Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad 3 – Auditoria y bitácora

Seguridad informática II

Ingeniería en Desarrollo de Software

Tutor:

Jessica Hernández Romero

Alumno:

Alejandro Abarca Gerónimo

Fecha:

28 de septiembre de 2024

Indice

Introducción

La ciberseguridad es fundamental para prevenir ataques e intentos de robo de información, violaciones de seguridad y daños a la propiedad. Los dispositivos de todo tipo, incluidas tabletas y teléfonos, corren cada vez más riesgos porque ahora almacenan más datos públicos y privados que la mayoría de las computadoras.

La seguridad de la tecnología de la información incluye una amplia gama de medidas de seguridad interdisciplinaria diseñada para proteger las redes informáticas y sus datos de cualquier forma de daño, fuga, filtración de información privada o ataques.

Dado que los ataques cibernéticos han aumentado exponencialmente durante años anteriores, la mayoría de las empresas y las personas enfrentan interrupciones comerciales y robo de datos.

Algunas herramientas pueden supervisar las redes durante todo el día incluidos equipos de hardware, aplicaciones, ancho de banda, tráfico de red entre otros componentes de la red. Estas herramientas notifican de inmediato en caso de que un servidor, switch o router este causando problemas para poder aplicar las medidas rápidamente asegurándose de que el equipo en general se mantenga en condiciones óptimas. También permiten mantener las interrupciones y bloqueos al mínimo, asi como realizar monitoreo constante de toda la red, al instalar una herramienta de este tipo se escanean y agregan automáticamente todos los dispositivos dentro de rango de IP concreta.

Descripción

Tomando en cuenta las actividades 1 y 2, se realizará lo siguiente:
Auditoría y bitácora:

- Realizar una auditoría del equipo desde el Panel de control > Herramientas administrativas; o desde una herramienta digital.

- Guardar la bitácora e iniciar una nueva.
- Adjuntar capturas de pantalla.

A continuación se procederá a realizar una auditoría desde el equipo de cómputo o utilizando una herramienta especializada, esto permitirá identificar las licencias de los recursos instalados y obtener información precisa de los recursos del equipo de cómputo.

Las auditorías y bitácoras proporcionan un escenario de los posibles ataques que se pueden presentar y a su vez poder prevenirlos, de igual manera otorga información legal respectos las licencias obtenidas y faltantes, mantener un control total del equipo apertura una mayor seguridad en los mecanismos que se implementen para salvaguardar los recursos valiosos como es la información.

- Validar las licencias de sus recursos por cuestiones de los aspectos legales y regulatorios.
- Control total y auditoría cada semana del sistema, hardware, software, licencias y red.
- Es importante que se guarde la bitácora, eliminarla e iniciar una nueva para detectar los cambios desde el día 1.

Justificación

La ciberseguridad proporciona a los clientes y empresas protección contra los ciberataques. Si su información no está protegida, puede causar pérdidas financieras importantes y afectar su reputación como organización.

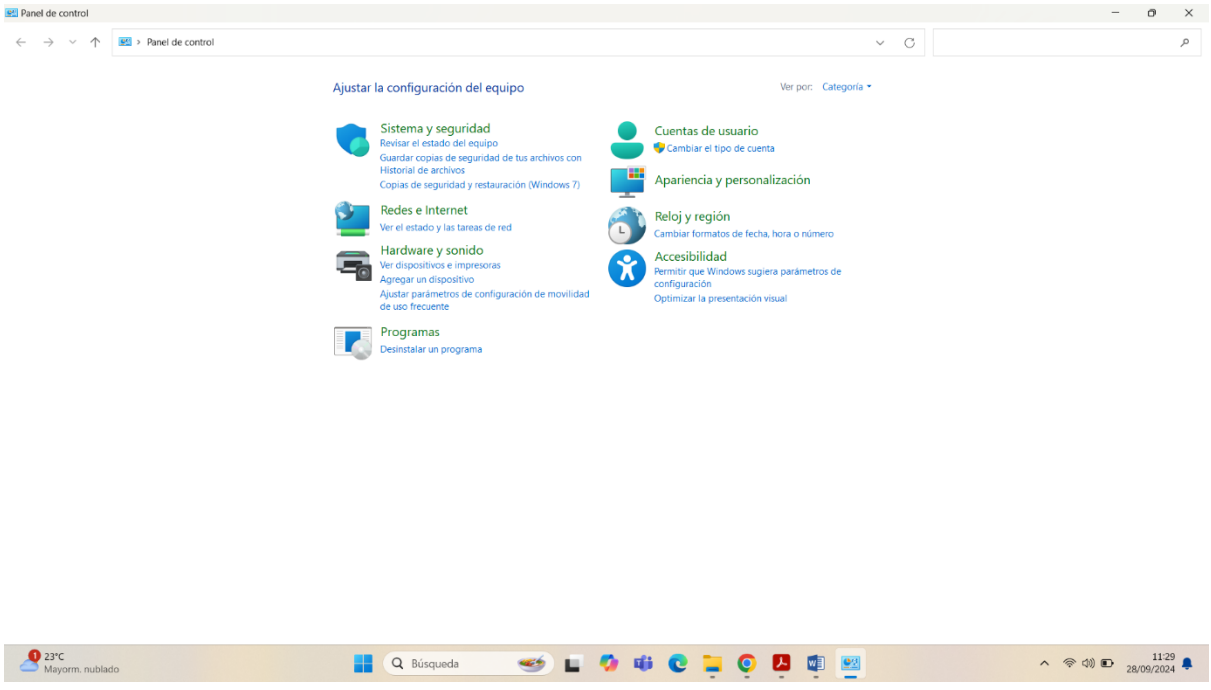
Los ciberataques representan una amenaza cada vez mayor para las empresas de todo el mundo. En los últimos años, con el aumento de los ataques a la información, los cortafuegos, el software antivirus y el software antispyware son esenciales para la seguridad operativa. Todos ellos incluyen un conjunto de

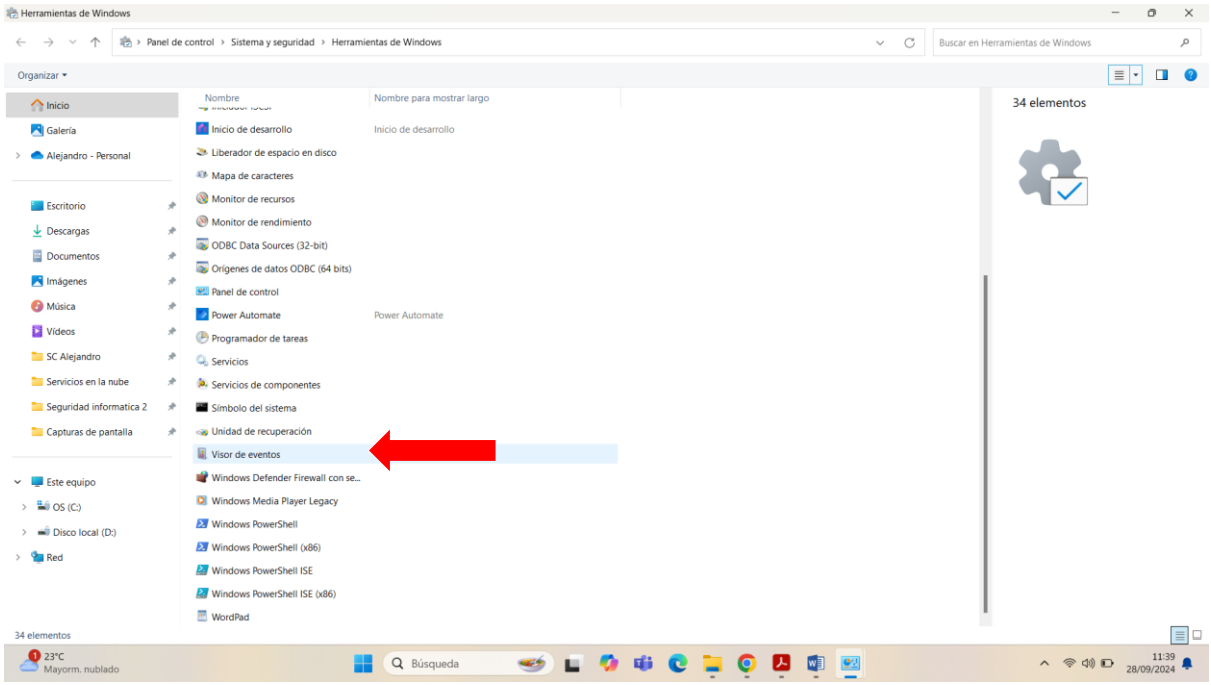
procesos y herramientas, cuyo objetivo principal es proteger los recursos informáticos de la organización del uso no autorizado de los sistemas informáticos y sus recursos.

La protección incluye servidores e infraestructura de comunicaciones, sistemas informáticos, bases de datos, archivos y equipos terminales o puntos finales. En definitiva, todos los componentes informáticos que ayudan al funcionamiento de una empresa. Cuando se trata de ciberseguridad, la prevención es siempre la mejor opción, porque una vez que eres víctima de un ataque, la recuperación puede ser difícil. Por ello, es importante identificar los elementos que hacen de la ciberseguridad un aspecto importante.

Desarrollo:

Comenzamos ingresando al Panel de control de nuestro sistema en el equipo de cómputo para después continuar en el Visor de eventos.

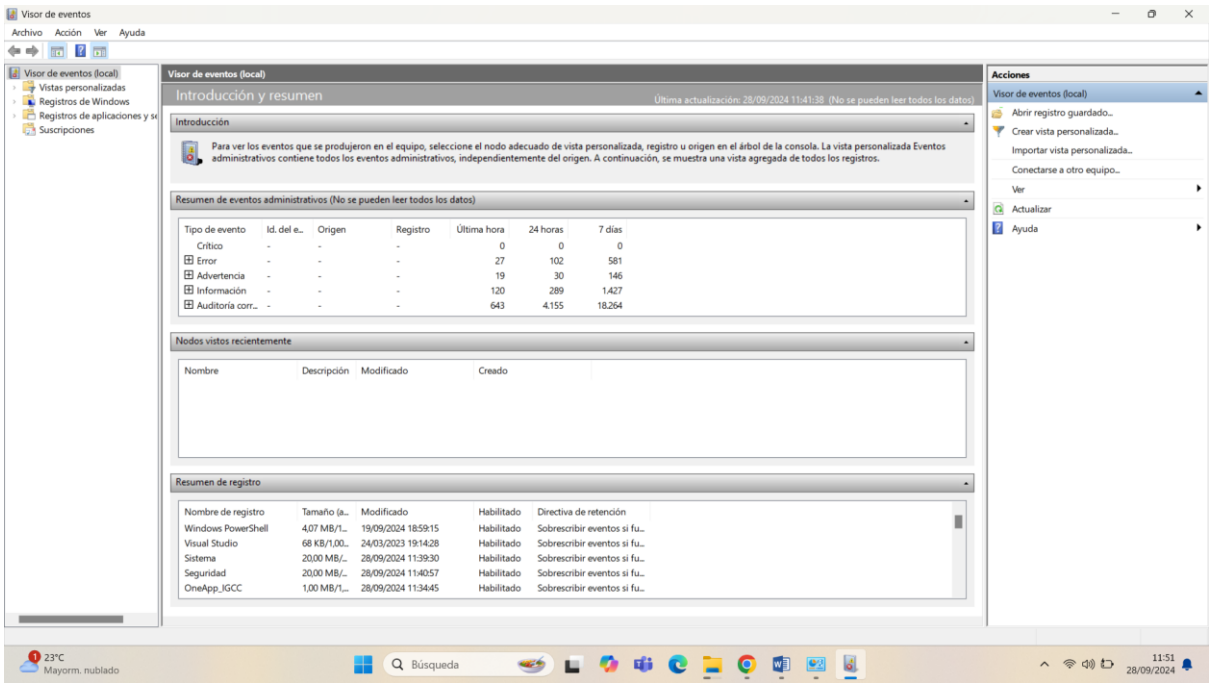




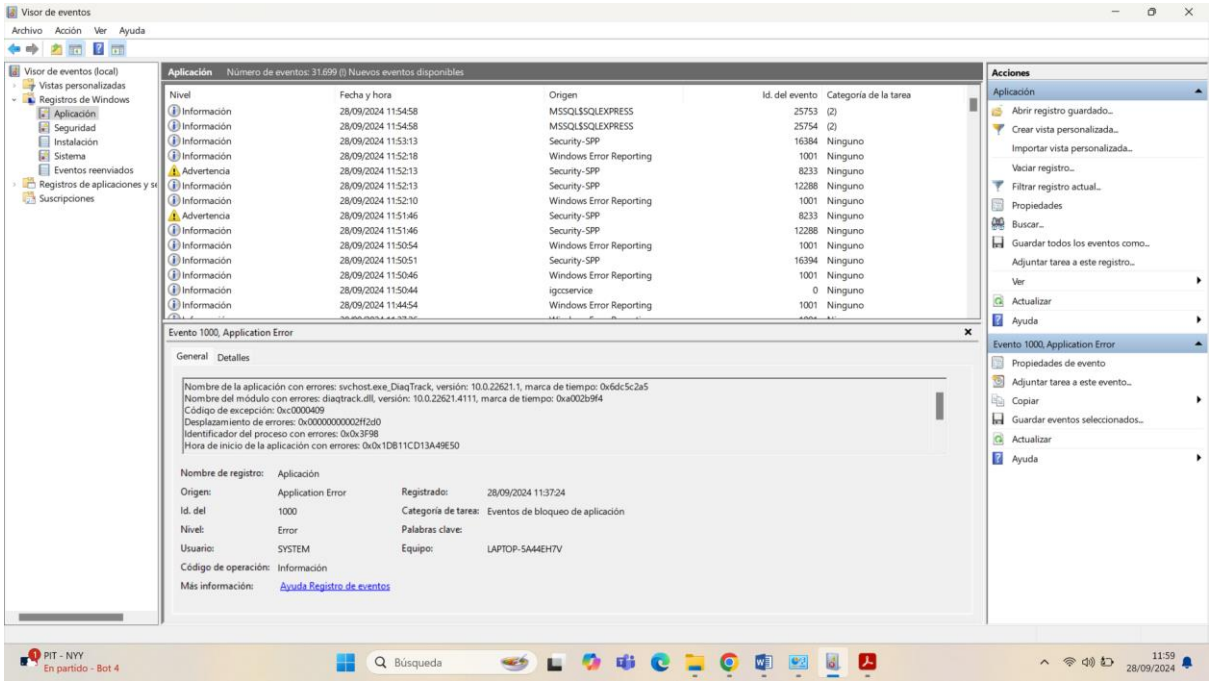
Auditoría y Bitácora:

Bitácora

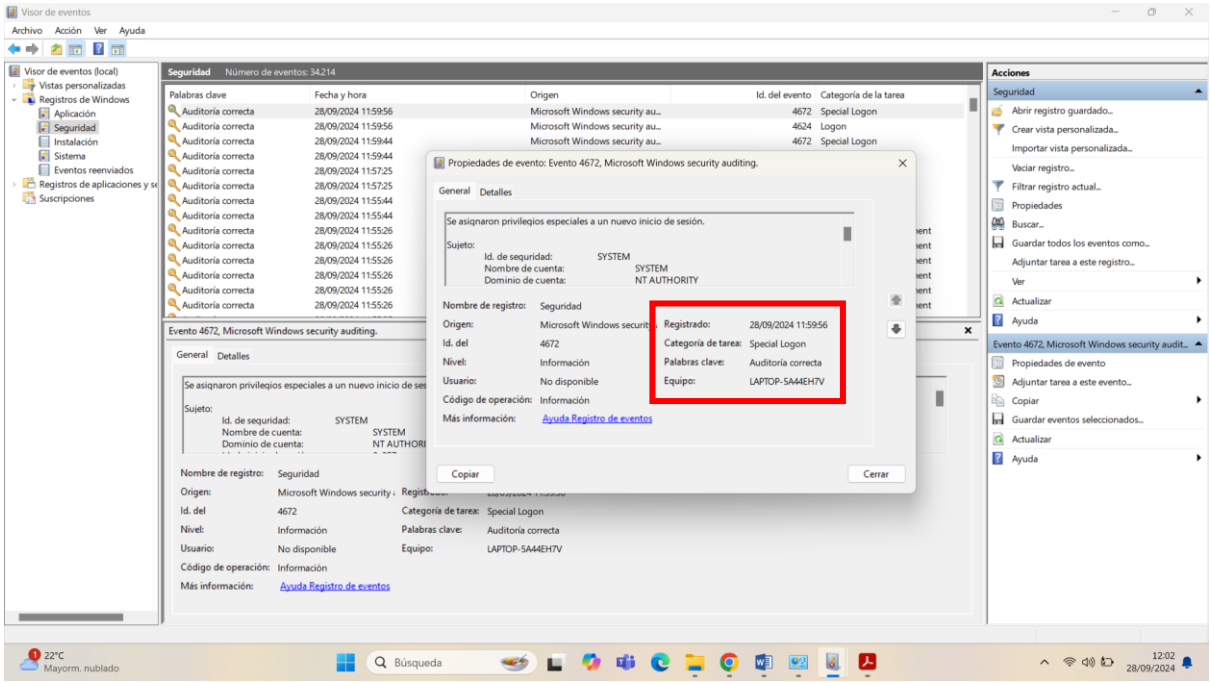
En este primer analisis revisamos un resumen de eventos administrativos en el cual podemos ver la cantidad de eventos que se han generado satisfactoriamente asi como eventos criticos y de advertencia.



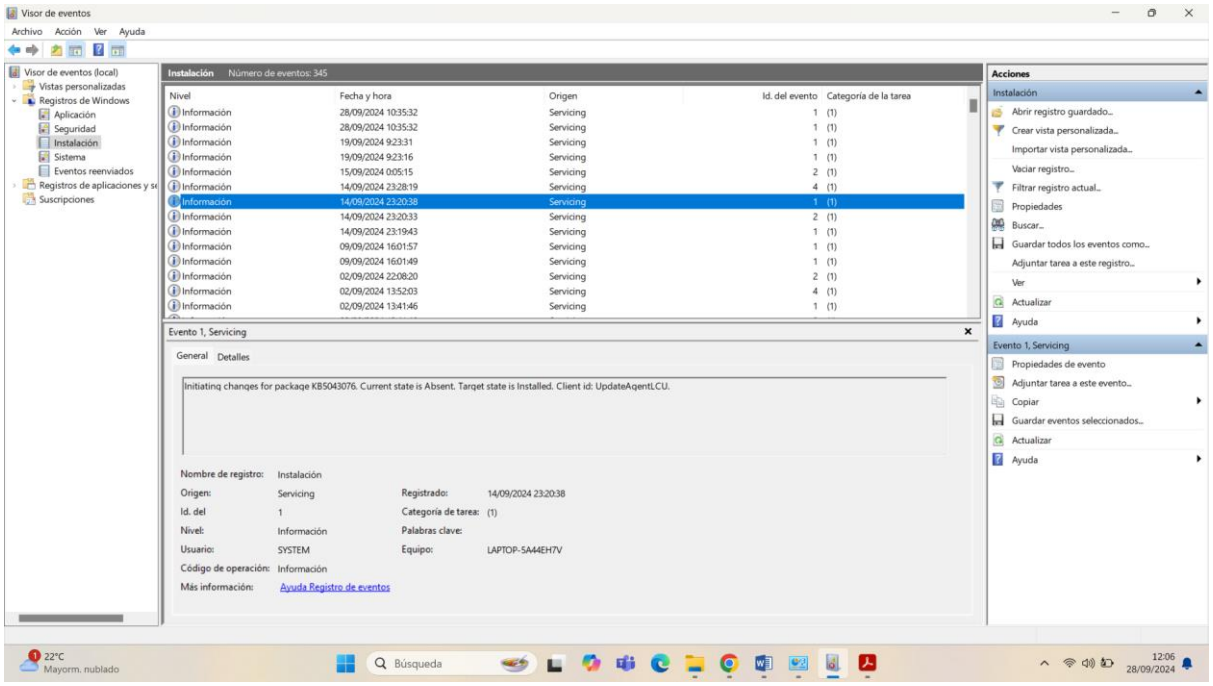
Auditoría de equipo.
Análisis por aplicación.



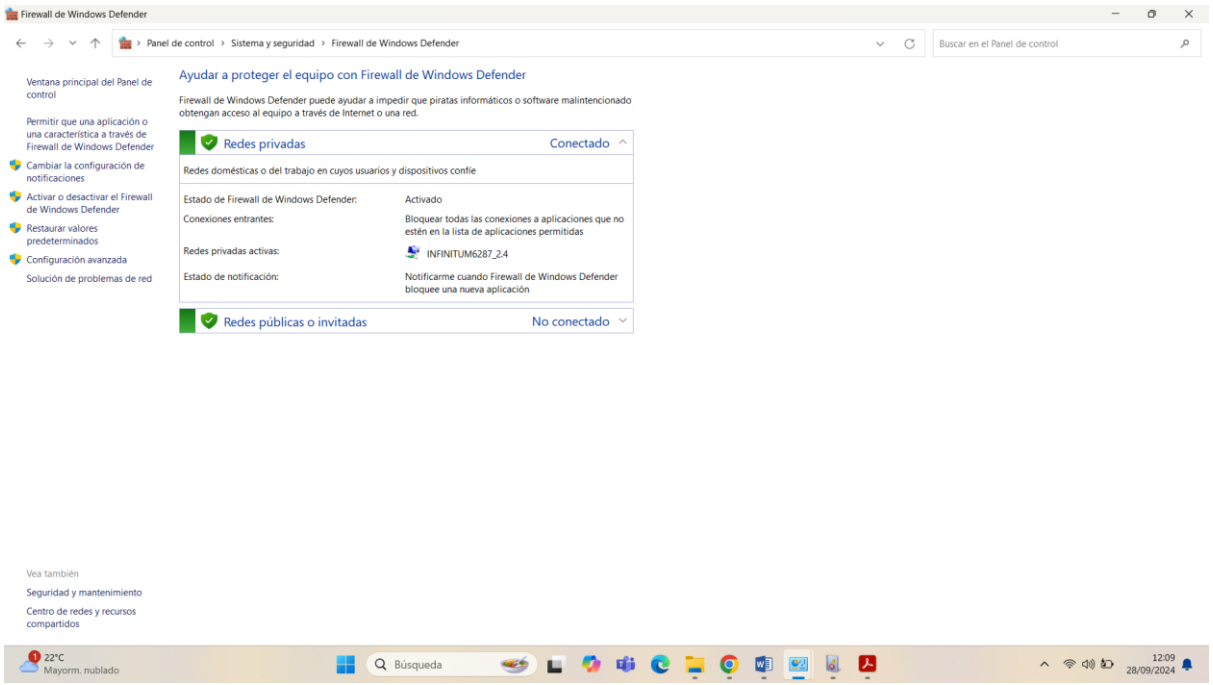
Al revisar en el submenú de seguridad se detectó que la auditoria fue realizada de forma correcta.



A continuación revisamos los registros de instalación de nuestro equipo.



Por ultimo ingresamos al apartado de Firewall de Windows defender para validar las conexiones a la red y que se encuentren activos algunas opciones en específico del equipo para una mayor seguridad.



Importancia de seguridad (prevención, monitoreo, auditoría)

Las auditorías de seguridad tienen una gran importancia dentro de los sistemas informáticos de las empresas ya que por medio de estos análisis se determinar si los procesos existentes son efectivos para garantizar que una organización sea verdaderamente segura y cumpla con los estándares y regulaciones aplicables de la industria. Las auditorías de seguridad recopilan información crítica sobre la seguridad, confiabilidad, eficiencia y eficacia de una organización. Durante el proceso de auditoría, los auditores examinan el entorno de trabajo, los equipos y diversos procesos para evaluar la eficiencia de la organización, las prácticas de seguridad.

Al realizar una auditoría de seguridad, los auditores deben realizar un examen exhaustivo del negocio, identificar problemas y proponer soluciones, así como diversas formas de mejorar la organización.

Los auditores no pueden dejar nada sin remover, ya que esto puede generar problemas en el futuro. A través de auditorías, las organizaciones pueden identificar riesgos que podrían haber pasado desapercibidos durante las operaciones de rutina y mitigar los riesgos para garantizar la seguridad de los empleados.

Conclusión

En resumen, las auditorías de seguridad son una herramienta importante para cualquier organización que quiera proteger sus activos y datos. No solo ayudan a identificar y mitigar vulnerabilidades, sino que también garantizan el cumplimiento y fomentan una cultura de seguridad proactiva. Al realizar auditorías de seguridad periódicas, las organizaciones pueden adaptarse al cambiante panorama de amenazas, mejorar los procesos internos y aumentar la confianza de los clientes y socios.

En un mundo digital cada vez más riesgoso, invertir en una auditoría de seguridad es una decisión estratégica que puede marcar la diferencia entre la resiliencia y el riesgo de posibles incidentes de seguridad.

La auditoría en redes es una herramienta vital para cualquier organización que busque proteger sus activos digitales, mejorar la eficiencia operativa y cumplir con las normativas vigentes. Implementar auditorías de manera regular ayuda a anticiparse a problemas y fortalece la infraestructura de red ante las amenazas emergentes.

Referencias

1. Seguridad informatica. (2024). hewlett packard enterprise. recuperado 1 de abril de 2024, de https://www.hpe.com/mx/es/what-is/it-security.html#:~:text=la%20seguridad%20de%20la%20tecnolog%c3%ada,de%20informaci%c3%b3n%20privada%20o%20ataque

2. Auditorías de red: herramientas, informes y procedimientos. (s. f.). https://www.paessler.com/es/network-audit?utm_term=&utm_campaign=1635204137&utm_content=&utm_source=google&utm_medium=cpc&utm_adgroup=94233284309&utm_device=c&gad_source=1&gclid=cj0kcqjwo8s3bhdearisafrmkooskakmzfcdd2fyt1lqhl4qmyh259v7lqz52jqlvs0wtbz5imwh_w4aavxdealw_wcb

3. Seguridad informatica. (2024). hewlett packard enterprise. recuperado 1 de abril de 2024, de https://www.hpe.com/mx/es/what-is/it-security.html#:~:text=la%20seguridad%20de%20la%20tecnolog%c3%ada,de%20informaci%c3%b3n%20privada%20o%20ataque