SEGURIDAD EN INTERNET

Ingeniería Aplicada
Conectando el futuro

Justificación

El propósito es profundizar sobre la seguridad informática, adquiriendo conceptos que se realizan en el ámbito laboral y tener conceptos técnicos el cual podamos aplicar en el futuro o presente. Se dará una explicación de los tipos de riesgos y amenazas que se presenta.

Daremos a conocer mecanismos de seguridad y su función. Beneficia el entorno laboral tener esta información al día, lo que permite dar soluciones a los problemas que se presenta en el entorno laboral y personal. Se brinda una mayor seguridad en la protección de los datos, asegurando confidencialidad, integridad y seguridad.

Debido a la protección de datos de nuestra empresa, se creó un VPN para tener acceso remoto a los equipos para tener un soporte a cualquier eventualidad que se presente, por parte del personal encargado desde cualquier parte del mundo.

Para que nuestros usuarios tengan un buen desempeño en su ambiente laboral es indispensable el buen uso de las herramientas que facilita la empresa, también es necesario gestionar la red y así comprobar y cerciorar el rendimiento de los recursos de información. Estas herramientas han permitido que se ajusten toda gestión de red, también han permitido garantizar la disponibilidad y ha rendido tanto en la información como la tecnología.

Objetivos

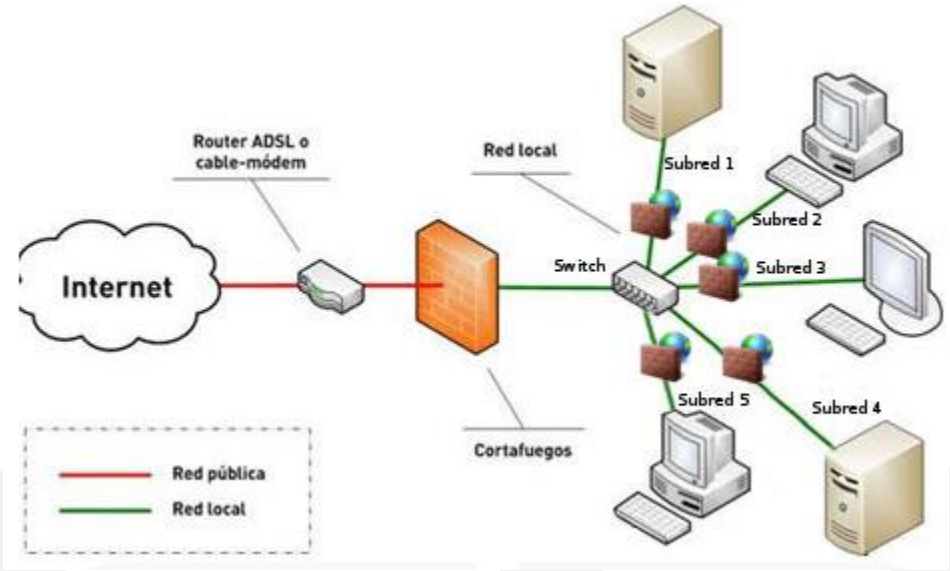
- Explicar conceptos básicos sobre los modelos de seguridad.
- Que es el firewall.
- Conocer los riesgos y ataques que se presentan a un usuario en la red.
- Implementar diferentes estrategias de seguridad para evitar ataques cibernéticos a los usuarios y la información de la red.
- El objetivo principal es mantener una buena imagen contando con integridad, privacidad, disponibilidad y un buen manejo en el control y autenticidad de nuestra información almacenada en nuestro dispositivo.

Conceptos

- **Antivirus:** Software creado específicamente para ayudar a detectar, evitar y eliminar malware (software malicioso).
- **Ataque de fuerza bruta:** Tipo de ataque en el que un actor malicioso utiliza diferentes tipos de métodos para descubrir o descifrar contraseñas de un tercero.
- **Firewall:** Sistema cuya función es prevenir y proteger nuestra información en nuestra red privada y bloqueando el acceso a terceros.
- **Malware:** Software que daña dispositivos, roba información y siembra caos en el sistema.
- **Phishing:** Método más utilizado por los ciberdelincuentes para estafar y obtener información confidencial de forma fraudulenta como las contraseñas e información sobre tarjetas de crédito e información bancaria de los usuarios.
- **Spam:** Correo basura, mensajes masivos no solicitados, también llamado spamming (espamear) persona que participa en esta práctica se le conoce como spammer.

SEGURIDAD INFORMATICA

1. Firewall o Cortafuegos



1. **Tomado de:** https://geekland.eu/

Un **firewall** o **cortafuegos** es un sistema diseñado para para prohibir o permitir el acceso desde o hacia una red. Un **firewall** puede ser físico o digital (virtual), es decir, puede estar en un dispositivo dedicado o trabajar cómo **cortafuegos** como un programa software, indispensable para mantener la seguridad de su red, especialmente a la hora de conectar a internet.

Los **firewalls**, durante más de 25 años, han sido la primera línea de defensa en seguridad informática, pero eso no quiere decir que estén obsoletos, siguen siendo **uno de los componentes más importantes en seguridad**. Un **firewall** le protegerá de las intrusiones, robo de identidad, malware o fraude.

Aplicación de Firewall en la red de Convergencia Digital.

- Reglas del uso en las Mikrotik:

IP-Firewall del Mikrotik se utiliza para abrir y bloquear puertos desde fuera de la red y dentro de nuestra red.

En el caso de Convergencia Digital, como primera medida de protección contamos con la modificación de puertos específicos en nuestros dispositivos como:

- 8023 http
- 9010 Acceso remoto por software propietario (winbox)

Un segundo paso es la rotación mensual de la contraseña de acceso al Router de Frontera, posteriormente iniciamos la configuración del Router de frontera con reglas generales básicas de acceso y funcionamiento de nuestra red interna, a continuación se muestra el script de configuración del Firewall:

```
/ip firewall filter

add action=accept chain=input comment="Permitir entrada del Protocolo TCP" \
in-interface=Ether01-WAN protocol=tcp

add action=accept chain=input comment="Permitir entrada del Protocolo UDP" \
in-interface=Ether01-WAN protocol=udp

add action=accept chain=input comment="Permitir Entradas Establecidas" \
connection-state=established in-interface=Ether01-WAN

add action=accept chain=input comment="Permitir Entradas Related" \
connection-state=related in-interface=Ether01-WAN

add action=accept chain=forward comment="Permitir TCP dentro de la RED" \
protocol=tcp

add action=accept chain=forward comment="Permitir UDP dentro de la RED" \
protocol=udp

add action=accept chain=input comment="Permitir el Protocolo PING Limitado" \
in-interface=Ether01-WAN limit=50,5:packet protocol=icmp

add action=drop chain=input comment="Denegar Conexiones Invalidas" \
connection-state=invalid in-interface=Ether01-WAN
```

Tipos de reglas que se pueden implementar en un Firewall

1. **Administrar los accesos de los usuarios a los servicios** privados **de la red** como por ejemplo aplicaciones de un servidor.
2. **Registrar todos los intentos de entrada y salida** de una red. Los intentos de entrada y salida se almacenan en logs.
3. Filtrar paquetes en función de su origen, destino, y número de puerto. Esto se conoce como **filtro de direcciones**.

4. Filtrar determinados tipos de tráfico en nuestra red u ordenador personal. Esto también se conoce como **filtrado de protocolo**. El filtro de protocolo permite aceptar o rechazar el tráfico en función del protocolo utilizado. Distintos tipos de protocolos que se pueden utilizar son **http, https, Telnet, TCP, UDP, SSH, FTP**, etc.
5. **Controlar el número de conexiones que se están produciendo desde un mismo punto** y bloquearlas en el caso que superen un determinado límite. De este modo es posible evitar algunos ataques de denegación de servicio.
6. **Controlar las aplicaciones que pueden acceder a Internet**. Así por lo tanto podemos restringir el acceso a ciertas aplicaciones, como por ejemplo Dropbox, a un determinado grupo de usuarios.
7. **Detección de puertos que están en escucha y en principio no deberían estarlo**. Así por lo tanto el firewall nos puede advertir que una aplicación quiere utilizar un puerto para esperar conexiones entrantes.

Sistema de Firewall que se está implementando en la red de Convergencia Digital.

La red de convergencia es alimentada por un servicio de internet a través de fibra Óptica, el cual es entregada con una OLT, la empresa conecta la OLT a una router Board para la administración de la red existente.

Esta red está diseñada para ser administrable, ya que, los equipos deben ser accesibles a la administración y monitoreo: router y switches. También manejamos soporte de monitoreo SNMP, ICMP, DNS y TCP, monitoreo estadístico y grafico de los enlaces, acceso remoto a las herramientas de control. Manejamos niveles de control y acceso como son firewall, NAT, segmentación por Vlans, Vpns.

RIESGOS DE SEGURDAD EN INTERNET

2. Antivirus

La protección de una buena aplicación o antivirus es importante para proteger la seguridad de cualquier sistema de información. También conocer su función y las limitaciones que este conlleven.

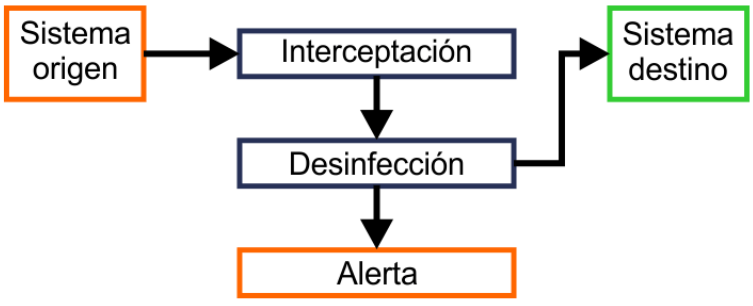
El antivirus intenta cubrir los principales ataques que hay en un dispositivo, sea pc o Dispositivo móvil, que no tenga ningún tipo de protección, sabiendo la funcionalidad del antivirus, son muchas las amenazas que se presentan cuando te encuentras navegando por internet o copiando información al dispositivo pc o móvil.

Cómo funciona el antivirus

Los antivirus actúan en un segundo plano, analizan cada archivo o página que este abierto en el dispositivo que se está utilizando.

Hay tres métodos que se utiliza para proteger nuestro sistema:

a) **Analizar** archivos que se encuentran en una base de datos de software o programas malignos.
b) **Monitorizar** archivos del ordenador a medida que van siendo abiertos o creados para certificar que no estén infectados. Es una protección en tiempo real contra cualquier amenaza, que pueda afectar el funcionamiento del dispositivo que estamos utilizando.
c) **Inspeccionar** el sistema para la verificación de archivos malintencionados y eliminar virus existentes, ya que se pudo infiltrar en nuestro dispositivo.



Funciones de un antivirus

- Reparar el archivo
- Ponerlo en cuarentena
- Eliminar el archivo
- Analizar la conducta de los archivos del sistema

Características

- Cortafuegos
- Analizar direcciones web url's
- Protección del correo electrónico
- Antispyware
- Anti pop-ups
- Copias de seguridad

3. Como evitar los riesgos del phishing

- Identificar claramente los correos electrónicos que sean sospechosos de ser un phishing.
- Verificar el origen de la información de tus corres entrantes.
- Ingresar a la web de un Banco pulsando un link inadecuado que se encuentre incluido en el correo electrónico.
- Reforzar la seguridad de tu dispositivo.
- Introducir tu información confidencial en sitios seguros y que no afecten tu integridad.
- Revisar constantemente tus cuentas.
- No solo de entidades online vive el phishing
- El phishing sabe idiomas
- Si tienes alguna inquietud ser lo mayormente prudente para no arriesgar tu información.
- Estar actualizado sobre todos los cambios o evolución que tengan las diferentes amenazas en la actualidad.

4. Como proteger mi información del malware

- ✓ Usar software de antivirus.
- ✓ Desconfiar de los archivos adjuntos y sospechosos.
- ✓ Ejecutar las actualizaciones del software.
- ✓ Tomar nota de los indicadores de vulnerabilidad.

Que hacer en caso que un malware se encuentre en mi ordenador

Desconectar inmediatamente del internet y dejar de usarlo ya que cada tecla que pulses será enviada al atacante. En estos casos es preferible llevar tu equipo a una persona experta en seguridad, el cual puede encontrar más detalles de la amenaza o malware. Eso quiere decir que si se elimina el archivo malicioso no se puede cerciorar la seguridad del equipo. El atacante tiene la capacidad de generar códigos en el equipo siempre y cuando el programa malicioso se lo permita.

Iniciar sesión en un equipo que usted crea que sea seguro y cambie las contraseñas; tener en cuenta todas las contraseñas que se encuentran en el equipo mientras se encontraba infectado.

Bibliografía

1. **Justificación tomada de:**
   https://securitycharmander.weebly.com/justificacioacuten-y-objetivos.html

2. **Terminología tomada de:**
   https://www.onasystems.net/glosario-terminos-seguridad/

3. **Firewall tomado de:**
   https://geekland.eu/que-es-y-para-que-sirve-un-firewall/#:~:text=El%20tipo%20de%20reglas%20y,ejemplo%20aplicaciones%20de%20un%20servidor.&text=Filtrar%20determinados%20tipos%20de%20tr%C3%A1fico%20en%20nuestra%20red%20u%20ordenador%20personal.

4. **Antivirus tomado de:**
   https://ceminfor.es/como-funciona-antivirus/

5. **Phishing tomado de**
   https://www.pandasecurity.com/es/mediacenter/consejos/10-consejos-para-evitar-ataques-de-phishing/

6. **Malware tomado de:**
   https://ssd.eff.org/es/module/%C2%BFc%C3%B3mo-protegerme-contra-el-malware