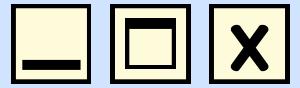


# Atividad fundamental 4

*Redes y seguridad:  
sistemas distribuidos*



## Integrantes



Jose Angel Cardenas Contreras  
1935156,IAS



Isac Alfredo Almaguer Espinosa,  
2049903, IAS



Frida Jaziry Juárez Fuentes  
2028420, IAS



Fátima Arizpe Sánchez  
2025106,IAS

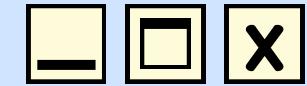


Francisco Gael Reyes Cantu  
1995983,IAS





## ¿Que es un virus?



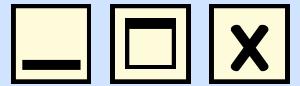
Un virus informatico es una aplicacion o codigo malicioso que se emplea para ejecutar actividades destructivas en un dispositivo o red local. La actividad de este código puede dañar el sistema local de archivos, robar datos, interrumpir servicios, descargar mas malware o cualquier otra acción que este codificada en el programa.

Muchos virus simulan ser programas legítimos para convencer a los usuarios de que los ejecuten en su dispositivo, insertando así la carga útil del virus





## Tipos de virus informáticos según sus particularidades



### Virus de arranque



tipo de malware que infecta el sector de arranque de un disco duro, disco flexible (floppy) o unidad USB. Este virus se activa cuando el sistema operativo intenta iniciarse, antes de que el usuario tenga control sobre la computadora.

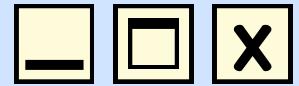
¿Cómo funcionan?

1. Se instalan en el MBR (Master Boot Record) o en el sector de arranque del disco.
2. Se ejecutan antes de que el sistema operativo cargue, permitiendo que el virus tome control del equipo.
3. Pueden modificar archivos, corromper datos o impedir el arranque del sistema.





## Tipos de virus informáticos según sus particularidades



### Virus residentes

Un virus residente es un tipo de malware que se instala en la memoria RAM del sistema y permanece activo incluso después de eliminar el archivo infectado. Su principal característica es que puede infectar otros programas y procesos en ejecución sin necesidad de ser ejecutado nuevamente.

¿Cómo funcionan los virus residentes?

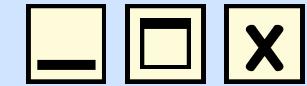


1. Se alojan en la memoria RAM cuando el usuario ejecuta un archivo infectado.
2. Modifican funciones del sistema, permitiendo que el virus se active automáticamente.
3. Infectan otros archivos y programas en segundo plano.
4. Permanecen en la memoria incluso si se cierra el programa infectado.





## Tipos de virus informáticos según sus particularidades



### Virus de archivo

es un programa malicioso que se adhiere a archivos legítimos para dañarlos o alterar el funcionamiento del sistema. Son un tipo de malware que se propaga de un ordenador a otro. borran la información contenida en los ficheros que infectan, haciéndolos parcial o totalmente inútiles. Una vez infectados, el virus reemplaza el contenido del fichero sin cambiar su tamaño.

¿Cómo funcionan?



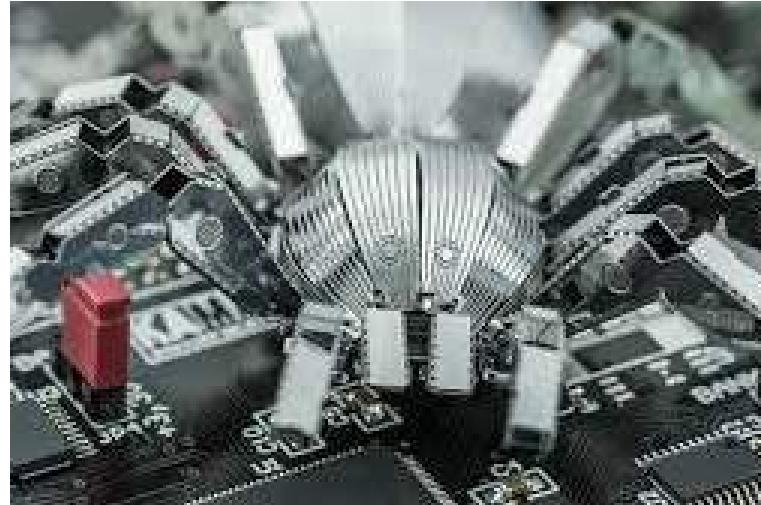
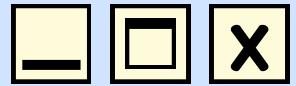
File Infected

1. Se adjuntan a archivos ejecutables sin modificar su funcionamiento aparente.
2. Se activan cuando el archivo infectado es ejecutado.
3. Pueden replicarse e infectar otros archivos en el sistema.
4. Algunos ocultan su presencia para evitar ser detectados por antivirus.





## Tipos de virus informáticos según sus particularidades



### Macro Virus

virus informático que infecta documentos de Microsoft Office (.docx, .xls, .ppt, etc.) a través de macros. Estos virus se activan cuando el usuario abre un archivo infectado y pueden propagarse a otros documentos en el sistema.

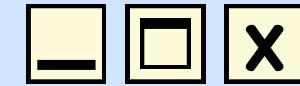
¿Cómo funcionan los macrovirus?

1. Se ocultan en macros, que son secuencias de comandos automatizadas en programas como Word o Excel.
2. Se activan al abrir el documento infectado.
3. Se propagan a otros archivos al compartir o guardar documentos en equipos no protegidos.
4. Pueden ejecutar acciones dañinas, como modificar textos, enviar correos con archivos infectados o robar información.





## Tipos de virus informáticos según sus particularidades



### Virus polimórfico

Forma avanzada de malware, tiene la capacidad de cambiar su código y estructura cada vez que se replica. Su principal objetivo es evadir la seguridad del sistema y continuar propagándose sin ser detectado.



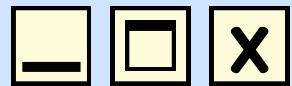
¿Cómo funciona un virus polimórfico?

1. Infecta un archivo o programa en el sistema.
2. Se replica y cambia su estructura interna, generando una variante diferente en cada infección.
3. Oculta su código malicioso mediante técnicas de cifrado y ofuscación.
4. Dificulta la detección por firmas de antivirus, ya que cada versión del virus es distinta.





## Tipos de virus informáticos en función del tipo de ataque



# Virus de Troya

tipo de malware que se descarga en una computadora disfrazado de programa legítimo. El método de entrega suele hacer que un atacante utilice la ingeniería social para ocultar código malicioso dentro del software legítimo para intentar obtener acceso al sistema de los usuarios con su software.

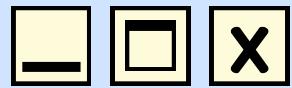
¿Cómo se propagan los troyanos?

- Archivos adjuntos en correos electrónicos maliciosos
- Descarga de software pirata o cracks
- Sitios web falsos que engañan al usuario
- Memorias USB infectadas o dispositivos externos





## Tipos de virus informáticos en función del tipo de ataque



### Virus de Secuencias de Comandos Web

tipo de malware que se inyecta en páginas web mediante scripts maliciosos. Cuando un usuario visita un sitio web infectado, el virus puede robar información, instalar otros malware o redirigir al usuario a sitios peligrosos.

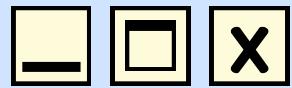
¿Cómo funciona?

1. Los ciberdelincuentes inyectan código malicioso en sitios web legítimos mediante vulnerabilidades.
2. El código infecta el navegador del usuario al visitar la página.
3. Puede robar información, instalar malware o redirigir a sitios fraudulentos.





## Tipos de virus informáticos en función del tipo de ataque



### Spyware

Son programas que se infiltran en un ordenador sin el conocimiento del usuario con el propósito de recopilar información personal o de navegación. Esta información pueden ser contraseñas, historiales de navegación y otros datos sensibles.

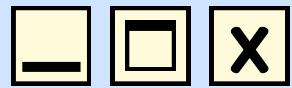
¿Cómo se propaga el Spyware?

- Descarga de software pirata o gratuito sospechoso
- Correos electrónicos de phishing con archivos adjuntos maliciosos
- Publicidad engañosa y pop-ups en sitios web
- Memorias USB o archivos compartidos infectados





## Tipos de virus informáticos en función del tipo de ataque



### Adware

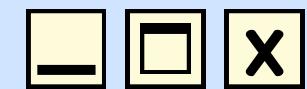
Es otro tipo de software no deseado que muestra anuncios no solicitados en la pantalla del usuario. Estos pueden ser intrusivos y afectar negativamente la experiencia de navegación. A menudo, el adware se instala junto con software gratuito o comparte el mismo paquete de instalación.

El adware suele instalarse junto con otros programas gratuitos, y los usuarios a menudo lo aceptan sin darse cuenta al instalar software desde fuentes no confiables. Para eliminar el adware, es recomendable utilizar programas antivirus o antimalware, y ser cauteloso al descargar aplicaciones de sitios no verificados.





# Gusano Informático



## ¿Qué es?

Son una subclase de virus, por lo que comparten características.

Son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador

## Principal objetivo

Propagarse y afectar al mayor número de dispositivos posible.

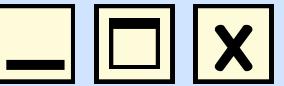
Para ello, crean copias de sí mismos en el ordenador afectado, que distribuyen a través de diferentes medios, como el correo electrónico o programas P2P, etc

## Como evitarlo

Para protegernos, existen una serie de consejos que ayudarán a tener tu dispositivo mucho más seguro frente a los gusanos:

- Evitar abrir mensajes y archivos adjuntos desconocidos
- No utilizar páginas web no seguras
- Actualizar tus sistemas operativos.





## Ransomware

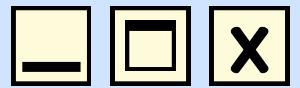


Son virus que cifran los archivos de la víctima y luego exigen un rescate para proporcionar la clave de descifrado. Este tipo de ataque puede resultar en la pérdida de datos valiosos y daños financieros si la víctima paga el rescate.

## Rootkit

Son programas diseñados para ocultar la presencia de otros malware en un PC. Son difíciles de detectar y eliminar, lo que los convierte en una amenaza para la seguridad cibernética. Estos proporcionan acceso no autorizado al sistema y permiten que los ciberdelincuentes realicen acciones maliciosas sin ser detectados.





## Intruso Informatico

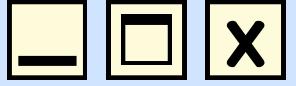


Un intruso informático es una persona que intenta acceder a un sistema informático sin autorización, haciendo un mal uso del dispositivo





# Intruso Informatico



## Hacker

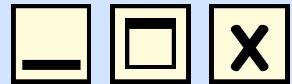
Destaca por su excelencia en programación y electrónica, un conocimiento avanzado en ordenadores y redes informáticas.

Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. Buscan y descubren las debilidades de una computadora o red informática.





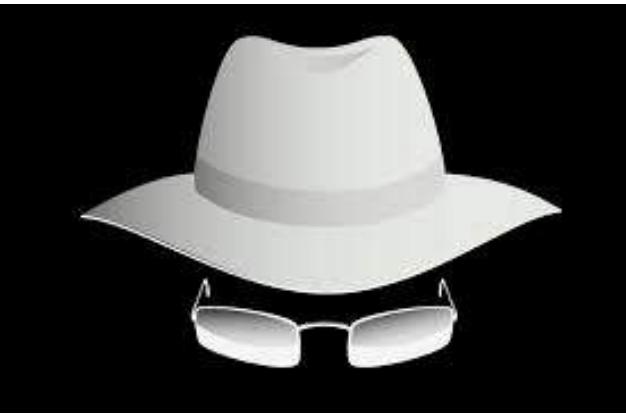
## Intruso Informatico



# White Hats

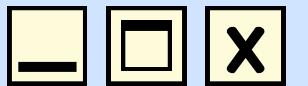
A los sombreros blancos también se les llama hackers éticos. Estos expertos en informática utilizan sus conocimientos para buscar vulnerabilidades y hacer test de penetración, para estudiar y corregir fallos de seguridad y mejoras en los sistemas.

Alertan de un fallo en algún programa comercial, comunicándose al fabricante. Pueden formar parte de un equipo de seguridad empresarial o gubernamental.





## Intruso Informatico



### Grey Hats

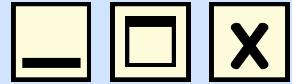
Como su color indica, tienen una ética ambigua. Suelen utilizar las mismas técnicas que los sombreros negros para encontrar vulnerabilidades y luego venderlas a quién este dispuesto a pagar por ellas.

Su clientela abarca gobiernos, servicios militares y otros hackers. Además, se pueden presentar como expertos en seguridad para resolver los fallos encontrados. Su enfoque suele estar en el lucro más que en perjudicar a las empresas de manera directa.





# Intruso Informatico



## Black Hats

Black Hat o también llamados Ciberdelincuentes. Estos hackers acceden a sistemas o redes no autorizadas con el fin de infringir daños, obtener acceso a información financiera, datos personales, contraseñas e introducir virus.

Dentro de esta clasificación existen dos tipos:

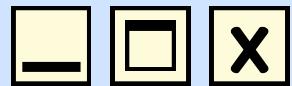
Phreakers: actúan en el ámbito de las telecomunicaciones.

Crackers: modifican softwares, crean malwares, colapsan servidores e infectan las redes





# Intruso Informatico

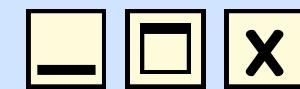


## Cracks

Ser un cracker es saber romper algo, en este caso sistemas y software. Dicho en otras palabras, la edición desautorizada de software de propiedad.

Siempre encuentran el modo de romper una protección y estas roturas se suelen filtrar o difundir en la red para el conocimiento de los demás.





## Tipos de autenticaciones

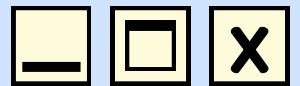


La autenticación es el proceso que usan las empresas para confirmar que solo las personas, servicios y aplicaciones adecuados con los permisos correctos puedan acceder a recursos de la organización. Es parte importante de la ciberseguridad.





## Tipos de autenticaciones



### Autenticación basada en contraseñas

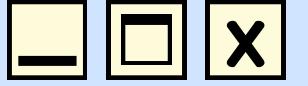
Esta autenticación es la forma de autenticación más frecuente.. Muchas aplicaciones y servicios requieren que las personas creen contraseñas formadas por una combinación de números, letras y símbolos para reducir el riesgo de que un infiltrado las adivine.

Lo negativo es que a las personas les resulta difícil crear y memorizar una contraseña exclusiva para cada una de sus cuentas online, razón por la cual suelen reutilizar o robar contraseñas





## Tipos de autentificaciones



### Autenticación Biométrica

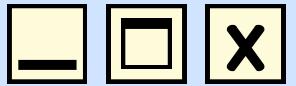
La autenticación biométrica se basa en la verificación de la identidad de una persona mediante sus características biológicas.

Muchas personas utilizan un dedo para iniciar sesión en sus teléfonos, y algunos ordenadores escanean la cara o la retina de una persona para verificar su identidad





## Tipos de autenticaciones



### Autenticación Basada en tokens

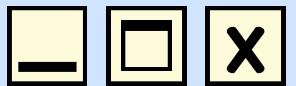
En la autenticación basada en tokens, tanto el dispositivo como el sistema generan un nuevo número singular llamado PIN temporal de un solo uso (TOTP).

Si los números coinciden, el sistema comprueba que el usuario tiene el dispositivo.





## Tipos de autenticaciones

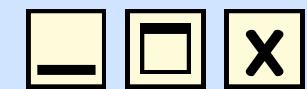


### Autenticación Multifactor

Es una buena forma para reducir el riesgo de vulnerabilidad de cuentas, el usar dos o más formas de autenticación, entre los que se pueden incluir cualquier autenticación anterior

Por ejemplo, muchas organizaciones solicitan una contraseña (algo que el usuario conoce) y también envían una OTP a través de SMS a un dispositivo de confianza (algo que el usuario posee) antes de permitir el acceso





## Niveles de Seguridad

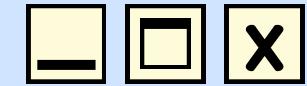


El nivel de seguridad en vigor determina el nivel de detalle que los perfiles de usuario deben proporcionar para otorgar acceso adecuado a los recursos del sistema. Este nivel de detalle puede ir desde la gestión simple de contraseñas hasta proporcionar explícitamente un nivel de acceso a cada objeto que un usuario puede leer o cambiar.





## Niveles de Seguridad



# Control de acceso obligatorio (MAC)

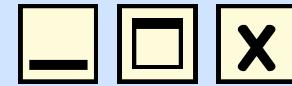
Es un mecanismo de seguridad que se utiliza en los sistemas y redes informáticos para hacer cumplir políticas de acceso estrictas y definidas de forma centralizada en los recursos informáticos. Está diseñado para limitar y controlar las acciones que los usuarios pueden realizar en los objetos en función de reglas predeterminadas establecidas por el administrador del sistema o la política de seguridad.

Cuando un sujeto intenta acceder a un objeto, el sistema MAC verifica las etiquetas de seguridad tanto del sujeto como del objeto y las compara con la política de acceso. El acceso se otorga solo si el nivel de seguridad del sujeto cumple o supera el nivel de seguridad del objeto según la política de acceso.





## Niveles de Seguridad



# Control de acceso discrecional (DAC)

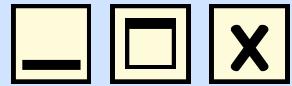
Es un mecanismo de software para controlar el acceso de usuarios a archivos y directorios. DAC deja que la configuración de protecciones para archivos y directorios las realice el propietario según su criterio. Las dos formas de DAC son los bits de permisos UNIX y las listas de control de acceso (ACL).

Los bits de permisos permiten que el propietario establezca protección de lectura, escritura y ejecución por propietario, grupo y otros usuarios.





## Niveles de Seguridad



# Núcleo de seguridad (Security Kernel)

El núcleo de seguridad es un componente fundamental dentro de los sistemas operativos diseñados con altos niveles de seguridad. Su propósito es reducir al mínimo el código que tiene acceso directo a las operaciones más críticas del sistema. Esto disminuye la superficie de ataque, ya que menos componentes del sistema tienen acceso a funciones vitales, como el control de acceso a los recursos.

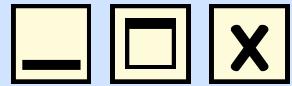


El núcleo de seguridad actúa como un intermediario entre el hardware y los procesos del usuario, garantizando que solo las operaciones seguras se realicen. Funciona implementando mecanismos estrictos de control de acceso y separando privilegios de usuario.





## Niveles de Seguridad



# Núcleo de seguridad (Security Kernel)

El núcleo de seguridad es un componente fundamental dentro de los sistemas operativos diseñados con altos niveles de seguridad. Su propósito es reducir al mínimo el código que tiene acceso directo a las operaciones más críticas del sistema. Esto disminuye la superficie de ataque, ya que menos componentes del sistema tienen acceso a funciones vitales, como el control de acceso a los recursos.

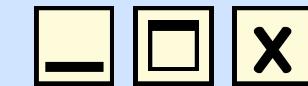


El núcleo de seguridad actúa como un intermediario entre el hardware y los procesos del usuario, garantizando que solo las operaciones seguras se realicen. Funciona implementando mecanismos estrictos de control de acceso y separando privilegios de usuario.





## Niveles de Seguridad



### Niveles de seguridad según IBM



### Nivel 20

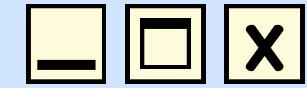
Este nivel se conoce como seguridad de contraseña. Es decir, los usuarios deben tener una contraseña y un ID de usuario que el sistema reconozca para obtener acceso al sistema. El administrador del sistema crea tanto el ID de usuario como la contraseña inicial para los usuarios.

Este nivel de seguridad ofrece a todos los usuarios de la autoridad total del sistema todo lo que deseen. Eso significa que pueden acceder a todos los datos, archivos, objetos, etc., en su sistema.





## Niveles de seguridad según IBM



### Nivel 30

Este nivel se conoce como seguridad de recursos. Es decir, los usuarios deben tener un ID de usuario y una contraseña válidos definidos para ellos por el administrador del sistema, y ya no tienen acceso automático a todo en el sistema. El acceso de usuario está limitado por las políticas de seguridad de la empresa.



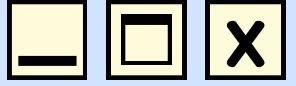
### Nivel 40

Este nivel se conoce como seguridad de integridad del sistema. Es decir, a este nivel, el propio sistema está protegido ante los usuarios. Los programas escritos por el usuario no pueden acceder directamente a los bloques de control internos mediante la manipulación de puntero.





## Niveles de seguridad según IBM



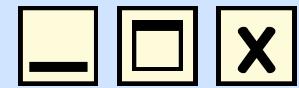
### Nivel 50

Es el nivel recomendado de seguridad para la mayoría de las empresas, porque ofrece el nivel más alto de seguridad posible actualmente. El sistema no sólo está protegido ante programas escritos por el usuario, sino que garantiza que los usuarios sólo tengan acceso a los datos en el sistema, en lugar de a la información sobre el propio sistema.





# Niveles de Seguridad



## Niveles de seguridad según Microsoft

La seguridad empresarial es adecuada para todos los usuarios empresariales y escenarios de productividad. En el desarrollo del plan de modernización rápida, la empresa también sirve como punto inicial para el acceso especializado y con privilegios, ya que se están basados progresivamente en los controles de seguridad de la seguridad empresarial.



## Empresa

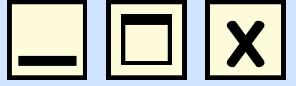
## Especializada

Proporciona controles de seguridad mejorada para los roles que tienen un impacto empresarial elevado (si un atacante o un infiltrado malintencionado los ponen en peligro).





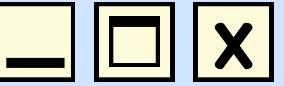
## Niveles de seguridad según Microsoft



### Privileged

La seguridad con privilegios es el nivel de seguridad más alto y está diseñado para roles que podrían causar fácilmente incidentes importantes y posibles daños materiales a la organización en manos de un atacante o un infiltrado malintencionado. Este nivel normalmente incluye roles técnicos con permisos administrativos en la mayoría o en todos los sistemas empresariales.





## Análisis de Posibles Problemas

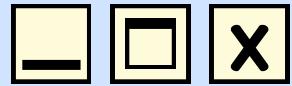
### Vulnerabilidades en el arranque seguro

El software "shim" utilizado en muchas distribuciones de Linux para gestionar el arranque seguro puede ser vulnerable a ataques como CVE-2023-40547. Este exploit permite a los atacantes interceptar el tráfico HTTP durante el proceso de arranque o manipular las variables EFI, ganando control antes de que el kernel del sistema operativo sea cargado. Esto compromete la integridad de la cadena de confianza del sistema.

### Exploits del kernel

El ataque denominado "SLUBStick" es otro ejemplo de cómo los atacantes pueden aprovechar vulnerabilidades en la gestión de memoria del kernel de Linux. Este ataque explota errores en el manejo de asignaciones de memoria (heap) y permite escalar privilegios, otorgando al atacante acceso de root. Aunque requiere acceso local al sistema, tiene una alta tasa de éxito, haciendo que las defensas modernas del kernel sean menos efectivas.





## Prevencion de desastres

La prevención de desastres en la seguridad de sistemas operativos se enfoca en minimizar el impacto de posibles fallos o ciberataques. Esto se logra a través de varias estrategias clave, que buscan proteger tanto el hardware como el software y garantizar la integridad y disponibilidad de los sistemas.

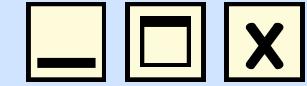
### Fortalecimiento del sistema (System Hardening)

Consiste en reducir la superficie de ataque de un sistema operativo eliminando servicios, aplicaciones o puertos innecesarios. Este proceso incluye la actualización constante de los sistemas operativos y parches de seguridad, la configuración correcta de las opciones de seguridad, y el uso de prácticas como el control de acceso basado en el principio de mínimo privilegio. Este enfoque ayuda a prevenir vulnerabilidades antes de que puedan ser explotadas.





## Prevencion de desastres



### Auditorías y monitoreo continuo

Es fundamental realizar auditorías frecuentes y monitorear las actividades del sistema para detectar cambios no autorizados o comportamientos inusuales. Esto permite reaccionar rápidamente a incidentes, evitar desastres de seguridad y garantizar la conformidad con las normativas de seguridad.

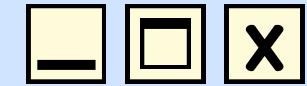
### Parches y actualizaciones regulares

Mantener el software y los sistemas operativos actualizados con los últimos parches de seguridad es esencial para prevenir vulnerabilidades explotadas comúnmente en ataques. Se recomienda priorizar la actualización de servidores que procesan datos desde internet o aquellos que manejan información sensible.





## Prevencion de desastres



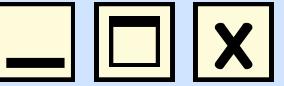
### Control de cambios y gestión de configuraciones

Implementar un control de cambios estructurado que garantice que todas las modificaciones del sistema estén documentadas, aprobadas y revisadas antes de su implementación, reduce la posibilidad de errores de configuración que podrían dar lugar a fallas de seguridad.normativas de seguridad.

### Desactivar servicios no esenciales

Algunos servicios, como el protocolo SMB (Server Message Block), deben ser desactivados o actualizados a versiones más seguras (como SMBv3) cuando no son necesarios, para evitar la propagación de malware o accesos no autorizados.





## Administracion de riesgos y seguridad

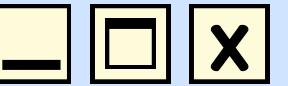
Es un proceso fundamental para proteger los activos digitales y minimizar el impacto de las amenazas. Este enfoque implica identificar, evaluar y mitigar los riesgos de seguridad en un entorno de TI, con el fin de evitar brechas que puedan comprometer la confidencialidad, integridad y disponibilidad de los datos.



### Identificación de riesgos

El primer paso es identificar las amenazas potenciales que pueden afectar a los sistemas operativos. Las amenazas pueden ser tanto externas (como ataques cibernéticos) como internas (errores humanos o fallos de software). Las vulnerabilidades son los puntos débiles en el sistema que pueden ser explotados por estas amenazas, como fallos en la configuración del firewall o errores en el código del sistema operativo.





## Evaluación de riesgos

Una vez identificadas las amenazas, se realiza una evaluación para medir su impacto potencial y su probabilidad de ocurrencia. Esto permite a las organizaciones priorizar los riesgos según su criticidad. Durante esta etapa, se analizan factores como los controles de seguridad existentes y la sensibilidad de los datos que manejan los sistemas operativos.



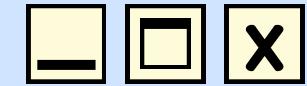
## Mitigación y respuesta

Las organizaciones pueden optar por diferentes enfoques de respuesta ante los riesgos. Algunas medidas incluyen la implementación de controles tecnológicos, como firewalls, sistemas de detección de intrusiones, y la aplicación de parches de seguridad. También pueden implementar prácticas organizacionales como la capacitación en ciberseguridad y el uso de autenticación multifactor.





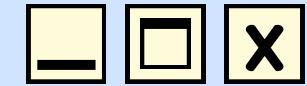
## Bibliografias



- Norton. (2023, March 6). ¿Qué es un virus informático? [Norton. \(2023, March 6\). ¿Qué es un virus informático?](https://mx.norton.com/blog/malware/what-is-a-computer-virus)  
<https://mx.norton.com/blog/malware/what-is-a-computer-virus>
- ¿Qué son los virus informáticos? | Tipos de virus | Fortinet. (n.d.). Fortinet. [¿Qué son los virus informáticos? | Tipos de virus | Fortinet. \(n.d.\). Fortinet.](https://www.fortinet.com/lat/resources/cyberglossary/computer-virus) <https://www.fortinet.com/lat/resources/cyberglossary/computer-virus>
- ¿Qué es un virus informático? - Tipos, ejemplos y más | Proofpoint ES. (2024, January 26). Proofpoint. [Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut nulla erat, venenatis sed sapien scelerisque, dapibus venenatis urna. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque ac lorem pretium, eleifend nisi nec, lacinia diam. Mauris dignissim purus nec est sollicitudin, quis molestie velit tincidunt. Pellentesque commodo varius leo a hendrerit. In a velit auctor, accumsan diam in, bibendum libero. Nulla facilisi.](#)
- ¿Cuáles son los virus informáticos más conocidos? (n.d.). [Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut nulla erat, venenatis sed sapien scelerisque, dapibus venenatis urna. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque ac lorem pretium, eleifend nisi nec, lacinia diam. Mauris dignissim purus nec est sollicitudin, quis molestie velit tincidunt. Pellentesque commodo varius leo a hendrerit. In a velit auctor, accumsan diam in, bibendum libero. Nulla facilisi.](#)
- Szell, C. (2024, February 2). Intrusos informáticos: Hackers y Crackers - Conecta Magazine. Conecta Magazine. [Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut nulla erat, venenatis sed sapien scelerisque, dapibus venenatis urna. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque ac lorem pretium, eleifend nisi nec, lacinia diam. Mauris dignissim purus nec est sollicitudin, quis molestie velit tincidunt. Pellentesque commodo varius leo a hendrerit. In a velit auctor, accumsan diam in, bibendum libero. Nulla facilisi.](#)



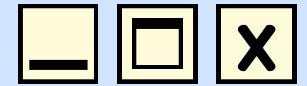
## Bibliografias



- Butts, J. (2024, agosto 6). New Linux kernel attack slips past modern defenses — SLUBStick boasts a 99% success rate. Tom's Hardware. [Añadir un poco de texto](#)
- Control de acceso discrecional - Guía del usuario de Trusted Extensions. (2015, enero 20). Oracle.com. [Añadir un poco de texto](#)
- Garland, C. (2024, febrero 6). The real shim shady - how CVE-2023-40547 impacts most Linux systems. Eclypsium | Supply Chain Security for the Modern Enterprise; Eclypsium.
- MicrosoftGuyJFlo. (s/f). Protección de los niveles de seguridad de acceso con privilegios - Privileged access. Microsoft.com. <https://learn.microsoft.com/es-es/security/privileged-access-workstations/privileged-access-security-levels>
- Schrader, D. (s/f). What is System Hardening and Why is it Important?. <https://blog.netwrix.com/2023/02/22/system-hardening/>
- Spasojevic, A. (2023, agosto 1). Definición de control de acceso obligatorio (MAC). phoenixNAP IT Glossary; phoenixNAP. <https://phoenixnap.mx/glosario/control-de-acceso-obligatorio-mac>
- #StopRansomware Guide. (s/f). Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/stopransomware/ransomware-guide>
- What is Cyber Risk Management? (2024, octubre 7). Ibm.com. <https://www.ibm.com/topics/cyber-risk-management>



# Conclusiones



Jose Angel Cardenas Contreras

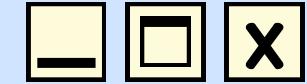
I935156 IAS

Las redes y la seguridad en sistemas distribuidos son fundamentales para garantizar la comunicación eficiente y la protección de los datos en entornos donde múltiples dispositivos y nodos interactúan. Los sistemas distribuidos permiten una mayor escalabilidad, redundancia y disponibilidad de los servicios, pero también presentan desafíos en términos de vulnerabilidades y ataques cibernéticos. Para mitigar riesgos, es esencial implementar estrategias de seguridad como cifrado, autenticación, control de acceso y monitoreo constante. Un enfoque bien estructurado en redes y seguridad asegura la integridad, confidencialidad y disponibilidad de la información en estos entornos interconectados.





# Conclusiones

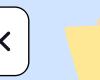


Francisco Gael Reyes Cantú  
1995983  
IAS

En los sistemas distribuidos, las redes y la seguridad son aspectos fundamentales para que todo funcione correctamente. Las redes permiten que diferentes computadoras, servidores u otros dispositivos se comuniquen entre sí, aunque estén en distintos lugares. Gracias a esto, es posible compartir información, archivos, programas y otros recursos sin importar la distancia.

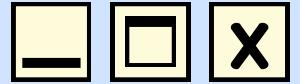
Sin embargo, al estar conectados por una red, también existe el riesgo de que personas no autorizadas intenten acceder a la información o causar daños. Por eso, la seguridad es clave en estos sistemas. Se deben tomar medidas como el uso de contraseñas, permisos de acceso, cifrado de datos y programas que detecten actividades sospechosas.

Tener buenas redes y buena seguridad ayuda a que el sistema sea confiable, rápido y protegido. Además, permite que los usuarios trabajen al mismo tiempo sin interferencias, manteniendo la privacidad y la integridad de la información. En resumen, redes y seguridad son dos pilares que deben ir de la mano para que los sistemas distribuidos funcionen bien y de forma segura.





# Conclusiones



Isac Alfredo Almaguer Espinosa, 2049903

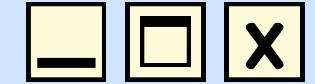
IAS

A lo largo de esta presentación, he comprendido que las amenazas ciberneticas no son estáticas, sino que evolucionan constantemente, lo que exige un enfoque dinámico y proactivo para proteger sistemas, redes y datos. Desde virus y ransomware hasta ataques avanzados como APTs, los riesgos son diversos y pueden afectar tanto a usuarios individuales como a grandes organizaciones. Sin embargo, también he aprendido que existen múltiples estrategias de defensa, como la autenticación multifactor, el cifrado de datos, firewalls y la educación en concienciación de seguridad, que pueden reducir significativamente estos riesgos. Además, la gestión de riesgos y la prevención de desastres no son solo responsabilidad de los expertos en ciberseguridad, sino también de los ingenieros y desarrolladores que diseñan sistemas seguros desde su concepción.





# Conclusiones



Frida Jaziry Juárez Fuentes  
2028420, IAS

Los sistemas distribuidos han revolucionado la forma en que se procesan y almacenan datos al permitir la descentralización de los recursos y mejorar la disponibilidad. Sin embargo, esta misma descentralización implica nuevos desafíos en términos de seguridad. Con múltiples puntos de acceso y nodos interconectados, las vulnerabilidades pueden aumentar si no se implementan medidas de protección adecuadas. Para garantizar un funcionamiento seguro sin afectar la eficiencia, es fundamental establecer un equilibrio entre accesibilidad y seguridad. Esto implica el uso de mecanismos como la autenticación multifactor para restringir el acceso no autorizado, cifrado de extremo a extremo para proteger la integridad y privacidad de los datos, y la segmentación de red para aislar componentes críticos y minimizar el impacto de posibles ataques.





# Conclusiones



Fátima Arizpe Sánchez  
2025106,IAS

En un entorno distribuido, la seguridad no puede depender exclusivamente de medidas centralizadas, ya que los sistemas están conformados por múltiples nodos que operan en distintos entornos y ubicaciones. A medida que crecen las amenazas ciberneticas, es necesario adoptar estrategias de seguridad proactivas que permitan detectar y mitigar ataques antes de que causen daños significativos. Una de las mejores prácticas en este sentido es la implementación de arquitecturas de confianza cero (Zero Trust), en las que ningún usuario o dispositivo es considerado seguro por defecto, sino que cada acceso debe ser verificado y autorizado constantemente. Además, la inteligencia artificial y el aprendizaje automático juegan un papel crucial en la detección de patrones anómalos dentro del tráfico de la red, permitiendo una respuesta rápida ante posibles incidentes.

