**INVESTIGACIÓN ACTIVIDAD III**

de la cruz Calel Katheryne Drushenka

5to Bachiller Industrial y Perito en Computación con Orientación en Desarrollo de

Aplicaciones Web y Móvil

**CURSO:** Análisis de Sistemas y Programación

**Laura Sofía Reiche Gonzales**

**Gerbin Adolfo Chun Icuté**

Cobán, Alta Verapaz, julio de 2023

**INDICE**

[INTRODUCCIÓN iii](#_Toc140045667)

[OBJETIVOS iv](#_Toc140045668)

[FIREWALL O CORTAFUEGOS 5](#_Toc140045669)

[SOFTWARE ANTIVIRUS 5](#_Toc140045670)

[INFRAESTRUCTURA DE CLAVE PÚBLICA O PKI 6](#_Toc140045671)

[SERVICIOS MDF 7](#_Toc140045672)

[PENTESTING 8](#_Toc140045673)

[STEGO Y TECNICAS DE CIFRADO ACTUALES 9](#_Toc140045674)

# INTRODUCCIÓN

Las herramientas que se encuentran actualmente en internet nos han brindado un gran apoyo para mejorar la elaboración de diversas tareas tanto colaborativas y personales. Además, podemos usar esta tecnología para aumentar la seguridad de nuestros datos personales, ya que en este ámbito no todo es positivo, así como puede sernos de una gran utilidad también tenemos el riesgo de exponer toda nuestra información por este medio. Esta investigación da a conocer herramientas que ofrecen diferentes funciones, tanto para asegurar nuestra información como mantener en un buen estado a nuestro equipo.

# OBJETIVOS

Objetivo General:

Ampliar nuestro conocimiento a cerca de aplicaciones que pueden beneficiar la seguridad de nuestra información por medio de la investigación y uso de estas apps para poder solucionar problemas de seguridad o evitar algún virus no deseado.

Objetivos específicos:

Buscar las aplicaciones que cumplan con dicha función y probar su funcionamiento.

Comenzar con pruebas para observar si realmente son eficaces y tengan la capacidad de mantener nuestro equipo y nuestros datos de forma segura.

# FIREWALL O CORTAFUEGOS

Esta basado en un software y hardware que es un sistema de seguridad que sirve como filtración entre las redes consideradas seguras con las que son dañinas para el equipo. Existente una diversidad de firewalls y cada uno usa un determinado tipo de filtración. Los primeros cortafuegos usaban una comparación de información básica como, el origen y el destino originales del paquete y el puerto que se utiliza. Los últimos firewalls pertenecen a la tercera generación, llamándose (NGFW). Realizan una inspección más profunda comparando la información con una base de datos de detección.

Sin embargo, los cortafuegos no podrán proteger los datos que se envíen por correo de protocolo simple de transferencia de correo (SMTP), FTP y Telnet.

# SOFTWARE ANTIVIRUS

Programas que fueron creados para detectar y eliminar virus informáticos. Con la evolución de los sistemas operativos, también los antivirus se han ido actualizando, permitiendo ampliar sus funciones y ya no solo detectan virus, si no también, los bloquean, desinfectan archivos y previenen infecciones.

Estos programas reconocen diferentes virus como:

* Malware: Programa diseñado para dañar, infectar o comprometer un sistema informático sin el consentimiento del usuario. Estos pueden dañar archivos y robar información.
* Spyware: Tipo de malware que se instala en un dispositivo sin el consentimiento del usuario con el propósito de supervisar las actividades del usuario para obtener contraseñas, recopilar información personal y espiar la actividad en línea.
* Gusanos: Se propaga de forma automática a través de redes sin la intervención del usuario. Los gusanos se replican a si mismos por vulnerabilidades en el software y lo hacen a través de redes sociales y correos electrónicos
* Troyanos: Programas que se disfrazan de software legítimo, pero en realidad tienen intenciones maliciosas, engañando a los usuarios haciéndoles creer que están instalando una aplicación útil; una vez estén en el sistema pueden abrir una puerta trasera robando información confidencial y permitiendo el ingreso de otros tipos de malware.
* Rootkits: Son extremadamente difíciles de detectar ya que son herramientas diseñados para ocultar la presencia de malware u otras actividades maliciosas en un sistema. Se instalan con privilegios de administrador (root) y modifican el sistema operativo.

# INFRAESTRUCTURA DE CLAVE PÚBLICA O PKI

Infraestructura de red formada por servidores y servicios, además es un protocolo para el intercambio seguro de la información. Puede considerarse como un equivalente electrónico de una firma en papel; así mismo posee políticas de seguridad.

* Establecer y definir la dirección de una organización sobre seguridad de información.
* Procesos y principios para el uso de la criptografía.
* Declaraciones sobre como gestionara la empresa las claves y la información.
* Establecerá el nivel de control requerido para afrontar los niveles de riesgo.

Propiedades de PKI

* Confidencialidad: Protege la información en su totalidad y sus piezas individuales.
* Integridad: Protege respaldos, documentación, registros de contabilidad del sistema y tránsito en una red.
* Autenticidad: Posee mecanismos para verificar quien está enviando la información, así como el origen de la información sea correctamente identificada.

# SERVICIOS MDF

Generalmente se denomina Main Distribution Frame, que es adecuado para usar con equipos de conmutación telefónica de gran capacidad para conectar líneas internas y externas. Además, cumple con una función muy importante que es la de proteger contra fuerzas ajenas al sistema que provenga desde la planta externa hacia los equipos de comunicación, a través de dispositivos de operación rápida; tiene la función de cablear, probar y proteger los equipos y seguridad personal en el buró, todas las líneas externas están conectadas al Main Distribution Frame, y luego el Main Distribution Frame está conectado al equipo relacionado.

Las funciones básicas son las siguientes:

1. Con la función de cableado cualquier cable interno se puede conectar a cualquier cable externo a través de un puente.
2. Tiene un dispositivo de protección y junto con las instalaciones de protección en la línea exterior y el interruptor, forma un sistema de protección que evita la sobretensión y la sobre corriente que ingresan desde la línea exterior y así causen daños y lesiones a los equipos.
3. Posee un lugar para probar cables internos y externos.
4. Tiene una función de alarma, que puede enviar señales audibles y visibles.

# PENTESTING

También conocido como prueba de penetración, es un tipo de prueba que utilizan las empresas para realizar un análisis en sus vulnerabilidades y debilidades en su seguridad informática; ataca diferentes sistemas para evitar posibles fallos, se deben de realizar al menos 2 pruebas de penetración al año, existen diferentes tipos de pentesting:

Black box: En este tipo de prueba, el equipo de ejecución no dispone de conocimiento previo acerca de la infraestructura que va hacer probada, este tipo de prueba es parecido a un ataque real.

Gray box: Es la combinación de black box y White box, en este caso se contará con algo de información a la hora de realizar el test, aunque sigue siendo un buen simulacro de ataque ajeno al sistema

White box: Es la prueba más completa ya que se parte de un conocimiento completo de la infraestructura a ser probada, es realizado normalmente con apoyo de personal interno de los clientes. El pentesting cuenta con 5 fases:

* Recopilación y planificación.
* Análisis de vulnerabilidades.
* Modelado de amenazas.
* Explotación del sistema.
* Elaboración de los informes.

# STEGO Y TECNICAS DE CIFRADO ACTUALES

La esteganografía es la práctica de ocultar información dentro de otro mensaje u objeto físico para evitar su detección. Se puede usar para ocultar casi cualquier tipo de contenido digital, ya sea texto, imágenes, videos o audios. Luego, dichos datos ocultos se extraen; compone mensajes ocultos para que solo el remitente y el receptor sepan que el mensaje existe. No hay que confundirla con la criptografía, ya que no implica realmente ocultar datos “encriptados” ni usando una clave para protegerlos.

El cifrado web es la conversión de datos de un formato legible a un formato codificado. Los datos cifrados solo se pueden leer o procesar luego de descifrarlos. El cifrado implica convertir texto sin formato legible por humanos en un texto incomprensible, conocido como texto cifrado.

Existen 2 técnicas de cifrado comunes las cuales son:

Claves de cifrado simétrico: También se conoce como cifrado de clave privada. La clave que se usa en la codificación es la misma que se utiliza en la descodificación, lo que resulta más conveniente para usuarios individuales y sistemas cerrados.

Claves de cifrado asimétrico: en este tipo de cifrado, se utilizan dos claves diferentes (pública y privada) que están vinculadas entre sí matemáticamente. Las claves son básicamente números extensos vinculados entre sí, pero no son idénticos.

Ejemplos de algoritmo de cifrado:

Cifrado DES: Este es un algoritmo de cifrado simétrico y obsoleto que no se considera apto para los usos de hoy.

Cifrado 3DES: Es la sigla de "estandar de cifrado triple de datos". Este es un algoritmo de cifrado simétrico que usa la palabra "triple" debido a que los datos pasan por el algoritmo DES original tres veces durante el proceso de cifrado.

Cifrado AES: ES la sigla de "estándar de cifrado avanzado" y se desarrolló para actualizar el algoritmo DES original. Entre algunas de las aplicaciones más comunes, se incluyen las aplicaciones de mensajería.

Cifrado Twofish: Se usa para hardware y software, y se considera uno de los cifrados más rápidos de su tipo. Este tipo de cifrado no está patentado, por lo cual está disponible de forma gratuita.