**Colegio Nacional de Educación Profesional Técnica**

**Plantel Aguascalientes I Profr. J. Refugio Esparza Reyes**

**Profesional Técnico Bachiller en Informática**

**Turno Matutino**



**Modulo**

**Aplicación de la seguridad cibernetica**

***Actividad***

*Reporte 1.1*

**Docente**

*Lopez lopez jose guadalupe*

**Alumno**

*Jose David Tavarez Marquez*

**Grupo**

*608*

**Fecha de entrega**

# Introducción

La ciberseguridad no solo se enfoca en defender sistemas y redes de amenazas externas, sino también en educar a los usuarios sobre prácticas seguras y la importancia de mantener actualizados sus dispositivos y software. La rápida evolución tecnológica ha dado lugar a nuevas formas de ataque, lo que hace imprescindible un enfoque proactivo y adaptable para prevenir y responder a incidentes de seguridad.

En este contexto, es crucial entender los diferentes tipos de amenazas y las estrategias más efectivas para mitigarlas. Abordaremos cómo se diseñan las infraestructuras de red seguras, la importancia de los firewalls y los sistemas de detección de intrusos (IDS), así como las mejores prácticas para la gestión de contraseñas y la autenticación multifactor (MFA).

Además, exploraremos los fundamentos de la seguridad en la comunicación inalámbrica, un área de creciente relevancia debido al auge del Internet de las cosas (IoT) y la conectividad ubicua. Analizaremos las vulnerabilidades específicas de las redes Wi-Fi y las medidas para asegurar las conexiones, como el cifrado WPA3 y las redes privadas virtuales (VPNs).

Finalmente, el reporte incluirá casos de estudio y ejemplos reales de ataques cibernéticos y sus consecuencias, ofreciendo una visión integral de la ciberseguridad en el mundo contemporáneo y destacando la importancia de una cultura de seguridad robusta tanto a nivel individual como organizacional.

# Ataques a la ciberseguridad



## Amenazas comunes

Las amenazas comunes a la ciberseguridad incluyen malware, phishing, ransomware y ataques de denegación de servicio (DDoS).

* Malware: Software malicioso diseñado para dañar, interrumpir o robar información. Ejemplo: virus, troyanos y spyware.
* Phishing: Técnica de ingeniería social utilizada para engañar a los usuarios y obtener información confidencial, como contraseñas. Ejemplo: correos electrónicos falsos que parecen ser de instituciones legítimas.
* Ransomware: Tipo de malware que cifra los archivos del usuario y exige un rescate para liberarlos. Ejemplo: el ataque de WannaCry en 2017.
* DDoS: Ataques que sobrecargan un servidor con tráfico excesivo, causando la interrupción del servicio. Ejemplo: ataques a grandes empresas como GitHub.

## Ataques cibernéticos

Los ataques cibernéticos varían en complejidad y objetivos, desde la interrupción de servicios hasta el robo de información confidencial.

* Ataques de fuerza bruta: Intentos repetidos de adivinar contraseñas para acceder a cuentas. Ejemplo: ataques a cuentas de redes sociales.
* Ataques de inyección SQL: Inserción de código malicioso en sistemas de bases de datos para acceder a información no autorizada. Ejemplo: ataques a sitios web que no validan adecuadamente las entradas de usuario.

## Ataques a dispositivos

Los dispositivos conectados a internet, como computadoras, smartphones y dispositivos IoT, son vulnerables a varios tipos de ataques.

* Rootkits: Software que permite a los atacantes obtener acceso privilegiado a un dispositivo. Ejemplo: rootkits en sistemas operativos de ordenadores.
* Exploit kits: Herramientas que buscan vulnerabilidades en dispositivos para explotarlas. Ejemplo: exploit kits en navegadores web.

## Ataques a las aplicaciones

Las aplicaciones también pueden ser objetivos de ataques, comprometiendo la seguridad de los datos que manejan.

* XSS (Cross-Site Scripting): Inyección de scripts maliciosos en páginas web vistas por otros usuarios. Ejemplo: ataques XSS en foros de discusión.
* Man-in-the-middle: Interceptación y alteración de la comunicación entre dos partes. Ejemplo: ataques a través de redes Wi-Fi no seguras.

# Protección de redes



## Estado actual

La protección de redes es crucial para prevenir y mitigar ataques cibernéticos. Las redes deben estar equipadas con medidas de seguridad actualizadas para enfrentar las amenazas modernas.

## Ataque de red

Los ataques de red pueden tener graves consecuencias, como el acceso no autorizado a datos sensibles y la interrupción del servicio.

* Sniffing: Monitorización y captura de tráfico de red. Ejemplo: uso de herramientas como Wireshark.
* Spoofing: Suplantación de identidad en comunicaciones de red. Ejemplo: ataques de ARP spoofing.

## Seguridad en red

Las estrategias de seguridad en red incluyen el uso de firewalls, sistemas de detección de intrusos (IDS) y la implementación de protocolos seguros.

* Firewalls: Filtran el tráfico entrante y saliente según reglas predefinidas. Ejemplo: firewalls enrutadores domésticos.
* IDS: Sistemas que monitorean el tráfico de red en busca de actividades sospechosas. Ejemplo: sistemas IDS como Snort.

# Ataque a los fundamentos



## Detalles de la PDU de IP

La Unidad de Datos del Protocolo (PDU) de IP incluye información crucial para la entrega de paquetes en una red. Los ataques a la PDU pueden comprometer la comunicación de red.

## Vulnerabilidades IP, TCP y UDP

Los protocolos de internet, TCP y UDP tienen vulnerabilidades que los atacantes pueden explotar.

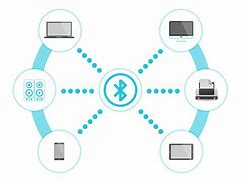
* IP spoofing: Suplantación de direcciones IP para hacerse pasar por una fuente confiable.
* TCP SYN flood: Ataque de denegación de servicio que consume recursos del servidor mediante solicitudes TCP incompletas.
* UDP flood: Envío masivo de paquetes UDP a un servidor, saturando su capacidad de respuesta.

## Mitigación de ataques

La mitigación de ataques incluye estrategias y medidas para reducir el impacto de los ataques cibernéticos.

* Filtrado de paquetes: Revisa y filtra el tráfico entrante y saliente en busca de actividades sospechosas.
* Seguridad perimetral: Implementación de medidas de seguridad en el perímetro de la red.

# Comunicación de red inalámbrica



## Amenazas

Las redes inalámbricas son vulnerables a diversas amenazas debido a su naturaleza abierta.

* Wardriving: Recorrido en busca de redes Wi-Fi desprotegidas para utilizarlas sin autorización.
* Cracking de Wi-Fi: Explotación de vulnerabilidades en protocolos de seguridad inalámbrica para acceder a redes sin permiso.

## WLAN seguras

La implementación de redes inalámbricas seguras es esencial para proteger la información y la comunicación.

* WPA3: Protocolo de seguridad actualizado que ofrece mayor protección contra ataques de fuerza bruta.
* Redes ocultas: Ocultar el SSID de la red para dificultar su detección por parte de atacantes.

## Dispositivos de comunicación

Los dispositivos de comunicación como routers y puntos de acceso deben estar configurados adecuadamente para garantizar la seguridad de la red.

* Actualizaciones de firmware: Mantener el firmware de los dispositivos actualizado para protegerse contra vulnerabilidades conocidas.
* Contraseñas seguras: Utilizar contraseñas robustas y cambiarlas periódicamente para evitar accesos no autorizados.

# Infraestructura de seguridad de redes



Para proteger una red de posibles amenazas y vulnerabilidades, es crucial implementar una infraestructura de seguridad robusta. Esto incluye una combinación de dispositivos y servicios diseñados para salvaguardar la integridad, confidencialidad y disponibilidad de la información.

Dispositivos de seguridad

Los dispositivos de seguridad son esenciales para establecer barreras y controles que impidan el acceso no autorizado y detecten actividades maliciosas. Algunos ejemplos y características incluyen:

* Firewalls: Actúan como una barrera entre una red interna segura y redes externas no confiables, filtrando el tráfico basado en reglas de seguridad predefinidas. Pueden ser hardware, software o combinaciones de ambos.
* Sistemas de Prevención de Intrusiones (IPS): Monitorean el tráfico de red en busca de actividades sospechosas y pueden tomar medidas automáticas para bloquear amenazas.
* Routers seguros: Además de dirigir el tráfico de red, los routers avanzados ofrecen funcionalidades de seguridad como VPN, filtrado de contenido y protección contra malware.
* Accesos a puntos de acceso seguros: Estos dispositivos permiten la conexión inalámbrica a la red, garantizando que solo los usuarios autorizados puedan acceder mediante autenticación robusta.

Servicios de seguridad

Además de los dispositivos físicos, una infraestructura de seguridad de red debe incluir servicios que garanticen la vigilancia continua y la respuesta a incidentes. Algunos ejemplos y características incluyen:

* Servicios de monitoreo de red: Proveedores de servicios gestionados (MSP) que monitorizan la red en tiempo real, identificando y respondiendo a posibles amenazas.
* Evaluaciones de vulnerabilidad: Servicios que analizan la red en busca de debilidades y proporcionan recomendaciones para mitigarlas.
* Servicios de respuesta a incidentes: Equipos especializados que se activan en caso de una brecha de seguridad, trabajando para contenerla y minimizar el impacto.
* Servicios de actualización y parcheo: Mantener el software y el firmware al día es fundamental para protegerse contra nuevas amenazas.

# Conclusión

La ciberseguridad es un campo dinámico y en constante evolución, que requiere una vigilancia continua y la implementación de medidas de protección robustas. Con el aumento exponencial de dispositivos conectados y la sofisticación de los métodos de ataque, es crucial que tanto individuos como organizaciones adopten una postura proactiva en la gestión de la seguridad de la información. Este enfoque debe incluir desde la concientización sobre los ataques más comunes, como el wardriving y el cracking de Wi-Fi, hasta la implementación de protocolos avanzados como WPA3 para la protección de redes.

Además, la configuración adecuada de dispositivos de comunicación, como routers y puntos de acceso, desempeña un papel fundamental. Mantener el firmware actualizado y utilizar contraseñas robustas son prácticas esenciales para prevenir accesos no autorizados. Asimismo, ocultar el SSID de la red y monitorear continuamente las actividades sospechosas puede reducir significativamente el riesgo de intrusiones.

La protección de redes inalámbricas no solo es una responsabilidad técnica, sino también una cuestión de concientización y educación. Las personas deben conocer las posibles amenazas y las mejores prácticas para proteger sus datos y comunicación. La colaboración entre usuarios, profesionales de TI y fabricantes es vital para desarrollar soluciones efectivas y resilientes ante las amenazas emergentes.

Solo a través de un enfoque integral y colaborativo se podrá garantizar la seguridad en el entorno digital y proteger la integridad de la información en la era moderna. La ciberseguridad no es una meta estática, sino un proceso continuo de adaptación y mejora, esencial para salvaguardar nuestra creciente dependencia de la tecnología.