

- Portada
- Índice
- Introducción
- Descripción
- Justificación
- Desarrollo:
- Auditoría y Bitácora:
- Auditoría de equipo.
- Bitácora
- Importancia de seguridad (prevención, monitoreo, auditoría)
- Conclusión
- Referencias



Actividad [#] - 3

[Nombre de la Actividad] Auditoria y bitácora

[Nombre del Curso] Seguridad Informática II

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: Daniel Alcudia Aleyda

Fecha: 28/05/2023

● Índice

Contenido

● Introducción	3
● Descripción	4
● Justificación	5
● Desarrollo:.....	5
● Auditoría y Bitácora:	11
● Auditoría de equipo.	13
● Bitácora	13
● Importancia de seguridad (prevención, monitoreo, auditoría) .	14
● Conclusión	15
● Referencias	15

● Introducción

La auditoría en informática es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre se logre una utilización más eficiente se y segura la información que servirá para una adecuada toma de decisiones. Un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas procedimientos controles archivos seguridad y obtención de información. La auditoría es de vital importancia para el buen desempeño de los sistemas de información ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad además de evaluar todo informática, organización de centros de información, hardware y software. La auditoría informática es llevada a cabo por profesionales capacitados.

● Descripción

Las auditorías son importantes ya que permiten mostrar el estado en el que se encuentra la protección de la información y se los activos dentro de las organizaciones además involucran la identificación análisis y evaluación de debilidades en las medidas de seguridad que han sido aplicadas, así como los componentes tecnológicos de la empresa. Es por ello que además de conocer diferentes tipos de software para realizar un escaneo de nuestras redes y equipos, para identificar los posibles riesgos de seguridad. También podemos realizar una auditoría a través de nuestro panel de control de nuestro equipo que tengamos en uso, para ello debemos identificar las opciones para poder ingresar, en donde encontraremos las especificaciones en general, la seguridad, las aplicaciones o guardar datos de una auditoría ya realizada.

En el caso específico de las redes la auditoría está relacionada con un método o un conjunto de ellos para verificar el cumplimiento de los requisitos de seguridad, necesarios dentro de una recolección de dispositivos interconectados como pueden ser routers, switches, hubs computadoras y dispositivos móviles.

• Justificación

La auditoría informática es una parte fundamental de la seguridad computacional que permite medir y controlar riesgos informáticos que pueden ser aprovechados por personas o sistemas ajenos a nuestra organización o que no deben tener acceso a nuestros datos. En este sentido identificar los riesgos de manera oportuna ayudará a implementar de manera preventiva, las medidas de seguridad para facilitar esta actividad existen diferentes metodologías que ayudan en el proceso de revisión de riesgos informáticos. El principal objetivo de la auditoría es mejorar cualquier posible incidencia que pueda presentarse en el sistema, así como establecer una serie de criterios vinculados con un uso adecuado del mismo. La historia de sistemas es la que abarca la revisión y evaluación de los sistemas automáticos de procesamiento de información en todos sus aspectos o parte de ellos incluidos los procedimientos relacionados con ellos y las interfaces correspondientes en general se encarga de la revisión y evaluación de los recursos informáticos software, hardware, comunicaciones, personal, políticas, procedimientos, controles y seguridad.

• Desarrollo:

- **En esta pantalla podemos visualizar los registros de cada evento, su estatus y también podemos importarlos o guardarlos.**

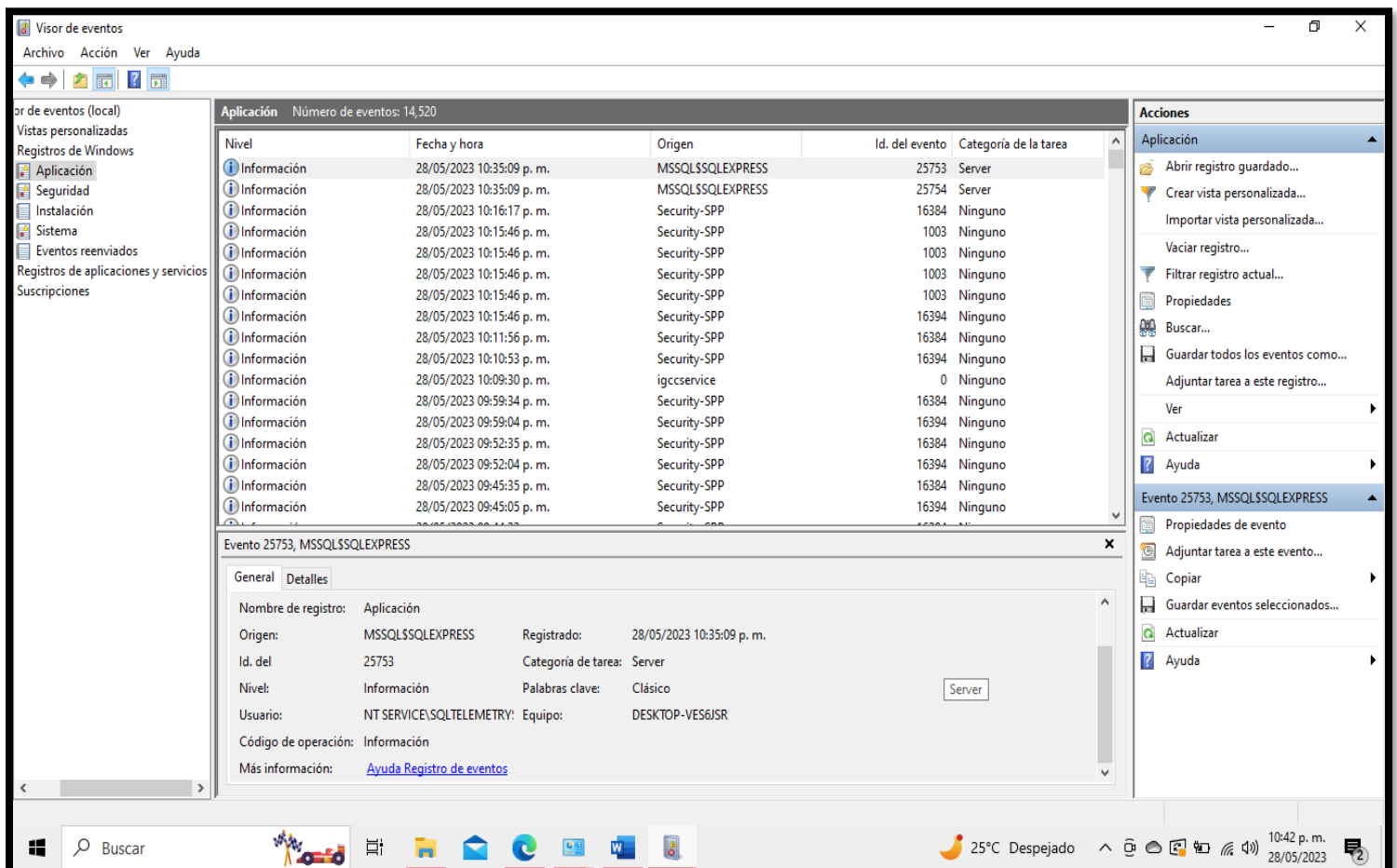
The screenshot shows the Windows Event Viewer application. The main pane displays the 'Introducción y resumen' (Introduction and Summary) view. It includes a section for 'Resumen de eventos administrativos' (Summary of administrative events) with a table showing event counts over time.

Tipo de evento	Id. del e...	Origen	Registro	Última hora	24 horas	7 días
Advertencia	-	-	-	1	9	39
Información	-	-	-	47	338	1,320
Auditoría cor...	-	-	-	718	3,898	15,740

Below the table is a section for 'Nodos vistos recientemente' (Recently viewed nodes) with columns for Nombre, Descripción, Modificado, and Creado.

The right-hand pane shows the 'Acciones' (Actions) menu, which includes options like 'Abrir registro guardado...' (Open saved log), 'Crear vista personalizada...' (Create custom view), and 'Actualizar' (Update).

- Aquí podemos visualizar las aplicaciones y ver los detalles generales.



The screenshot shows the Windows Event Viewer interface. The left pane displays the 'Aplicación' (Application) log. The main pane shows a list of events with columns: Nivel, Fecha y hora, Origen, Id. del evento, and Categoría de la tarea. The right pane shows the 'Acciones' (Actions) menu.

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	28/05/2023 10:35:09 p. m.	MSSQL\$SQLEXPRESS	25753	Server
Información	28/05/2023 10:35:09 p. m.	MSSQL\$SQLEXPRESS	25754	Server
Información	28/05/2023 10:16:17 p. m.	Security-SPP	16384	Ninguno
Información	28/05/2023 10:15:46 p. m.	Security-SPP	1003	Ninguno
Información	28/05/2023 10:15:46 p. m.	Security-SPP	1003	Ninguno
Información	28/05/2023 10:15:46 p. m.	Security-SPP	1003	Ninguno
Información	28/05/2023 10:15:46 p. m.	Security-SPP	1003	Ninguno
Información	28/05/2023 10:15:46 p. m.	Security-SPP	16394	Ninguno
Información	28/05/2023 10:11:56 p. m.	Security-SPP	16384	Ninguno
Información	28/05/2023 10:10:53 p. m.	Security-SPP	16394	Ninguno
Información	28/05/2023 10:09:30 p. m.	igccservice	0	Ninguno
Información	28/05/2023 09:59:34 p. m.	Security-SPP	16384	Ninguno
Información	28/05/2023 09:59:04 p. m.	Security-SPP	16394	Ninguno
Información	28/05/2023 09:52:35 p. m.	Security-SPP	16384	Ninguno
Información	28/05/2023 09:52:04 p. m.	Security-SPP	16394	Ninguno
Información	28/05/2023 09:45:35 p. m.	Security-SPP	16384	Ninguno
Información	28/05/2023 09:45:05 p. m.	Security-SPP	16394	Ninguno

Evento 25753, MSSQL\$SQLEXPRESS

General Detalles

Nombre de registro: Aplicación

Origen: MSSQL\$SQLEXPRESS Registrado: 28/05/2023 10:35:09 p. m.

Id. del: 25753 Categoría de tarea: Server

Nivel: Información Palabras clave: Clásico Server

Usuario: NT SERVICE\SQLTELEMETRY Equipo: DESKTOP-VE56JSR

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...
- Copiar
- Guardar eventos seleccionados...
- Actualizar
- Ayuda

- En esta pantalla podremos ver los detalles de la seguridad o también mostrar los datos de manera general

The screenshot displays the Windows Event Viewer interface. The main window is titled 'Visor de eventos' and shows the 'Propiedades de evento: Evento 4798, Microsoft Windows security auditing.' dialog box. The 'General' tab is selected, showing the following details:

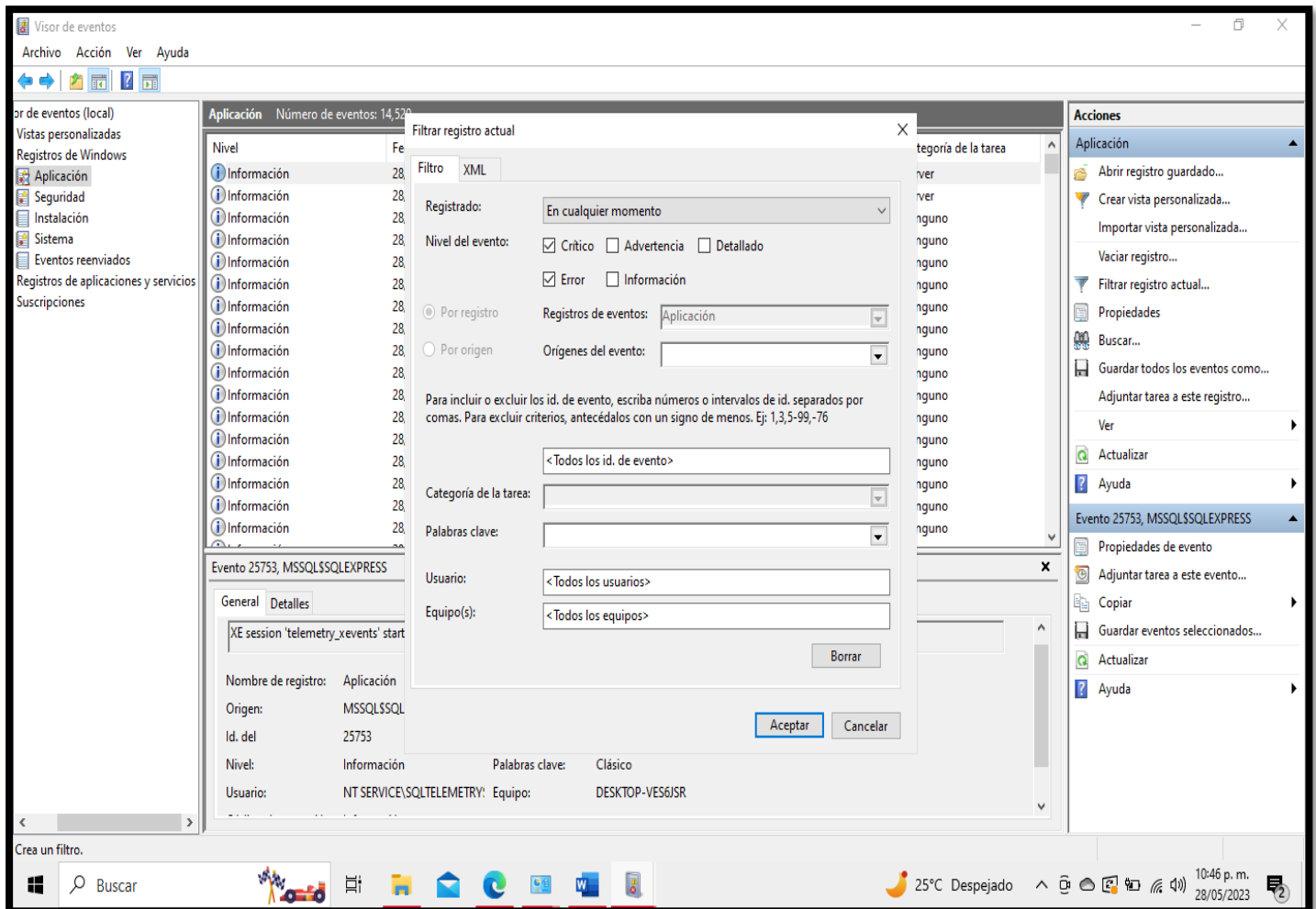
- Se enumeró la pertenencia a grupos locales de un usuario.**
- Firmante:** Id. de seguridad: DESKTOP-VES6JSR\Lenovo, Nombre de cuenta: Lenovo, Dominio de cuenta: DESKTOP-VES6JSR
- Nombre de registro:** Seguridad
- Origen:** Microsoft Windows security, **Registrado:** 28/05/2023 10:42:30 p. m.
- Id. del:** 4798, **Categoría de tarea:** User Account Management
- Nivel:** Información, **Palabras clave:** Auditoría correcta
- Usuario:** No disponible, **Equipo:** DESKTOP-VES6JSR
- Código de operación:** Información
- Más información:** [Ayuda Registro de eventos](#)

Below the dialog box, a table lists several events:

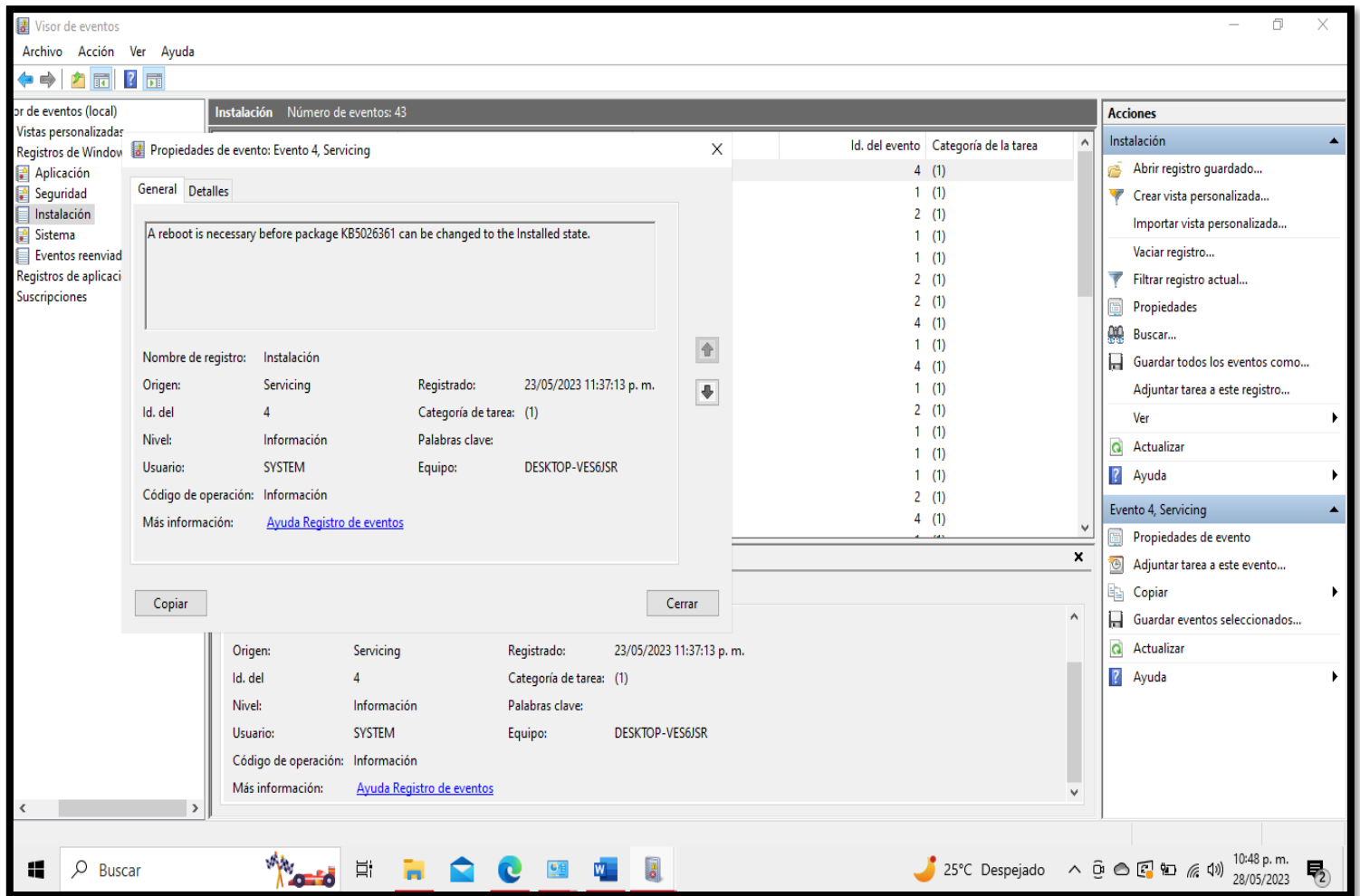
	Id. del evento	Categoría de la tarea
ift Windows securi...	4798	User Account Management
ift Windows securi...	4798	User Account Management
ift Windows securi...	4672	Special Logon
ift Windows securi...	4624	Logon
ift Windows securi...	5379	User Account Management
ift Windows securi...	5379	User Account Management
ift Windows securi...	5379	User Account Management
ift Windows securi...	5379	User Account Management
ift Windows securi...	5379	User Account Management
ift Windows securi...	5379	User Account Management
ift Windows securi...	5379	User Account Management
ift Windows securi...	5379	User Account Management
ift Windows securi...	5379	User Account Management
ift Windows securi...	5379	User Account Management
ift Windows securi...	5379	User Account Management
ift Windows securi...	5379	User Account Management

On the right side, the 'Acciones' pane shows various actions for the selected event, including 'Propiedades de evento', 'Copiar', 'Guardar eventos seleccionados...', 'Actualizar', and 'Ayuda'. The bottom of the screen shows the Windows taskbar with the search bar, task icons, and system tray information (25°C Despejado, 10:44 p. m., 28/05/2023).

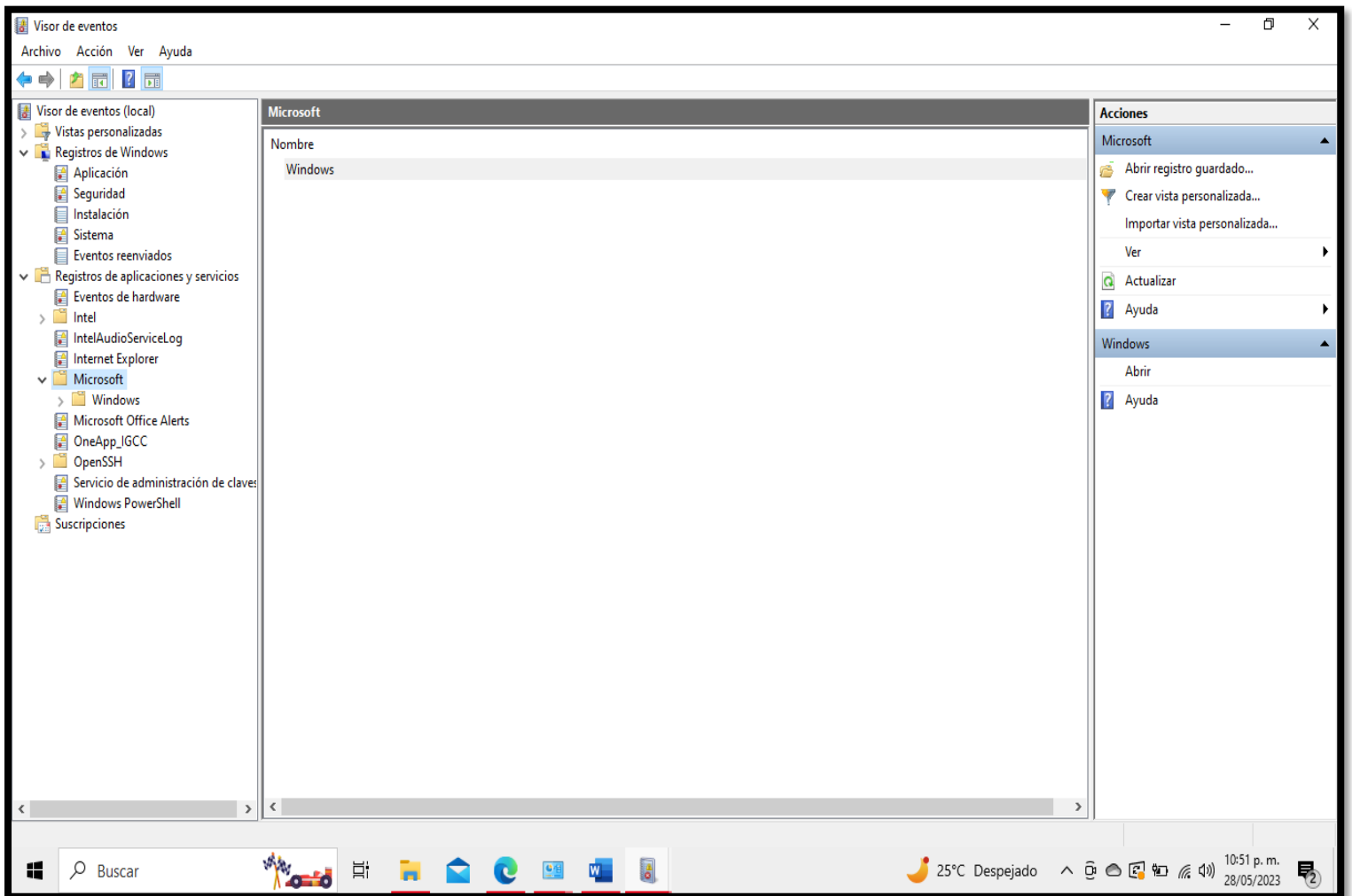
- Aquí podemos filtrar un registro como critico o por error, para poder encontrar los errores criticos que pueda contener nuestro equipo.



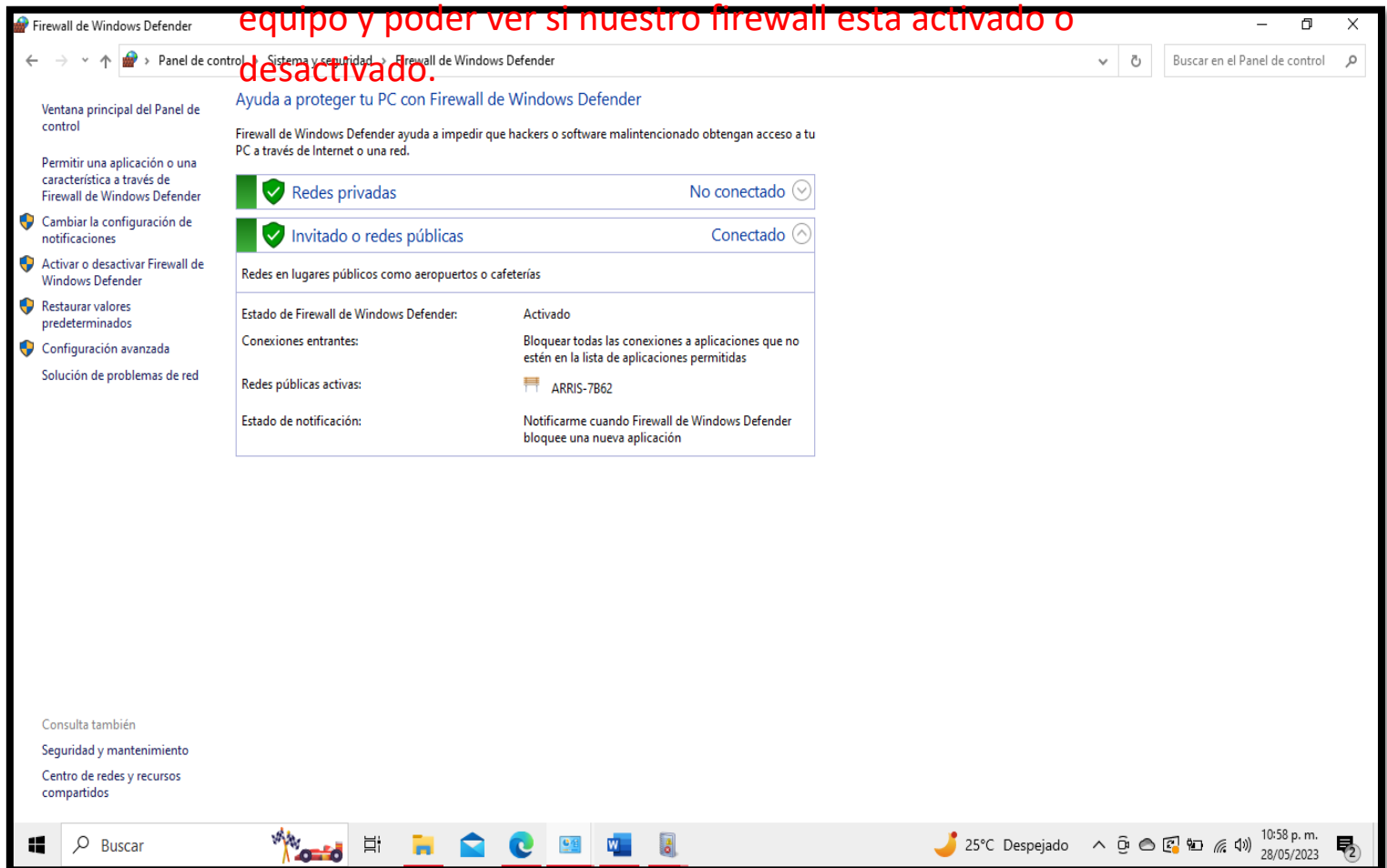
- En este apartado podremos examinar todos los registros de la instalacion.



- Esta pantalla nos muestra los registros de Microsoft, para poder ver algún tipo de malware o alertas de office.



- Aquí podremos revisar la seguridad del firewall de nuestro equipo y poder ver si nuestro firewall esta activado o desactivado.



- Auditoría y Bitácora:

- Visor de eventos**

Archivo Acción Ver Ayuda

Orde de eventos (local)
Vistas personalizadas
Registros de Windows

 - Aplicación
 - Seguridad**
 - Instalación
 - Sistema
 - Eventos reenviados
 - Registros de aplicaciones y servicios
 - Suscripciones

Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Auditoría correcta	28/05/2023 10:42:30 p. m.	Microsoft Windows securi...	4798	User Account Management
Auditoría correcta	28/05/2023 10:42:28 p. m.	Microsoft Windows securi...	4798	User Account Management
Auditoría correcta	28/05/2023 10:41:16 p. m.	Microsoft Windows securi...	4672	Special Logon
Auditoría correcta	28/05/2023 10:41:16 p. m.	Microsoft Windows securi...	4624	Logon
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management
Auditoría correcta	28/05/2023 10:39:41 p. m.	Microsoft Windows securi...	5379	User Account Management

Evento 4798, Microsoft Windows security auditing.

General Detalles

Se enumeró la pertenencia a grupos locales de un usuario.

Nombre de registro: Seguridad

Origen: Microsoft Windows security Registrado: 28/05/2023 10:42:30 p. m.

Id. del 4798 Categoría de tarea: User Account Management

Nivel: Información Palabras clave: Auditoría correcta

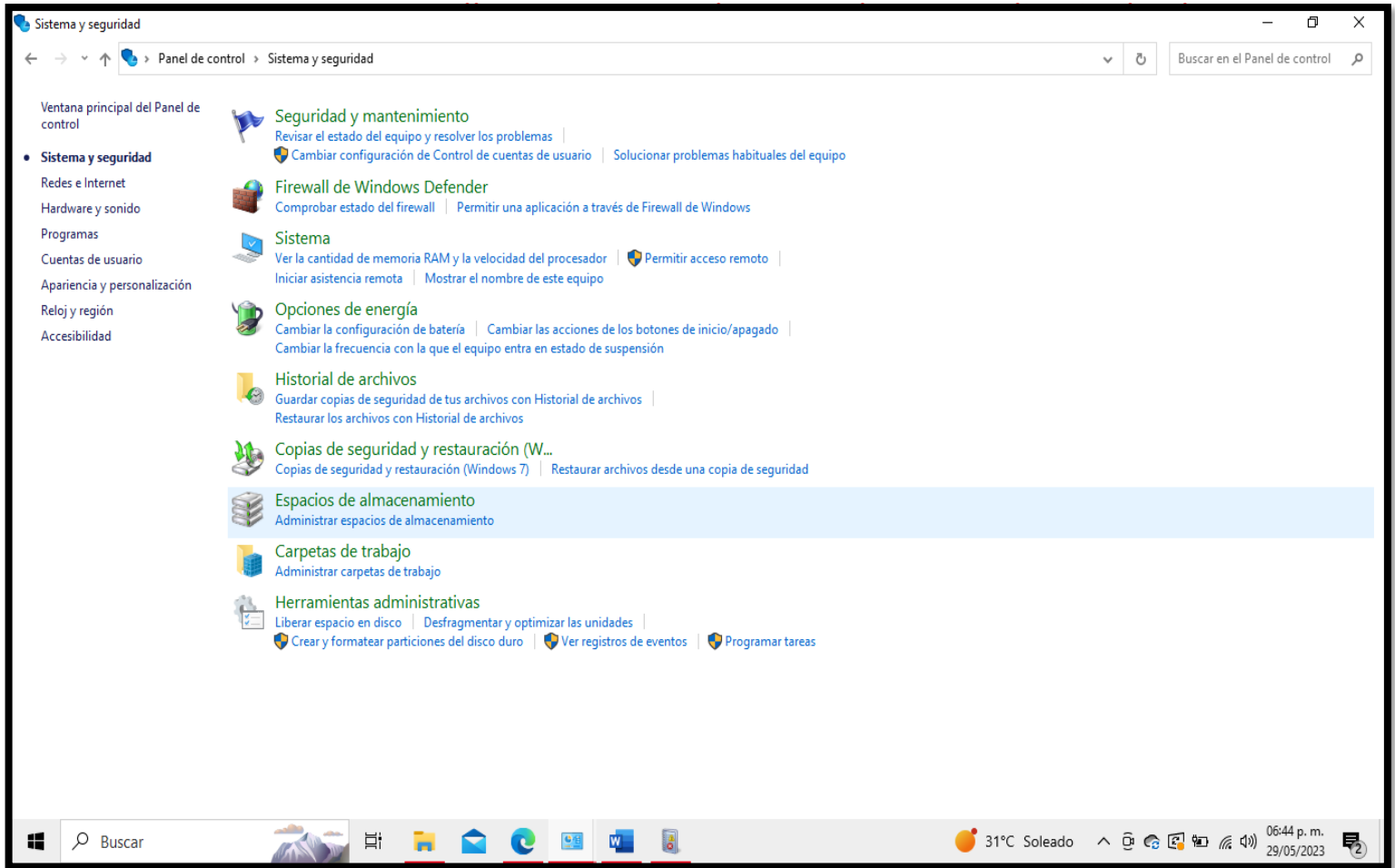
Usuario: No disponible Equipo: DESKTOP-VES6JSR

Acciones

Seguridad

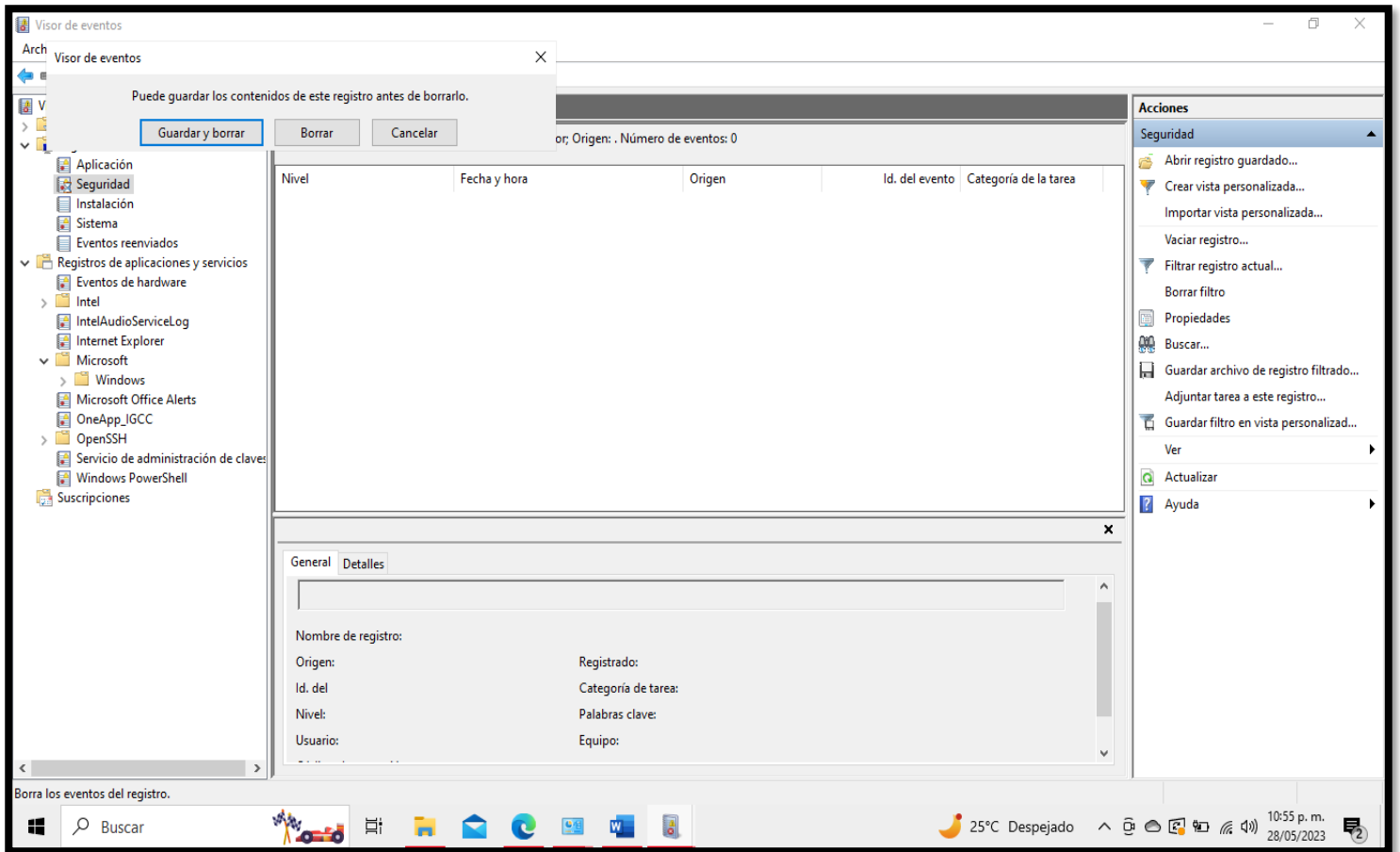
 - Abrir registro guardado...
 - Crear vista personalizada...
 - Importar vista personalizada...
 - Vaciar registro...
 - Filtrar registro actual...
 - Propiedades
 - Buscar...
 - Guardar todos los eventos como...
 - Adjuntar tarea a este registro...
 - Ver
 - Actualizar
 - Ayuda
 - Evento 4798, Microsoft Windows securi...
 - Propiedades de evento
 - Adjuntar tarea a este evento...
 - Copiar
 - Guardar eventos seleccionados...
 - Actualizar
 - Ayuda

● Auditoría de equipo.



● Bitácora

- Esta pantalla nos mostrara como podremos vaciar nuestros registros para poder empezar una nueva auditoria.



- Importancia de seguridad (prevención, monitoreo, auditoría)

Las auditorías de seguridad son evaluaciones estructuradas de cómo las actividades en el trabajo pueden afectar la integridad física y de quienes forman parte de una empresa. Ayuda a las entidades a evaluar y optimizar sus programas de salud y seguridad y a mejorar las gestiones y estrategias enfocadas en el bienestar de los trabajadores. Son un proceso esencial que debe realizarse con regularidad ya que están diseñadas para mantener la eficiencia operativa y reducir los costos de mantenimiento. Los hallazgos de éstas pueden mejorar las condiciones de trabajo ayudar con la programación de equipos establecer presupuestos específicos. El propósito primordial de las auditorías es establecer si la compañía cumple con la legislación de seguridad e identificar debilidades y deficiencias en sus programas. Estás identifican diferentes niveles de riesgos en todas las áreas particulares en tu empresa. Las auditorias de seguridad

promocionan la constante revisión de los sistemas para asegurar que no se debiliten con el tiempo, facilita mejoras en los programas políticas y procedimientos.

● Conclusión

La auditoría de los sistemas de información es muy importante, desafortunadamente muchas de las empresas visualizan este proceso como un requisito obligatorio que les hace perder tiempo y dinero cuando la realidad es que este proceso ayuda a las organizaciones a mantenerse en el camino hacia sus objetivos. La información que un sistema brinda es un recurso clave en la empresa para planear el futuro controlar presente y valor el pasado. La auditoría de los sistemas de información puede realizarse por una persona externa a la empresa o por algún empleado interno siempre y cuando cumpla con ser objetivo. Mas que nada lo que se busca es mantener los sistemas libres de cualquier amenaza que pueda causarles problemas. Con la auditoria de equipos podremos mantener identificar los posibles problemas o el estado actual de nuestros equipos, lo que para las empresas es de gran utilidad para poder mantener los equipos siempre actualizados y libres de cualquier problema que pueda causarles perdidas.

● Referencia

De los controles, L. A. en I. es la R. y la E., De cómputo, P. de I. de L. E., Utilización, S., Seguridad, E. y., De la información, de la O. Q. P. en el P., & de la información que servirá para una adecuada toma de decisiones., a. F. de Q. P. M. del S. de C. A. se L. U. U. M. E. y. S. (s/f). *CAPÍTULO IV AUDITORÍA DE SISTEMAS*. Uia.mx. Recuperado el 29 de mayo de 2023, de http://www.bib.uia.mx/tesis/pdf/014663/014663_04.pdf#:~:text=La%20auditor%C3%ADa%20en%20inform%C3%A1tica%20es%20de%20vital%20importancia,organizaci%C3%B3n%20de%20centros%20de%20informaci%C3%B3n%2C%20hardware%20y%20software%29.

Wikipedia contributors. (s/f). *Auditoría informática*. Wikipedia, The Free Encyclopedia.

https://es.wikipedia.org/w/index.php?title=Auditor%C3%ADa_inform%C3%A1tica&oldid=142188361

Guirao, S. F. (2015, octubre 5). *Auditoría de sistemas de información: objetivo y razones para implementarla*. gestiopolis; gestiopolis.com.

<https://www.gestiopolis.com/auditoria-de-sistemas-de-informacion-objetivo-y-razones-para-implementarla/>

Melo, S. (2021, septiembre 7). *La importancia de las auditorías de seguridad*.

DataScope. <https://datascope.io/es/blog/la-importancia-de-las-auditorias-de-seguridad/>

Mendoza, M. Á. (2015, abril 20). *Conoce los tipos de auditorías de redes y qué puede revisar cada una*. WeLiveSecurity.

<https://www.welivesecurity.com/la-es/2015/04/20/auditorias-de-redes/>