Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad |3| Auditoría y Bitácora.

Seguridad Informática II.

Ingeniería en Desarrollo de Software.

TUTOR: Jessica Hernández Romero.

ALUMNO: Ramón Ernesto Valdez Felix.

FECHA: 08/06/2025.

Introducción.

En esta actividad final de la materia de Seguridad Informática II, realizar una auditoría de equipos de cómputo, ya sea de forma manual o con herramientas especializadas, es crucial para conocer a fondo los recursos instalados y gestionar eficazmente las licencias. Este proceso no solo permite identificar licencias existentes y faltantes, lo cual es fundamental para cumplir con los aspectos legales y regulatorios, sino que también ofrece una visión clara del estado de seguridad. Las auditorías y bitácoras son herramientas preventivas clave que ayudan a identificar posibles vulnerabilidades y ataques, permitiendo implementar medidas de protección adecuadas. Mantener un control constante mediante auditorías semanales de software, hardware, licencias y red, y conservar las bitácoras para un seguimiento detallado, es esencial para salvaguardar la información valiosa y fortalecer la seguridad general de la infraestructura tecnológica laboral o personal. Las auditorías y bitácoras semanales son cruciales aquí, funcionando como herramientas preventivas que facilitan la implementación proactiva de medidas de protección.

Descripción.

En esta actividad final de la materia de Seguridad Informática II, la auditoría de equipos de cómputo emerge como una actividad primordial. Ya sea de forma manual o empleando herramientas especializadas, este proceso es crucial para comprender los recursos instalados y gestionar de manera eficiente las licencias de software. Su importancia radica no solo en la identificación de licencias existentes y faltantes aspecto vital para cumplir con las normativas legales y regulatorias sino también en ofrecer una visión clara del estado de seguridad de la infraestructura.

Las auditorías y bitácoras actúan como herramientas preventivas esenciales, permitiendo detectar vulnerabilidades y anticipar posibles ataques, lo que facilita la implementación de medidas de protección adecuadas. Para salvaguardar la información valiosa y robustecer la seguridad informática, es indispensable mantener un control constante a través de auditorías semanales de software, hardware,

licencias y red, y conservar meticulosamente las bitácoras para un seguimiento detallado.

Justificación.

Esta actividad final de la materia Seguridad Informática II, La auditoría de equipos de cómputo en Seguridad Informática es indispensable. Primero, garantiza la legalidad operativa al verificar y gestionar licencias de software, asegurando el cumplimiento normativo y evitando sanciones. Segundo, ofrece una visión integral de la seguridad, permitiendo identificar vulnerabilidades y anticipar amenazas de manera proactiva. Las auditorías y bitácoras semanales son cruciales, funcionando como herramientas preventivas que facilitan la implementación oportuna de medidas de protección.

Este control constante no solo salvaguarda la información valiosa, un activo crítico para cualquier organización, sino que también optimiza la infraestructura tecnológica. Al asegurar que cada componente, desde el hardware hasta la red, opere de forma segura y eficiente, la auditoría se convierte en un pilar para fortalecer la postura de seguridad, garantizar la integridad del sistema y proteger los datos frente a un panorama de amenazas en constante evolución.

Estos puntos adicionales a utilizar en la justificación para la realizar de la documentación de esta actividad que son los siguientes:

- PDF de está actividad en el portafolio GitHub.
- Anexa link de GitHub en documento.
- Utilizar la herramienta visor de eventos.

Desarrollo:

En estas la Actividad final: auditoría y bitácora, nos enfocaremos en una serie de pasos clave para fortalecer nuestras habilidades en seguridad informática. Iniciaremos con la auditoría del visor de evento de S.O. Windows 10 designada para esta actividad. Luego, documentados el resultado, generando

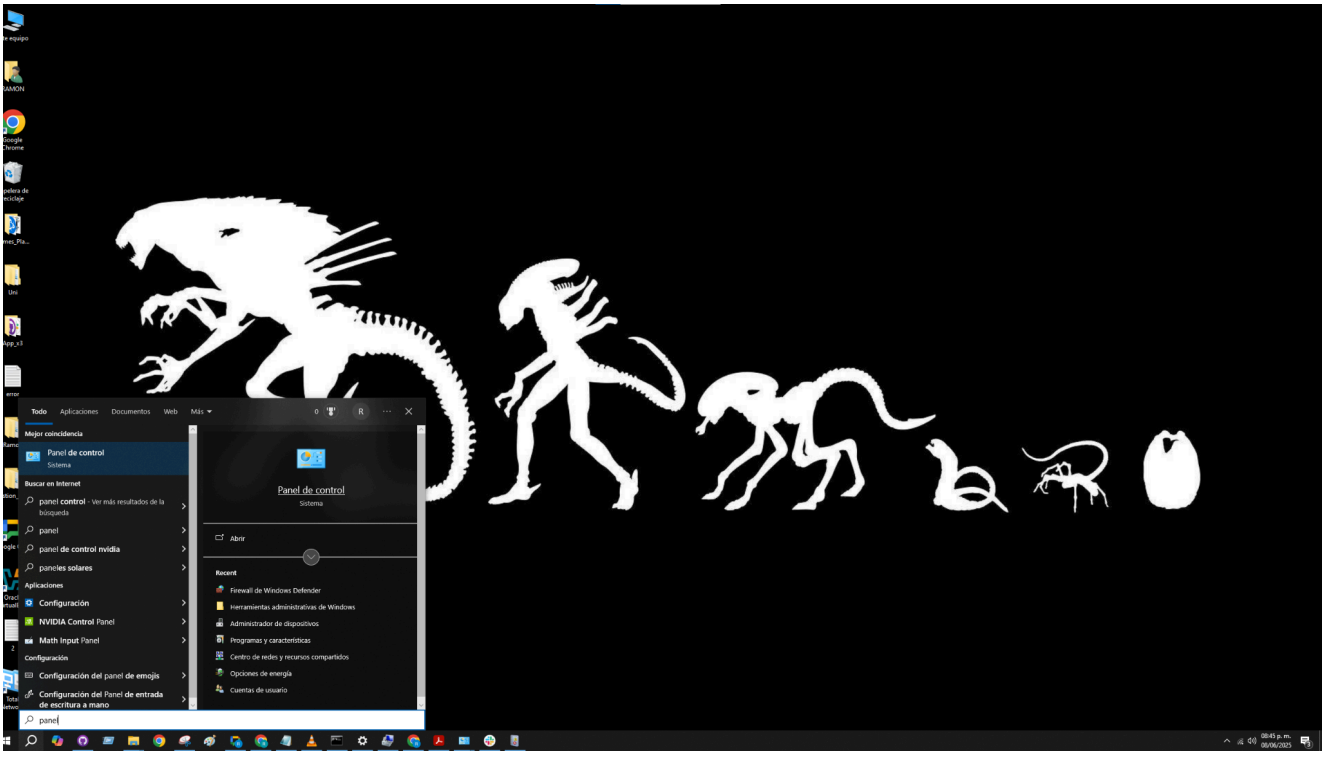
información detallada del equipo de computo. Este proceso no solo nos permitirá mejorar la seguridad de nuestra infraestructura, sino que también nos brindará habilidades prácticas esenciales para el manejo de amenazas cibernéticas.

Link: GitHub

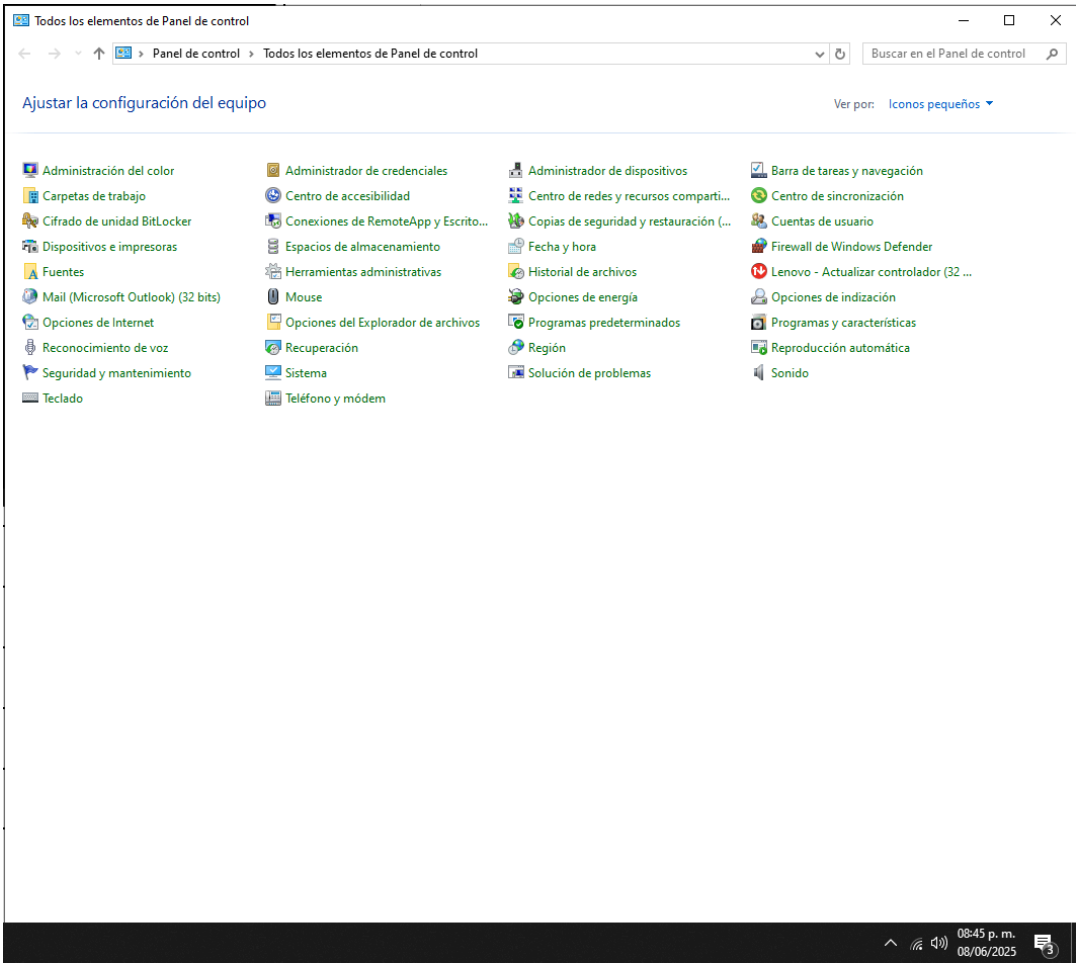
Auditoría y Bitácora:

Auditoría de equipo:

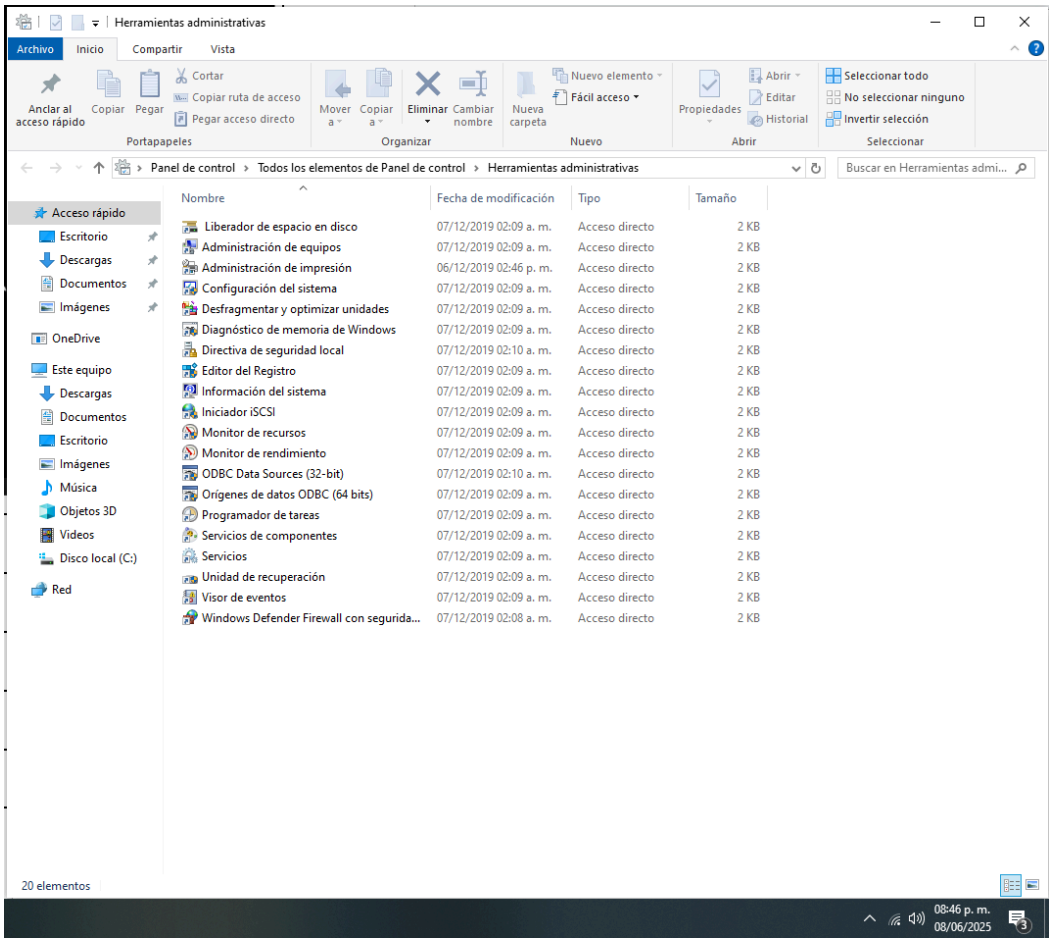
En este punto de la actividad mostraremos cómo llegar a la herramienta de eventos del S.O. Windows 10, donde se muestran los eventos de las actividades realizadas en el equipo de cómputo.

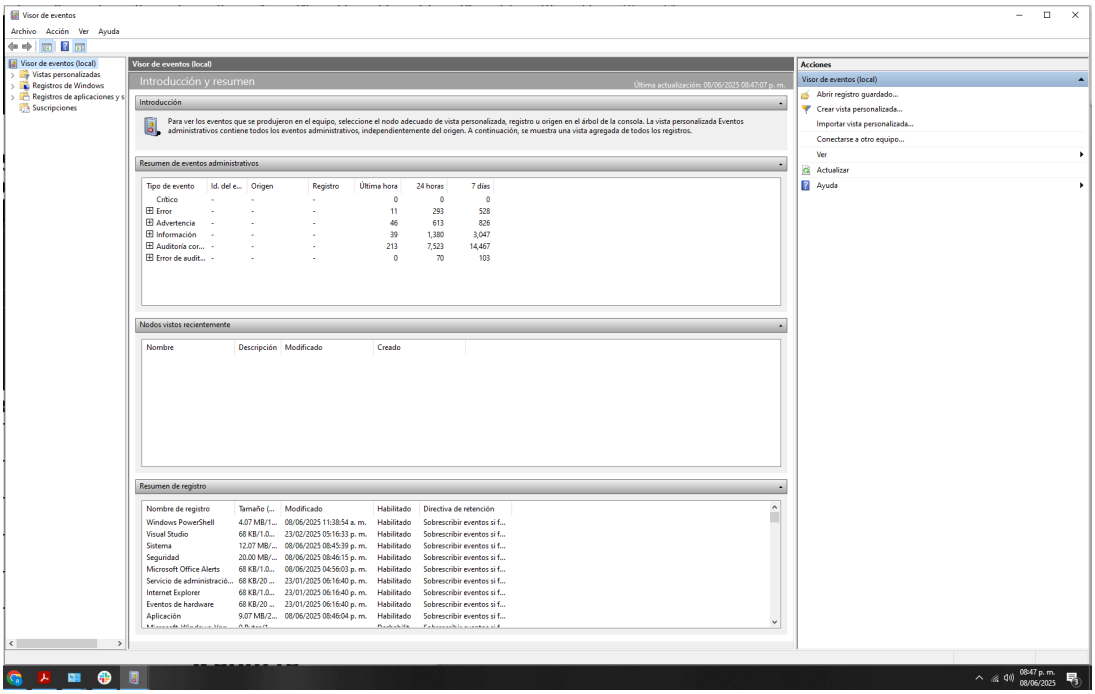


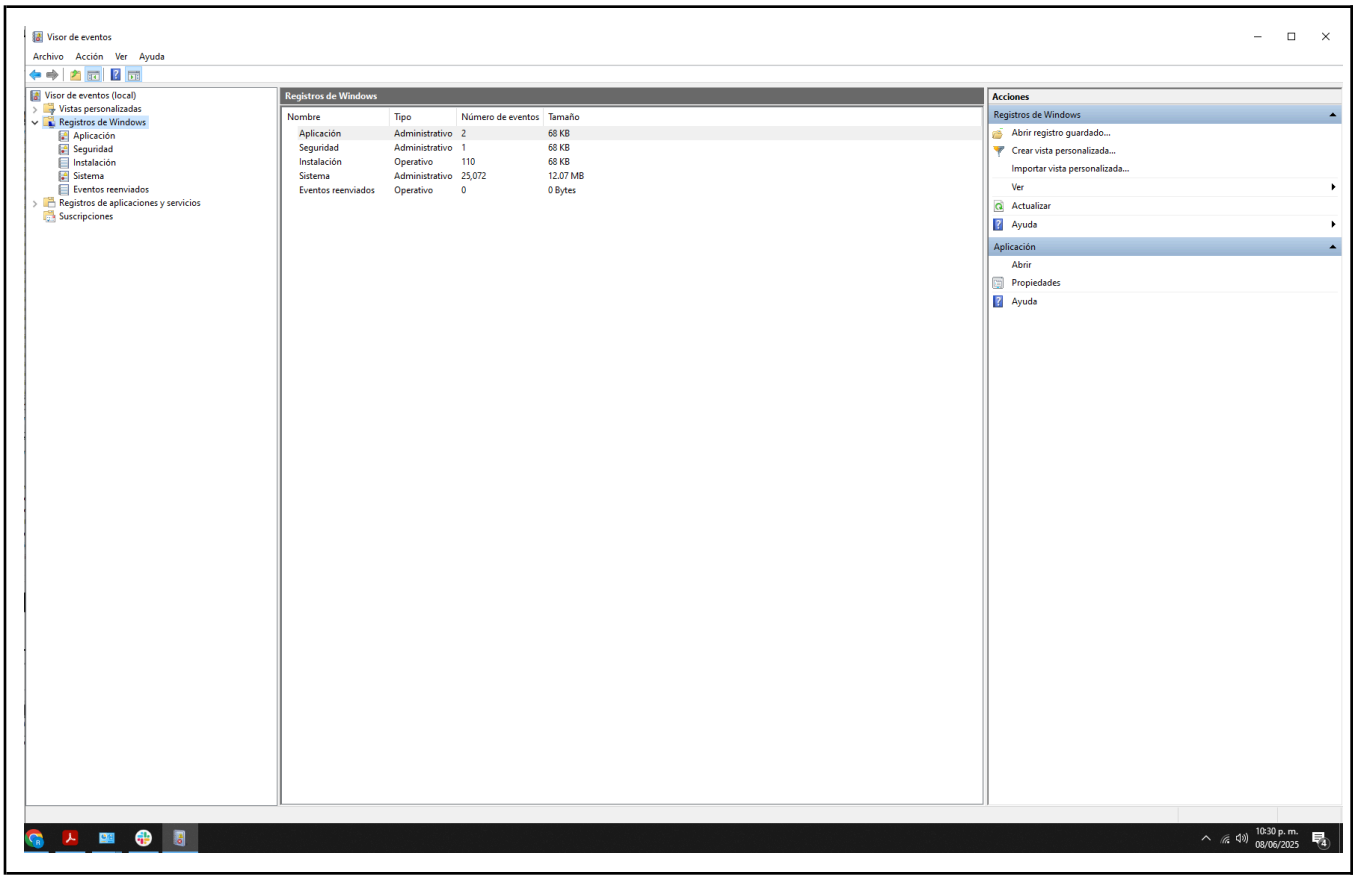
6


Todos los elementos de Panel de control
Panel de control › Todos los elementos de Panel de control
Buscar en el Panel de control
Ajustar la configuración del equipo
Ver por: Iconos pequeños
Administración del color
Administrador de credenciales
Administrador de dispositivos
Barra de tareas y navegación
Carpetas de trabajo
Centro de accesibilidad
Centro de redes y recursos compartí...
Centro de sincronización
Cifrado de unidad BitLocker
Conexiones de RemoteApp y Escrito...
Copias de seguridad y restauración (...
Cuentas de usuario
Dispositivos e impresoras
Espacios de almacenamiento
Fecha y hora
Firewall de Windows Defender
Fuentes
Herramientas administrativas
Historial de archivos
Lenovo - Actualizar controlador (32 ...
Mail (Microsoft Outlook) (32 bits)
Mouse
Opciones de energía
Opciones de indización
Opciones de Internet
Opciones del Explorador de archivos
Programas predeterminados
Programas y características
Reconocimiento de voz
Recuperación
Región
Reproducción automática
Seguridad y mantenimiento
Sistema
Solución de problemas
Sonido
Teclado
Teléfono y módem
08:45 p. m.
08/06/2025

7

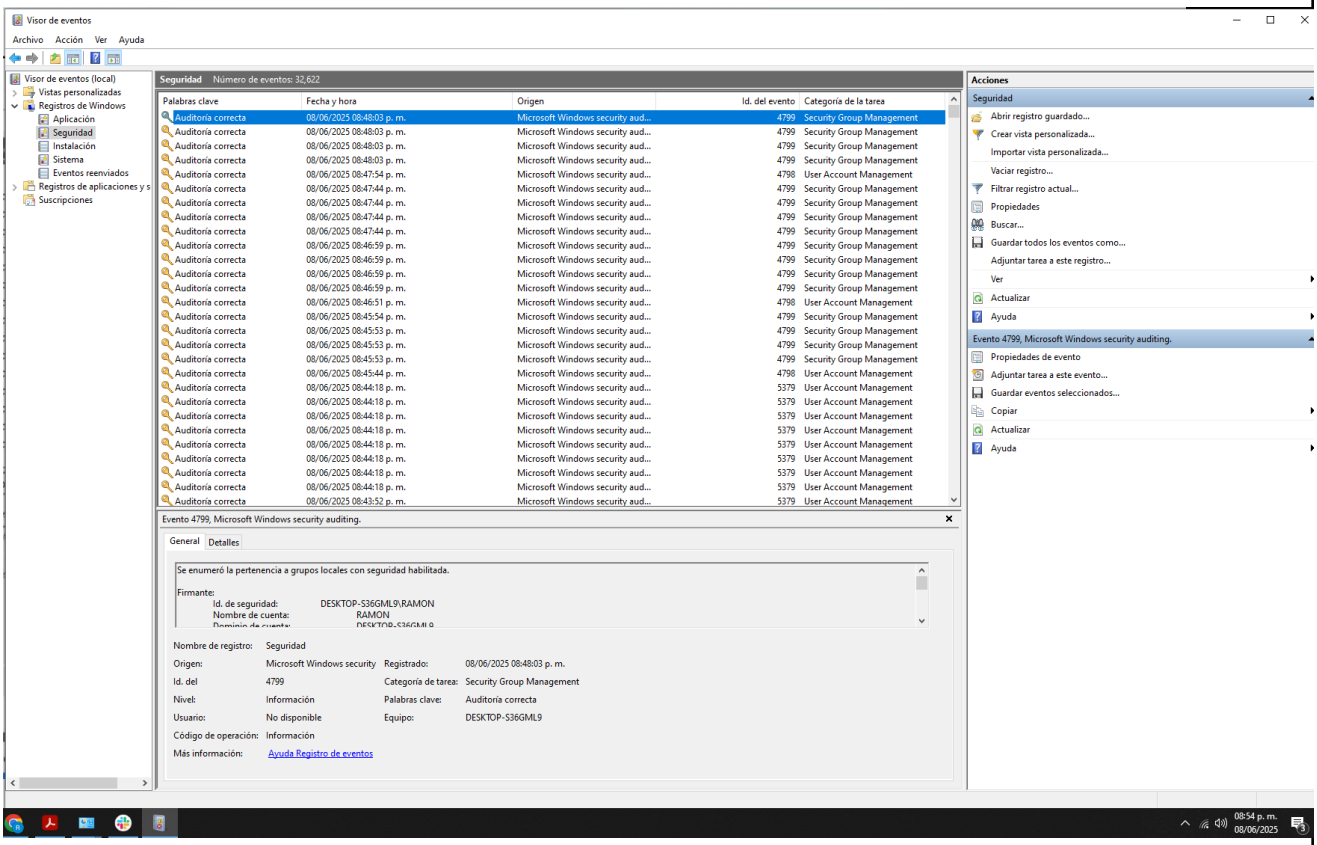

Herramientas administrativas
Archivo
Inicio
Compartir
Vista
Anclar al acceso rápido
Copiar
Pegar
Cortar
Copiar ruta de acceso
Pegar acceso directo
Portapapeles
Mover a
Copiar a
Eliminar
Cambiar nombre
Organizar
Nueva carpeta
Nuevo elemento
Fácil acceso
Nuevo
Propiedades
Abrir
Editar
Historial
Abrir
Seleccionar todo
No seleccionar ninguno
Invertir selección
Seleccionar
Panel de control › Todos los elementos de Panel de control › Herramientas administrativas
Buscar en Herramientas admi...
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
OneDrive
Este equipo
Descargas
Documentos
Escritorio
Imágenes
Música
Objetos 3D
Videos
Disco local (C:)
Red
Nombre
Fecha de modificación
Tipo
Tamaño
Liberador de espacio en disco 07/12/2019 02:09 a. m. Acceso directo 2 KB
Administración de equipos 07/12/2019 02:09 a. m. Acceso directo 2 KB
Administración de impresión 06/12/2019 02:46 p. m. Acceso directo 2 KB
Configuración del sistema 07/12/2019 02:09 a. m. Acceso directo 2 KB
Desfragmentar y optimizar unidades 07/12/2019 02:09 a. m. Acceso directo 2 KB
Diagnóstico de memoria de Windows 07/12/2019 02:09 a. m. Acceso directo 2 KB
Directiva de seguridad local 07/12/2019 02:10 a. m. Acceso directo 2 KB
Editor del Registro 07/12/2019 02:09 a. m. Acceso directo 2 KB
Información del sistema 07/12/2019 02:09 a. m. Acceso directo 2 KB
Iniciador iSCSI 07/12/2019 02:09 a. m. Acceso directo 2 KB
Monitor de recursos 07/12/2019 02:09 a. m. Acceso directo 2 KB
Monitor de rendimiento 07/12/2019 02:09 a. m. Acceso directo 2 KB
ODBC Data Sources (32-bit) 07/12/2019 02:10 a. m. Acceso directo 2 KB
Orígenes de datos ODBC (64 bits) 07/12/2019 02:09 a. m. Acceso directo 2 KB
Programador de tareas 07/12/2019 02:09 a. m. Acceso directo 2 KB
Servicios de componentes 07/12/2019 02:09 a. m. Acceso directo 2 KB
Servicios 07/12/2019 02:09 a. m. Acceso directo 2 KB
Unidad de recuperación 07/12/2019 02:09 a. m. Acceso directo 2 KB
Visor de eventos 07/12/2019 02:09 a. m. Acceso directo 2 KB
Windows Defender Firewall con seguridad... 07/12/2019 02:08 a. m. Acceso directo 2 KB
20 elementos
08:46 p. m.
08/06/2025


Visor de eventos
Archivo
Acción
Ver
Ayuda
Visor de eventos (local)
Vistas personalizadas
Registros de Windows
Registros de aplicaciones y s
Suscripciones
Introducción y resumen
Introducción
Para ver los eventos que se produjeron en el equipo, seleccione el nodo adecuado de vista personalizada, registro u origen en el árbol de la consola. La vista personalizada Eventos administrativos contiene todos los eventos administrativos, independientemente del origen. A continuación, se muestra una vista agregada de todos los registros.
Resumen de eventos administrativos
Tipo de evento
Id. del e...
Origen
Registro
Última hora
24 horas
7 días
Crítico
Error
Advertencia
Información
Auditoría con...
Error de audit...
Nodos vistos recientemente
Nombre
Descripción
Modificado
Creado
Resumen de registro
Nombre de registro
Tamaño (...
Modificado
Habilitado
Directiva de retención
Windows PowerShell
Visual Studio
Sistema
Seguridad
Microsoft Office Alerts
Servicio de administració...
Internet Explorer
Eventos de hardware
Aplicación
Acciones
Visor de eventos (local)
Abrir registro guardado...
Crear vista personalizada...
Importar vista personalizada...
Conectarse a otro equipo...
Ver
Actualizar
Ayuda



Bitácora.

En este punto de la actividad realizaremos la bitácora de seguridad donde se muestran los eventos de cada activador de la categoría de seguridad en la cual buscamos en el filtro de eventos todos los eventos críticos y error de los eventos de seguridad así como también los eventos de sistema, esto nos puede indicar si se está realizando algún ataque o un mal funcionamiento de tu equipo de computo.



Seguridad Número de eventos: 32,622

Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Auditoría correcta	08/06/2025 08:48:03 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:48:03 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:48:03 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:48:03 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:47:54 p. m.	Microsoft Windows security aud...	4798	User Account Management
Auditoría correcta	08/06/2025 08:47:44 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:47:44 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:47:44 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:47:44 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:46:59 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:46:59 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:46:59 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:46:59 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:46:51 p. m.	Microsoft Windows security aud...	4798	User Account Management
Auditoría correcta	08/06/2025 08:45:54 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:45:53 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:45:53 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:45:53 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:45:44 p. m.	Microsoft Windows security aud...	4798	User Account Management
Auditoría correcta	08/06/2025 08:44:18 p. m.	Microsoft Windows security aud...	5379	User Account Management
Auditoría correcta	08/06/2025 08:44:18 p. m.	Microsoft Windows security aud...	5379	User Account Management
Auditoría correcta	08/06/2025 08:44:18 p. m.	Microsoft Windows security aud...	5379	User Account Management
Auditoría correcta	08/06/2025 08:44:18 p. m.	Microsoft Windows security aud...	5379	User Account Management
Auditoría correcta	08/06/2025 08:44:18 p. m.	Microsoft Windows security aud...	5379	User Account Management
Auditoría correcta	08/06/2025 08:44:18 p. m.	Microsoft Windows security aud...	5379	User Account Management
Auditoría correcta	08/06/2025 08:44:18 p. m.	Microsoft Windows security aud...	5379	User Account Management
Auditoría correcta	08/06/2025 08:44:18 p. m.	Microsoft Windows security aud...	5379	User Account Management
Auditoría correcta	08/06/2025 08:43:52 p. m.	Microsoft Windows security aud...	5379	User Account Management

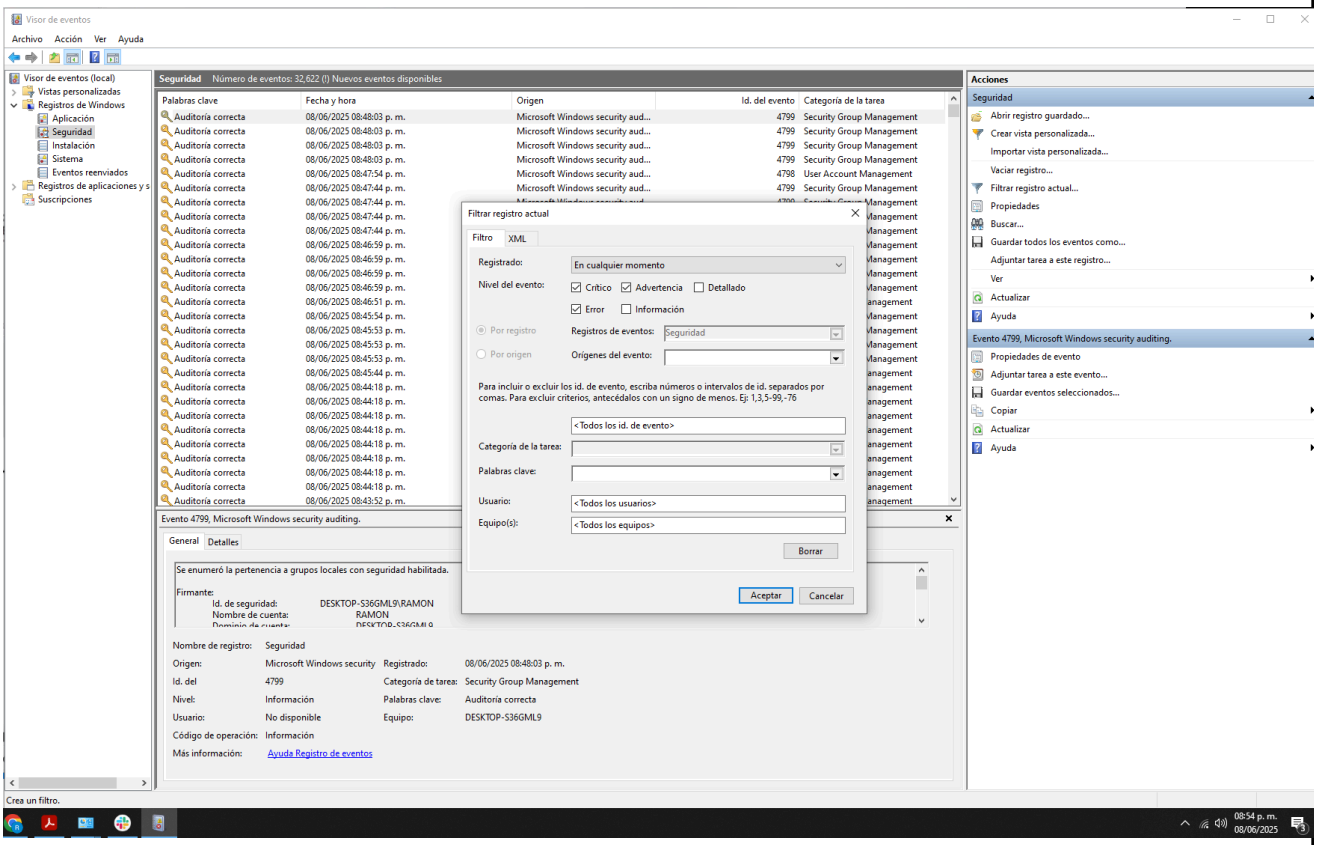
Evento 4799, Microsoft Windows security auditing.

General | Detalles

Se enumeró la pertenencia a grupos locales con seguridad habilitada.

Firmante:
Id. de seguridad: DESKTOP-S36GML9\RAMON
Nombre de cuenta: RAMON
Dominio de cuenta: DESKTOP-S36GML9

Nombre de registro: Seguridad
Origen: Microsoft Windows security
Registrado: 08/06/2025 08:48:03 p. m.
Id. del: 4799
Categoría de tarea: Security Group Management
Nivel: Información
Palabras clave: Auditoría correcta
Usuario: No disponible
Equipo: DESKTOP-S36GML9
Código de operación: Información
Más información: Ayuda Registro de eventos



Seguridad Número de eventos: 32,622 (!) Nuevos eventos disponibles

Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Auditoría correcta	08/06/2025 08:48:03 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:48:03 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:48:03 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:48:03 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:47:54 p. m.	Microsoft Windows security aud...	4798	User Account Management
Auditoría correcta	08/06/2025 08:47:44 p. m.	Microsoft Windows security aud...	4799	Security Group Management
Auditoría correcta	08/06/2025 08:47:44 p. m.			
Auditoría correcta	08/06/2025 08:47:44 p. m.			
Auditoría correcta	08/06/2025 08:47:44 p. m.			
Auditoría correcta	08/06/2025 08:46:59 p. m.			
Auditoría correcta	08/06/2025 08:46:59 p. m.			
Auditoría correcta	08/06/2025 08:46:59 p. m.			
Auditoría correcta	08/06/2025 08:46:59 p. m.			
Auditoría correcta	08/06/2025 08:46:51 p. m.			
Auditoría correcta	08/06/2025 08:45:54 p. m.			
Auditoría correcta	08/06/2025 08:45:53 p. m.			
Auditoría correcta	08/06/2025 08:45:53 p. m.			
Auditoría correcta	08/06/2025 08:45:53 p. m.			
Auditoría correcta	08/06/2025 08:45:44 p. m.			
Auditoría correcta	08/06/2025 08:44:18 p. m.			
Auditoría correcta	08/06/2025 08:44:18 p. m.			
Auditoría correcta	08/06/2025 08:44:18 p. m.			
Auditoría correcta	08/06/2025 08:44:18 p. m.			
Auditoría correcta	08/06/2025 08:44:18 p. m.			
Auditoría correcta	08/06/2025 08:44:18 p. m.			
Auditoría correcta	08/06/2025 08:44:18 p. m.			
Auditoría correcta	08/06/2025 08:44:18 p. m.			
Auditoría correcta	08/06/2025 08:43:52 p. m.			

Filtrar registro actual

Registrado: En cualquier momento

Nivel del evento: ☑ Crítico ☑ Advertencia ☐ Detallado ☑ Error ☐ Información

● Por registro — Registros de eventos: Seguridad

○ Por origen — Orígenes del evento:

Para incluir o excluir los id. de evento, escriba números o intervalos de id. separados por comas. Para excluir criterios, antecédalos con un signo de menos. Ej: 1,3,5-99,-76

<Todos los id. de evento>

Categoría de la tarea:

Palabras clave:

Usuario: <Todos los usuarios>

Equipo(s): <Todos los equipos>

Evento 4799, Microsoft Windows security auditing.

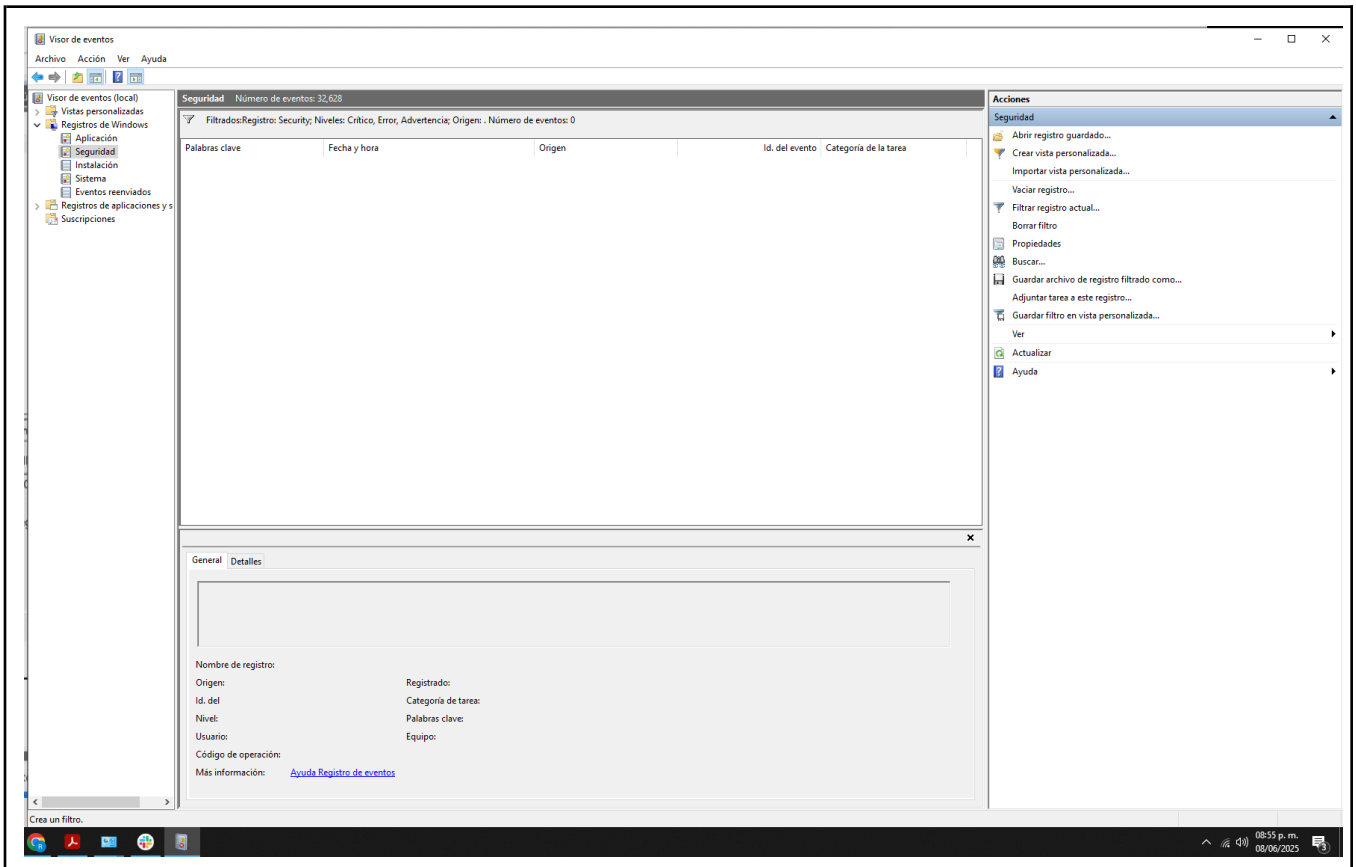
General | Detalles

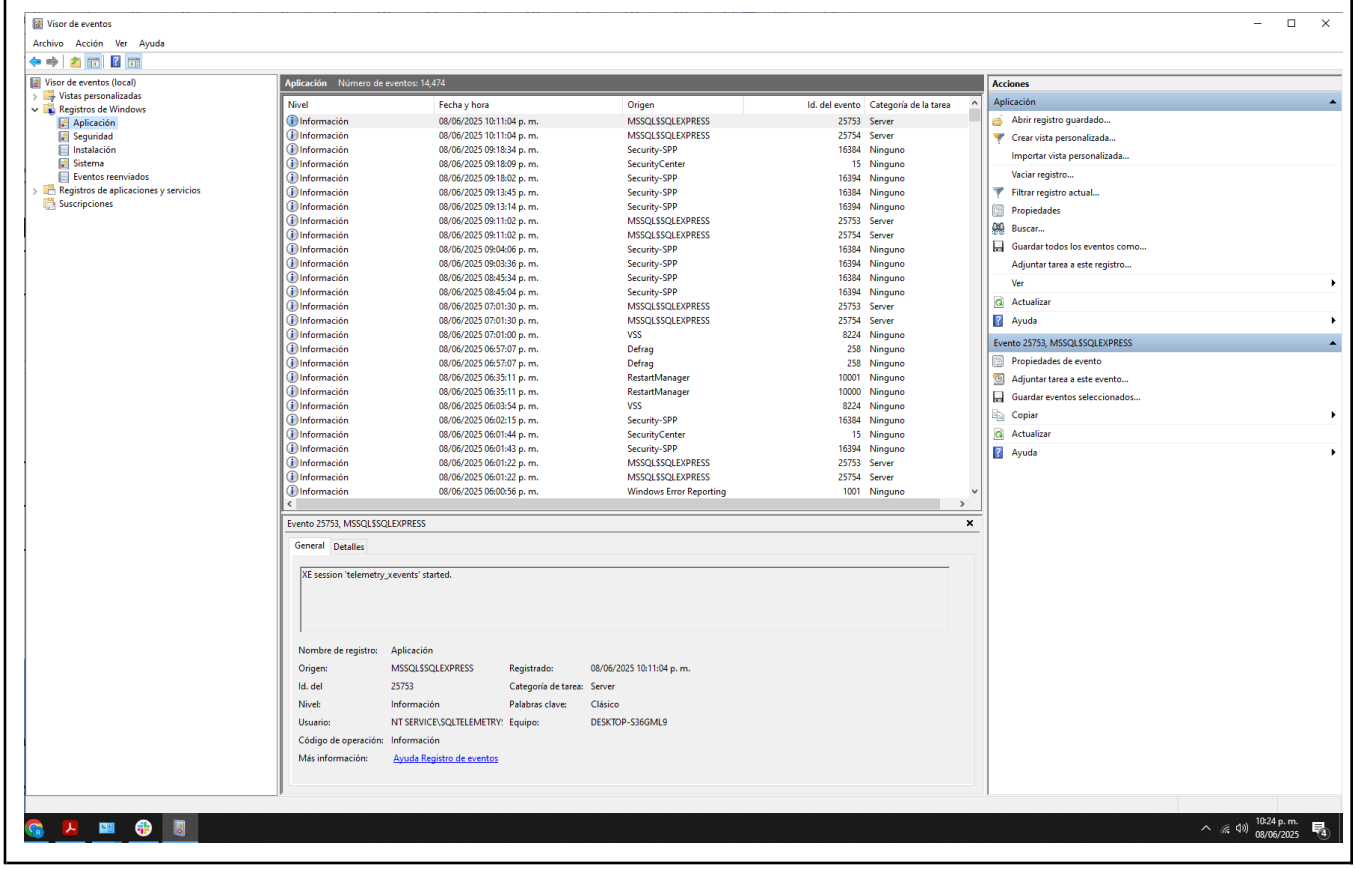
Se enumeró la pertenencia a grupos locales con seguridad habilitada.

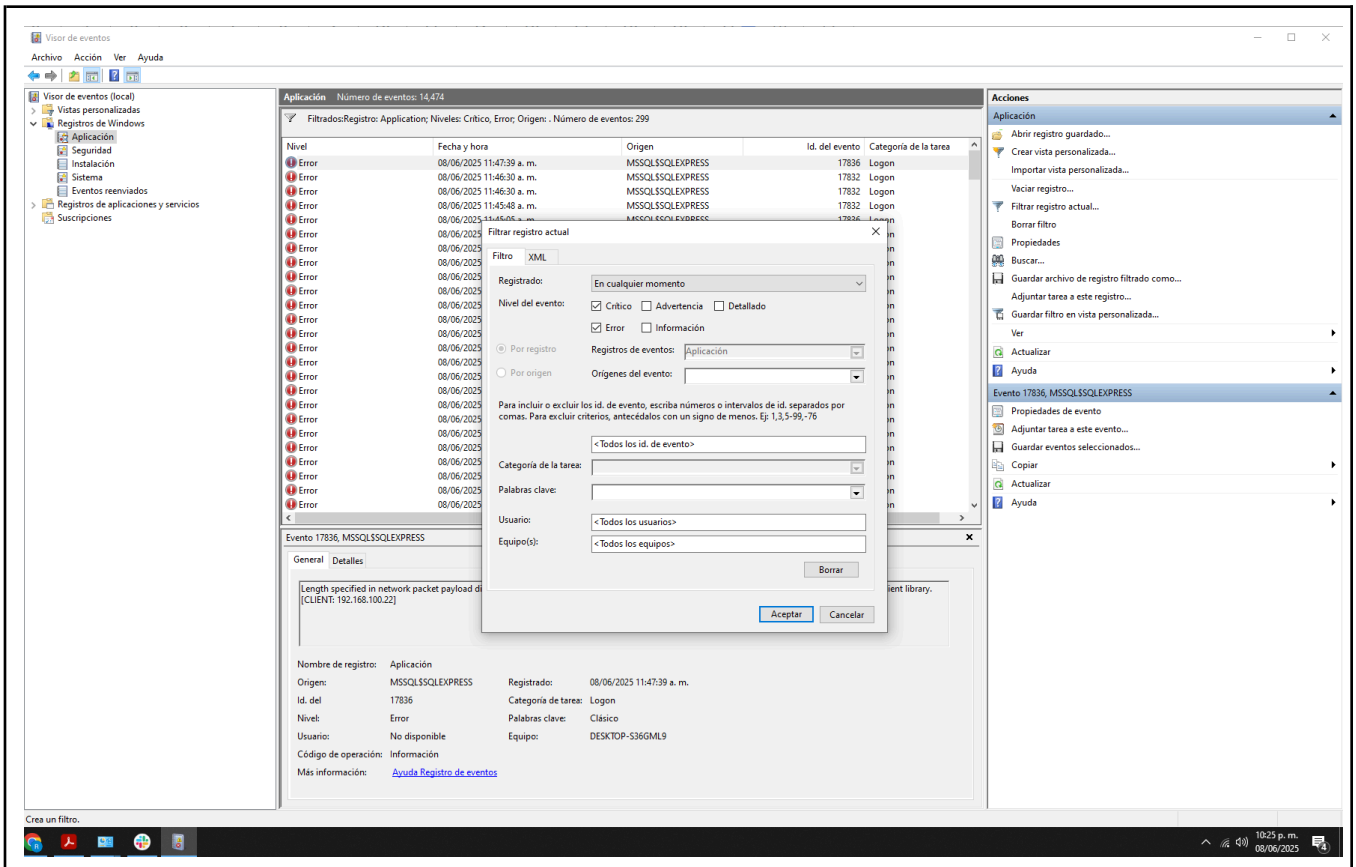
Firmante:
Id. de seguridad: DESKTOP-S36GML9\RAMON
Nombre de cuenta: RAMON
Dominio de cuenta: DESKTOP-S36GML9

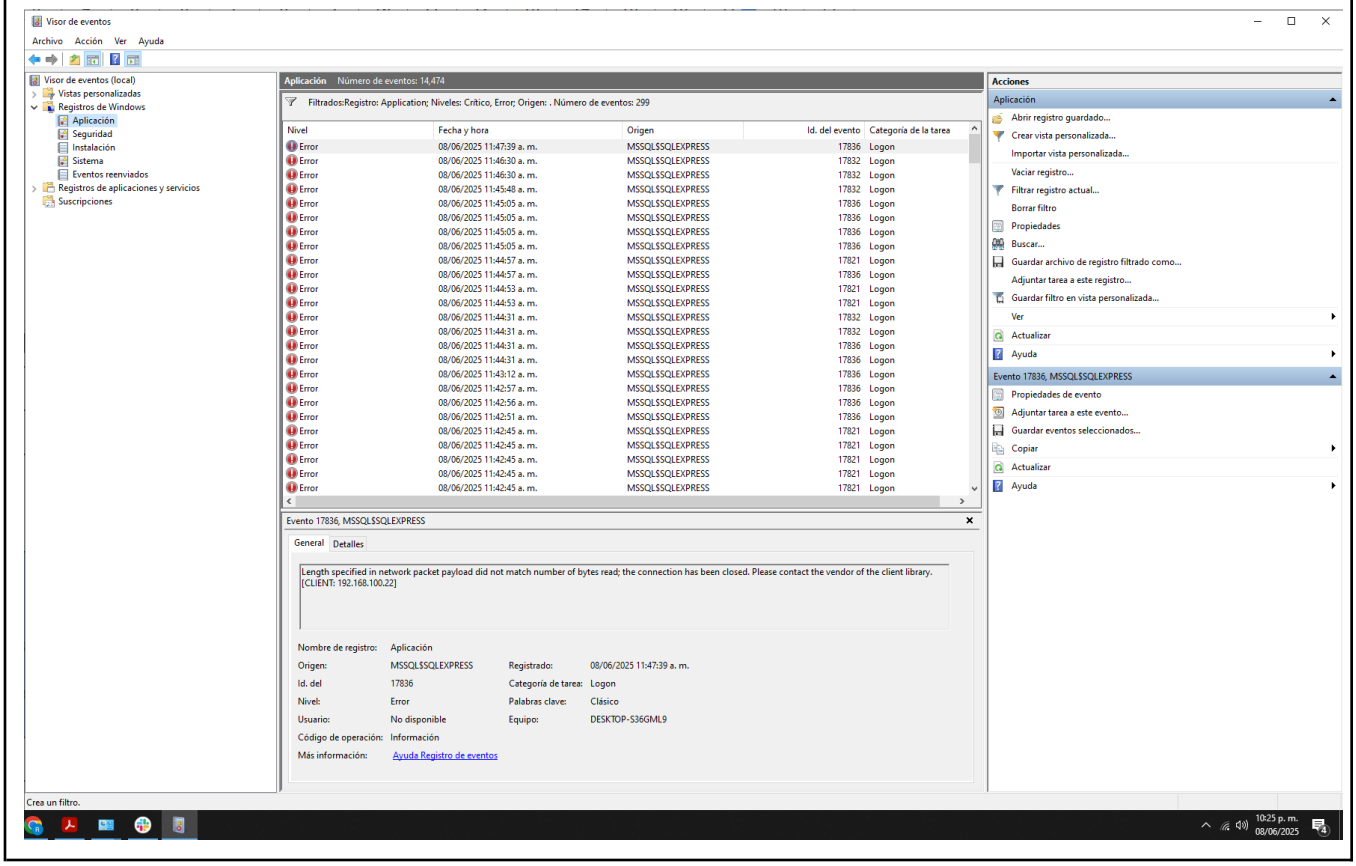
Nombre de registro: Seguridad
Origen: Microsoft Windows security
Registrado: 08/06/2025 08:48:03 p. m.
Id. del: 4799
Categoría de tarea: Security Group Management
Nivel: Información
Palabras clave: Auditoría correcta
Usuario: No disponible
Equipo: DESKTOP-S36GML9
Código de operación: Información
Más información: Ayuda Registro de eventos

Crea un filtro.


Visor de eventos
Archivo Acción Ver Ayuda
Visor de eventos (local)
Vistas personalizadas
Registros de Windows
Aplicación
Seguridad
Instalación
Sistema
Eventos reenviados
Registros de aplicaciones y s
Suscripciones
Seguridad Número de eventos: 32,628
Filtrados:Registro: Security; Niveles: Crítico, Error, Advertencia; Origen: . Número de eventos: 0
Palabras clave
Fecha y hora
Origen
Id. del evento
Categoría de la tarea
General Detalles
Nombre de registro:
Origen:
Registrado:
Id. del
Categoría de tarea:
Nivel:
Palabras clave:
Usuario:
Equipo:
Código de operación:
Más información:
Ayuda Registro de eventos
Acciones
Seguridad
Abrir registro guardado...
Crear vista personalizada...
Importar vista personalizada...
Vaciar registro...
Filtrar registro actual...
Borrar filtro
Propiedades
Buscar...
Guardar archivo de registro filtrado como...
Adjuntar tarea a este registro...
Guardar filtro en vista personalizada...
Ver
Actualizar
Ayuda
Crea un filtro.
08:55 p. m.
08/06/2025

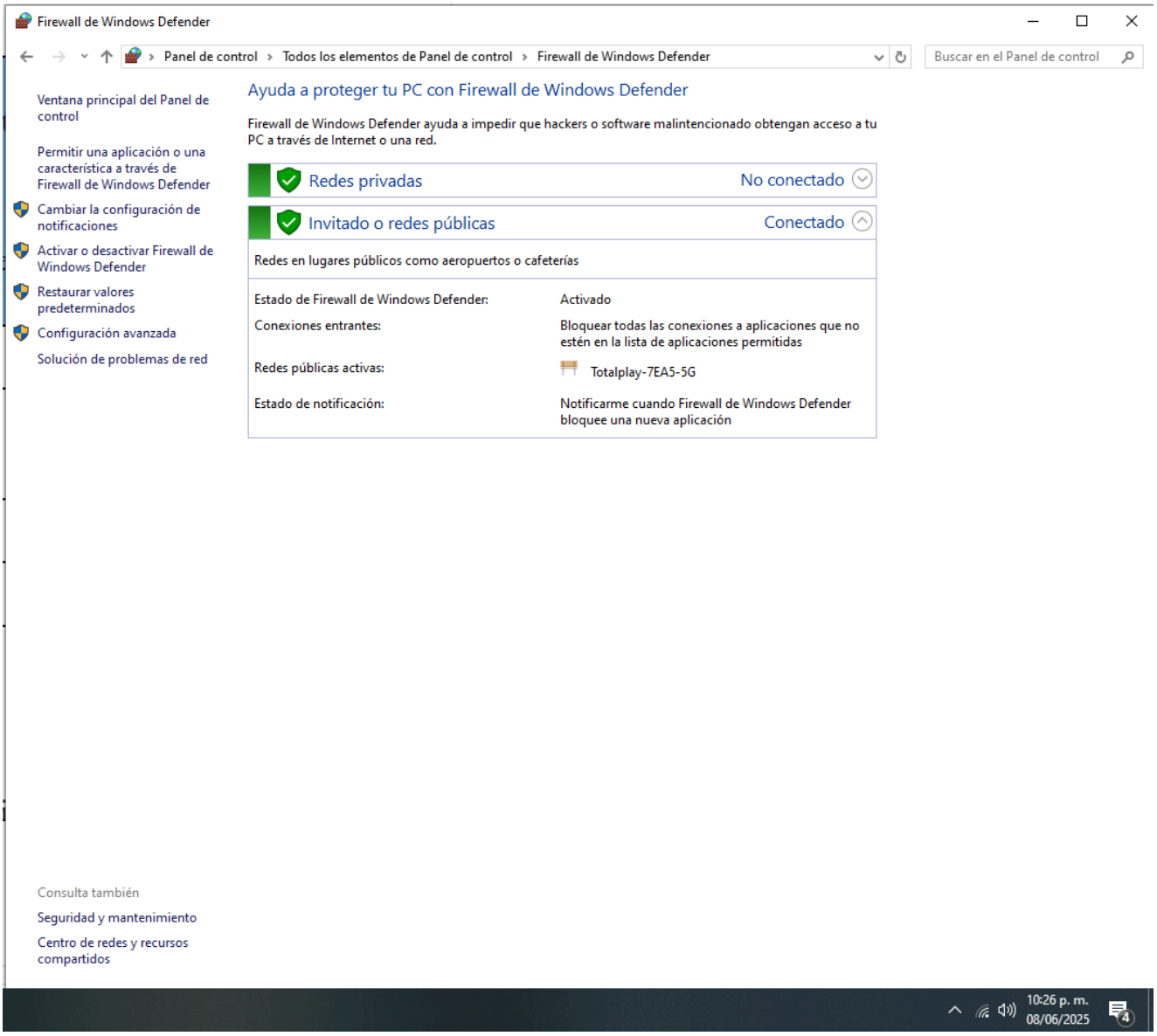

Visor de eventos
Archivo Acción Ver Ayuda
Visor de eventos (local)
Vistas personalizadas
Registros de Windows
Aplicación
Seguridad
Instalación
Sistema
Eventos reenviados
Registros de aplicaciones y servicios
Suscripciones
Aplicación Número de eventos: 14,474
Nivel
Fecha y hora
Origen
Id. del evento
Categoría de la tarea
Información 08/06/2025 10:11:04 p. m. MSSQL$SQLEXPRESS 25753 Server
Información 08/06/2025 10:11:04 p. m. MSSQL$SQLEXPRESS 25754 Server
Información 08/06/2025 09:18:34 p. m. Security-SPP 16384 Ninguno
Información 08/06/2025 09:18:09 p. m. SecurityCenter 15 Ninguno
Información 08/06/2025 09:18:02 p. m. Security-SPP 16394 Ninguno
Información 08/06/2025 09:13:45 p. m. Security-SPP 16384 Ninguno
Información 08/06/2025 09:13:14 p. m. Security-SPP 16394 Ninguno
Información 08/06/2025 09:11:02 p. m. MSSQL$SQLEXPRESS 25753 Server
Información 08/06/2025 09:11:02 p. m. MSSQL$SQLEXPRESS 25754 Server
Información 08/06/2025 09:04:06 p. m. Security-SPP 16384 Ninguno
Información 08/06/2025 09:03:36 p. m. Security-SPP 16394 Ninguno
Información 08/06/2025 08:45:34 p. m. Security-SPP 16384 Ninguno
Información 08/06/2025 08:45:04 p. m. Security-SPP 16394 Ninguno
Información 08/06/2025 07:01:30 p. m. MSSQL$SQLEXPRESS 25753 Server
Información 08/06/2025 07:01:30 p. m. MSSQL$SQLEXPRESS 25754 Server
Información 08/06/2025 07:01:00 p. m. VSS 8224 Ninguno
Información 08/06/2025 06:57:07 p. m. Defrag 258 Ninguno
Información 08/06/2025 06:57:07 p. m. Defrag 258 Ninguno
Información 08/06/2025 06:35:11 p. m. RestartManager 10001 Ninguno
Información 08/06/2025 06:35:11 p. m. RestartManager 10000 Ninguno
Información 08/06/2025 06:03:54 p. m. VSS 8224 Ninguno
Información 08/06/2025 06:02:15 p. m. Security-SPP 16384 Ninguno
Información 08/06/2025 06:01:44 p. m. SecurityCenter 15 Ninguno
Información 08/06/2025 06:01:43 p. m. Security-SPP 16394 Ninguno
Información 08/06/2025 06:01:22 p. m. MSSQL$SQLEXPRESS 25753 Server
Información 08/06/2025 06:01:22 p. m. MSSQL$SQLEXPRESS 25754 Server
Información 08/06/2025 06:00:56 p. m. Windows Error Reporting 1001 Ninguno
Evento 25753, MSSQL$SQLEXPRESS
General Detalles
XE session 'telemetry_xevents' started.
Nombre de registro: Aplicación
Origen: MSSQL$SQLEXPRESS
Registrado: 08/06/2025 10:11:04 p. m.
Id. del 25753
Categoría de tarea: Server
Nivel: Información
Palabras clave: Clásico
Usuario: NT SERVICE\SQLTELEMETRY
Equipo: DESKTOP-S36GML9
Código de operación: Información
Más información:
Ayuda Registro de eventos
Acciones
Aplicación
Abrir registro guardado...
Crear vista personalizada...
Importar vista personalizada...
Vaciar registro...
Filtrar registro actual...
Propiedades
Buscar...
Guardar todos los eventos como...
Adjuntar tarea a este registro...
Ver
Actualizar
Ayuda
Evento 25753, MSSQL$SQLEXPRESS
Propiedades de evento
Adjuntar tarea a este evento...
Guardar eventos seleccionados...
Copiar
Actualizar
Ayuda
10:24 p. m.
08/06/2025


Visor de eventos
Archivo Acción Ver Ayuda
Visor de eventos (local)
Vistas personalizadas
Registros de Windows
Aplicación
Seguridad
Instalación
Sistema
Eventos reenviados
Registros de aplicaciones y servicios
Suscripciones
Aplicación Número de eventos: 14,474
Filtrados:Registro: Application; Niveles: Crítico, Error; Origen: . Número de eventos: 299
Nivel Fecha y hora Origen Id. del evento Categoría de la tarea
Error 08/06/2025 11:47:39 a. m. MSSQL$SQLEXPRESS 17836 Logon
Error 08/06/2025 11:46:30 a. m. MSSQL$SQLEXPRESS 17832 Logon
Error 08/06/2025 11:46:30 a. m. MSSQL$SQLEXPRESS 17832 Logon
Error 08/06/2025 11:45:48 a. m. MSSQL$SQLEXPRESS 17832 Logon
Filtrar registro actual
Filtro XML
Registrado: En cualquier momento
Nivel del evento: Crítico Advertencia Detallado Error Información
Por registro Registros de eventos: Aplicación
Por origen Orígenes del evento:
Para incluir o excluir los id. de evento, escriba números o intervalos de id. separados por comas. Para excluir criterios, antecédalos con un signo de menos. Ej: 1,3,5-99,-76
<Todos los id. de evento>
Categoría de la tarea:
Palabras clave:
Usuario: <Todos los usuarios>
Equipo(s): <Todos los equipos>
Borrar
Aceptar Cancelar
Evento 17836, MSSQL$SQLEXPRESS
General Detalles
Length specified in network packet payload di
[CLIENT: 192.168.100.22]
ient library.
Nombre de registro: Aplicación
Origen: MSSQL$SQLEXPRESS
Registrado: 08/06/2025 11:47:39 a. m.
Id. del 17836
Categoría de tarea: Logon
Nivel: Error
Palabras clave: Clásico
Usuario: No disponible
Equipo: DESKTOP-S36GML9
Código de operación: Información
Más información: Ayuda Registro de eventos
Acciones
Aplicación
Abrir registro guardado...
Crear vista personalizada...
Importar vista personalizada...
Vaciar registro...
Filtrar registro actual...
Borrar filtro
Propiedades
Buscar...
Guardar archivo de registro filtrado como...
Adjuntar tarea a este registro...
Guardar filtro en vista personalizada...
Ver
Actualizar
Ayuda
Evento 17836, MSSQL$SQLEXPRESS
Propiedades de evento
Adjuntar tarea a este evento...
Guardar eventos seleccionados...
Copiar
Actualizar
Ayuda
Crea un filtro.
10:25 p. m.
08/06/2025


Visor de eventos
Archivo Acción Ver Ayuda
Visor de eventos (local)
Vistas personalizadas
Registros de Windows
Aplicación
Seguridad
Instalación
Sistema
Eventos reenviados
Registros de aplicaciones y servicios
Suscripciones
Aplicación Número de eventos: 14,474
Filtrados:Registro: Application; Niveles: Crítico, Error; Origen: . Número de eventos: 299
Nivel Fecha y hora Origen Id. del evento Categoría de la tarea
Error 08/06/2025 11:47:39 a. m. MSSQL$SQLEXPRESS 17836 Logon
Error 08/06/2025 11:46:30 a. m. MSSQL$SQLEXPRESS 17832 Logon
Error 08/06/2025 11:46:30 a. m. MSSQL$SQLEXPRESS 17832 Logon
Error 08/06/2025 11:45:48 a. m. MSSQL$SQLEXPRESS 17832 Logon
Error 08/06/2025 11:45:05 a. m. MSSQL$SQLEXPRESS 17836 Logon
Error 08/06/2025 11:45:05 a. m. MSSQL$SQLEXPRESS 17836 Logon
Error 08/06/2025 11:45:05 a. m. MSSQL$SQLEXPRESS 17836 Logon
Error 08/06/2025 11:45:05 a. m. MSSQL$SQLEXPRESS 17836 Logon
Error 08/06/2025 11:44:57 a. m. MSSQL$SQLEXPRESS 17821 Logon
Error 08/06/2025 11:44:57 a. m. MSSQL$SQLEXPRESS 17836 Logon
Error 08/06/2025 11:44:53 a. m. MSSQL$SQLEXPRESS 17821 Logon
Error 08/06/2025 11:44:53 a. m. MSSQL$SQLEXPRESS 17821 Logon
Error 08/06/2025 11:44:31 a. m. MSSQL$SQLEXPRESS 17832 Logon
Error 08/06/2025 11:44:31 a. m. MSSQL$SQLEXPRESS 17832 Logon
Error 08/06/2025 11:44:31 a. m. MSSQL$SQLEXPRESS 17836 Logon
Error 08/06/2025 11:44:31 a. m. MSSQL$SQLEXPRESS 17836 Logon
Error 08/06/2025 11:43:12 a. m. MSSQL$SQLEXPRESS 17836 Logon
Error 08/06/2025 11:42:57 a. m. MSSQL$SQLEXPRESS 17836 Logon
Error 08/06/2025 11:42:56 a. m. MSSQL$SQLEXPRESS 17836 Logon
Error 08/06/2025 11:42:51 a. m. MSSQL$SQLEXPRESS 17836 Logon
Error 08/06/2025 11:42:45 a. m. MSSQL$SQLEXPRESS 17821 Logon
Error 08/06/2025 11:42:45 a. m. MSSQL$SQLEXPRESS 17821 Logon
Error 08/06/2025 11:42:45 a. m. MSSQL$SQLEXPRESS 17821 Logon
Error 08/06/2025 11:42:45 a. m. MSSQL$SQLEXPRESS 17821 Logon
Evento 17836, MSSQL$SQLEXPRESS
General Detalles
Length specified in network packet payload did not match number of bytes read; the connection has been closed. Please contact the vendor of the client library.
[CLIENT: 192.168.100.22]
Nombre de registro: Aplicación
Origen: MSSQL$SQLEXPRESS
Registrado: 08/06/2025 11:47:39 a. m.
Id. del 17836
Categoría de tarea: Logon
Nivel: Error
Palabras clave: Clásico
Usuario: No disponible
Equipo: DESKTOP-S36GML9
Código de operación: Información
Más información: Ayuda Registro de eventos
Acciones
Aplicación
Abrir registro guardado...
Crear vista personalizada...
Importar vista personalizada...
Vaciar registro...
Filtrar registro actual...
Borrar filtro
Propiedades
Buscar...
Guardar archivo de registro filtrado como...
Adjuntar tarea a este registro...
Guardar filtro en vista personalizada...
Ver
Actualizar
Ayuda
Evento 17836, MSSQL$SQLEXPRESS
Propiedades de evento
Adjuntar tarea a este evento...
Guardar eventos seleccionados...
Copiar
Actualizar
Ayuda
Crea un filtro.
10:25 p. m.
08/06/2025

Importancia de seguridad.

En este punto de la actividad se redactará la importancia de la seguridad para la prevención, monitoreo y auditorías que nos permitirán identificar posibles ataques o problemas en la operación del equipo de computo.



La prevención es la primera línea de defensa y se enfoca en evitar que los incidentes de seguridad ocurran en primer lugar. Esto implica la implementación de políticas, procedimientos y tecnologías diseñadas para reducir las vulnerabilidades. Algunas medidas preventivas clave incluyen:

- Firewall, antivirus.
- Actualización de parcheo
- Control de acceso.

Entre otras medidas de prevención.

El monitoreo es el proceso continuo de supervisar los sistemas, redes y aplicaciones para detectar actividades inusuales o sospechosas en tiempo real. Es el "ojo vigilante" que alerta sobre posibles problemas antes de que escalen. Sus componentes clave incluyen:

- Detección de intrusos.
- Gestion de eventos.
- Análisis de riesgos.

Entre otros componentes.

La auditoría es un examen sistemático y periódico de los sistemas, procesos y controles de seguridad para evaluar su efectividad y cumplimiento. A diferencia del monitoreo, que es continuo, la auditoría es un proceso puntual que verifica el estado de la seguridad en un momento dado. Sus objetivos principales son:

- Cumplimiento Normativo.
- Revisión de Políticas.
- Análisis de Vulnerabilidades y Pruebas de Penetración.

Entre otros objetivos adicionales.

Conclusion.

En conclusión: En el ámbito laboral o en nuestra vida cotidiana, la auditoría de equipos, tal como lo hemos explorado en Seguridad Informática II, se traduce en una práctica indispensable para nuestra tranquilidad y eficiencia digital. Al igual que una empresa verifica sus licencias para evitar problemas legales, nosotros deberíamos revisar periódicamente el software en nuestros dispositivos personales para asegurar su legitimidad y evitar el uso de programas piratas que pueden contener malware. Este control no solo nos protege de sanciones, sino que también nos brinda una visión clara de la seguridad de nuestros propios equipos.

Implementar auditorías sencillas y revisar las bitácoras (o historiales de actividad) en nuestros dispositivos, incluso semanalmente, nos permite detectar vulnerabilidades antes de que se conviertan en un problema. Esto es clave para proteger nuestra información personal, desde fotos y documentos importantes hasta datos bancarios. Al mantener un control constante y proactivo, no solo salvaguardamos nuestros activos digitales más valiosos, sino que también aseguramos que nuestros equipos funcionen de manera óptima. En un mundo donde las amenazas evolucionan rápidamente, adoptar una mentalidad de auditoría es fundamental para mantener nuestra seguridad y privacidad.

Referencias.

Gemini - chat to supercharge your ideas. (n.d.). Gemini. Retrieved January 9, 2025, from https://gemini.google.com/

Ingeniería en desarrollo de software. (n.d.). Edu.Mx. Retrieved January 9, 2025, from https://umi.edu.mx/coppel/IDS/login/index.php