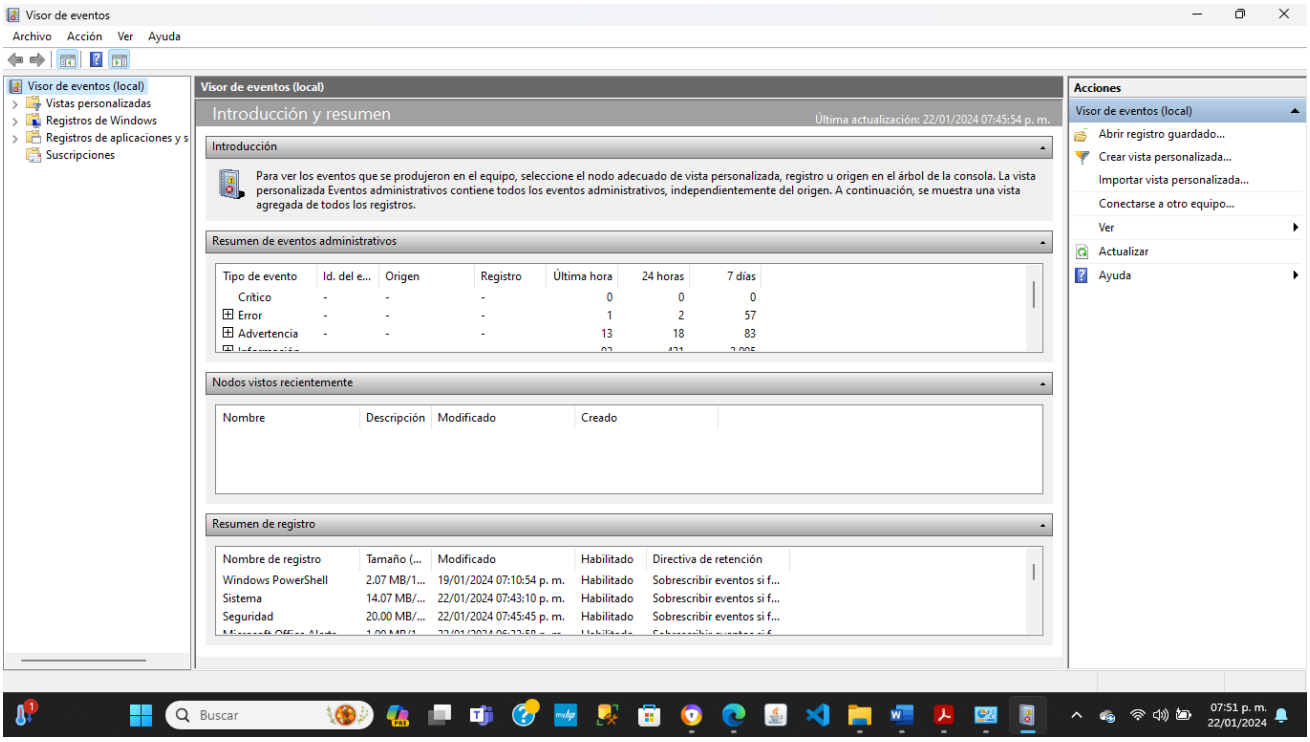
Después de haber seleccionado herramientas de Windows nos arroja el siguiente menú.



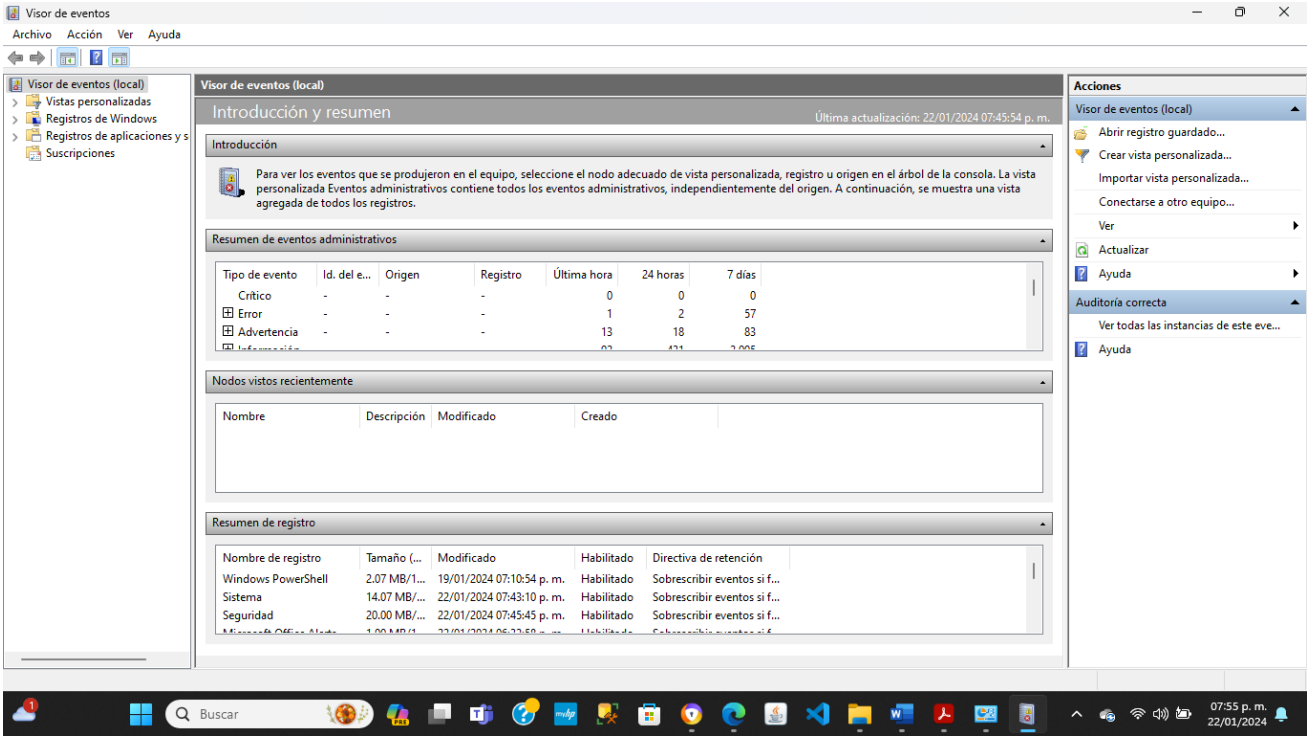

Seleccionamos visor de eventos.



Enseguida nos arroja la siguiente pantalla en la cual podemos observar el registro de los eventos.

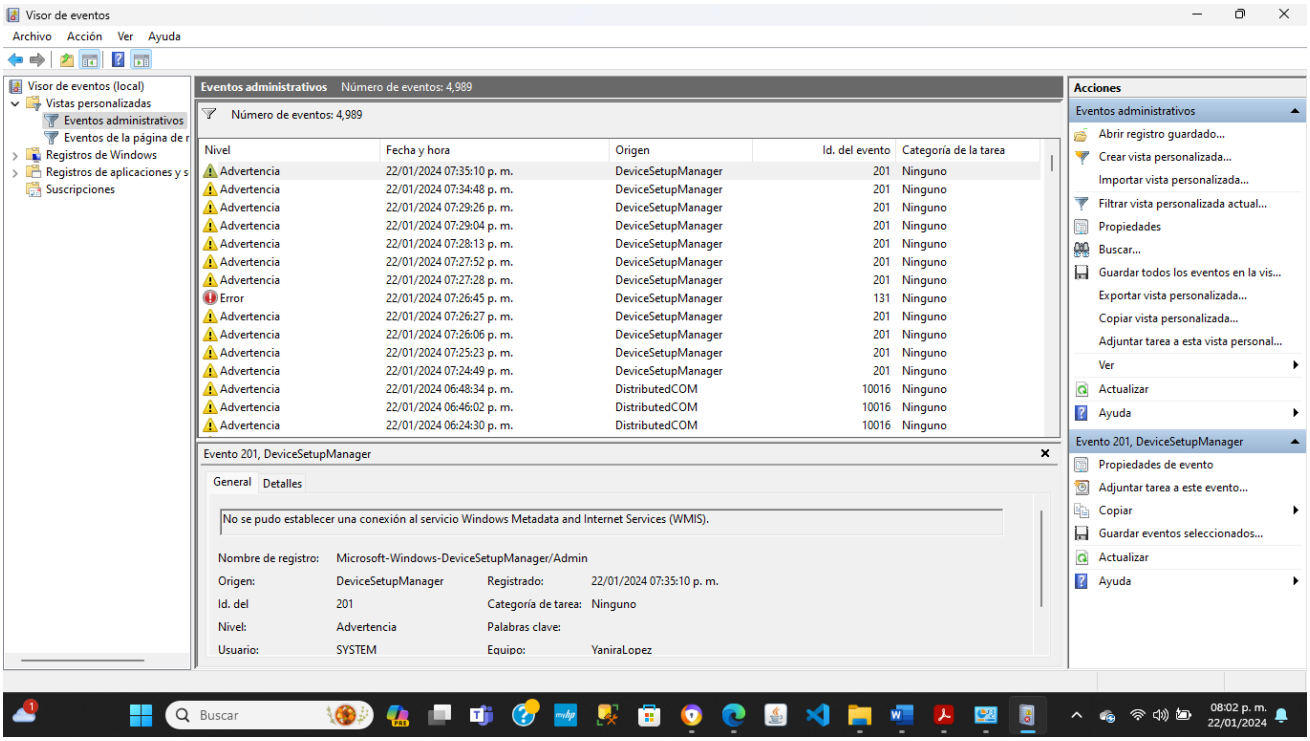



Una vez que nos encontramos en el visor de eventos podemos auditar los eventos y revisar su estatus. En el cual podemos observar que durante 7 días no tuve eventos críticos, en un día tuve 1 error ,en 24 horas tuve2 errores y en 7 días tuve 52 errores.



# Auditoría de equipo

Aquí podemos observar el registro de los eventos administrativos una vez que realizamos las auditoras del equipo.



Eventos administrativos Número de eventos: 4,989

Número de eventos: 4,989

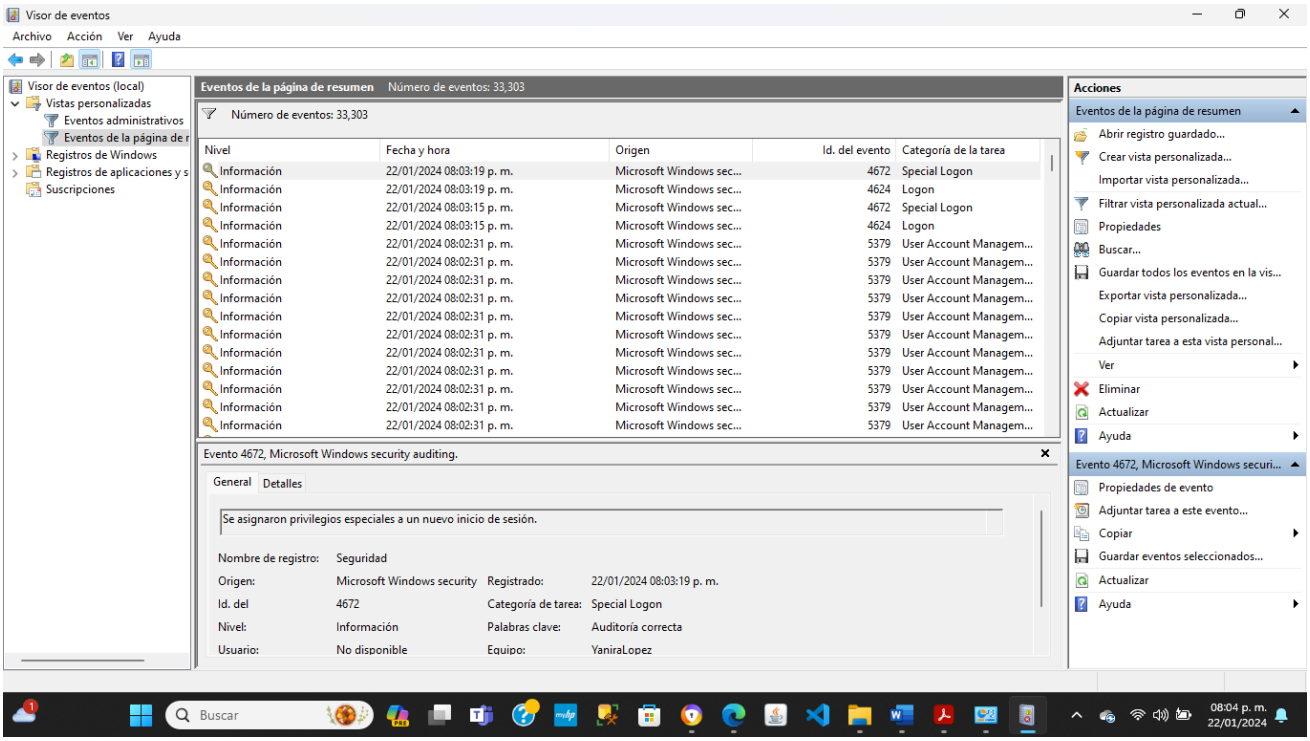
| Nivel | Fecha y hora | Origen | Id. del evento | Categoría de la tarea |
|---|---|---|---|---|
| Advertencia | 22/01/2024 07:35:10 p. m. | DeviceSetupManager | 201 | Ninguno |
| Advertencia | 22/01/2024 07:34:48 p. m. | DeviceSetupManager | 201 | Ninguno |
| Advertencia | 22/01/2024 07:29:26 p. m. | DeviceSetupManager | 201 | Ninguno |
| Advertencia | 22/01/2024 07:29:04 p. m. | DeviceSetupManager | 201 | Ninguno |
| Advertencia | 22/01/2024 07:28:13 p. m. | DeviceSetupManager | 201 | Ninguno |
| Advertencia | 22/01/2024 07:27:52 p. m. | DeviceSetupManager | 201 | Ninguno |
| Advertencia | 22/01/2024 07:27:28 p. m. | DeviceSetupManager | 201 | Ninguno |
| Error | 22/01/2024 07:26:45 p. m. | DeviceSetupManager | 131 | Ninguno |
| Advertencia | 22/01/2024 07:26:27 p. m. | DeviceSetupManager | 201 | Ninguno |
| Advertencia | 22/01/2024 07:26:06 p. m. | DeviceSetupManager | 201 | Ninguno |
| Advertencia | 22/01/2024 07:25:23 p. m. | DeviceSetupManager | 201 | Ninguno |
| Advertencia | 22/01/2024 07:24:49 p. m. | DeviceSetupManager | 201 | Ninguno |
| Advertencia | 22/01/2024 06:48:34 p. m. | DistributedCOM | 10016 | Ninguno |
| Advertencia | 22/01/2024 06:46:02 p. m. | DistributedCOM | 10016 | Ninguno |
| Advertencia | 22/01/2024 06:24:30 p. m. | DistributedCOM | 10016 | Ninguno |

Evento 201, DeviceSetupManager

No se pudo establecer una conexión al servicio Windows Metadata and Internet Services (WMIS).

Nombre de registro: Microsoft-Windows-DeviceSetupManager/Admin
Origen: DeviceSetupManager Registrado: 22/01/2024 07:35:10 p. m.
Id. del 201 Categoría de tarea: Ninguno
Nivel: Advertencia Palabras clave:
Usuario: SYSTEM Equipo: YaniraLopez

Aquí nos muestra los eventos de la página de resumen.



Eventos de la página de resumen Número de eventos: 33,303

Número de eventos: 33,303

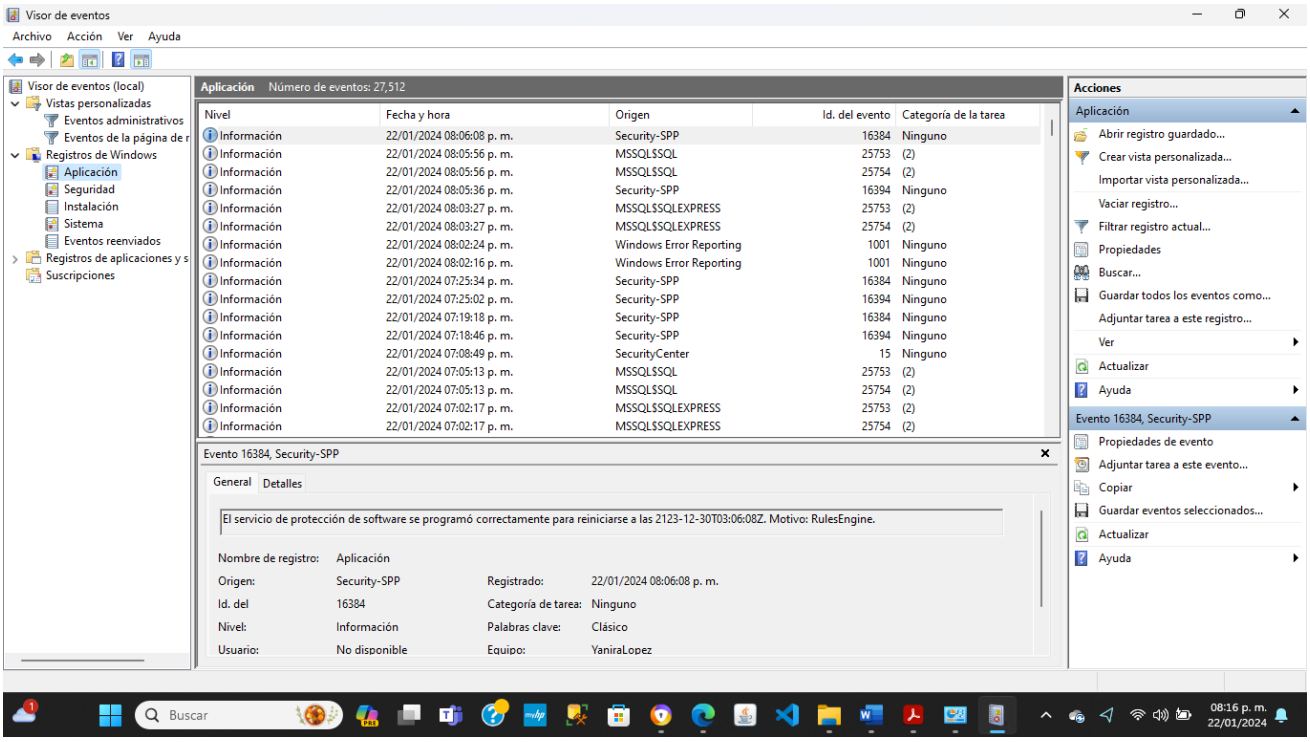
| Nivel | Fecha y hora | Origen | Id. del evento | Categoría de la tarea |
|---|---|---|---|---|
| Información | 22/01/2024 08:03:19 p. m. | Microsoft Windows sec... | 4672 | Special Logon |
| Información | 22/01/2024 08:03:19 p. m. | Microsoft Windows sec... | 4624 | Logon |
| Información | 22/01/2024 08:03:15 p. m. | Microsoft Windows sec... | 4672 | Special Logon |
| Información | 22/01/2024 08:03:15 p. m. | Microsoft Windows sec... | 4624 | Logon |
| Información | 22/01/2024 08:02:31 p. m. | Microsoft Windows sec... | 5379 | User Account Managem... |
| Información | 22/01/2024 08:02:31 p. m. | Microsoft Windows sec... | 5379 | User Account Managem... |
| Información | 22/01/2024 08:02:31 p. m. | Microsoft Windows sec... | 5379 | User Account Managem... |
| Información | 22/01/2024 08:02:31 p. m. | Microsoft Windows sec... | 5379 | User Account Managem... |
| Información | 22/01/2024 08:02:31 p. m. | Microsoft Windows sec... | 5379 | User Account Managem... |
| Información | 22/01/2024 08:02:31 p. m. | Microsoft Windows sec... | 5379 | User Account Managem... |
| Información | 22/01/2024 08:02:31 p. m. | Microsoft Windows sec... | 5379 | User Account Managem... |
| Información | 22/01/2024 08:02:31 p. m. | Microsoft Windows sec... | 5379 | User Account Managem... |
| Información | 22/01/2024 08:02:31 p. m. | Microsoft Windows sec... | 5379 | User Account Managem... |
| Información | 22/01/2024 08:02:31 p. m. | Microsoft Windows sec... | 5379 | User Account Managem... |
| Información | 22/01/2024 08:02:31 p. m. | Microsoft Windows sec... | 5379 | User Account Managem... |

Evento 4672, Microsoft Windows security auditing.

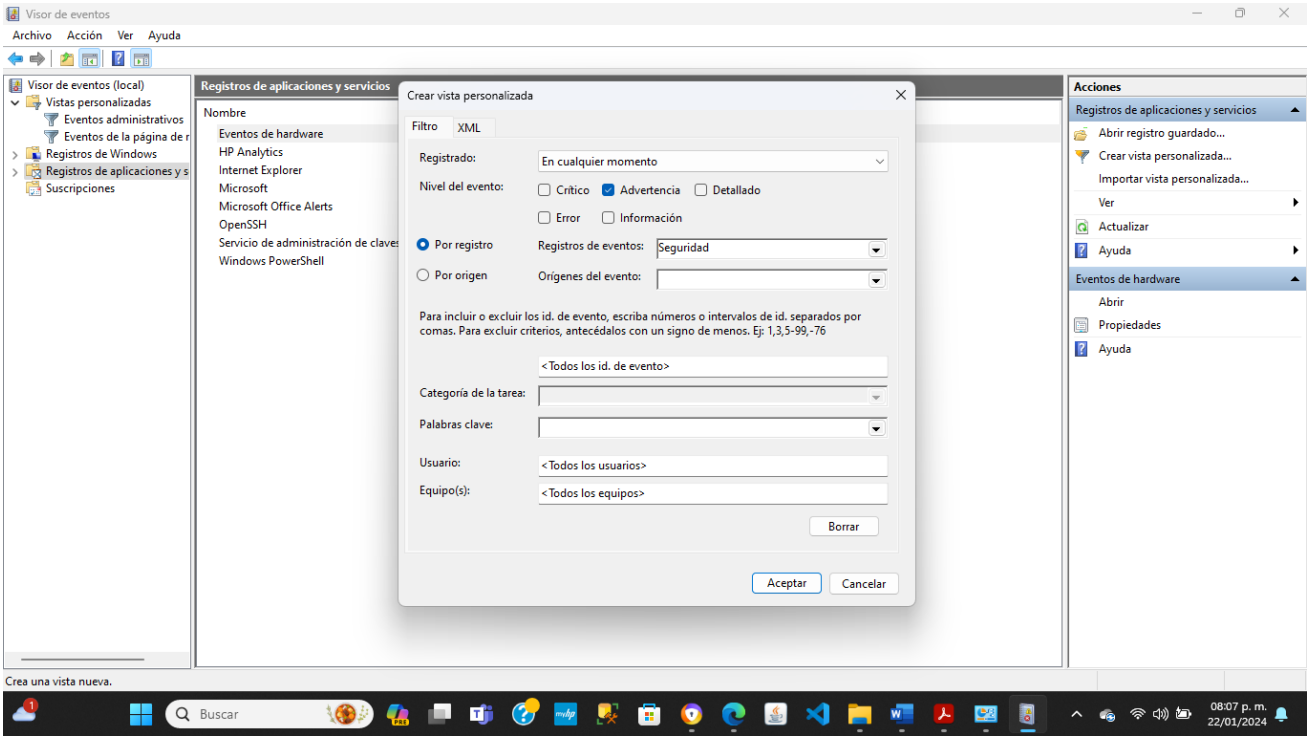
Se asignaron privilegios especiales a un nuevo inicio de sesión.

Nombre de registro: Seguridad
Origen: Microsoft Windows security Registrado: 22/01/2024 08:03:19 p. m.
Id. del 4672 Categoría de tarea: Special Logon
Nivel: Información Palabras clave: Auditoría correcta
Usuario: No disponible Equipo: YaniraLopez

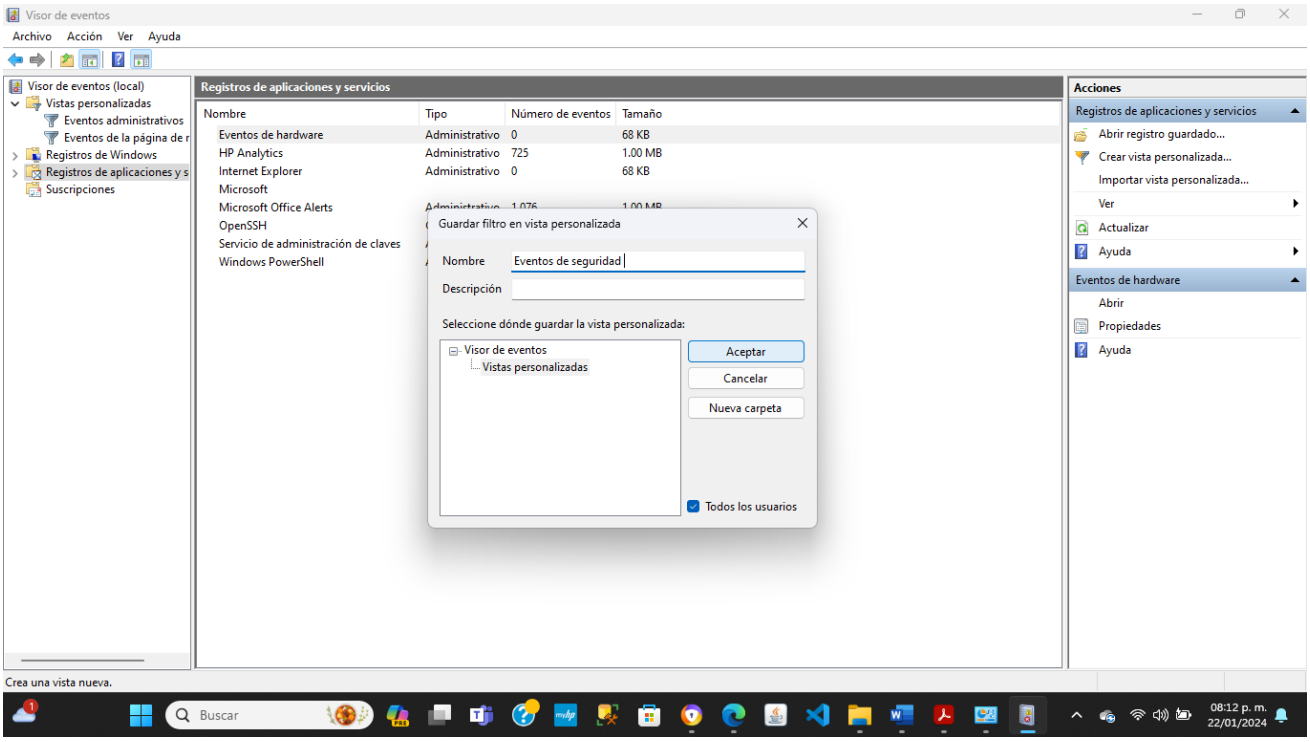
En seguida se muestra la auditorias de las aplicaciones.



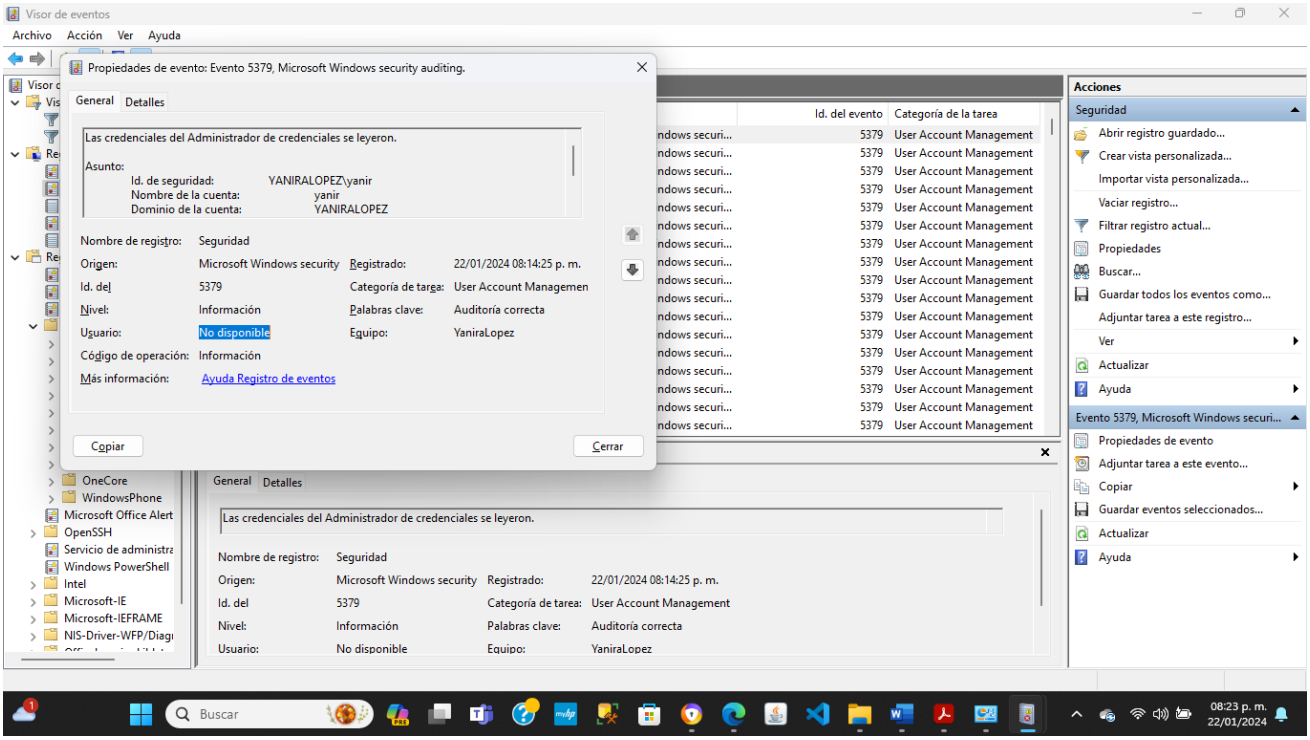

En la siguiente imagen nos muestra los filtros que podemos utilizar y seleccionamos en nivel que queremos filtrar.



Una vez que seleccionamos el evento que queremos filtrar lo podemos guardar.

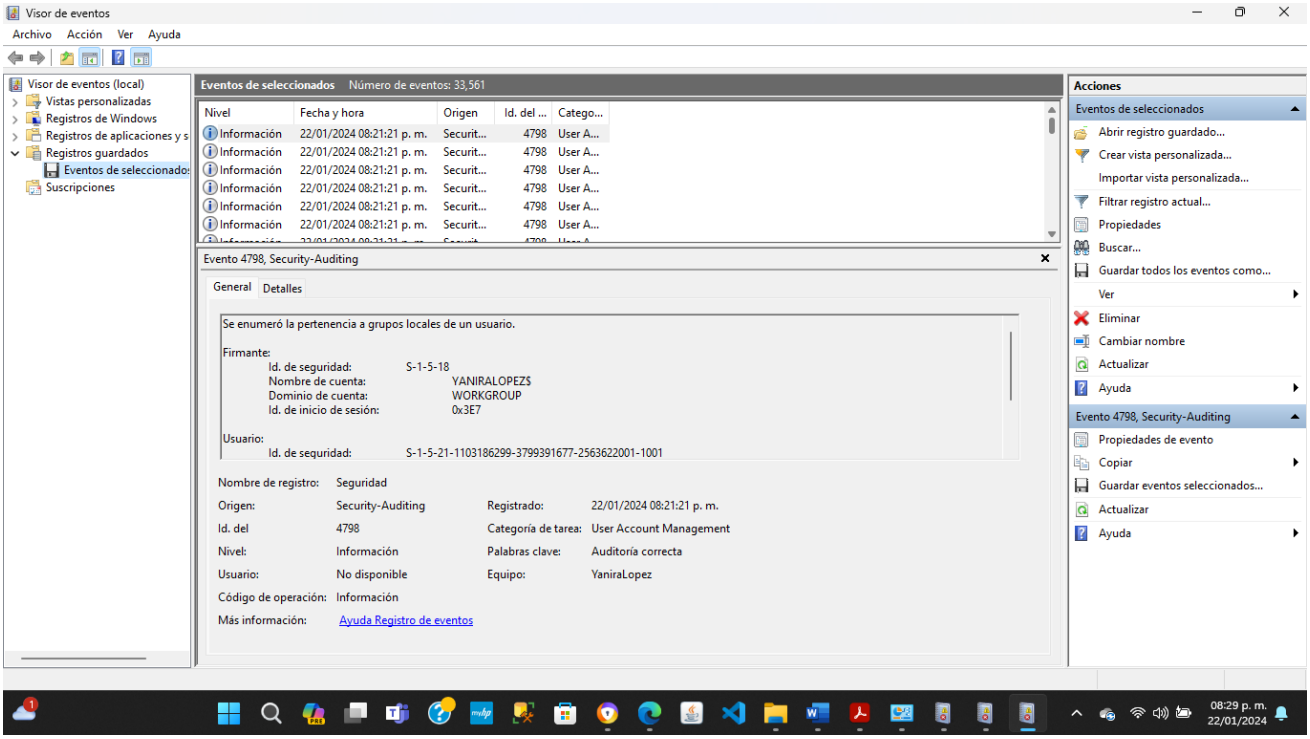



Además, nos muestra las licencias.

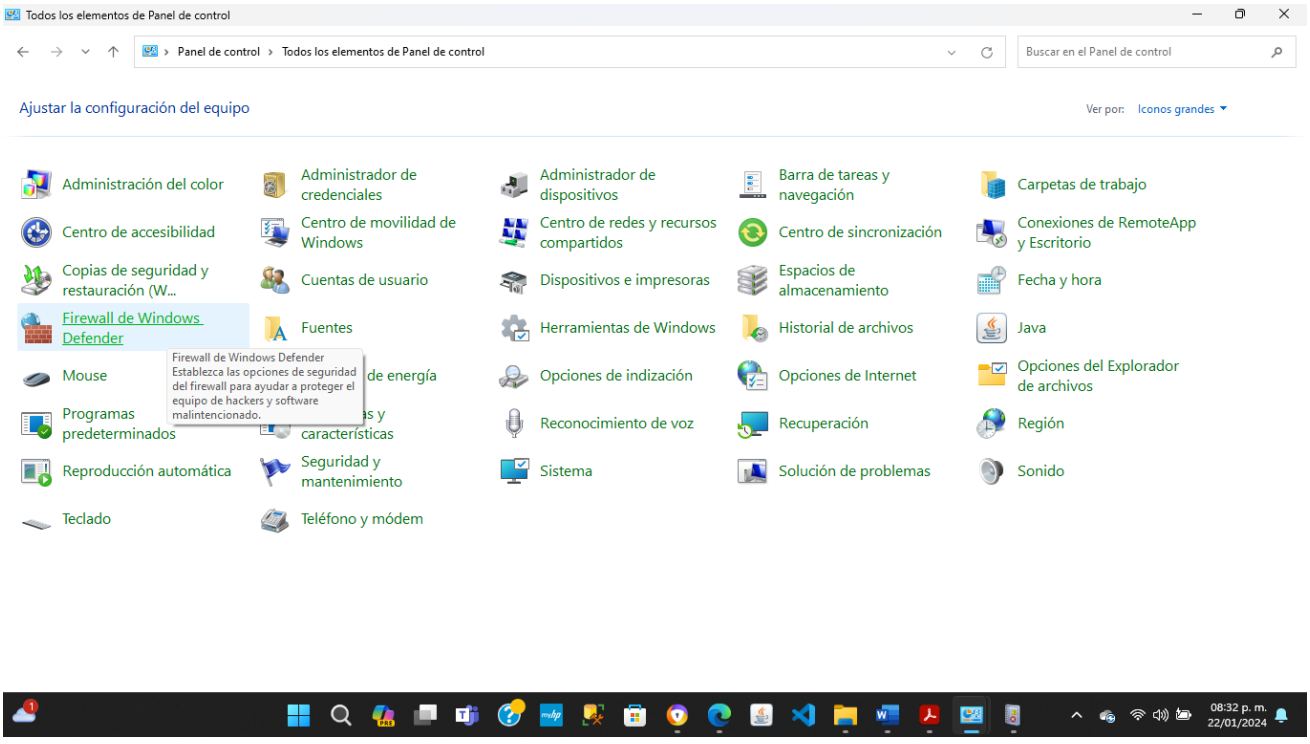


# Bitácora

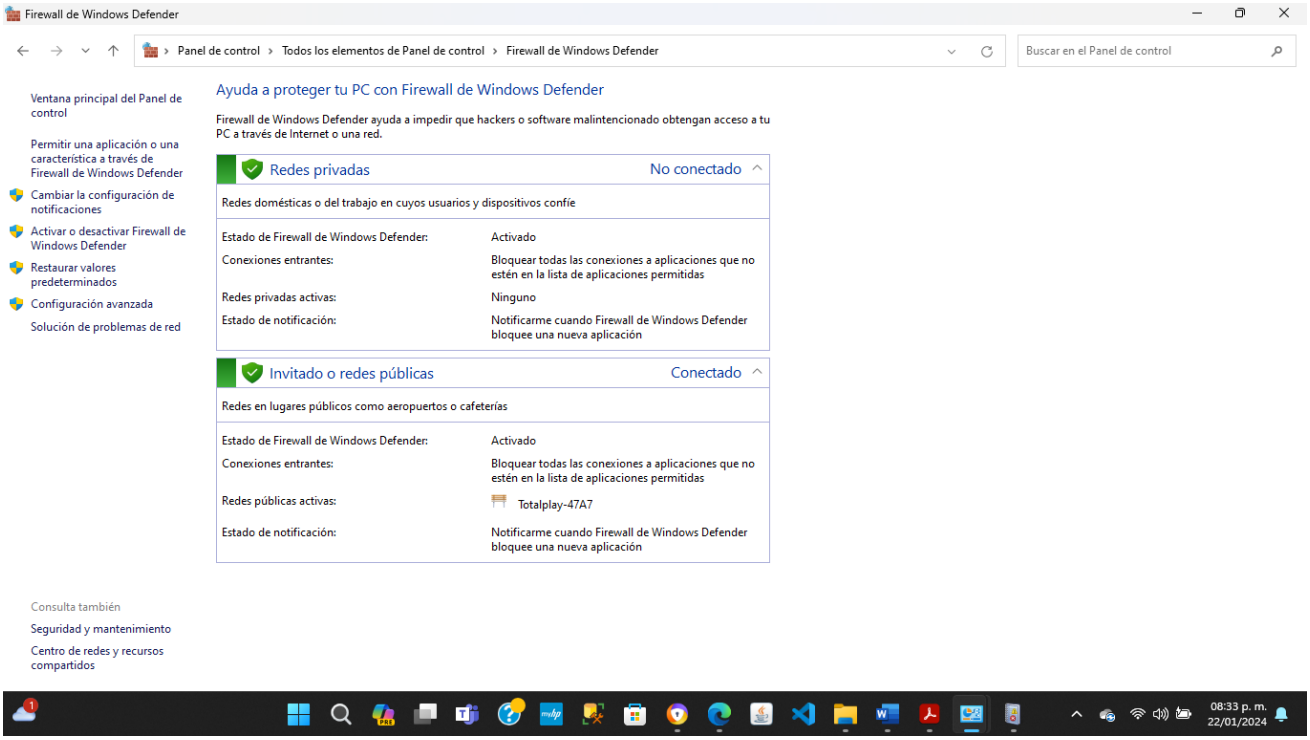
Aquí podemos observar el listado de los eventos guardados.




Aquí podemos ver las configuraciones del firewall de Windows.



Una vez seleccionado nos arroja la siguiente pantalla que nos muestra datos de la red a la que está conectado mi equipo.



# Importancia de seguridad (prevención, monitoreo, auditoría)

La importancia de la seguridad informática, abarcando la prevención de ataques de acceso, el monitoreo de red, así como la auditoría y gestión de bitácoras, es fundamental en la preservación de la integridad y confidencialidad de los sistemas.

La prevención de ataques de acceso se erige como la primera línea de defensa en la seguridad informática. Implementar medidas robustas, como autenticación multifactor y firewalls, no solo disuade a posibles intrusos, sino que también fortalece la resiliencia del sistema frente a amenazas cibernéticas. La limitación cuidadosa de privilegios y el establecimiento de políticas de acceso contribuyen significativamente a minimizar la exposición a riesgos, formando un escudo efectivo contra intrusiones no autorizadas.

El monitoreo de red actúa como una herramienta de vigilancia constante. La capacidad de supervisar el tráfico en tiempo real permite la identificación temprana de patrones inusuales o actividades maliciosas. Este enfoque proactivo es esencial para detectar y mitigar amenazas antes de que puedan causar daño significativo. La implementación de sistemas de monitoreo no solo proporciona una visión integral del entorno de red, sino que también asegura respuestas rápidas y precisas ante cualquier anomalía.

Las auditorías y bitácoras de acceso son esenciales para evaluar y fortalecer la seguridad de los sistemas. Las auditorías, realizadas desde el Panel de control o mediante herramientas especializadas, identifican posibles vulnerabilidades y validan licencias, contribuyendo a la prevención de futuros ataques. Por otro lado, las bitácoras actúan como registros detallados de cambios y actividades, no solo facilitando la detección temprana de incidentes, sino también cumpliendo con exigencias legales y normativas.

La prevención, monitoreo, auditoría y gestión de bitácoras de acceso forman un conjunto interconectado de estrategias esenciales para salvaguardar la integridad y confidencialidad de los sistemas informáticos. Su implementación coherente y efectiva constituye un pilar sólido en la defensa contra amenazas cibernéticas en un entorno digital dinámico y cada vez más complejo.

# Conclusión

En conclusión, la realización de la actividad centrada en auditorías y bitácoras demuestra ser de suma importancia tanto en el ámbito laboral como en la vida cotidiana. En el contexto laboral, estas prácticas se erigen como pilares fundamentales para garantizar la seguridad y la integridad de los sistemas informáticos. La identificación de vulnerabilidades a través de auditorías proporciona una capa de defensa crucial contra posibles amenazas cibernéticas.

La gestión adecuada de bitácoras, por su parte, no solo facilita la detección temprana de incidentes, sino que también se convierte en un respaldo invaluable para cumplir con requisitos legales y normativos. Estos registros detallados no solo sirven como evidencia en caso de investigaciones, sino que también contribuyen a mantener un entorno de trabajo seguro y conforme con las regulaciones vigentes.

En la vida cotidiana, la aplicación de estas prácticas se traduce en un mayor control y conciencia sobre la seguridad digital personal. La realización periódica de auditorías y la gestión de bitácoras permiten a los usuarios proteger sus datos y dispositivos, mitigando riesgos asociados con posibles amenazas en el entorno digital actual. En última instancia, la importancia de estas acciones radica en la creación de entornos informáticos robustos y seguros, tanto en el ámbito laboral como en la vida cotidiana.

# Referencias


Ingeniería en desarrollo de software. Universidad México Internacional. Recuperado el día 22 de enero de 2024, https://umi.edu.mx/coppel/IDS/mod/scorm/player.php

Global, A. (2024, 9 enero). *Video 1 DynaTrace Synthetic Monitoring Monitorización de disponibilidad y rendimiento de las aplicaciones web..mp4* [Vídeo]. Vimeo. https://vimeo.com/660530504/e6e2591340

Global, A. (2024b, enero 14). *Video 2 Auditoría de vulnerabilidades en la red con Nessus* [Vídeo]. Vimeo. https://vimeo.com/660530360/ad1982a98c

Global, A. (2024c, enero 21). *Video 4 Auditoría de bitácora desde Localhost.mp4* [Vídeo]. Vimeo. https://vimeo.com/660530684/03c3b00223

*Video conferencing, web conferencing, webinars, screen sharing*. (s. f.-b). Zoom. https://academiaglobal-mx.zoom.us/rec/play/00HdWT47PjrySwOhn7OOCVsAUT9TWpoJb204j6rrWqg9nGT8KzHTCXU5I-QUeFDyYDsKrR8_OR_TnY7G.aBukoMtiQ0Na79Bq?canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2FhskxhKCAtsDDb1qRoT3Ydx3Ktyt6YDcHTiWDfJWUpyP6OG0mhQJbbC7lj8TiV0o-.3lrWsIPZUd7VbHnt