



# MULTITAREA: REDES Y SEGURIDAD: SISTEMAS DISTRIBUIDOS

Hora: N4-N6 Salón: 3103 Grupo: 004

Equipo2:














1949469 Saul Edrei Silva Rodriguez IAS **Si  
trabajo**

1948705 Gabriel Monroy Gracia IAS **Si  
trabajo**

1950074 José Amhed Vela Canales IAS **No  
trabajo**

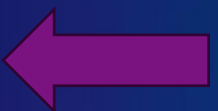
# INDICE



<b>Introducción .....</b>	
<b>¿Qué es la seguridad de red?.....</b>	
<b>¿En qué me beneficia la seguridad de red?.....</b>	
<b>Tipos de virus .....</b>	
<b>principales tipos de virus informáticos.....</b>	
<b>consejos básicos para prevenir su entrada.....</b>	
<b>Tipos de autenticación.....</b>	
<b>Análisis de Posibles Problemas.....</b>	
<b>Tipos de Daños.....</b>	
<b>Admon de Riesgos .....</b>	
<b>Prevención de desastres/Posibles soluciones.....</b>	
<b>conclusión .....</b>	
<b>Bibliografía .....</b>	

# INTRODUCCIÓN

En la era digital en la que vivimos, las redes de computadoras desempeñan un papel fundamental al permitir la comunicación y el intercambio de información entre dispositivos en todo el mundo. Desde el envío de correos electrónicos hasta la transmisión de datos críticos en organizaciones, las redes son el tejido que conecta nuestro mundo digital. Sin embargo, esta interconexión también conlleva riesgos, ya que las amenazas cibernéticas están al acecho. La seguridad de redes se convierte en un aspecto vital para proteger la privacidad y la integridad de la información, y en esta introducción, exploraremos cómo las redes y la seguridad se entrelazan para garantizar que nuestros datos estén resguardados en el vasto paisaje digital.





## ¿QUÉ ES LA SEGURIDAD DE RED?

cualquier actividad diseñada para proteger el acceso, el uso y la seguridad de los datos.

- Incluye tecnologías de hardware y software.
- Está orientada a diversas amenazas.
- Evita que ingresen o se propaguen por la red.
- La seguridad de red eficaz administra el acceso a la red.

Cuenta con ciertas capas de defensa, donde bien pueden permitir o denegar el acceso dependiendo el tipo de usuario que sea: usuario administrador o usuario malicioso



# ¿EN QUÉ ME BENEFICIA LA SEGURIDAD DE RED?

La digitalización ha transformado al mundo. Ha cambiado nuestra manera de vivir, trabajar, aprender y entretenernos. Todas las organizaciones que quieren prestar los servicios que exigen los clientes y los empleados deben proteger su red. La seguridad de red también ayuda a proteger la información confidencial de los ataques. En última instancia, protege su reputación.

## Tipos de seguridad de red

1. **Firewalls**
2. **Seguridad del correo electrónico**
3. **Software antivirus y antimalware**
4. **Segmentación de la red**
5. **Control de acceso**
6. **Sistemas de prevención de intrusiones**
7. **VPN**
8. **Seguridad web**



# TIPOS DE VIRUS

Los tipos de virus informáticos pueden clasificarse según el ataque para el que están programados o por las características que los definen.

Los virus diseñados para realizar los conocidos como ciberataques, son acciones dirigidas a desestabilizar sistemas de información.

- **Adware.** También conocido como software de publicidad, muestra anuncios basados en visitas o búsquedas. Además, reduce la capacidad de cómputo del equipo.
- **Spybot.** El tipo de virus informático spyware recopila información de un dispositivo para transmitirlo a una entidad externa sin el consentimiento del usuario, posiblemente para extorsionarlo.
- **Malware.** Altera el funcionamiento normal del equipo al destruir o corromper el sistema operativo o programas. Puede propagarse mediante códigos por correo electrónico.





• **Ransomware.** Secuestra la información del equipo mediante cifrado para que el usuario no pueda acceder a ella y, de este modo, solicitarle un rescate económico. De lo contrario, la información podría destruirse o publicarse en internet.

• **Virus informático o gusano.** Se caracteriza por multiplicarse mediante el envío masivo de copias de sí mismo por correo electrónico u otras vías de contacto. Suele infectar los equipos que se conectan a redes públicas.

• **Troyano.** Bajo la apariencia de un programa, un documento o un juego legítimo, entra en el sistema porque el usuario lo instala. Al ejecutarlo, accede a toda la información del equipo.



# PRINCIPALES TIPOS DE VIRUS INFORMÁTICOS

- **Virus residentes.** Infectan cualquier archivo que se copie, abra, cierre o renombre.
- **Virus de acción directa.** Se replican y actúan cuando se cumple una condición específica para su ejecución.
- **Virus de sobreescritura.** Borran la información de los ficheros afectados para sustituir el contenido.
- **Virus de sector de arranque.** Impiden que el sistema operativo se ejecute.
- **Virus de macro.** Infectan archivos que utilizan ciertos programas con macros, como Word o Excel.
- **Virus polimórficos.** Se codifican de forma diferente cada vez que infectan un sistema dificultando su detección.
- **Virus FAT.** Impiden el acceso a ciertas secciones del disco duro donde se guardan archivos importantes.
- **Virus de secuencias de comandos web.** Aprovechan el código de las páginas para producir determinadas acciones indeseables.





# CONSEJOS BÁSICOS PARA PREVENIR SU ENTRADA:

- Una de las principales fuentes de infección son las **memorias USB**, así que es recomendable analizarlas previamente y solo usarlas si son de confianza.
- Evitar navegar por **páginas inseguras** o **ejecutar archivos de origen desconocido**. Además, los correos electrónicos y las redes sociales son otra de las vías de propagación más habituales. Por tanto, es aconsejable comprobar el remitente real de cualquier mensaje sospechoso y únicamente seguir hipervínculos claramente identificados de fuentes oficiales.



# TIPOS DE AUTENTICACIÓN

**Autenticación por usuario y contraseña(Típica)**

**Autenticación por Biometría(Un poco mas segura)**

**Autenticación de dos factores(complicada)**

**Autenticación por sesión(Difícil)**

**Autenticación por voz (Difícil)**

**Autenticacion métrica de retina (Difícil)**

Independientemente del método adoptado, lo importante es que al diseñar una solución de software, el desarrollador “esté atento” a la implementación de métodos de autenticación que permitan la escalabilidad de la aplicación con el menor inconveniente, además de un mantenimiento sin estrés.



# Análisis de Posibles Problemas

Hardware, Software,  
archivos e información





# TIPOS DE DAÑOS

- Detener Sistema
- Comportamiento Erróneo
- Despliegue de mensajes

Error en Ejecución  
/Errores en  
Pantalla



- Archivos
- Desorden

Datos



- Transferencia de datos

Envío de mensajes



# ADMÓN. DE RIESGOS



Cuantificación de la efectividad del programa



Valoración de riesgos



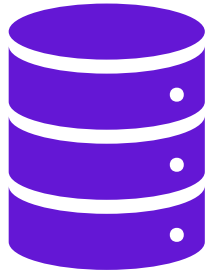
Petición de soporte técnico



Implementación de controles



# PREVENCIÓN DE DESASTRES / POSIBLES SOLUCIONES



Copias de  
seguridad



Antivirus



Observaciones





# CONCLUSIÓN

En un mundo cada vez más interconectado, las redes desempeñan un papel esencial al facilitar la comunicación y el intercambio de información. Sin embargo, la seguridad de redes se ha vuelto igualmente crucial debido a la creciente amenaza de ataques cibernéticos. Garantizar la protección de los datos y la privacidad en las redes es un desafío constante. Por lo tanto, la comprensión y la implementación de prácticas de seguridad sólidas son esenciales para mantener la integridad de la información en el entorno digital actual. La combinación efectiva de redes y seguridad se traduce en un equilibrio vital que permite aprovechar los beneficios de la conectividad global sin poner en riesgo la confidencialidad y la disponibilidad de los datos.



# REFERENCIAS BIBLIOGRÁFICAS

- Bessa, A. (21 de Abril de 2023). *Tipos de Autenticación: Contraseña, Token, JWT, Dos Factores y Más*. Obtenido de <https://www.aluracursos.com/blog/tipos-de-autenticacion>
- Buenning, M. (10 de Agosto de 2023). *Copias de seguridad anti-ransomware: cómo prevenir un desastre*. Obtenido de <https://www.ninjaone.com/es/blog/como-prevenir-desastres-con-una-copia-de-seguridad-anti-ransomware/#:~:text=Tener%20un%20antivirus%2C%20aplicar%20parches,es%20v%C3%ADctima%20de%20un%20ataque.>
- CISCO. (24 de Octubre de 2023). *¿Qué es la seguridad de red?* Obtenido de [https://www.cisco.com/c/es\\_mx/products/security/what-is-network-security.html#~tipos](https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html#~tipos)
- Microsoft. (24 de Octubre de 2023). *¿Qué es la autenticación?* Obtenido de <https://www.microsoft.com/es-es/security/business/security-101/what-is-authentication>
- Microsoft. (24 de Octubre de 2023). *Estrategias para la administración de riesgos de malware*. Obtenido de <https://learn.microsoft.com/es-es/security-updates/security/estrategiasparalaadministracinderiesgosdemalware>
- Segu. Info. (24 de Octubre de 2023). *Virus - Tipos de Daños Ocasionados por los Virus*. Obtenido de <https://www.segu-info.com.ar/virus/danios#:~:text=En%20general%20los%20da%C3%B1os%20que,reduce%20la%20memoria%20total.>
- unir. (15 de Junio de 2021). *¿Qué es la seguridad informática y cuáles son sus tipos?* Obtenido de <https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/>
- Universidad Isabel I. (04 de Julio de 2023). *¿Cuáles son los virus informáticos más conocidos?* Obtenido de <https://www.ui1.es/blog-ui1/cuales-son-los-virus-informaticos-mas-conocidos>

