

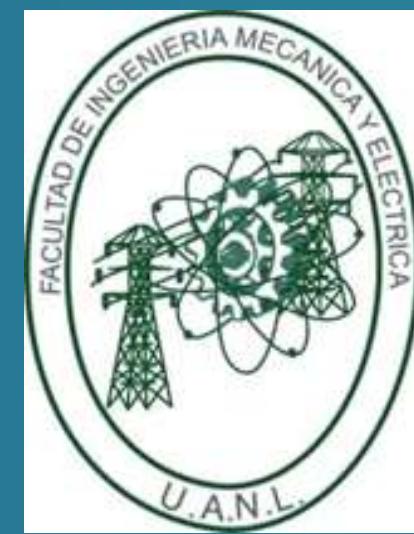
REDES Y SEGURIDAD: SISTEMAS DISTRIBUIDOS





Universidad Autónoma de Nuevo León

Facultad de Ingeniería Mecánica y Eléctrica



Sistemas Operativos

Actividad Fundamental #4

“Redes y seguridad: sistemas distribuidos”

Docente: DR. Norma Edith Marín Martínez

Grupo: 010 Hora: M4

Equipo: 2

Semestre Agosto - Diciembre 2024
San Nicolás De Los Garza, Nuevo León a 20 de octubre de 2024

Foto	Matricula	Nombre	Carrera	Aportacion
	1948932	Antonio Enrique Hernández Ramírez	ITS	100
	2005930	Eden Leonardo Candelas Andrade	ITS	100
	2022830	Daniel Alejandro Segura Vázquez	ITS	100
	2045231	Denilson Gustavo Aguilar PuentE	IAS	100
	2052523	Jorge Paz Villarreal	IAS	85

Foto	Matricula	Nombre	Carrera	Aportacion
	2131973	Uriel Ramiro De La Fuente Del Ángel	ITS	100
	196213	Alexis Yahir Soria Salazar	IAS	100
	1958098	Alan Jahir Rivas Urbina	ITS	70
	2052193	Sofia Giovanna Espinoza Zapata	IAS	100

INTRODUCCIÓN

¿Qué es la ciberseguridad? La ciberseguridad es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales. Este campo abarca un conjunto de estrategias y medidas preventivas que buscan mitigar riesgos, proteger la información y asegurar la continuidad de las operaciones tecnológicas.

En un mundo donde la tecnología evoluciona a pasos agigantados, la seguridad informática se ha convertido en una prioridad fundamental para garantizar la integridad y confidencialidad de la información. Las amenazas digitales han crecido no solo en frecuencia, sino también en complejidad, afectando tanto a usuarios individuales como a empresas globales.

Enfrentamos una amplia gama de riesgos que van desde ataques de malware hasta intrusiones cibernéticas altamente sofisticadas, lo que ha hecho de la ciberseguridad un elemento esencial para mantener seguros nuestros dispositivos y datos.

AMENAZAS Y TIPOS DE MALWARE



Una amenaza de ciberseguridad es cualquier circunstancia o evento que pueda tener consecuencias adversas para las operaciones, funciones, reputación, o activos de una organización, afectando el acceso, la integridad, o el valor de los datos. Las amenazas surgen cuando un ataque se dirige a los sistemas, redes o dispositivos con el objetivo de obtener acceso no autorizado o explotar vulnerabilidades, comprometiendo así la confidencialidad, integridad y disponibilidad de la información y los recursos tecnológicos de la organización.





MALWARE



El malware es software o código malicioso diseñado para dañar, interrumpir o comprometer el funcionamiento habitual de dispositivos, como computadoras, teléfonos móviles o redes. Cuando un dispositivo es infectado con malware, puede ser accedido sin autorización, sus datos pueden ser expuestos o alterados, e incluso el acceso al dispositivo puede ser bloqueado hasta que se pague un rescate, en el caso de ataques como el ransomware.

Los ciberdelincuentes, motivados principalmente por el beneficio económico, utilizan el malware para realizar ataques, como el robo de credenciales bancarias, la recopilación de información personal para venderla, o la extorsión a las víctimas a cambio de liberar sus dispositivos o datos comprometidos.





TIPOS DE MALWARE

01

Phishing

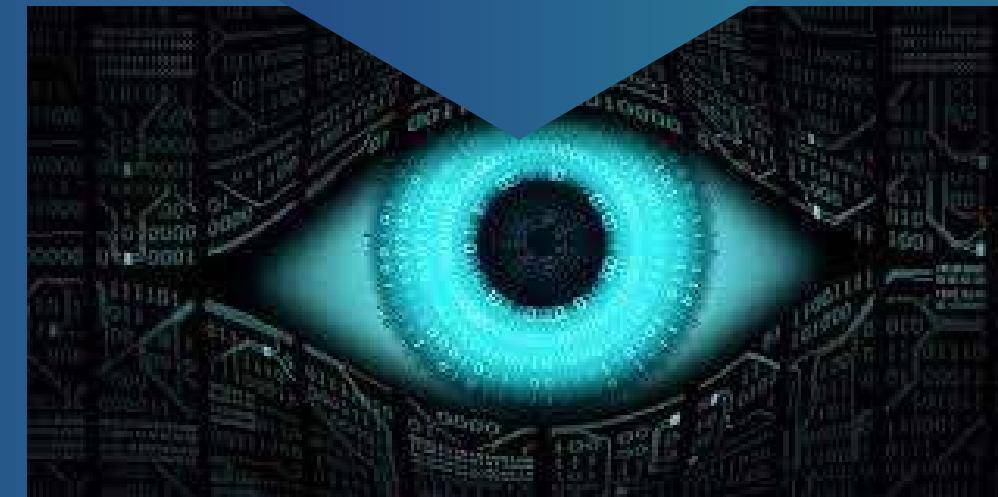
Ataque en el que un ciberdelincuente se hace pasar por una fuente confiable para robar información confidencial, como contraseñas o datos bancarios.



02

Spyware

Software que recopila información del usuario sin su consentimiento, como hábitos de navegación o datos personales.



03

Adware

Programa que muestra anuncios invasivos y ralentiza el dispositivo.





TIPOS DE MALWARE

04

Virus

Código malicioso que se replica al ejecutar archivos infectados y daña el sistema.



05

Malware sin archivos

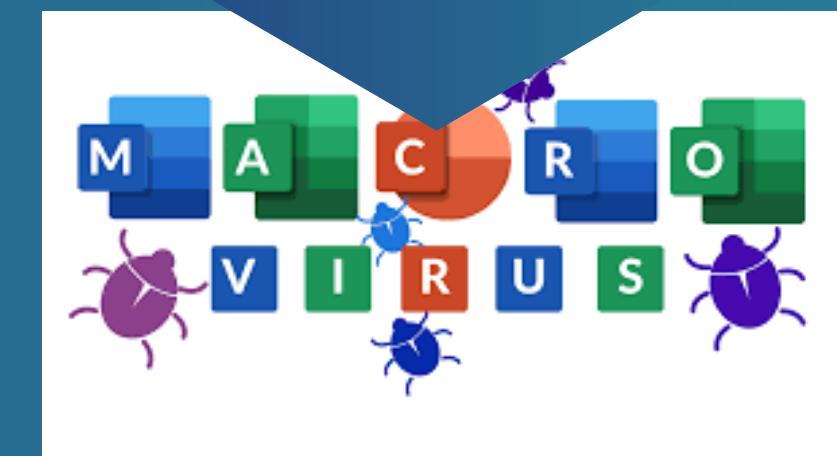
Malware que se ejecuta en la memoria del sistema sin dejar rastros en el disco, lo que dificulta su detección.



06

Malware de macros

Malware que utiliza la función de macros en documentos para infectar sistemas.





TIPOS DE MALWARE

07

Ransomware

Malware que cifra los datos de la víctima y exige un rescate para liberarlos.



08

Rootkits

Software que oculta la presencia de malware, permitiendo a los atacantes controlar el dispositivo sin ser detectados.



09

Ataques a la cadena de suministro

Infiltración de malware en el software legítimo de un proveedor para afectar a sus clientes.





TIPOS DE MALWARE

10

Estafas de soporte técnico

Los atacantes engañan a las víctimas haciéndose pasar por soporte técnico para que instalen malware o paguen por servicios falsos.



11

Troyanos

Malware que se disfraza de software legítimo para instalar otros programas maliciosos o robar datos.



12

Gusanos

Malware que se autoreplica y se propaga por redes sin intervención del usuario.



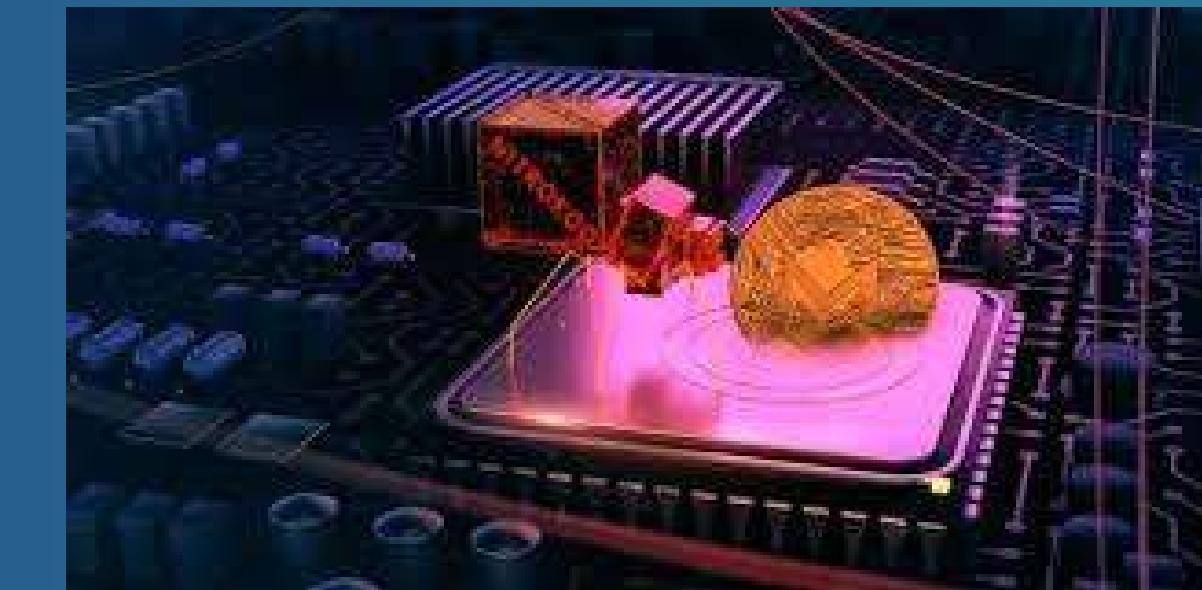


TIPOS DE MALWARE

13

Mineros de monedas

Software que utiliza recursos de un dispositivo sin autorización para minar criptomonedas.





INTRUSOS INFORMATICOS



Se puede resumir en pocas palabras como una persona que intenta acceder a un sistema informático sin autorización.

El termino Hacker es quizás el termino más conocido y se utiliza como termino paraguas para todo tipo de intrusos informáticos. Sobre todo gracias a películas y series se ha creado un estereotipo, una imagen que evocamos al pensar en un Hacker.





TIPOS DE INTRUSOS

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.

White Hats

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

Alertan de un fallo en algún programa comercial, comunicándose al fabricante.

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 esté dispuesto a pagar por ellas. Su clientela abarca gobiernos, servicios militares y otros hackers.

Black Hats

Utilizan sus conocimientos para realizar actividades ilegales, normalmente con ánimo de lucro y para aumentar su reputación. Suelen ser creadores de tipo de malware.

Crackers

Ser un cracker es saber romper algo, en este caso sistemas y software. Tienen un conocimiento profundo de programación y electrónica. Nos pueden sonar de los cracks que permiten utilizar un software sin haber pagado por la licencia. Dicho en otras palabras, la edición desautorizada de software de propiedad. La fascinación de un cracker por romper sistemas y software suele ser motivado por una multitud de razones, desde el lucro, pasando por actos de protesta hasta el simple desafío.



TIPOS DE INTRUSOS

Lamer

Este grupo es quizás el que más número de miembros posee y quizás son los que mayor presencia tienen en la red. Normalmente son individuos con ganas de hacer Hacking, pero que carecen de cualquier conocimiento. Habitualmente son individuos que apenas si saben lo que es una computadora, pero el uso de este y las grandes oportunidades que brinda Internet, convierten al nuevo internauta en un obsesivo ser que rebusca y relee toda la información que le fascina y que se puede encontrar en Internet.

Script Kiddies

Es un individuo no calificado que utiliza scripts o programas desarrollados por otros para atacar sistemas informáticos, redes y defectos de sitios web. Se supone generalmente son niños que carecen de la capacidad de escribir programas sofisticados o exploits y su objetivo es intentar impresionar a sus amigos o ganar el crédito en las comunidades de entusiastas de la computadora. Sin embargo, el término no se relaciona con la edad real del participante.

Phreakers

Phreaking es un término de argot acuñado para describir la actividad de una cultura de personas que estudian, experimentan o exploran sistemas de telecomunicaciones, tales como equipos y sistemas conectados a redes telefónicas públicas.

Insiders

Son empleados, contratistas o cualquier persona con acceso interno a los sistemas y datos de una organización. A diferencia de los hackers externos, estos individuos ya están dentro de los muros digitales y pueden aprovechar su posición para llevar a cabo ataques internos.



METODOS DE ATAQUES



Phishing

Es el uso de correos electrónicos o sitios web falsos para engañar a las personas y hacer que revelen información confidencial, como contraseñas o números de tarjetas de crédito.



Inyección SQL

Es un ataque que aprovecha vulnerabilidades en aplicaciones web para manipular las bases de datos subyacentes mediante comandos SQL maliciosos.



Denegación de servicio (DoS/DDoS)

Ataques que buscan sobrecargar un servidor o red con tráfico hasta que no pueda responder o funcione correctamente.



Malware (virus, troyanos, ransomware)

Software malicioso que se instala en un sistema sin el conocimiento del usuario, con el fin de robar información, dañar el sistema o extorsionar.



Exploits de día cero

Descripción: Ataques que aprovechan vulnerabilidades en software que aún no han sido descubiertas o corregidas por los desarrolladores.



Robo de credenciales

El atacante obtiene las credenciales de inicio de sesión de un usuario legítimo para acceder a sus cuentas o sistemas.



AUTENTICACIÓN Y CONTROL DE ACCESO

Los métodos y tecnologías de autenticación son mecanismos utilizados para verificar la identidad de un usuario o sistema antes de permitir el acceso a ciertos recursos o servicios.

Estos métodos tienen como objetivo asegurar que quien intenta acceder sea realmente quien dice ser, protegiendo así la integridad y confidencialidad de la información.



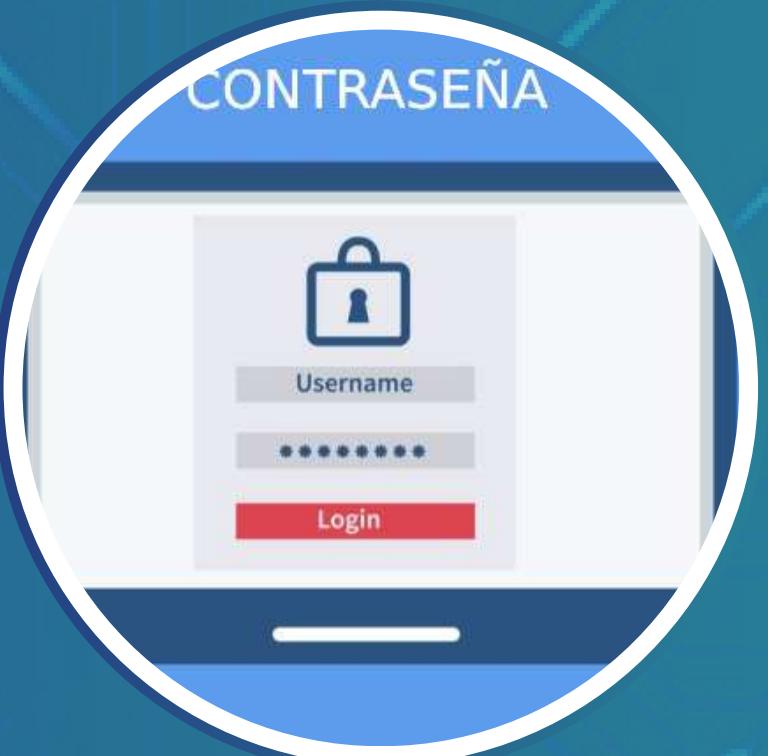


Métodos de Autenticación

1. AUTENTICACIÓN BASADA EN CONOCIMIENTO

Contraseñas o PINs: El usuario proporciona una contraseña o código que solo él debería conocer. Es el método más común, pero su seguridad depende de la complejidad de la contraseña.

Preguntas de seguridad: Preguntas cuya respuesta solo debería conocer el usuario. Su uso está disminuyendo por problemas de seguridad, ya que pueden ser adivinadas o descubiertas.





Métodos de Autenticación

2. AUTENTICACIÓN BASADA EN POSESIÓN

- **Tokens de seguridad:** Dispositivos físicos (como tarjetas inteligentes, llaves USB o llaves criptográficas) que generan o almacenan códigos de autenticación. El acceso requiere poseer el dispositivo.
- **Aplicaciones de autenticación:** Aplicaciones móviles como Google Authenticator o Authy, que generan códigos de un solo uso (OTP) para acceder a servicios
- **Autenticación por SMS:** Se envía un código temporal al número de teléfono registrado, que el usuario debe ingresar para verificar su identidad.





Métodos de Autenticación

3. AUTENTICACIÓN BASADA EN INHERENCIA

- **Biometría:** Usa características físicas o comportamentales únicas del usuario, como huellas dactilares, reconocimiento facial, reconocimiento de voz o escaneo de iris. Este método es difícil de falsificar, pero puede ser costoso de implementar.
- **Ejemplos:** Apple Face ID, Windows Hello, y lectores de huellas dactilares en dispositivos móviles o computadoras.





Métodos de Autenticación

4. AUTENTICACIÓN BASADA EN UBICACIÓN

- Utiliza la ubicación geográfica del usuario para ayudar a validar su identidad. Si se detecta un inicio de sesión desde un lugar no reconocido, se puede solicitar una verificación adicional.
- **Ejemplo:** Servicios como Google o Facebook pueden alertar al usuario si su cuenta es accedida desde un país o dispositivo no familiar.





Métodos de Autenticación

5. AUTENTICACIÓN MULTIFACTOR (MFA)

- Combinación de dos o más métodos de autenticación para aumentar la seguridad. Un ejemplo típico es la autenticación de dos factores (2FA), que combina una contraseña (algo que el usuario sabe) con un código generado por una aplicación o enviado por SMS (algo que el usuario posee).
- **Ejemplo:** Acceder a una cuenta bancaria en línea utilizando una contraseña y un código enviado al teléfono del usuario.





NIVELES DE SEGURIDAD





La seguridad en el ámbito de la informática se puede clasificar en tres niveles principales: usuarios individuales, redes y empresas. Cada nivel tiene diferentes necesidades y medidas de seguridad que deben aplicarse para proteger la integridad, confidencialidad y disponibilidad de la información. Los tres niveles que se clasifican son:

- 1. Seguridad para Usuarios Individuales**
- 2. Seguridad en Redes**
- 3. Seguridad en Redes**





1.- Seguridad para Usuarios Individuales

Medidas de Seguridad:

- **Contraseñas seguras:** Utilizar contraseñas complejas y únicas para cada cuenta, con autenticación de dos factores (2FA) siempre que sea posible.
- **Actualizaciones de software:** Mantener el sistema operativo, aplicaciones y antivirus actualizados para proteger contra vulnerabilidades.
- **Software antivirus y antimalware:** Instalar programas que detecten y eliminen amenazas como virus, troyanos y ransomware
- **Cifrado de datos:** Usar cifrado en discos duros, archivos y comunicaciones para proteger la información sensible.
- **Concienciación y educación:** Capacitar a los usuarios sobre los riesgos de seguridad y prácticas seguras, como identificar correos electrónicos de phishing.





2.-Seguridad en Redes



Medidas de Seguridad:

- **Firewalls:** Implementar firewalls para filtrar el tráfico entrante y saliente, evitando accesos no autorizados.
- **VPN (Redes Privadas Virtuales):** Asegurar las comunicaciones remotas a través de redes públicas mediante VPNs que cifran los datos transmitidos.
- **Sistemas de detección y prevención de intrusos (IDS/IPS):** Monitorizar la red para detectar y prevenir actividades sospechosas o maliciosas.
- **Segmentación de la red:** Dividir la red en segmentos para limitar el acceso y minimizar el impacto de posibles brechas de seguridad.
- **Control de acceso a la red (NAC):** Restringir el acceso a la red solo a dispositivos y usuarios autorizados.



3.-Seguridad en Empresas

Medidas de Seguridad:

- **Cifrado de datos empresariales:** Asegurar que todos los datos sensibles se cifren, tanto en reposo como en tránsito.
- **Gestión de identidades y accesos (IAM):** Controlar quién tiene acceso a qué recursos dentro de la organización, y auditar el acceso.
- **Copias de seguridad y recuperación ante desastres:** Implementar copias de seguridad regulares y planes de recuperación para minimizar el impacto de posibles pérdidas de datos.
- **Sistemas de gestión de seguridad de la información (SGSI):** Implementar políticas de seguridad basadas en estándares internacionales (ISO 27001, por ejemplo).
- **Seguridad física:** Controlar el acceso físico a las instalaciones para evitar robos de hardware y proteger centros de datos.





Cada una de las 3 clasificaciones:



Necesidades de Seguridad:

1.-

- **Protección contra malware y virus.**
- **Seguridad en las contraseñas.**
- **Privacidad en la navegación y comunicación.**

Necesidades de Seguridad:

2.-

- **Protección contra ataques de red (DDoS, MITM, etc.).**
- **Seguridad en el tráfico de datos.**

Necesidades de Seguridad:

3.-

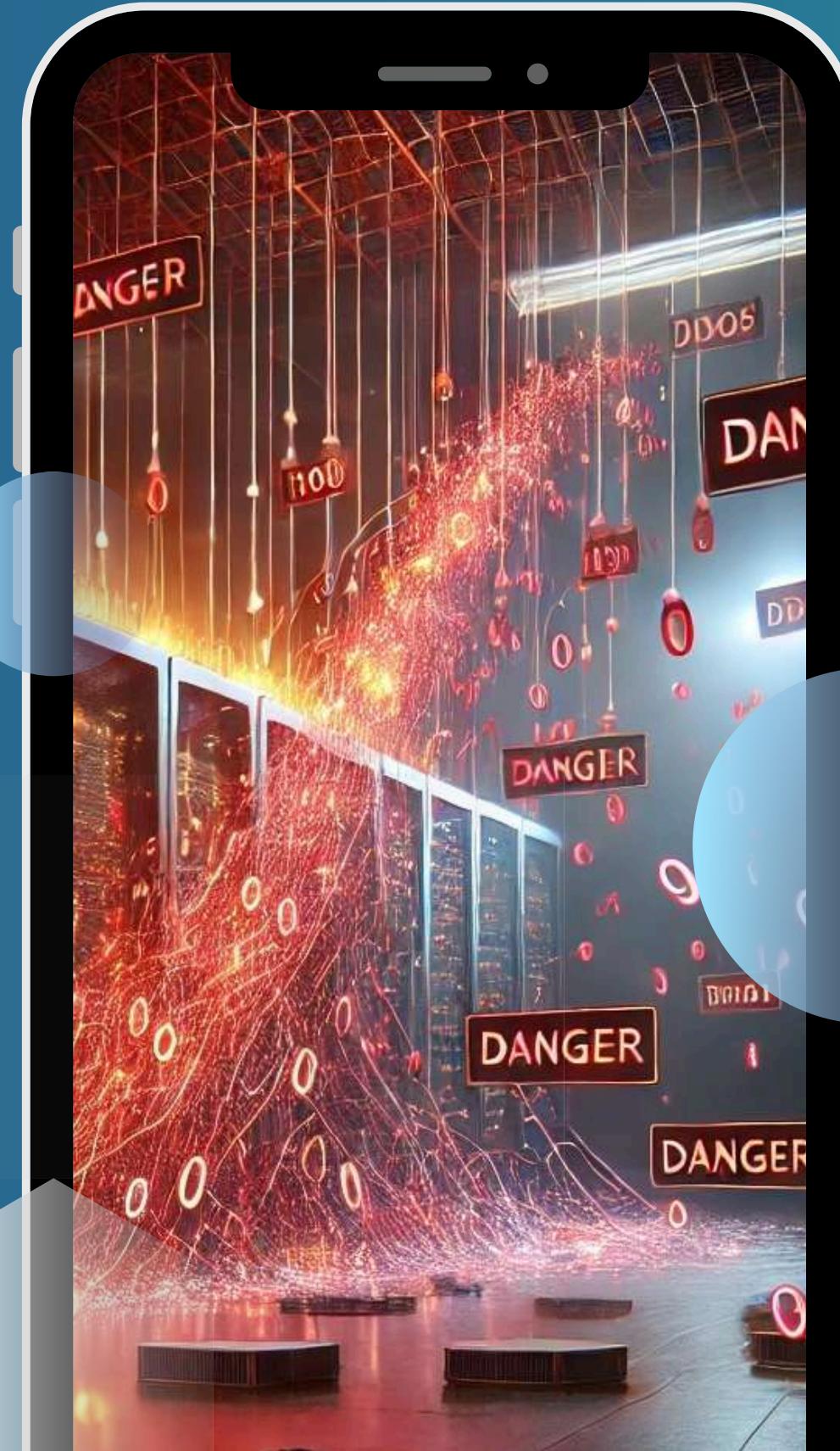
- **Protección contra pérdida y robo de datos.**
- **Cumplimiento de normativas de seguridad y privacidad.**
- **Seguridad integral en todos los niveles (usuarios, sistemas, red, físico). Monitorización y control de accesos.**



ANÁLISIS DE POSIBLES PROBLEMAS DE SEGURIDAD

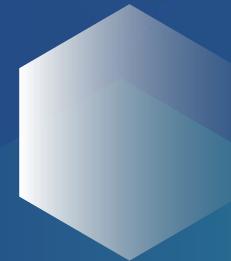
ATAQUES DDOS (DENIAL OF SERVICE DISTRIBUIDO)

Los ataques DDoS tienen como objetivo saturar un servidor, red o servicio con un volumen masivo de tráfico, provocando que los recursos se agoten y que el servicio legítimo se vuelva inaccesible para los usuarios. Estos ataques se realizan usando múltiples sistemas infectados, conocidos como botnets, para enviar solicitudes simultáneamente.





IMPACTO Y CONSECUENCIAS



Interrupción del Servicio

Los ataques DDoS pueden hacer que un sitio web o servicio deje de funcionar durante horas o incluso días.



Perdida Financiera

Empresas que dependen de servicios en línea pueden experimentar pérdidas significativas debido a la interrupción del servicio.



Daño y Reputación

Si un sitio web sufre repetidos ataques DDoS, los clientes pueden perder confianza en la capacidad de la empresa para proteger sus servicios.





EJEMPLO DE INCIDENTES



Dyn (2016)

En octubre de 2016, un ataque DDoS a los servidores de Dyn, un proveedor de DNS, afectó a varios servicios importantes como Twitter, Spotify y Reddit. El ataque fue realizado utilizando una botnet llamada Mirai, que comprometió dispositivos IoT.

GitHub (2018)

En 2018, GitHub sufrió el mayor ataque DDoS registrado en ese momento, con un pico de tráfico de 1.35 Tbps, aunque el servicio fue capaz de mitigarlo en minutos.



SUPLANTACIÓN DE IDENTIDAD (PHISHING Y SPOOFING)

La suplantación de identidad incluye técnicas para engañar a las víctimas y obtener sus datos confidenciales, como contraseñas y detalles bancarios. Los métodos comunes incluyen phishing (envío de correos electrónicos falsos) y spoofing (falsificación de direcciones IP o páginas web).



IMPACTO Y CONSECUENCIAS



Robo de Información Personal

Los ataques de phishing pueden llevar al robo de contraseñas, datos financieros, y otros tipos de información personal.



Acceso No Autorizado

Los atacantes pueden usar la información obtenida para acceder a cuentas y sistemas críticos.



Fraude Financiero

La información robada puede utilizarse para realizar transacciones fraudulentas, retiradas de dinero y compras no autorizadas.



EJEMPLO DE INCIDENTES



SONY
PICTURES

Ataque de phishing a Ubiquiti (2020)

Empleados de Ubiquiti fueron engañados por un ataque de phishing, lo que permitió a los atacantes acceder a sistemas internos y potencialmente a datos de clientes.

Caso de suplantación de identidad a la empresa Sony Pictures (2014)

Los atacantes lograron acceder a información confidencial de la empresa, incluidos correos electrónicos personales y películas inéditas, usando técnicas de spoofing y phishing.





IMPACTO Y CONSECUENCIAS

FILTRACIONES DE DATOS

Las filtraciones de datos se producen cuando información sensible se divulga sin autorización. Esto puede deberse a ataques externos, errores humanos o fallos en la seguridad de los sistemas.

Pérdida de Confidencialidad

Información privada, financiera o sensible puede quedar expuesta, afectando a clientes y empresas.

Implicaciones Legales y Multas

Las empresas pueden enfrentar multas significativas por incumplimiento de regulaciones de privacidad de datos, como el GDPR.

Daño a la Reputación

Las filtraciones dañan la reputación de la empresa y pueden llevar a la pérdida de clientes.



EJEMPLO DE INCIDENTES



Facebook (2019)

Se descubrió que millones de registros de usuarios estaban almacenados de forma insegura en servidores de Amazon, accesibles públicamente sin autenticación.

Equifax (2017)

Un ataque a Equifax expuso datos personales, incluyendo números de seguridad social, de aproximadamente 147 millones de personas. Este incidente tuvo consecuencias legales y financieras significativas para la empresa.





PREVENCIÓN DE DESASTRES Y ADMINISTRACIÓN DE RIESGOS





SISTEMA DE PREVENCIÓN DE INTRUSIONES

Un sistema de prevención de intrusiones, también conocidos como IPS por sus siglas en inglés, supervisa el tráfico de red para detectar posibles amenazas y las bloquea automáticamente alertando al equipo de seguridad, terminando conexiones peligrosas, eliminando contenido maligno o activando otros dispositivos de seguridad.



PREVENCIÓN CONTRA INTRUSOS





METODOS DE PREVENCIÓN DE AMENAZAS DE IPS

BLOQUEO DE TRAFICO MALIGNO

Un IPS puede finalizar la sesión de un usuario, bloquear una dirección IP específica o incluso bloquear todo el tráfico hacia un objetivo. Algunos IPS pueden redirigir el tráfico a un honeypot, un recurso señuelo que hace que los hackers piensen que han tenido éxito cuando, en realidad, el centro de operaciones de seguridad los está viendo.



ELIMINAR CONTENIDO MALIGNO

Un IPS puede permitir que el tráfico continúe, pero elimina las partes peligrosas, por ejemplo, descartando los paquetes malignos de un flujo o eliminando un archivo adjunto maligno de un correo electrónico.





METODOS DE PREVENCIÓN DE AMENAZAS DE IPS

ACTIVAR OTROS DISPOSITIVOS DE SEGURIDAD

Un IPS puede solicitar que otros dispositivos de seguridad actúen, por ejemplo, actualizando reglas de firewall para bloquear una amenaza o cambiar la configuración del enrutador para evitar que los hackers alcancen sus objetivos.



APLICACIÓN DE POLÍTICAS DE SEGURIDAD

Algunos IPS pueden evitar que los atacantes y usuarios no autorizados hagan algo que infrinja las políticas de seguridad de la empresa. Por ejemplo, si un usuario intenta transferir información confidencial fuera de una base de datos de la que se supone que no debe salir, el IPS lo bloquearía.





PREVENCIÓN CONTRA MALWARE

INSTALA UN SOFTWARE ANTIVIRUS/MALWARE

Es importante tener en cuenta que la efectividad de un antivirus depende de su capacidad para detectar nuevas amenazas, por lo que es esencial mantenerlo actualizado. Los desarrolladores de software antivirus lanzan regularmente actualizaciones que contienen nuevas definiciones y algoritmos de detección para contrarrestar las últimas amenazas.

REALIZA ANÁLISIS PROGRAMADOS REGULARMENTE

Configura tu software antivirus para realizar análisis periódicos de tu dispositivo. Esto te ayudará a detectar y eliminar cualquier malware existente. Programa los análisis en momentos en los que no necesites utilizar tu dispositivo para evitar interrupciones.





PREVENCIÓN CONTRA MALWARE

MANTÉN TU SISTEMA OPERATIVO ACTUALIZADO

Los parches de seguridad proporcionados por los desarrolladores ayudan a cerrar las brechas y proteger tu dispositivo de las vulnerabilidades del malware.

PROTEGE TU RED

Asegúrate de utilizar contraseñas seguras y cifrado WPA2 en tu red Wi-Fi. Evita las conexiones a Wi-Fi abiertas, como lo pueden ser las de lugares públicos como cafeterías o aeropuertos, y deshabilita la difusión del SSID de tu red. Considera el uso de una VPN para cifrar tu conexión y proteger tu privacidad en línea.





PREVENCIÓN CONTRA MALWARE

CUIDADO AL ABRIR CORREOS ELECTRÓNICOS Y DESCARGAR ARCHIVOS ADJUNTOS

Evita abrir correos electrónicos de remitentes desconocidos o sospechosos. No hagas clic en enlaces o descargas archivos adjuntos de fuentes no confiables. Verifica la autenticidad del correo electrónico antes de interactuar con él.

MANTÉN TU INFORMACIÓN PERSONAL SEGURA

Evita proporcionar datos sensibles en tablones de mensajes y redes sociales. Configura adecuadamente la privacidad de tus cuentas y evita utilizar tu nombre real en foros de discusión.





PREVENCIÓN CONTRA MALWARE

HAZ UNA COPIA DE SEGURIDAD DE TUS ARCHIVOS

Es fundamental realizar copias de seguridad periódicas de tus datos. Guarda tus archivos importantes en dispositivos de almacenamiento externos o en la nube. Mantén al menos tres copias de tus archivos: una en tu dispositivo, otra en un disco duro externo y una tercera en una ubicación fuera del sitio, como un servicio de almacenamiento en la nube o un disco duro en un lugar seguro.

UTILIZA CONTRASEÑAS SEGURAS Y ÚNICAS

Evita utilizar la misma contraseña para múltiples cuentas. Crea contraseñas fuertes que incluyan una combinación de letras mayúsculas y minúsculas, números y caracteres especiales. No utilices información personal obvia en tus contraseñas y cámbialas regularmente.





ESTRATEGIAS DE RECUPERACIÓN

PLAN DE RECUPERACIÓN ANTE DESASTRES

Un plan de recuperación ante desastres (DRP o disaster recovery plan) es la documentación y procesos estratégicos de una organización para restaurar el acceso a los sistemas e infraestructuras comprometidos después de un ciberataque, error humano, desastre natural u otros eventos catastróficos. Es la metodología sistemática mediante la cual un equipo asigna sus recursos para retomar eficazmente el control de sistemas clave de datos e información después de un desastre.





ESTRATEGIAS DE RECUPERACIÓN

EVALUACIÓN DE RIESGOS

Los equipos deben evaluar concienzudamente todas las potenciales amenazas y debilidades en la infraestructura de TI de la organización, con especial interés en las áreas que sean más susceptibles ante ciberataques.

CONTINUIDAD DE NEGOCIO

Determinación de los procedimientos y recursos a utilizar para mantener activas las operaciones clave del negocio en caso de desastre.



ESTRATEGIAS DE RECUPERACIÓN

ARCHIVADO, RESPALDO
Y RECUPERACIÓN DE
DATOS

Documentación e implementación de los procesos de mantenimiento para respaldar periódicamente los datos y sistemas clave, incluyendo planes para restaurar estos activos si quedan comprometidos debido a un desastre o ataque.

RESPUESTA ANTE
INCIDENCIAS

Desarrollar un flujo de procedimientos y ejercicios que articulen claramente cómo debe responder un equipo a un ciberataque, filtración o desastre, incluyendo el cómo identificar y contener la amenazas, evaluar los daños y restaurar los sistemas afectados.



ESTRATEGIAS DE RECUPERACIÓN

COMUNICACIÓN

Un plan de recuperación ante desastres para corporaciones debe incluir instrucciones acerca de cómo comunicar la situación a los interesados clave en caso de ataque. Esto incluye a los empleados, clientes, proveedores, inversores afectados, y a los medios de comunicación.

CAPACITACIÓN Y FORMACIÓN

Crear un sistema para capacitar y formar adecuadamente a los empleados en buenas prácticas de ciberseguridad y respuesta a desastres, particularmente en ejercicios clave indicados en el plan de la organización y para qué se debe estar preparado si ocurre un desastre.



ESTRATEGIAS DE RECUPERACIÓN

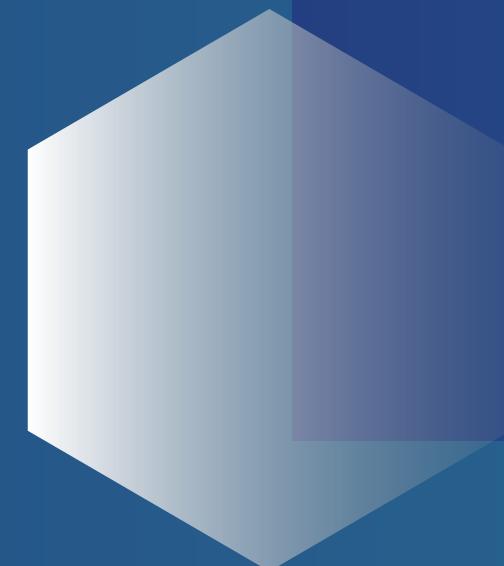
PRUEBAS Y SIMULACROS

La ejecución y práctica consistente de los planes de recuperación ante desastres son vitales para garantizar su eficacia y que su equipo pueda tener confianza en sus papeles y responsabilidades para manejar las amenazas a medida que vayan surgiendo.





SEGURIDAD DE HADWARE



La seguridad de hardware se refiere a las medidas y controles implementados para proteger los dispositivos físicos de amenazas que pueden afectar su funcionamiento, como robos, manipulación o accesos no autorizados. Asegurar el hardware es esencial para proteger la infraestructura informática y los datos que estos dispositivos manejan.



CONTROL DE ACCESO FÍSICO

Restricción de Acceso

Las áreas donde se encuentran equipos sensibles deben tener acceso limitado solo al personal autorizado.

Supervisión y Vigilancia

El uso de cámaras de seguridad y sistemas de monitoreo para vigilar áreas críticas puede ayudar a disuadir intentos de acceso no autorizado y proporcionar evidencia en caso de incidentes.



MEDIDAS PARA PROTEGER EL HADWARE

SEGURIDAD FÍSICA DEL HARDWARE

Bloqueos y Candados de Seguridad

Los servidores, estaciones de trabajo y otros dispositivos importantes pueden estar protegidos con candados físicos que previenen su apertura o desconexión sin las llaves adecuadas.



Protección contra Robos

Se pueden usar anclajes para fijar computadoras portátiles o pequeños dispositivos a escritorios, evitando que sean removidos fácilmente.

PROTECCIÓN DE LA INFORMACIÓN

Confidencialidad de los Datos

Si alguien tiene acceso físico a un servidor, puede extraer información directa del dispositivo sin necesidad de penetrar las defensas digitales.

Prevención de Manipulación de Hardware

Un atacante con acceso físico puede manipular el hardware para insertar dispositivos de espionaje o malware, lo que podría comprometer la red entera.

Normativas de Protección de Datos

Muchas regulaciones, como el GDPR o la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA), exigen que las empresas protejan no solo los datos en sí, sino también los dispositivos que almacenan dichos datos. La falta de medidas de seguridad adecuadas puede resultar en sanciones financieras.

IMPORTANCIA DE

MANTENER SEGUROS LOS DISPOSITIVOS FÍSICOS



CUMPLIMIENTO DE REGULACIONES

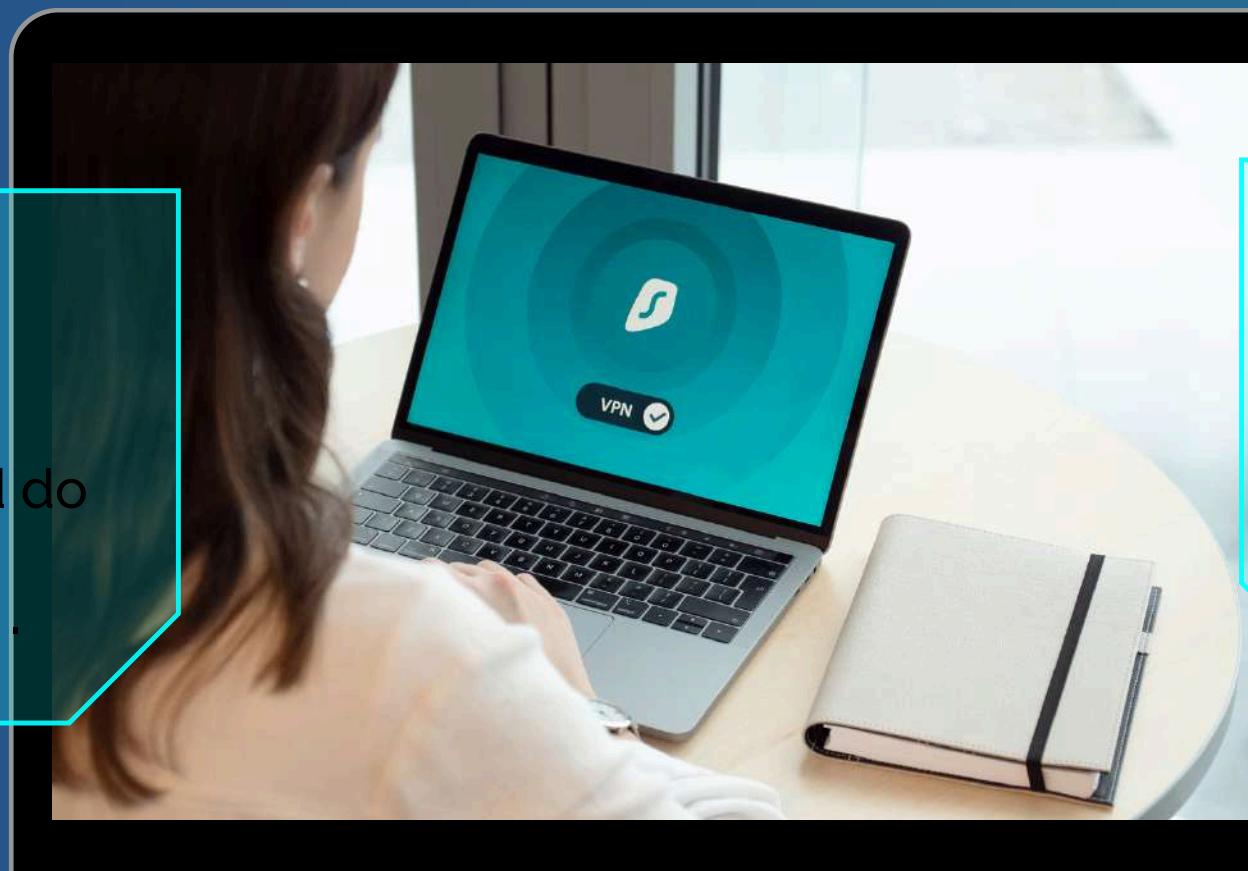


Studio Shodwe

PERSONAL TIPS

Keep Software Updated

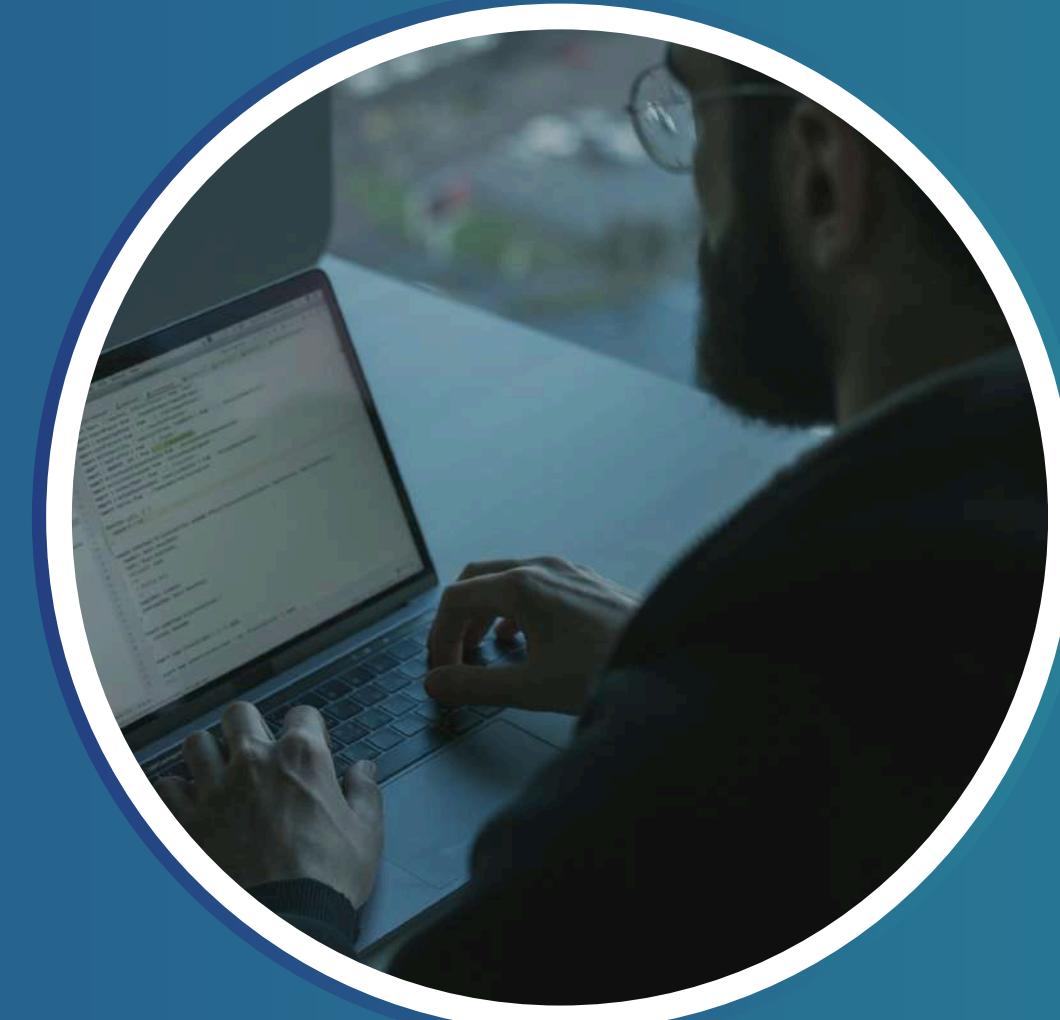
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua..



Secure Home Networks

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua..





SEGURIDAD DE SOFTWARE Y ARCHIVOS



SEGURIDAD



La seguridad es la garantía que tienen las personas de estar libres de todo daño, amenaza, peligro o riesgo, es la necesidad de sentirse protegidas, contra todo aquello que pueda perturbar o atentar contra su integridad física, moral, social y hasta económica.



SOFTWARE



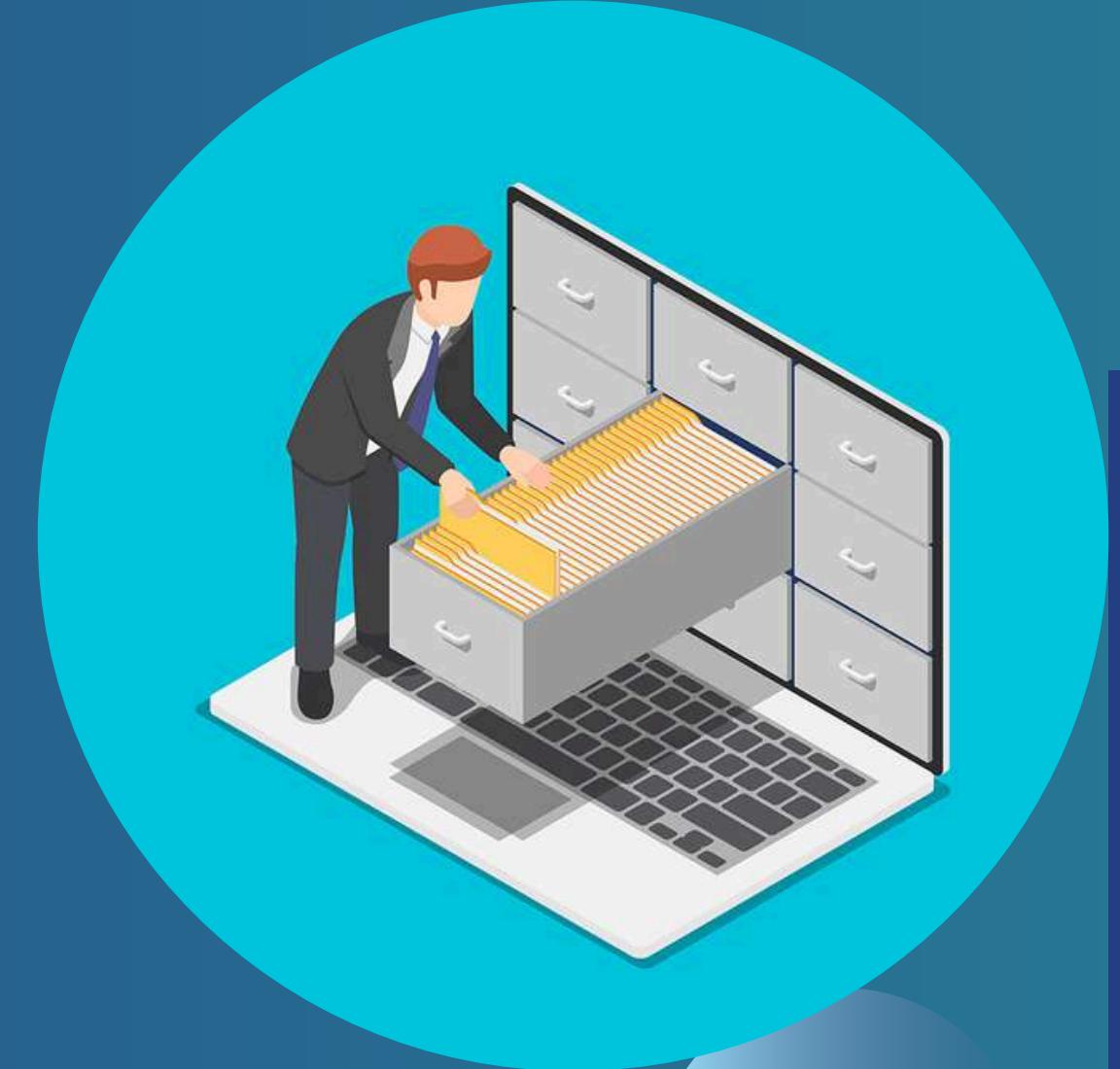
Es un programa o conjunto de programas de cómputo, así como datos, procedimientos y pautas que permiten realizar distintas tareas en un sistema informático.



ARCHIVOS



es una secuencia de bytes almacenados en un dispositivo. Un archivo es identificado por un nombre y la descripción de la carpeta o directorio que lo contiene.



SEGURIDAD DE SOFTWARE



Es la encargada de proteger los programas informáticos de los ciberataques de terceros malintencionados, como el malware y los hackers, este concepto se implementa en mecanismos en la construcción de la seguridad para ayudar a permanecer resistente a los ataques, esto significa que una pieza de software se somete a pruebas de seguridad antes de salir al mercado para comprobar su capacidad para resistir ataques maliciosos



SEGURIDAD DE ARCHIVOS



La seguridad de los archivos se define como el acceso, distribución y almacenamiento seguros de archivos digitales, entre ellos se incluyen documentos, información crítica para la empresa, archivos de registro y código fuente, las medidas de seguridad de los archivos impiden que estos activos sean borrados, manipulados o accedidos por personas no autorizadas.



PARCHEO DE VULNERABILIDADES



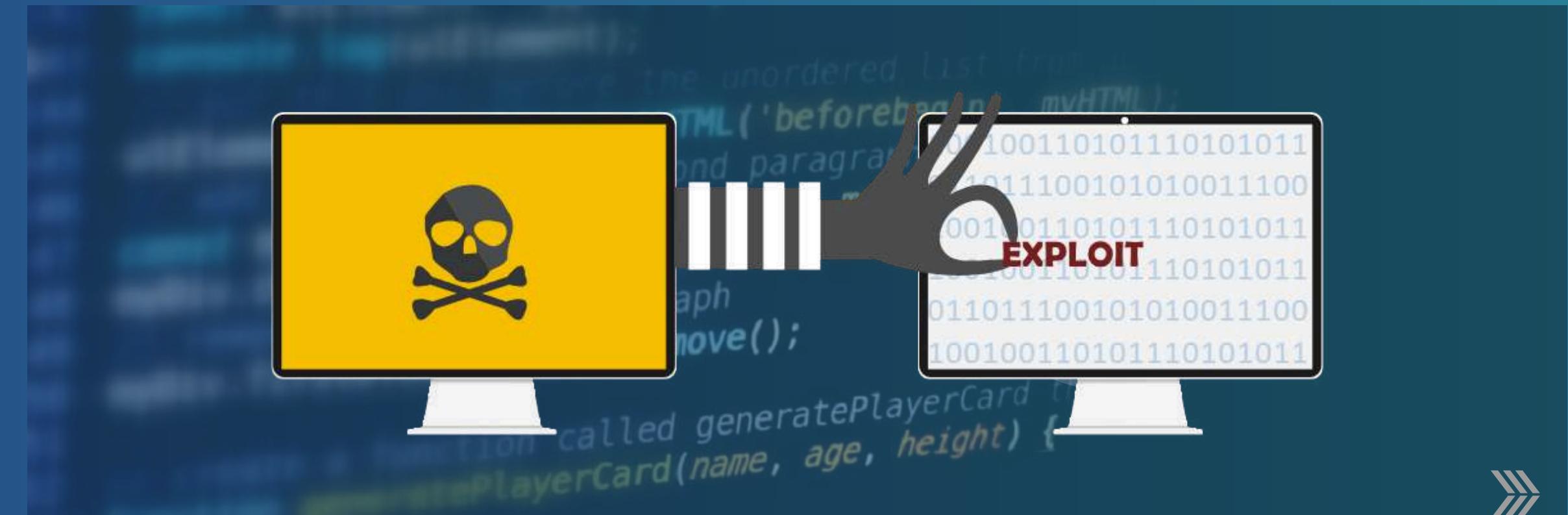
El parcheo de vulnerabilidades son actualizaciones de software diseñadas específicamente para corregir vulnerabilidades y errores detectados en sistemas operativos, aplicaciones y firmware, todo esto con el objetivo de proteger la información del usuario o la empresa de malware, virus, hacking.



EXPLOITS



Un exploit es un fragmento de código o una secuencia de comandos diseñado para aprovechar una vulnerabilidad o fallo en una aplicación o sistema, con el fin de causar un comportamiento no deseado o imprevisto, como la obtención de acceso no autorizado, la ejecución de código arbitrario o la interrupción de los servicios.



PROTECCIÓN CONTRA EXPLOITS:



Son un conjunto de técnicas y herramientas diseñadas para prevenir, mitigar o bloquear intentos de aprovechar vulnerabilidades en software o sistemas, estas protecciones trabajan para evitar que los atacantes utilicen exploits para ejecutar código malicioso, obtener acceso no autorizado o causar daños a un sistema.



EJEMPLOS DE TÉCNICAS DE PROTECCIÓN CONTRA EXPLOITS INCLUYEN

01

Data Execution Prevention (DEP)

Evita que ciertas áreas de la memoria, que deberían contener solo datos, se utilicen para ejecutar código.

02

Address Space Layout Randomization (ASLR)

Desordena la disposición de los componentes clave de un programa en la memoria, dificultando que los atacantes predigan dónde se encuentran.

03

Control Flow Integrity (CFI)

Asegura que el flujo de control de un programa siga las rutas previstas, previniendo ataques que desvíen su ejecución.

01

Sandboxing

Aisla las aplicaciones en entornos limitados para minimizar el impacto de un exploit si ocurre.



MÉTODOS DE CIFRADO



El cifrado es un método de criptografía moderno que codifica la información de tal manera que solo las partes autorizadas pueden acceder a ella. Hoy en día, la mayoría de los servicios centrados en la seguridad y la privacidad lo utilizan, uno de los ejemplos más habituales y fáciles de entender es el correo electrónico, si envías un correo electrónico cifrado, significa que solo tú y tu destinatario pueden verlo.



TIPOS DE CIFRADO

01

Simétrico

emplea la misma clave secreta tanto para codificar texto sin formato como para decodificar texto cifrado, esto significa que ambas partes deben conocer la clave, el cifrado simétrico es la opción más indicada para transferir grandes cantidades de datos, ya que se tarda menos tiempo en cifrarlos y descifrarlos.

02

Asimétrico

cifra y descifra los datos utilizando dos claves asimétricas criptográficas independientes. estas dos claves se conocen como "clave pública" y "clave privada"



MÉTODOS COMUNES DE CIFRADO ASIMÉTRICO



- RSA: RSA, que lleva el nombre de los científicos informáticos Ron Rivest, Adi Shamir y Leonard Adleman, es un algoritmo popular que se utiliza para cifrar datos con una clave pública y descifrarlos con una clave privada para una transmisión segura de datos.
- Infraestructura de clave pública (PKI): PKI es una forma de gestionar las claves de cifrado mediante la emisión y gestión de certificados digitales.



MÉTODOS COMUNES DE CIFRADO SIMÉTRICO



- Modo flujo: cada bit de datos se cifra de forma independiente y se transmite como un flujo continuo.
- Modo bloque: los datos que se van a cifrar se dividen primero en bloques de 56, 128, 192 o 256 bits, a continuación estos bloques se encriptan y se transmiten.



PERMISO PARA ARCHIVOS



Los permisos de archivo protegen a los archivos y los directorios para que no se puedan leer ni escribir sin autorización, los permisos de archivo le permiten controlar el acceso a sus archivos.



TIPOS BÁSICOS DE ACCESO DE ARCHIVOS Y DIRECTORIOS



- permiso de lectura. Un archivo debe poderse leer si se quiere examinar o copiar. Un directorio debe poderse leer si se quiere listar su contenido.
- permiso de escritura. Un archivo debe poder escribirse si desea modificarlo, eliminarlo o renombrarlo. Un directorio debe poder escribirse para agregar o eliminar archivos en él. •
- permiso de ejecución. Un archivo con permisos ejecutables es aquel que el usuario. puede procesar, como por ejemplo un programa. Un directorio debe ser ejecutable si quiere tener acceso a cualquiera de sus subdirectorios.

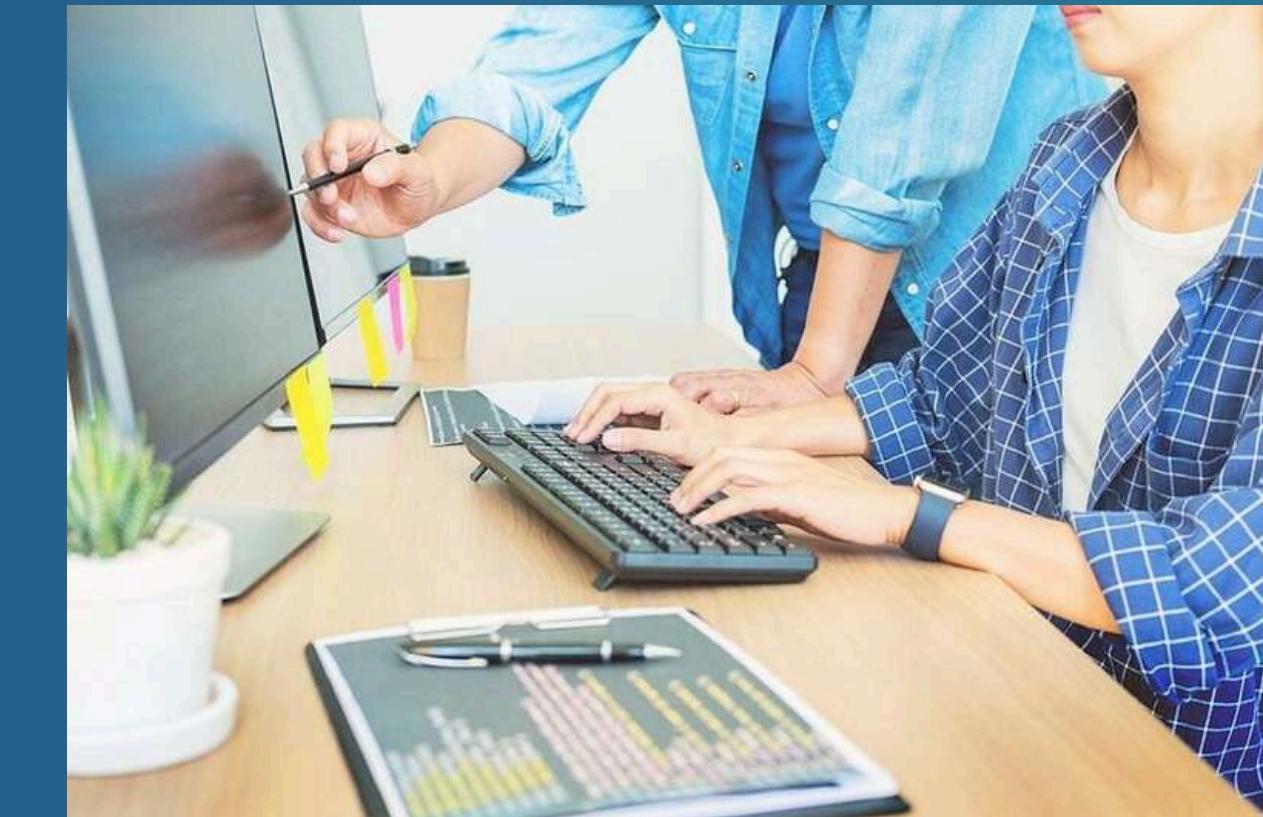


USUARIOS PARA LOS QUE SE PUEDE ESTABLECER PERMISOS



Uno mismo – El usuario

- Grupo – Otros usuarios pertenecientes al mismo grupo del usuario (por ejemplo, todos los usuarios con cuenta de acceso).
- Los grupos los establece y mantiene el administrador de su sistema.
- Otros – Todos los demás



SOLUCIONES DE SEGURIDAD

Y BUENAS PRÁCTICAS

En la era digital actual, proteger la seguridad de los datos y la continuidad de nuestros sistemas operativos es esencial. Para mitigar los riesgos, se utilizan diversas soluciones de seguridad, como:



ANTIVIRUS



IDS/IPS (Sistemas de Detección/Prevención de Intrusiones)



FIREWALLS





ANTIVIRUS

¿QUÉ SON?

Los antivirus son herramientas diseñadas para detectar, bloquear y eliminar software malicioso como virus, gusanos y troyanos. Estas soluciones protegen tanto sistemas individuales como redes completas.



Funciones Principales

- Detección de malware en tiempo real.
- Análisis de archivos y descargas.
- Bloqueo de sitios web maliciosos.
- Escaneo periódico del sistema.



Ejemplos de herramientas antivirus:

- Norton Antivirus
- Kaspersky
- McAfee
- Avast





FIREWALLS

¿QUÉ ES?

Es un sistema de seguridad que controla el tráfico de red para permitir el paso de datos no amenazantes y bloquear el tráfico peligroso.

Los firewalls pueden ser de hardware, de software o una combinación de ambos. Su funcionamiento se basa en un conjunto de reglas de seguridad que permiten o bloquean el paso de paquetes de datos.

Tipos de Firewalls

- **Firewall de red:** protege toda una red.
- **Firewall de host:** instalado en dispositivos individuales.
- **Firewalls de próxima generación (NGFW):** incluyen características avanzadas como inspección profunda de paquetes y protección contra amenazas avanzadas.





IDS/IPS (SISTEMAS DE DETECCIÓN/PREVENCIÓN DE INTRUSIONES)

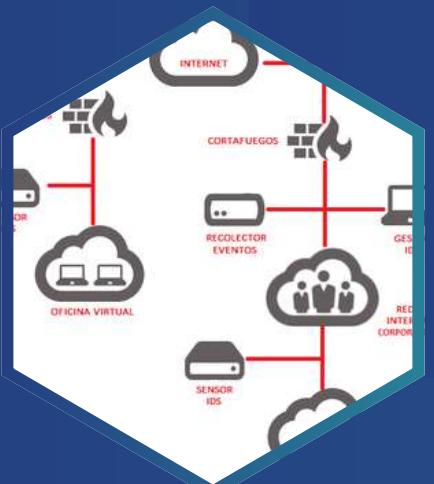
¿QUÉ ES?

El IDS/IPS es un sistema que monitorea la red o sistemas en busca de actividades maliciosas. El IDS detecta intrusiones, mientras que el IPS previene que dichas intrusiones causen daños.



Funciones Principales

- Detección de ataques en tiempo real.
- Bloqueo automático de actividad sospechosa (IPS).
- Registro de eventos y alertas.



Ejemplos de IDS/IPS:

- Norton Antivirus
- Kaspersky
- McAfee
- Avast

Detectan actividades sospechosas como:

- Ataques de suplantación de identidad (phishing)
- Infección y distribución de virus
- Instalación y descarga de malware y ransomware
- Denegación de servicio (DOS)
- Ataques de intermediarios
- Ataques de día cero
- Inyección SQL

BUENAS PRÁCTICAS

PARA IMPLEMENTAR POLÍTICAS DE SEGURIDAD



Actualizaciones y Parches Regulares



Las vulnerabilidades descubiertas en versiones antiguas pueden ser explotadas por atacantes, por lo que aplicar parches de seguridad y actualizaciones debe ser una tarea constante.

Cifrado de Datos

Es esencial cifrar los datos tanto en tránsito como en reposo para proteger la información sensible. Esto asegura que, en caso de un acceso no autorizado, los datos no puedan ser leídos.

Autenticación Multifactor (MFA)



Implementar mecanismos de autenticación multifactor añade una capa extra de seguridad. Además de la contraseña, se requiere un segundo factor de autenticación, como un código enviado al teléfono o un token físico.

Monitoreo Continuo y Respuesta a Incidentes

Establecer un sistema de monitoreo continuo de la red para identificar actividades sospechosas es vital. Además, debe existir un plan de respuesta a incidentes para actuar de manera rápida ante cualquier brecha de seguridad.



Studio Shodwe

**GRACIAS POR
SU ATENCIÓN**



CONCLUSIÓN GENERAL

Hemos visto que la seguridad informática es mucho más que solo tener instalado un antivirus. Los malware y las amenazas están en constante evolución, lo que significa que siempre debemos estar un paso adelante. Ya sea a un nivel personal, en nuestras redes o en una empresa, es fundamental tomar medidas para proteger nuestros datos y sistemas.

Existen diferentes tipos de intrusos y que el simple hecho de tener una contraseña ya no es suficiente. La seguridad no es algo que se hace una sola vez y ya está. Es un proceso continuo en el que tenemos que educarnos, actualizar nuestros sistemas y seguir las mejores prácticas. Al final, proteger nuestro hardware, software y archivos no solo nos beneficia a nosotros, sino que ayuda a mantener un entorno digital más seguro para todos.

En conclusión, la seguridad informática es responsabilidad de cada uno de nosotros. Con las herramientas adecuadas y la conciencia de los riesgos, podemos reducir las posibilidades de ser víctimas de ataques y proteger lo que más valoramos: nuestra información.

CONCLUSIONES INDIVIDUALES

1948932 - Antonio Enrique Hernández Ramírez

En conclusión, la seguridad de nuestros dispositivos e información es cada vez mas importante en nuestro día a día debido al aumento de las amenazas en línea. Los ciberdelincuentes están constantemente buscando nuevas formas de atacar los sistemas, robar datos o pedir rescates a cambio de liberar información. Por esto mismo, es importante que tanto las empresas como las personas sean conscientes de estas amenazas y tomen medidas para proteger los datos; como lo es usar contraseñas mas seguras, estar atentos a correos sospechosos o tener software de seguridad actualizados.

1962135 - Alexis Yahir Soria Salazar

Para concluir, después de hacer la investigación yo creo que la seguridad en los sistemas operativos debe de ser tomada como un tema muy importante ya que actualmente hay demasiadas maneras para que nuestra información y seguridad sean vulneradas muy fácilmente. La combinación de herramientas de seguridad como antivirus, firewalls e IDS/IPS, junto con la implementación de buenas prácticas de seguridad, nos permitirán proteger eficazmente las redes y los sistemas contra diversas amenazas. Además, una estrategia integral debe incluir la actualización constante de los sistemas, políticas claras, monitoreo activo y mantener un entorno seguro para estar más seguros.

CONCLUSIONES INDIVIDUALES

2131973-Uriel Ramiro De La Fuente Del Angel

Mi conclusión en esta actividad es que la seguridad de software y archivos son un parte esencial que debe traer consigo cualquier sistema operativo ya que este se encarga de proteger la información del usuario de malware y ataques cibernéticos, al igual también comprendí que esta seguridad debe estar en constante actualización agregando o mejorando parches contra las vulnerabilidades en nuestro sistema, ya que si no hay una actualización el malware o el ataque podría evolucionar y encontrar otra manera de obtener nuestra información , y si obtiene nuestra información seria algo muy negativo ya que esa información la pueden vender y usarla en nuestra contra.

2005930 - Eden Leonardo Candelas Andrade

En conclusión, después de realizar este análisis, considero que el tema de seguridades crucial ya que las amenazas a la información son cada vez más complejas y frecuentes. Hay muchas historias y ejemplos de los riesgos que nos pueden pasar si dejamos nuestra información desprotegida de los ataques. Por eso creo que es importante tener toda la protección necesario tanto de las empresas de las aplicaciones que usamos y de nosotros como usuarios. A medida que el panorama de ciberseguridad evoluciona, también es crucial promover una cultura de seguridad y concienciación entre los usuarios para reducir el impacto de ataques potenciales.

CONCLUSIONES INDIVIDUALES

2022830 - Daniel Alejandro Segura Vázquez

Gracias a la realización de esta actividad he podido aprender más acerca de la seguridad informática así como los diferentes peligros que existen con el simple hecho de estar navegando por el Internet. Además de ver las distintas estrategias que se pueden realizar para la prevención de estos ataques y los métodos para recuperarse de uno. Finalmente he podido conseguir una perspectiva más amplia acerca de la seguridad informática y he generar un poco de conciencia acerca de lo expuestos que estamos ante este tipo de amenazas y que siempre hay en cuenta el peligro a la hora de confiar ante archivos, correos o programas desconocidos.

2045231 - Denilson Gustavo Aguilar Puente

Para concluir este tema, después de hacer la investigación hay que aclarar que la seguridad en los sistemas operativos es un aspecto que debemos tomar con importancia a priori ya que no solo se pone en riesgo el dispositivo que se está utilizando, sino toda la información que tengamos almacenada ahí, provocando que nos roben información por un malware que obtuvimos en algún lado del internet. Estos virus provocan que nuestros datos sean utilizados por terceros para fines propios ya que sea comprar cosas en internet con nuestras y tarjetas bancarias o utilizar nuestras computadoras como tráfico de datos en el mercado negro. Gracias a esta investigación es que pude ser más consciente a este tipo de problemas haciendo que investigue de mejor manera sobre los posibles antivirus y protecciones para cuidar mi sistema operativo de terceros.

CONCLUSIONES INDIVIDUALES

2052523 - Jorge Paz Villareal

1958098 - Alan Jahir Rivas Urbina

Algo que me sorprendió fue darme cuenta de lo importante que es tener varios niveles de seguridad, no solo para mí como usuario individual, sino también pensando en redes y empresas. La autenticación, como las contraseñas y la autenticación de dos factores, es algo que damos por sentado, pero es esencial para evitar que alguien acceda a nuestros datos. También aprendí que la administración de riesgos no es solo para grandes compañías; todos podemos implementar medidas simples para estar preparados ante posibles problemas. En resumen, ahora sé que la seguridad es un proceso continuo y que depende de nosotros seguir las mejores prácticas."

CONCLUSIONES INDIVIDUALES

2052193 - Sofia Giovanna Espinoza Zapata

En esta actividad pude aprender que la seguridad informática requiere una protección integral que abarque tanto medidas digitales como físicas. Amenazas como ataques DDoS, suplantación de identidad y filtraciones de datos pueden tener consecuencias graves, mientras que la seguridad del hardware es esencial para evitar accesos no autorizados y proteger dispositivos críticos. Dicho todo lo anterior podemos observar y concluir que la implementar controles de acceso, monitoreo y redundancia, así como cumplir con normativas, es clave para garantizar la confidencialidad, integridad y disponibilidad de la información, asegurando la continuidad del negocio y la confianza de los clientes.



REFERENCIAS

- ¿Qué es una amenaza de ciberseguridad? | Glosario. (n.d.). HPE México. <https://www.hpe.com/mx/es/what-is/cybersecurity-threats.html>
- ¿Qué es el malware? Definición y tipos | Seguridad de Microsoft. (n.d.). <https://www.microsoft.com/es-mx/security/business/security-101/what-is-malware>
- Adobe. (2024, 9 abril). Autenticación basada en conocimientos. Recuperado 19 de octubre de 2024, de <https://helpx.adobe.com/mx/sign/config/send-settings/auth-methods/knowledge-based-auth.html>
- Bishop, M. (2003). Computer security: Art and science. Addison-Wesley.
- Gollmann, D. (2011). Computer security (3.a ed.). Wiley.
- Stallings, W. (2018). Sistemas operativos: Diseño e implementación (9.a ed.). Pearson Educación.
- Tanenbaum, A. S., & Bos, H. (2015). Modern operating systems (4.a ed.). Pearson.



REFERENCIAS

- Ibm. (2024, 16 julio). Sistema de prevención de intrusiones. IBM. <https://www.ibm.com/mx-es/topics/intrusion-prevention-system>
- Gbm. (2023, 15 junio). Malware: ¿Qué es y cómo protegerte? GBM Academy. <https://gbm.com/academy/malware-que-es-y-como-protegerte/>
- ¿Qué es DRP o plan de recuperación ante desastres? | Proofpoint ES. (2023, 23 diciembre). Proofpoint. <https://www.proofpoint.com/es/threat-reference/disaster-recovery>