

Actividad 3 - Auditoria y Bitácora


Seguridad Informática 2

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: Homero Ramirez Hurtado

Fecha: 28 de Mayo del 2024



Índice.

. Introducción.

. Descripción.

. Justificación.

. Desarrollo.

- Auditoria de Equipo.
 - Bitácora.
- Importancia de Seguridad (Prevención, Monitoreo, Auditoria)

. Conclusión.

. Referencias.



Introducción.

La seguridad informática es un aspecto crucial en la protección de los recursos y la información en cualquier entorno tecnológico. Una de las prácticas fundamentales para garantizar esta seguridad es llevar a cabo auditorías regulares. Estas auditorías pueden realizarse desde el propio equipo de cómputo o mediante herramientas especializadas.

Durante una auditoría, se evalúan diversos aspectos, como el sistema operativo, el hardware, el software instalado y, especialmente, las licencias asociadas a estos recursos. Validar las licencias es esencial no solo por cuestiones legales y regulatorias, sino también para prevenir posibles vulnerabilidades. Al identificar licencias faltantes o no autorizadas, se pueden tomar medidas correctivas y evitar riesgos innecesarios.

Además, mantener una bitácora detallada es crucial. Registrar los cambios desde el día 1 permite detectar cualquier alteración o actividad sospechosa. Esta bitácora no solo sirve como evidencia legal, sino también como una herramienta para anticipar posibles ataques y salvaguardar los recursos valiosos, como la información confidencial.

En resumen, las auditorías y el control total del sistema, hardware, software, licencias y red son pilares fundamentales para mantener la seguridad informática en cualquier organización. Mantenerse al día con estas prácticas contribuye a proteger los activos tecnológicos y garantizar la integridad de los datos.

Descripción.

Una auditoría de seguridad informática es un proceso exhaustivo y sistémico diseñado para evaluar la robustez de las medidas de protección dentro de una empresa. Durante este estudio, se analizan detalladamente las políticas, sistemas, infraestructuras de TI y procedimientos para identificar vulnerabilidades y riesgos potenciales. Estas auditorías son esenciales para garantizar la seguridad de la información en las organizaciones.

Las auditorías de seguridad informática pueden seguir un esquema o procedimiento que se divide en cuatro fases principales:

1. **Objetivos y planificación:** En esta fase, se define el alcance, los criterios, la metodología y los objetivos de la auditoría. Se determina qué se va a auditar, cuándo, cómo y por quién. Además, se establece el marco legal y normativo que se aplicará, así como los recursos y herramientas necesarios. El plan de auditoría incluye elementos como el propósito, el alcance, los objetivos específicos, los criterios de evaluación y el equipo auditor responsable.
2. **Recopilación de evidencia:** Durante esta etapa, se recopila información relevante sobre los sistemas informáticos, políticas de seguridad y controles implementados. Se realizan pruebas técnicas para analizar las vulnerabilidades y se evalúa el cumplimiento de las normas de seguridad establecidas por la empresa.
3. **Análisis y evaluación:** Aquí se examina la evidencia recopilada y se evalúa la eficiencia de los sistemas de seguridad. Se identifican posibles vulnerabilidades o brechas en

cualquier nivel de seguridad de la empresa. Además, se verifica si los controles de seguridad están siendo efectivamente implementados.

4. Informe final y recomendaciones: La auditoría culmina con la elaboración de un informe final. Este documento detalla los equipos, servidores y programas analizados, el cumplimiento de las normas de seguridad, la eficiencia de los sistemas de seguridad y las posibles vulnerabilidades detectadas. Además, se proporcionan recomendaciones para mejorar la ciberseguridad de la organización.

En cuanto a la bitácora de seguridad informática, esta consiste en un registro detallado de eventos y actividades relacionadas con la seguridad de los sistemas. Se documentan incidentes, cambios en la configuración, actualizaciones, accesos no autorizados y otros eventos relevantes. La bitácora es fundamental para el seguimiento y la detección temprana de posibles amenazas o irregularidades en la seguridad de la información

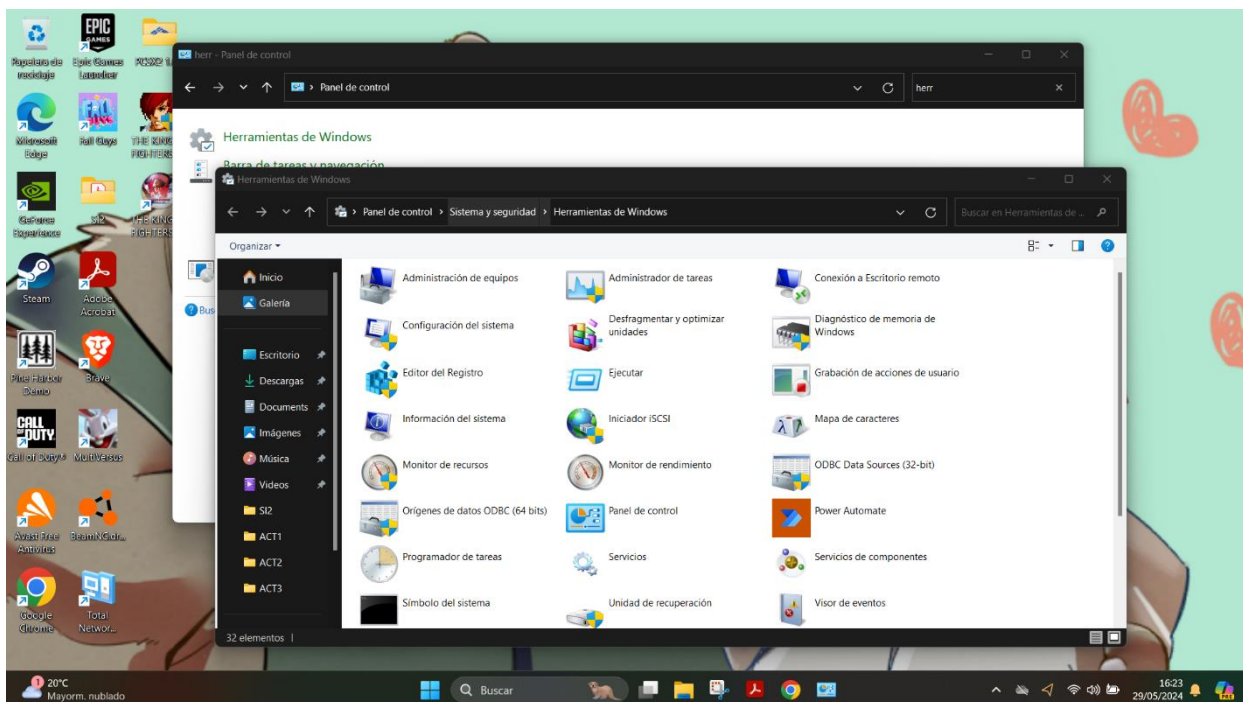
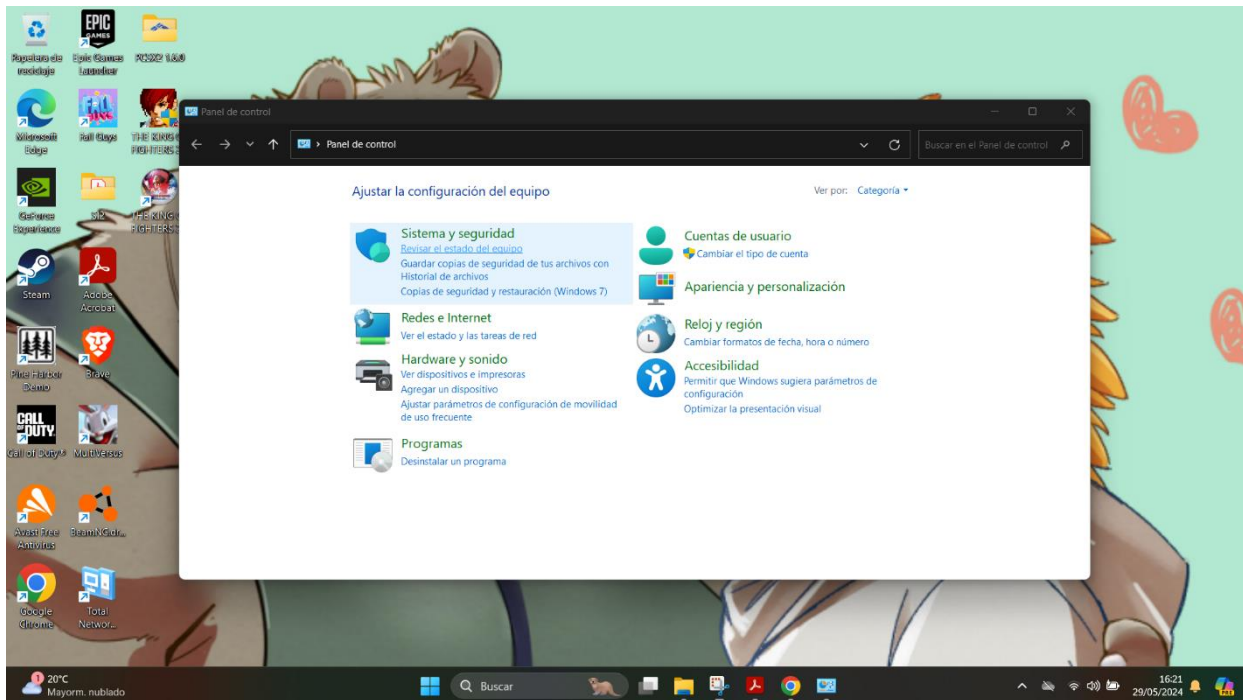
Justificación.

Las auditorías de seguridad informática y las bitácoras son elementos cruciales para garantizar la integridad y confidencialidad de la información en las organizaciones. Permíteme explicarte por qué son tan importantes:

1. Auditorías de seguridad informática:
 - Detectan errores y debilidades: Estas evaluaciones minuciosas identifican vulnerabilidades y brechas en los sistemas informáticos. Al descubrir debilidades, las empresas pueden tomar medidas correctivas para fortalecer su seguridad.
 - Control de información sensible: Las auditorías permiten un mayor control sobre la información confidencial de empleados, clientes y proveedores. Al evaluar los sistemas, se asegura que los datos estén protegidos adecuadamente.
 - Previenen fraudes: Al detectar posibles actuaciones fraudulentas, tanto internas como externas, las auditorías ayudan a prevenir pérdidas financieras y daños a la reputación de la empresa.
2. Bitácoras de seguridad informática:
 - Registro detallado: Las bitácoras registran eventos y actividades relacionadas con la seguridad. Esto incluye cambios en la configuración, accesos no autorizados y otros incidentes. Estos registros son esenciales para el seguimiento y la detección temprana de amenazas.
 - Evidencia y trazabilidad: Las bitácoras proporcionan una línea de tiempo detallada de lo que sucede en los sistemas. Esto ayuda a rastrear incidentes y a demostrar el cumplimiento de políticas de seguridad ante autoridades o auditores externos.

En resumen, las auditorías y las bitácoras son herramientas fundamentales para mantener la seguridad informática y proteger los activos de información en las organizaciones. Su implementación contribuye a una ciberseguridad más sólida y confiable.

Desarrollo.



Visor de eventos

Archivo Acción Ver Ayuda

Visor de eventos (local)

Introducción y resumen Última actualización: 29/05/2024 16:24:05

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	-	-	-	0	0	0
Error	-	-	-	13	69	171
Advertencia	-	-	-	16	30	209
Información	-	-	-	135	712	2.982
Auditoría corr..	-	-	-	694	3.873	15.043

Nodos vistos recientemente

Nombre	Descripción	Modificado	Creado
--------	-------------	------------	--------

Resumen de registro

Nombre de registro	Tamaño (a..	Modificado	Habilitado	Directiva de retención
Windows PowerShell	1,07 MB/1..	26/05/2024 20:39:36	Habilitado	Sobrescribir eventos si fu..
Sistema	4,07 MB/2..	29/05/2024 16:23:35	Habilitado	Sobrescribir eventos si fu..
Seguridad	20,00 MB/..	29/05/2024 16:24:04	Habilitado	Sobrescribir eventos si fu..
RefreshRateService_log	68 KB/1,00..	16/05/2024 21:01:48	Habilitado	Sobrescribir eventos si fu..
OneApp_JGCC	68 KB/1,00..	29/05/2024 16:10:39	Habilitado	Sobrescribir eventos si fu..

Acciones

Visor de eventos (local)

Abrir registro guardado..

Crear vista personalizada..

Importar vista personalizada..

Conectarse a otro equipo..

Ver

Actualizar

Ayuda

GBP/MXN +0.28%

Buscar

16:25 29/05/2024

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 suscripciones

Aplicación Número de eventos: 3.068

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	29/05/2024 16:22:06	Chrome	256	(1)
Información	29/05/2024 16:22:04	Chrome	256	(1)
Información	29/05/2024 16:20:48	Security-SPP	16384	Ninguno
Información	29/05/2024 16:20:18	Security-SPP	16394	Ninguno
Información	29/05/2024 16:17:39	Security-SPP	16384	Ninguno
Información	29/05/2024 16:17:06	Security-SPP	16394	Ninguno
Información	29/05/2024 16:11:14	Security-SPP	16384	Ninguno
Información	29/05/2024 16:10:44	Security-SPP	16394	Ninguno
Información	29/05/2024 16:05:53	Security-SPP	16384	Ninguno
Información	29/05/2024 16:05:32	brave	0	Ninguno
Advertencia	29/05/2024 16:05:23	Security-SPP	8233	Ninguno
Advertencia	29/05/2024 16:05:21	Security-SPP	8233	Ninguno

Evento 8233, Security-SPP

General Detalles

El motor de reglas informó de una activación de VL con errores.
Motivo:0x80070078
Id.aplicación = 0ff1ce15-a989-479d-af46-1275c6370663, id. SKU = fbd3be18-a8ef-4fb3-9183-dff60b0d0984
Desencadenador=UserLogon(13)

Nombre de registro: Aplicación

Origen: Security-SPP

Id. del: 8233

Nivel: Advertencia

Usuario: No disponible

Código de operación: Información

Más información: [Ayuda Registro de eventos](#)

Registrado: 29/05/2024 16:05:23

Categoría de tarea: Ninguno

Palabras clave: Clásico

Equipo: HYENMAX

Acciones

Aplicación

Abrir registro guardado..

Crear vista personalizada..

Importar vista personalizada..

Ver

Actualizar

Ayuda

Evento 8233, Security-SPP

Propiedades de evento

Adjuntar tarea a este evento..

Copiar

Guardar eventos seleccionados..

Actualizar

Ayuda

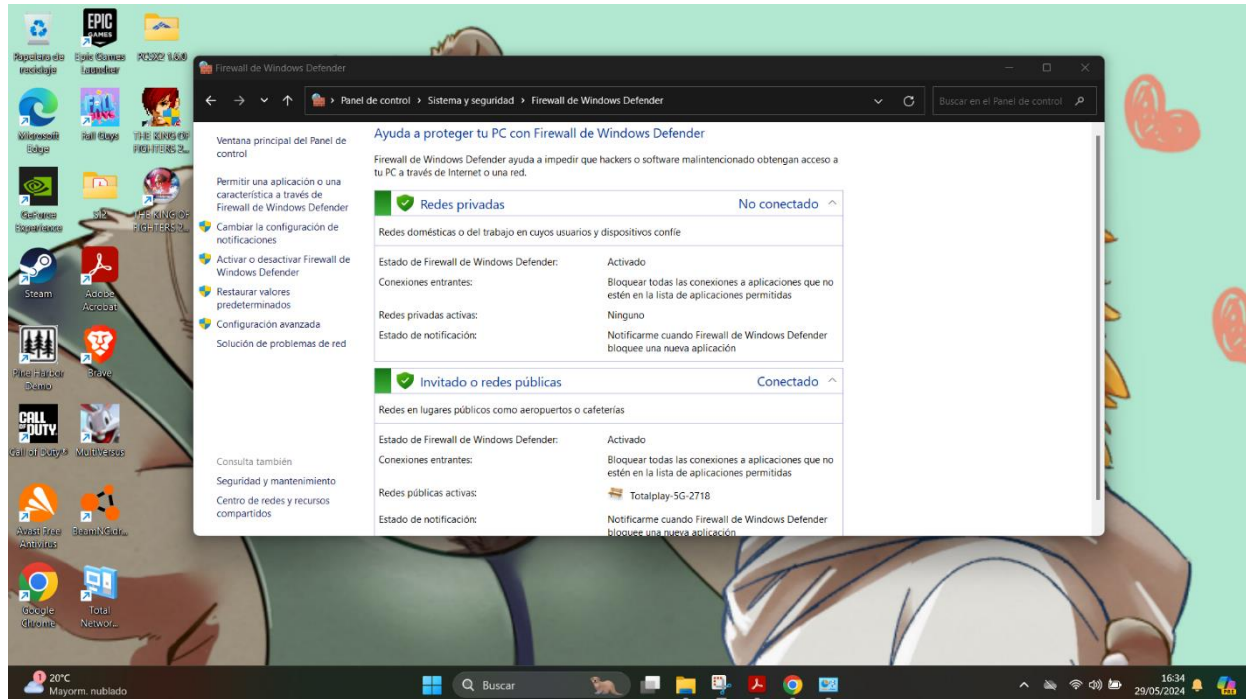
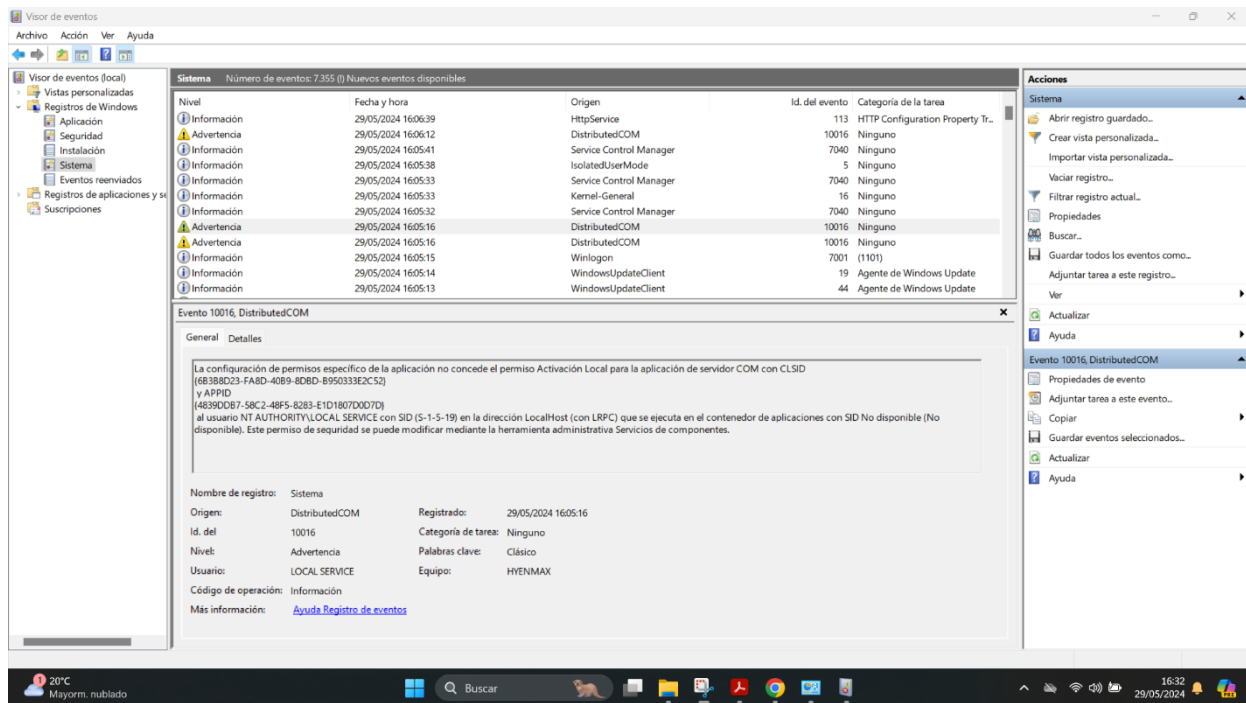
20°C Mayor, nublado

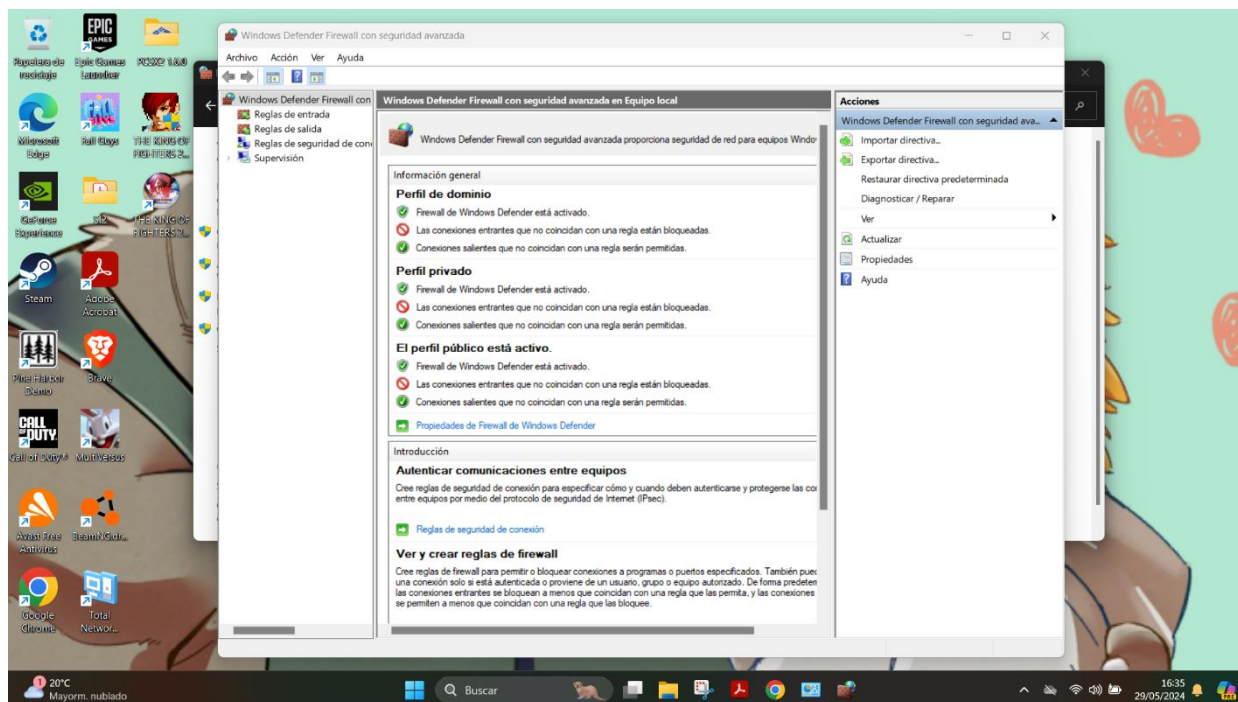
Buscar

16:27 29/05/2024

20°C Mayorm, nublado 16:30 29/05/2024

20°C Mayorm. nublado Buscar 16:31 29/05/2024





Coclucion.

La auditoría de seguridad informática es un proceso crucial para garantizar la integridad, confidencialidad y disponibilidad de los sistemas y datos en el ámbito de la informática. A través de una auditoría, se evalúan y verifican los controles de seguridad implementados en los equipos de cómputo, identificando posibles vulnerabilidades y riesgos.

En mi opinión, mantener una auditoría regular tiene varios beneficios:

1. **Detección temprana de amenazas:** La auditoría permite detectar actividades sospechosas o no autorizadas, como accesos no autorizados, intentos de intrusión o malware. Al identificar estas amenazas de manera temprana, se pueden tomar medidas preventivas para evitar daños mayores.
2. **Cumplimiento normativo:** Muchas organizaciones están sujetas a regulaciones y estándares de seguridad. La auditoría ayuda a garantizar que se cumplan estos requisitos, evitando sanciones legales y protegiendo la reputación de la empresa.
3. **Mejora continua:** La auditoría proporciona información valiosa sobre las debilidades y áreas de mejora en los sistemas. Esto permite implementar cambios y actualizaciones para fortalecer la seguridad y reducir los riesgos.
4. **Confianza y transparencia:** Las auditorías demuestran a los clientes, socios comerciales y partes interesadas que la organización se toma en serio la seguridad. La transparencia en los procesos de auditoría genera confianza y credibilidad.

En resumen, la auditoría en seguridad informática es esencial para proteger los activos digitales y garantizar un entorno seguro. Es una inversión que vale la pena para prevenir incidentes costosos y salvaguardar la confianza de todos los involucrados.