

# **Actividad 2 - Monitoreo de Red**


## **Seguridad Informática 2**

### **Ingeniería en Desarrollo de Software**

**Tutor: Jessica Hernández Romero**

**Alumno: Homero Ramirez Hurtado**

**Fecha: 21 de Mayo del 2024**



Índice.

. Introducción.

. Descripción.

. Justificación.

- . Desarrollo,
- Resultado del Escaneo.
    - Reporte.
  - Auditoría Semanal y Reporte.

. Conclusión.

. Referencias.



## Introducción.

La seguridad informática es fundamental para garantizar que los sistemas de información se mantengan de manera correcta y se utilicen según lo planeado. Uno de los aspectos clave en la seguridad informática es el monitoreo de red, que permite a los administradores supervisar y evaluar el funcionamiento de una red en tiempo real. A continuación, te presento una breve introducción:

El monitoreo de red proporciona a los administradores la información necesaria para determinar si una red está funcionando de manera óptima. Mediante herramientas como el software de monitoreo de redes, los administradores pueden identificar deficiencias y optimizar la eficiencia de manera proactiva. Algunos aspectos importantes del monitoreo de red son:

1. Visión completa de la red: El monitoreo permite obtener una imagen clara de todos los dispositivos conectados a la red y cómo se mueven los datos a través de ella. Esto incluye identificar los flujos de tráfico, la carga de trabajo y los posibles cuellos de botella.
2. Detección de problemas: El monitoreo continuo permite identificar rápidamente cualquier problema o anomalía en la red. Esto puede incluir fallas en dispositivos, congestión, ataques o comportamientos inusuales.
3. Optimización y corrección: Al detectar problemas de manera temprana, los administradores pueden tomar medidas correctivas para mantener la red funcionando sin interrupciones. Esto incluye ajustar configuraciones, aplicar parches de seguridad y resolver problemas de rendimiento.

En resumen, el monitoreo de red es esencial para mantener la seguridad y el rendimiento de las redes informáticas. Los administradores deben estar atentos a las señales de alerta y utilizar herramientas adecuadas para garantizar una operación fluida y proteger contra posibles amenazas.

## Descripción.

La seguridad informática y el monitoreo de redes son aspectos cruciales para proteger los sistemas y datos de posibles ataques. A continuación, describiré los factores que enfatizan su importancia:

1. Prevención de ataques de acceso:
  - Implementar medidas como autenticación multifactor (MFA), contraseñas seguras y control de acceso basado en roles.
  - Evitar que usuarios no autorizados obtengan acceso a sistemas y datos sensibles.
2. Prevención de accesos a las redes:
  - Configurar firewalls, segmentar redes y restringir el acceso a puertos y servicios.
  - Utilizar VPNs para conexiones remotas y cifrado para proteger la comunicación.

3. Validación de licencias:

- Garantizar que los recursos (software, hardware, servicios en la nube) tengan licencias válidas.
- Cumplir con regulaciones y evitar sanciones legales.

4. Auditoría y control total:

- Realizar auditorías periódicas para detectar vulnerabilidades y anomalías.
- Supervisar cambios en sistemas, software y licencias.
- Mantener actualizaciones y parches.

5. Monitoreo completo de la red:

- Utilizar herramientas de monitoreo para supervisar tráfico, eventos y comportamientos anómalos.
- Detectar intrusiones, malware y actividades sospechosas.

6. Bitácora y registro de cambios:

- Registrar eventos relevantes en una bitácora.
- Almacenar registros de auditoría y seguimiento.
- Iniciar nuevas bitácoras regularmente para detectar cambios desde el inicio.

En resumen, la seguridad informática y el monitoreo de redes son esenciales para proteger la integridad, confidencialidad y disponibilidad de los sistemas y datos empresariales. Mantenerse alerta y proactivo es fundamental para prevenir y mitigar riesgos.

Justificación.

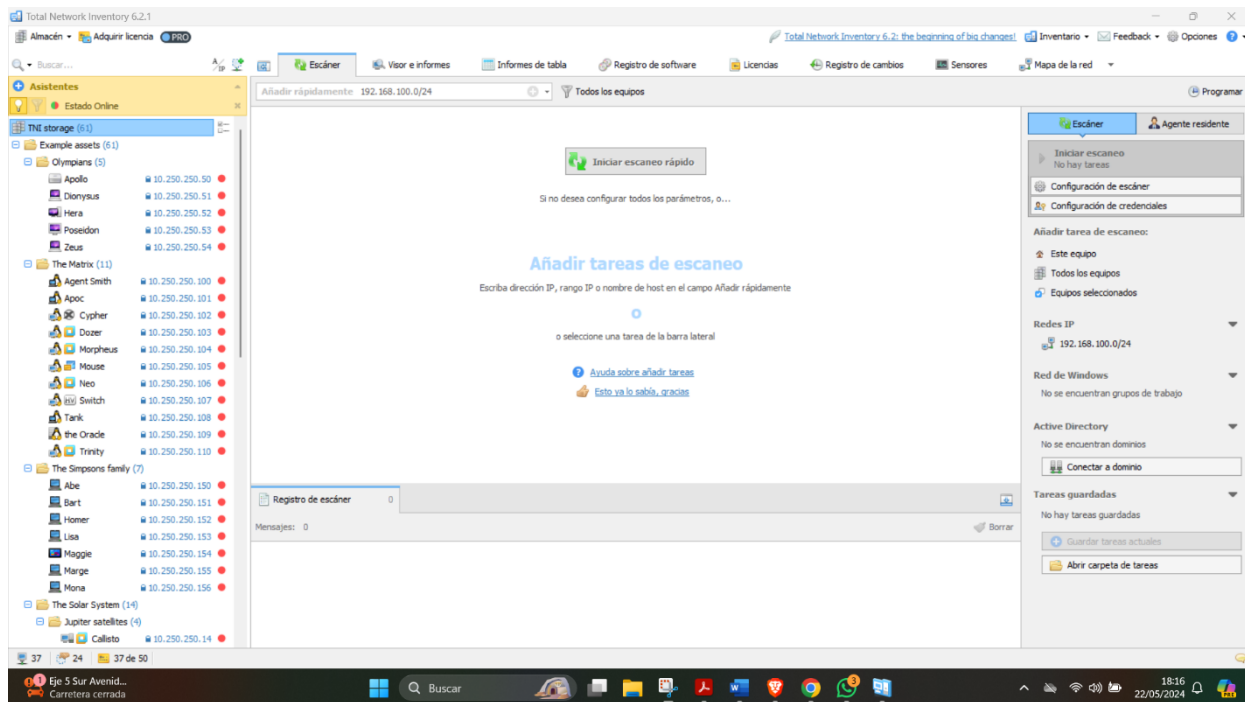
Total Network Inventory es una herramienta valiosa en el ámbito de la seguridad informática debido a sus características y funcionalidades. A continuación, te proporciono una justificación de su uso:

1. Monitorización en tiempo real: Total Network Inventory permite monitorizar el estado en línea de los equipos de la red. Esto es crucial para detectar problemas de seguridad de manera anticipada y tomar medidas preventivas.
2. Gestión de contraseñas: El software permite adjuntar contraseñas únicas a los dispositivos que las requieren. Esto es fundamental para garantizar la seguridad de los dispositivos y evitar accesos no autorizados.
3. Informes detallados: Total Network Inventory facilita la creación de informes complejos utilizando filtros y condiciones. Estos informes pueden ayudar a identificar vulnerabilidades, detectar cambios no autorizados y evaluar el cumplimiento de políticas de seguridad.

4. Automatización de inventarios: El software escanea automáticamente la red y crea informes sobre el software instalado y el hardware reemplazado. Esta automatización ahorra tiempo y reduce errores humanos al identificar dispositivos.
5. Costo efectivo: Total Network Inventory es una solución económica, pero de buena calidad. Al hacer uso de un software libre, las empresas pueden disminuir considerablemente sus costos en el manejo de inventarios.

En resumen, Total Network Inventory mejora la seguridad informática al proporcionar una visión completa de los dispositivos en la red, facilitar la gestión de contraseñas y generar informes detallados para una toma de decisiones más informada. Su uso contribuye a fortalecer la seguridad y eficiencia de las organizaciones.

## Desarrollo.



Total Network Inventory 6.2.1

Almacén • Adquirir licencia PRO

Escáner

Visor e informes

Informes de tabla

Registro de software

Licencias

Registro de cambios

Sensores

Mapa de la red

Asistentes

Estado Online

TNI storage (66)

Example assets (51)

Olympians (5)

Apollo 10.250.250.50

Dionysus 10.250.250.51

Hera 10.250.250.52

Poseidon 10.250.250.53

Zeus 10.250.250.54

The Matrix (11)

Agent Smith 10.250.250.100

Apoc 10.250.250.101

Cypher 10.250.250.102

Dozer 10.250.250.103

Morpheus 10.250.250.104

Mouse 10.250.250.105

Neo 10.250.250.106

Switch 10.250.250.107

Tank 10.250.250.108

the Oracle 10.250.250.109

Trinity 10.250.250.110

The Simpsons family (7)

Abe 10.250.250.150

Bart 10.250.250.151

Homer 10.250.250.152

Lisa 10.250.250.153

Maggie 10.250.250.154

Marge 10.250.250.155

Mona 10.250.250.156

The Solar System (14)

Jupiter satellites (4)

Callisto 10.250.250.14

Añadir rápidamente 192.168.100.0/24

Tareas (5)

Estado

100% Hecho

Fallo de escaneo: No hay puertos abiertos para protocolos soportados; SNMP: Comunidad incorrecta o SNMP no dispo

Fallo de escaneo: No hay puertos abiertos para protocolos soportados; SNMP: Comunidad incorrecta o SNMP no dispo

Fallo de escaneo: No hay puertos abiertos para protocolos soportados; SNMP: Comunidad incorrecta o SNMP no dispo

Fallo de escaneo: No hay puertos abiertos para protocolos soportados; SNMP: Comunidad incorrecta o SNMP no dispo

192.168.100.8 (HYPERMAX) 84-5C-F2-82-69-CD 100% Escaneo terminado

Registro de escáner

Mensajes: 1

22 may 2024 en 18:19 — Superencia: el error "No hay puertos abiertos para protocolos admitidos" puede deberse a la configuración del firewall en los equipos remotos. Haga clic en el botón Ayuda a la derecha para más información acerca de las posibles soluciones.

Escáner

Agente residente

Escaneo terminado

Existen errores

Volver a edición

Borrar finalizado

Borrar todo

Añadir tarea de escaneo:

Este equipo

Todos los equipos

Equipos seleccionados

Redes IP

192.168.100.0/24

Red de Windows

No se encuentran grupos de trabajo

Active Directory

No se encuentran dominios

Conectar a dominio

Tareas guardadas

No hay tareas guardadas

Guardar tareas actuales

Abrir carpeta de tareas

Temperatura act... Cerca del récord

38 4 24 38 de 50

18:20 22/05/2024

Total Network Inventory 6.2.1

Almacén • Adquirir licencia PRO

Escáner

Visor e informes

Informes de tabla

Registro de software

Licencias

Registro de cambios

Sensores

Mapa de la red

Asistentes

Estado Online

TNI storage (66)

Example assets (51)

Olympians (5)

Apollo 10.250.250.50

Dionysus 10.250.250.51

Hera 10.250.250.52

Poseidon 10.250.250.53

Zeus 10.250.250.54

The Matrix (11)

Agent Smith 10.250.250.100

Apoc 10.250.250.101

Cypher 10.250.250.102

Dozer 10.250.250.103

Morpheus 10.250.250.104

Mouse 10.250.250.105

Neo 10.250.250.106

Switch 10.250.250.107

Tank 10.250.250.108

the Oracle 10.250.250.109

Trinity 10.250.250.110

The Simpsons family (7)

Abe 10.250.250.150

Bart 10.250.250.151

Homer 10.250.250.152

Lisa 10.250.250.153

Maggie 10.250.250.154

Marge 10.250.250.155

Mona 10.250.250.156

The Solar System (14)

Jupiter satellites (4)

Callisto 10.250.250.14

Equipos seleccionados: 66 Equipos con información

Resumen de grupo

TNI storage

Gráficos circulares

Estado Online

Online 4

Offline 38

Nombre de host sin resolución 0

Desconocido 24

Equipos físicos: 27

Sobremesa Windows 7

Portátil Windows 7

Portátil Linux 3

Macbook 2

Windows tablet 1

Servidor Linux 1

Mac 1

Mac Pro 1

Mac Mini 1

Controlador de dominio 1

NAS 1

Servidor ESX/ESXi 1

Equipos virtuales: 11

VMware 8

Virtual PC 1

Xen 1

Hyper-V 1

Fabricante

ASUS 7

Apple Inc. 5

HP 3

LENOVO 3

Acer 1

Dell Inc. 1

Varias categorías

Resumen de grupo

Información general

Alertas 29

Árbol SNMP

Hardware

Detalles del sistema

Procesador

Memoria del sistema

Sistema de vídeo

Sistema de audio

Datos de la memoria

Red

Dispositivos periféricos

Dispositivos

Sensores de hardware

Batería

Software

Sistema operativo

Software

Microsoft Store

Claves de licencia

Revisiones

Actualizaciones de Windows

Historial de actualizaciones de Windows

Seguridad

Carpeta "Archivos de programa"

30°C Lluvia suave

38 4 24 38 de 50

18:25 22/05/2024

Total Network Inventory 6.2.1

Almacén • Adquirir licencia • PRO

Buscar... Escáner Visor e informes Informes de tabla Registro de software Licencias Registro de cambios Sensores Mapa de la red

Asistentes Estado Online

THI storage (66)

- Example assets (51)
  - Olympians (5)
    - Apollo 10.250.250.50
    - Dionysus 10.250.250.51
    - Hera 10.250.250.52
    - Poseidon 10.250.250.53
    - Zeus 10.250.250.54
  - The Matrix (11)
    - Agent Smith 10.250.250.100
    - Apoc 10.250.250.101
    - Cypher 10.250.250.102
    - Dozer 10.250.250.103
    - Morpheus 10.250.250.104
    - Mouse 10.250.250.105
    - Neo 10.250.250.106
    - Switch 10.250.250.107
    - Tank 10.250.250.108
    - the Oracle 10.250.250.109
    - Trinity 10.250.250.110
  - The Simpsons family (7)
    - Abe 10.250.250.150
    - Bart 10.250.250.151
    - Homer 10.250.250.152
    - Lisa 10.250.250.153
    - Maggie 10.250.250.154
    - Marge 10.250.250.155
    - Mona 10.250.250.156
  - The Solar System (14)
    - Jupiter satellites (4)
    - Callisto 10.250.250.14

Equipos seleccionados: 66 Equipos con información

Información sobre el inventario

Fecha de creación	14 ene 2022 - 4:48
Último análisis	14 ene 2022 - 4:48
Usuario asignado	OLYMP(Apollo aka God of the sun)
Nombre	APOLLO-PC (God of the sun)
Dirección IP	10.250.250.50
Dirección MAC	98-5A-EB-15-36-ID (Apple, Inc.)
Ubicación	Mount Olympus
Estado	Offline
Último ping correcto	Nunca
Puertos abiertos	22

Resumen de capturas

Fecha de escaneo	14 ene 2022 - 4:48
Tiempo de exploración	9 seg
Método de escaneo	Escaneo remoto de agente
Módulo de exploración	maci22.01.04.0
Usuario actual	root
Nombre	APOLLO-PC
Dirección IP	10.250.250.50
Dirección MAC	98-5A-EB-15-36-ID (Apple, Inc.)

Sistema operativo

Nombre	macOS v12.0 (Monterey) (64-bit)
Versión	12.0.1 (21A559)
Actualizar	Update 1

Resumen de hardware

Sistema del equipo	Macmini7,1
Número de serie	F2JNHWSZUMA
Procesador	1 x Dual-Core Intel Core i5
Memoria del sistema	8 GB (4 GB 1 x 4 GB)
Adaptador de vídeo	Intel Iris (1.5 GB)
Dispositivo de almacenamiento	Crucial_CT250MX200SSD1 (250 GB)

Dionysus

Información sobre el inventario

Varias categorías

- Resumen de grupo
- Información general
- Alertas 29
- Árbol SNMP
- Hardware
  - Detalles del sistema
  - Procesador
  - Memoria del sistema
  - Sistema de vídeo
  - Sistema de audio
  - Datos de la memoria
  - Red
  - Dispositivos periféricos
  - Dispositivos
  - Sensores de hardware
  - Batería
- Software
  - Sistema operativo
  - Software
  - Microsoft Store
  - Claves de licencia
  - Revisiones
  - Actualizaciones de Windows
  - Historial de actualizaciones de Windows
  - Seguridad
  - Carpeta "Archivos de programa"

Procesador

Apollo

- Dual-Core Intel Core i5
  - Velocidad actual del reloj 2600 MHz
  - Tamaño de caché L2 512 Kb
  - Tamaño de caché L3 3 MB
  - Número de núcleos 2

Dionysus

- Intel Core i7
  - Velocidad actual del reloj 2600 MHz
  - Tamaño de caché L2 1 MB
  - Tamaño de caché L3 6 MB
  - Número de núcleos 4

Hera

- Quad-Core Intel Xeon
  - Velocidad actual del reloj 2000 MHz
  - Tamaño de caché L2 12 MB
  - Número de núcleos 8
- Quad-Core Intel Xeon
  - Velocidad actual del reloj 2000 MHz
  - Tamaño de caché L2 12 MB
  - Número de núcleos 8

Poseidon

- Intel Core 2 Duo
  - Velocidad actual del reloj 2400 MHz
  - Tamaño de caché L2 4 MB
  - Número de núcleos 2

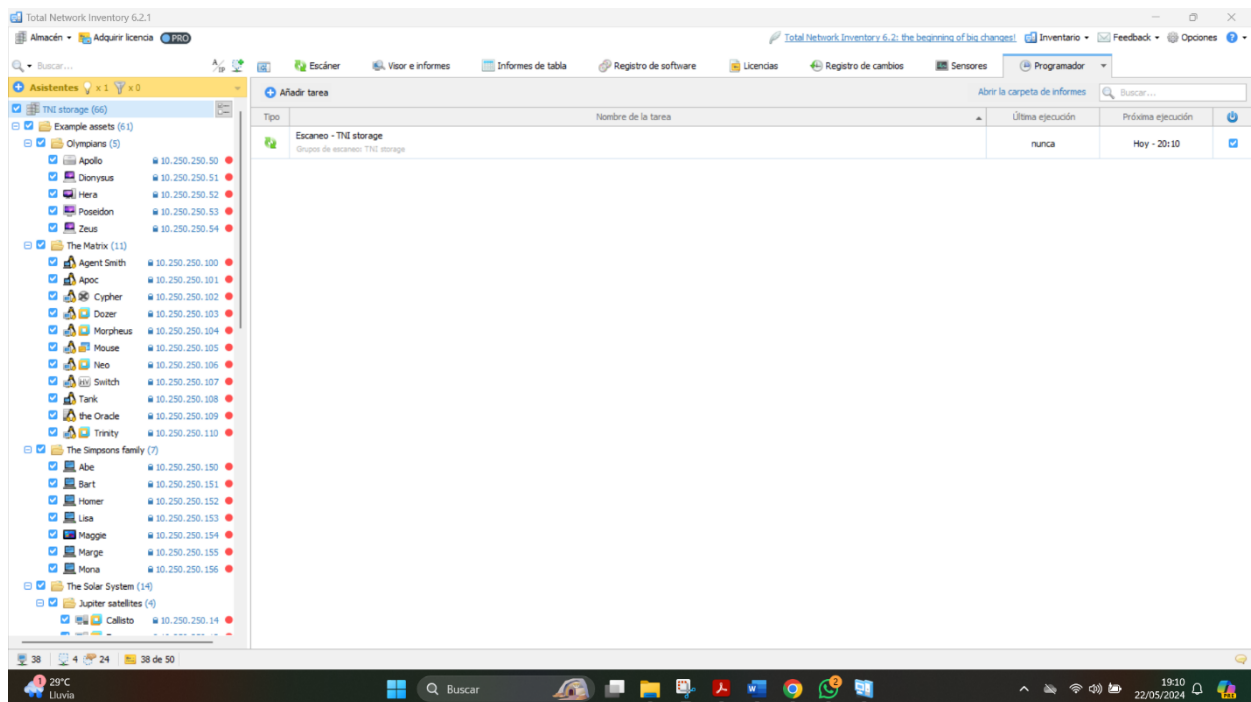
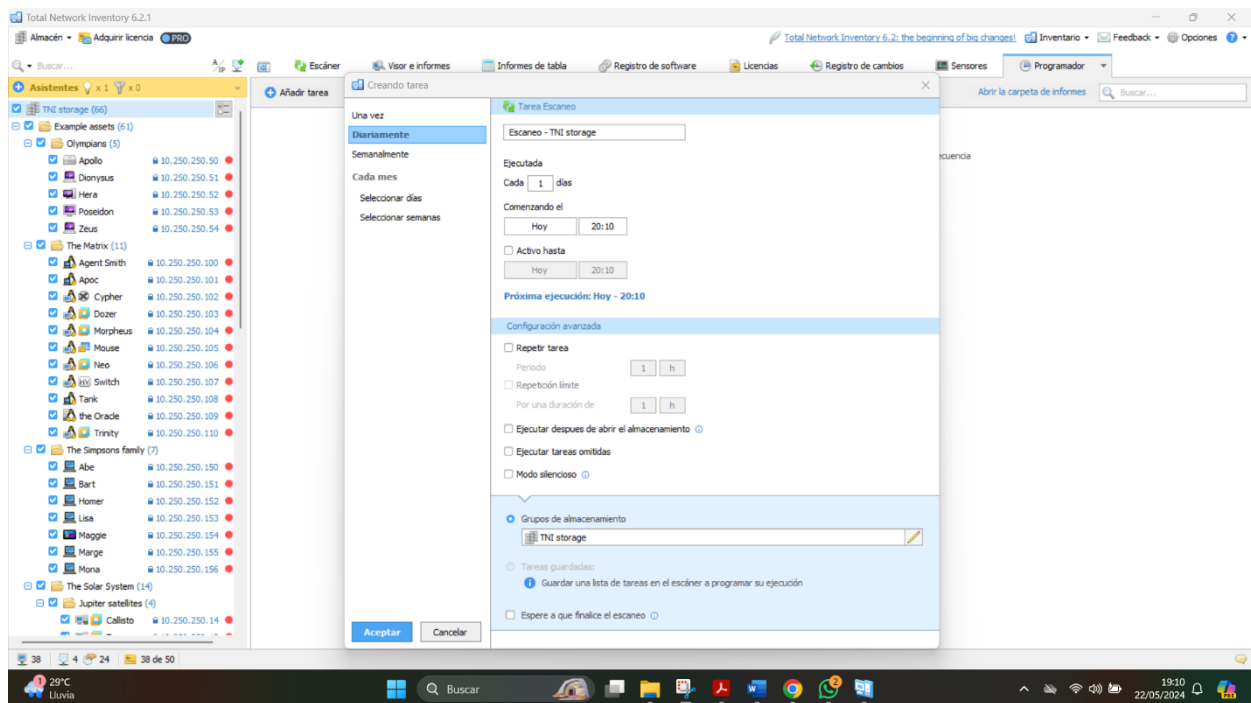
Zeus

Varias categorías

- Resumen de grupo
- Información general
- Alertas 29
- Árbol SNMP
- Hardware
  - Detalles del sistema
  - Procesador
  - Memoria del sistema
  - Sistema de vídeo
  - Sistema de audio
  - Datos de la memoria
  - Red
  - Dispositivos periféricos
  - Dispositivos
  - Sensores de hardware
  - Batería
- Software
  - Sistema operativo
  - Software
  - Microsoft Store
  - Claves de licencia
  - Revisiones
  - Actualizaciones de Windows
  - Historial de actualizaciones de Windows
  - Seguridad
  - Carpeta "Archivos de programa"







## Conclusion.

El monitoreo de red es una práctica esencial para mejorar la seguridad informática. Proporciona visibilidad y control sobre los sistemas y dispositivos conectados, permitiendo detectar, prevenir y responder de manera proactiva a posibles amenazas y vulnerabilidades.

En un mundo cada vez más digitalizado, las empresas enfrentan una gran cantidad de amenazas cibernéticas que atentan contra su continuidad operativa e integridad informática. Para minimizar los riesgos de ataques, es crucial implementar tecnologías y procesos que optimicen el desempeño empresarial y permitan la detección temprana de amenazas. Aquí es donde entra en juego el monitoreo de red.

¿En qué consiste el monitoreo de red? El monitoreo de red implica la supervisión constante de los equipos, aplicaciones y servicios de una red. Esto permite conocer el estado real en que se encuentran, garantizando la fiabilidad, estabilidad y capacidad de detectar incidencias a tiempo. Se realizan pruebas constantes para verificar que no existan brechas de seguridad, vulnerabilidades o amenazas que pongan en riesgo las operaciones empresariales y la integridad informática.

### Importancia del monitoreo:

1. Amenazas sofisticadas: A medida que las empresas implementan soluciones innovadoras, los atacantes también evolucionan sus amenazas. El monitoreo permite visualizar 24/7 el comportamiento de los equipos y detectar amenazas y vulnerabilidades de seguridad.
2. Detección temprana: El monitoreo proactivo ayuda a identificar problemas antes de que se conviertan en brechas de seguridad.
3. Automatización de respuestas: Los sistemas de monitoreo permiten automatizar respuestas ante cualquier incidente, protegiendo así la continuidad operativa y la confidencialidad de los datos.

En resumen, el monitoreo de red es una herramienta fundamental para mantener la seguridad y la integridad de las redes empresariales en un entorno cada vez más digital y amenazante.

## Referencias

### Video Tutoría 2:

[https://academiaglobal-mx.zoom.us/rec/share/lubDvHapDhO0P4BNdWLMKjyK4JG3l3yC7f02Scbl\\_E0xvEnPBzZaxIZlf0gRcu0b.Rf8S1D-UKdD\\_sv6a](https://academiaglobal-mx.zoom.us/rec/share/lubDvHapDhO0P4BNdWLMKjyK4JG3l3yC7f02Scbl_E0xvEnPBzZaxIZlf0gRcu0b.Rf8S1D-UKdD_sv6a)

Video de muestra del Programa: <https://vimeo.com/660530580/13ffe9b44b>