Comprensión de la Necesidad de las Redes de Computadoras y Seguridad en los Tiempos de Conectividad Absoluta

Jonathan R. Sosa Lugo
Ciencias de Computadoras
Mentor: Alfredo Cruz, Ph.D.
Universidad Politécnica de Puerto Rico
EXPO de Proyectos Graduados, Mayo 2025

Abstracto *—Comprender redes, seguridad informática y cifrados es esencial en ciberseguridad. Brindar a los estudiantes de nivel superior herramientas y fundamentos clave les permite reconocer componentes básicos del tema y tomar conciencia sobre la importancia de proteger las redes. A través de métodos de seguridad técnicos, lógicos y cifrados, se fortalecen sus conocimientos. Además, este aprendizaje beneficia a los maestros, permitiéndoles enseñar redes y seguridad de manera efectiva. También podrán usar programas para simular redes e implementar medidas de seguridad. Adquirir estos conocimientos ayuda a los estudiantes a explorar diversas áreas de desarrollo profesional en ciberseguridad.*

Términos *— Ciberseguridad, Cifrados, Redes, Seguridad Informática*

INTRODUCCIÓN

Crear módulos para maestros de secundaria para ampliar su perspectiva sobre tecnología es una necesidad en nuestra comunidad. Muchos estudiantes de nivel superior consideran carreras tradicionales y tienen ideas erróneas sobre ciberseguridad, asociándola con actividades ilícitas como el “hackeo”. Sin embargo, la seguridad tecnológica implica proteger organizaciones y empresas contra ataques.

En la actualidad, estar conectados a una red es esencial, ya sea inalámbrica, por cable o mediante puntos de acceso. Es importante comprender su configuración y seguridad, tanto técnica como física, para dificultar la extracción de datos. Mecanismos como el cifrado convierten la información en un formato ilegible para protegerla.

Este documento aborda temas clave como redes, cortafuegos, seguridad física y técnica, contraseñas y cifrados. Los cortafuegos son esenciales para la seguridad de una red, complementando medidas tradicionales como control de acceso, cámaras, vigilancia y sistemas de alarma.

El cortafuego lo podemos describir como un sistema de seguridad en la red de las computadoras que restringe el tráfico de internet entrante, saliente o dentro de una red privada [1]. Si colocamos esa descripción en un generados de imágenes de inteligencia artificial [2] podemos observar lo que apareció en la Figura 1. Donde hay una barrera de protección sobre una red privada y otras redes públicas intentando de entrar a esa red privada. Con esa demostración gráfica hace que podamos ver el trabajo efectivo que puede hacer un cortafuego a la hora de dividir redes públicas y privadas.



Figura 1
Imagen Construida con Inteligencia Artificial del Cortafuego

Por otra parte, si hablamos del término seguridad en términos generales podemos decir que es una forma de gobernar con el objetivo de garantizar que las personas individuales o colectivas estén en lo menos posible a ciertos peligros. Al pasar del tiempo, comenzó a utilizarse el termino de seguridad informática donde su enfoque principal es la protección de los datos y de la infraestructura computacional de un sistema informático determinado. Donde ya el enfoque principal era promover el uso del internet seguro, evitando los programas maliciosos, virus, gusanos, y troyanos informáticos.

El objetivo de este papel es poder presentar información relevante sobre las redes, seguridad, cifrados, implementación de contraseñas robustas, evitar sobornos, mencionar las categorías de amenazas, criptografía, y ataques a las contraseñas. Donde podemos incluir historia, topologías básicas, programas de simulación de redes, configuraciones básicas, métodos básicos criptográficos, ejemplos de cifrados, implementación de contraseñas, entre otras. También, en poderle brindarle a los maestros de escuela superior herramientas donde pueda impartir el conocimiento en la sala de clase.

PLANTEAMIENTO DEL TEMA

Al introducir el tema de las redes y el cortafuego hubo un interés en saber en cómo funciona las redes en nuestra sociedad. Como es de conocimiento, las redes es la pieza clave de comunicación en el ambiente en el que vivimos. También, se puede decir que es la primera fila de ataques cibernéticos en estos tiempos. Ya que, al estar conectados en la red, los atacantes cibernéticos pueden tomar ventaja para hacer sus crímenes. Los registros confirman que, en el primer trimestre del año 2024, por semana han alcanzado 1,308 de ataques. Aproximadamente es un aumento de 28% del año 2023 [3]. Es por esa razón que debemos de instruir, informar y enseñar a nuevas personas que puedan contribuir a la seguridad de las redes en estos tiempos.

Las redes informáticas surgieron con ARPANET a finales de los años 60. Esta red, creada en 1968, tenía como objetivo enviar datos militares de forma segura y conectar grupos de investigación en EE. UU. Con el tiempo, las redes se expandieron al ámbito comercial, permitiendo la transferencia de datos y la conexión de estaciones remotas a un ordenador central. Además, ARPANET fue una de las primeras redes en implementar la conmutación de paquetes, un principio clave del internet.

En 1984, Cisco fue pionera en redes de Área Local (LAN), desarrollando enrutadores multiprotocolo para conectar computadoras en distintos lugares. Más adelante, con la llegada del protocolo IPv4, la empresa amplió su oferta con módems y enrutadores centrales, facilitando el crecimiento de los proveedores de servicios de internet. Es por esa razón que Cisco se ha convertido en un proveedor esencial en compañías de comunicaciones [4].

Al hablar de los componentes básicos de una red, pensamos en dispositivos como computadoras, teléfonos, enrutadores y conmutadores, esenciales para su configuración e implementación. Los nodos son los dispositivos conectados a la red, y algunos actúan como servidores o gestores de datos. El medio de transmisión puede ser cableado o inalámbrico, y es clave conocer los protocolos de comunicación. Además, los cortafuegos protegen la red de amenazas externas y regulan el tráfico de datos.

Comprender tanto los componentes físicos como lógicos de una red permite conocer las distintas topologías que pueden implementarse. La primera topología se le conoce como topología estrella. En la Figura 2 muestra lo que es una topología estrella donde se caracteriza por la disposición de los dispositivos conectados a un único punto central (nodo central). Se pueden conectar mediante cables o enlaces inalámbricos.



Figura 2
Ejemplo de Topología Estrella

La próxima topología se llama topología de bus, donde la particularidad de dicha topología los dispositivos están enlazados a un canal o nodo principal. Eso lo podemos observar en la Figura 3.

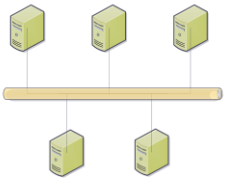


Figura 3
Ejemplo de Topología Bus

Como última topología encontramos la topología de anillo donde cada dispositivo conectado forma

parte dentro de la misma red. La información empieza a transmitirse desde el primer dispositivo conectado a la red hasta el último nodo. Lo podemos observar en la Figura 4.

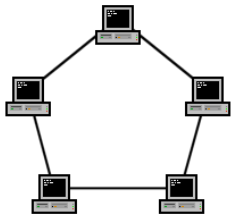


Figura 4
Ejemplo de Topología de Anillo

Existen unos componentes claves a la hora de configurar una red, esos componentes son direcciones IPv4, máscara de subred, puerta de enlace predeterminada (traducido del inglés "Default Gateway"), y el sistema de nombres de dominio (traducido del inglés "Domain Name System").

Las direcciones IPv4 identifican de forma única un dispositivo en una red mediante una representación numérica de 32 bits, divididos en cuatro octetos separados por puntos, como 192.168.1.1. Cada octeto varía entre 0 y 255 [5], y las direcciones se clasifican en rangos públicos y privados.

La máscara de subred permite dividir una red grande en subredes más pequeñas, diferenciando la parte de la dirección destinada a la red y la asignada a los dispositivos. Por ejemplo, una máscara 255.255.255.0 indica que los primeros 24 bits corresponden a la red y los últimos 8 a los dispositivos, permitiendo hasta 254 equipos en la subred [6].

La puerta de enlace predeterminado (en inglés llamado "Default Gateway") es donde la dirección de un dispositivo de red que actúa como punto de acceso para enviar fuera de la red local [7]. Por último, el servidor DNS traduce nombres de dominios legible a direcciones IP. Por ejemplo, si escribimos en nuestro navegador de internet www.google.com se traduce a 142.250.190.46 [8].

Con estas topologías, es posible implementar una red de comunicaciones en una organización y gestionar direcciones esenciales. Para ello, se requiere un programa que incluya componentes básicos, distintas topologías y direcciones IP, permitiendo crear un prototipo de configuración. Esto facilita la realización de pruebas y garantiza una implementación robusta en el entorno laboral.

El término seguridad surgió en 1979, asociado al liberalismo y a la protección de individuos y colectivos frente a diversos riesgos. Esto llevó a la implementación de medidas para controlar amenazas en salud, crimen y defensa [9]. Con el tiempo, el concepto evolucionó hasta referirse a la sensación de estar a salvo y libre de peligros.

Más adelante, nació la seguridad informática o ciberseguridad, enfocada en la protección de datos y sistemas. Su objetivo es prevenir ataques, extorsión y vandalismo mediante programas especializados. La ciberseguridad comenzó a desarrollarse en la década de 1950 con la creación de las primeras redes informáticas.

Para ese tiempo la única forma de amenaza era acceder físicamente a él. A los años, mediante la creación del internet fue donde se originó la protección de datos cibernéticos [10]. Para el caso de la protección de datos, pensamos en una caja fuerte, un cuarto con cámaras de seguridad vigilando si una persona no autorizada entra, o un sin número de escenario a la hora de proteger información. No estamos tan lejos de la imaginación cuando deseamos proteger información de gran valor en la agencia, empresa, y organización en la que trabajamos.

Lo podemos categorizar en dos elementos, en controles técnicos y físicos.

La Tabla 1 muestra los controles técnicos que nos podemos encontrar.

En la Tabla 2 nos muestra los controles físicos que están disponibles para poder implementar la seguridad en nuestros ambientes de trabajos.

A la hora de planificar la protección de ambos controles, debemos tener en cuenta el ambiente que vamos a trabajar. Para así llevar una construcción de sistema de seguridad eficiente y capaz de sobrellevar cualquier circunstancia.

El caso de las contraseñas lo podemos definir como son una combinación de caracteres (letras, números, símbolos) que se utiliza para autorizar a un usuario acceder a un sistema, dispositivo o cuenta. Donde debe ser conocida por el usuario para

garantizar la seguridad y privacidad de la información. En adición, podemos seguir las siguientes características para tener una contraseña robusta y difícil de obtener.

Tabla 1
Controles Técnicos

Controles técnicos	
Controles de acceso	Se implementa autenticación y autorización a mecanismos que restringe el acceso a recursos.
Encriptación	El uso de técnicas de criptografía para proteger datos en tránsitos y reposo
Cortafuegos	Control sobre el tráfico de red entrante y saliente.
Sistema de detección y prevención de intrusiones	Supervisan y responden a posibles brechas de seguridad
Antivirus y anti-programa malicioso	Protege el sistema de programas maliciosos a través de detección y herramientas de reemplazo
Gestión de parches	Donde regularmente hay actualizaciones en los programas para arreglar vulnerabilidades y mejorar la seguridad

Tabla 2
Controles Físicos

Controles físicos	
Cerraduras y tarjetas de acceso	Utiliza medidas de seguridad física para controlar la entrada a edificios y zonas sensibles. Pueden ser sistemas biométricos para acceder a lugares en la empresa.
Cámaras de vigilancia	Supervisar y grabar las actividades en las instalaciones seguras y sus alrededores.
Guardias de seguridad	Emplear personal para proteger los ambientes que necesiten extra-protección y hacer cumplir las políticas de seguridad
Controles de ambientes	Son sistemas de protección contra catástrofes naturales como sistemas de extinción de incendios y climáticos.

Longitud: Cuanto más larga sea la contraseña, más difícil será de adivinar o descifrar.

Complejidad: Combinación de letras, números y símbolos. Con la implementación de mayúsculas y minúsculas.

No incluya: Evitar utilizar información personal, por ejemplo, fechas de nacimiento, nombres propios, nombre de familiares, números que involucren cuentas de bancos.

Cambios: Se recomienda que se deba de cambiar la contraseña al menos 90 días, para así asegurar tu cuenta [11].

Dichos temas son piezas claves a la hora de conocer sobre las redes e implementar seguridad en nuestros ambientes de trabajo o inclusive en nuestro mismo hogar. Ya que podemos cambiar contraseñas que vienen por defecto de la compañía. Por ejemplo, nuestros servicios de internet en el hogar. En ocasiones cambiamos nuestras contraseñas y en otras no.

OBJETIVO DEL PROYECTO

El principal objetivo de este proyecto es poder brindarle un conocimiento básico de las redes de comunicaciones y cortafuego. También conocimientos en seguridad, importancia de las contraseñas y cifrados populares para poder implementarlas en nuestro diario vivir. En adición, poder implementarlas en un ambiente de prueba donde la persona pueda tener una experiencia en configurar su red y poder hacer diferentes pruebas en su configuración. Donde se le ofrecerá una guía sobre el programa común en las pruebas de redes.

PREGUNTAS SOBRE LA INVESTIGACIÓN

Las siguientes preguntas fueron piezas claves para hacer el desarrollo de la investigación en las redes, cortafuego, cifrados, criptografía y contraseñas. También en poder brindar un conocimiento que pueda ser de beneficio para futuras generaciones que puedan tener un conocimiento en redes y seguridad.

- ¿Qué tipo de programa se utiliza en las organizaciones para hacer pruebas, prototipos y configuraciones en la red?
- ¿Cuál es la primera fila de combate cibernético que podamos defender?
- ¿Los estudiantes de escuela secundaria saben de las redes?
- ¿Las configuraciones implementadas en la red necesitan mantenimiento para la robusticidad de la red?
- ¿Qué tiempo dura en conseguir las contraseñas mediante un ataque?

- ¿Cuáles son los métodos populares de los cifrados?
- ¿Cuál es el uso de la criptografía?
- ¿Cuáles son los ataques comunes para obtener las contraseñas?

PERTINENCIA E IMPORTANCIA

Este documento es importante para la educación de los estudiantes en redes y seguridad, áreas esenciales en nuestra vida cotidiana, ya que estamos constantemente conectados a redes y computadoras. Su objetivo es acercar a los estudiantes a estos temas mediante conceptos clave de manera accesible y comprensible. Las redes y la seguridad son fundamentales para el funcionamiento de Internet, aplicaciones móviles y sistemas digitales que usamos a diario. Además, la creciente demanda de conocimiento en estos temas resalta la necesidad de prepararnos y fomentar el interés por seguir aprendiendo sobre ellos.

METODOLOGÍA Y DISEÑO

En un tutorial de diseño en un programa de simulaciones de redes va a hacer pieza clave en la enseñanza y soluciones de problemas de las redes. Donde se va a poder adquirir destrezas de topologías, conexiones por cable o inalámbricas, configuraciones, y destrezas sobre programas importantes sobre redes como Telnet e interfaz de línea de comandos. Dichos programas que vienen integrados en una computadora hacen que nos familiaricemos para análisis de la computadora hasta respuestas de accidentes que son importantes en la seguridad cibernética. En adición, hace una contribución a las redes de computadoras de una forma técnica, sencilla y de aprendizaje.

En la parte de la seguridad vamos a seleccionar cuatro cifrados populares para poder brindar conocimientos básicos y encontrar escenarios pertinentes a la hora de su implementación. En adición, mencionar métodos de criptografía para asegurar la confidencialidad, integridad y autenticación de los datos en nuestro lugar de trabajo o documentos personales.

Selección de Criterio

La selección del programa que se va a utilizar para los tutoriales fue por los siguientes beneficios:

- Compatibilidad: El programa Cisco Packet Tracer tiene la compatibilidad de los sistemas operativos Windows y MacOS. Que son dos sistemas operativos más comunes que podemos encontrar en nuestro lugar de trabajo o estudios.
- Fácil de usar: La interfaz del programa hace que al usuario encuentre los objetos de una manera fácil, sin tener en cuenta su trasfondo técnico ya que utiliza dibujos para simular computadoras, enrutadores, conmutadores, entre otros.
- Apoyo comunitario: Al ser un programa pilar en las simulaciones de redes, es fácil conseguir ayuda o alternativas para solucionar los problemas.
- Estudios continuos: El mismo proveedor del programa, Cisco ofrece cursos para poder enriquecer el conocimiento del programa tanto en cómo usarlo y diferentes temas competentes a lo relacionado de las redes.
- Colaboración*:* Permite a los usuarios que puedan compartir sus configuraciones con otros para trabajar en proyectos de red en equipo.

La selección de los cifrados y criptografía que vamos a discutir fue por los siguientes beneficios:

- Simplicidad: Los cifrados a discutir podemos explicarlos de una manera donde cualquier tipo de audiencia pueda entenderlos e implementarlos donde mejor le parezca. También, en la criptografía mencionada es fácil de entender.
- Fácil de usar: Dichos temas de criptografía o cifrados son fácil de implementar en los documentos o programas que deseas utilizarlos. Ya que existen páginas en el internet donde puedes utilizarlo a su conveniencia en cualquier proyecto.
- Apoyo comunitario: Al ser temas importantes y básicos, existes diferentes métodos de aprendizaje o páginas de apoyo comunitario a la hora de evaluar problemas donde a la persona necesite buscar respuestas.

Instalación y Configuración

Al necesitar un programa para realizar o simular redes debemos de instalar y configurar un sistema apto para dicho proyecto. Es por esa razón que consideramos el programa *Cisco Packet Tracer.*

- *Cisco Packet Tracer:* Este programa va hacer instalado en un ambiente de MacOS para hacer diferentes prototipos y demostrar la configuración de un cortafuego con una topología [12].

Escenario de Prueba de Cisco Packet Tracer, Cifrados, Criptografía

El escenario de la prueba para el programa de Cisco Packet Tracer constara de hacer una configuración de tres computadoras personales, un conmutador, un enrutador y un servidor. Donde en el enrutador va a hacer capaz de hacer el trabajo del cortafuego. En la Figura 5 muestra el diagrama de las especificaciones provistas.

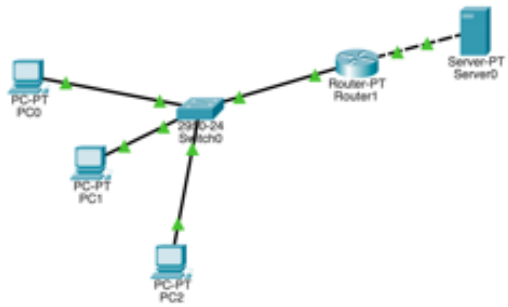


Figura 5
Simulación del Cortafuego

Cada computadora personal tiene una configuración específica para que puedan tener la comunicación entre ellas, servidores, enrutadores, y conmutadores.

Cabe destacar que el enrutador debe contar con la configuración del corta fuego. Recordando que a nivel del cortafuego hace que inspeccione todo el tráfico entrante y saliente de una red. Donde en las direcciones IP puedan permitir o bloquear el tráfico de direcciones IP específicas. También, pueden filtrar los protocolos de comunicación. Donde niega el protocolo de mensajes de control de internet (por sus abreviaciones en inglés ICMP) y permite el protocolo de control de transmisión (por sus siglas en inglés TCP).

Para los problemas del cifrado de Pigpen, Railfence, Playfair, y Vernam no necesitamos ningún tipo de programa para hacer uso de dichos cifrado.

Para el cifrado de Pigpen, la función de este cifrado es que cada letra le corresponde un símbolo o dibujo, y ese dibujo proviene de la posición en la que se colocan las letras dentro de una Tabla y dentro de una cruz, añadiendo puntos para poder alcanzar todas las letras del alfabeto.

Veamos la Figura 6 donde se podrá observar lo que nos dice la función del cifrado. Donde se distribuyeron las letras del abecedario en inglés en tablas para ser el cifrado.

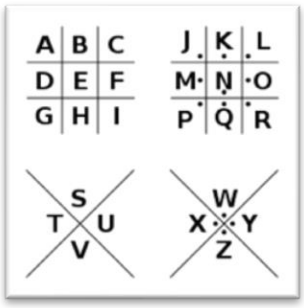


Figura 6
Distribución del Abecedario del Pigpen

En el caso que deseemos encriptar un mensaje debemos de comparar las letras con el símbolo. Veamos el siguiente ejemplo.

Mensaje por encriptar: Me gustan los chocolates.

Pasos a seguir:

1. Necesitamos la Figura 6 para hacer la comparación.
2. Vemos que la primera letra es M. Vamos a buscarla en la Figura 6 para ver como es el símbolo
3. Utilizamos el mismo proceso del segundo paso, pero esta vez utilizando la letra E.
4. Seguimos utilizando el mismo proceso hasta terminar el proceso de encriptación del mensaje.

El resultado del mensaje cifrado sería el siguiente:



Figura 7
Resultado de Encriptación del Ejemplo Pigpen

En el caso de descifrar el mensaje, se haría el mismo proceso, pero a la inversa. Buscando el símbolo primero y después la letra del abecedario.

Por otra parte, el cifrado Railfence se trata de un cifrado por transposición que reordena las letras de un mensaje siguiendo un patrón en "zig-zag". El método que utiliza este cifrado es que toma el texto plano donde se escribe hacia abajo diagonalmente a través de sucesivos tablones de una valla imaginaria y luego se escribe hacia arriba también diagonalmente. Ese proceso termina cuando se quiere cifrar el mensaje.

El proceso para dicho cifrado es el siguiente:

1. En el cifrado del "railfence", el texto sin formato se escribe hacia abajo y diagonalmente sobre rieles sucesivos de una valla imaginaria.
2. Cuando llegamos al riel inferior, cruzamos hacia arriba moviéndonos en diagonal, después de llegar al riel superior, la dirección cambia de nuevo. Por lo tanto, los alfabetos del mensaje están escritos en "zig-zag".
3. Después de que se haya escrito cada alfabeto, las filas individuales se combinan para obtener el texto cifrado.

Veamos el siguiente ejemplo para referencia.

Mensaje por encriptar: "LACRIPTOGRAFIAESFACINANTE"

La Figura 8 muestra el proceso de encriptar el mensaje.



Figura 8
Encriptación de "La Criptografía es Fascinante"

El mensaje cifrado sería como si estuviéramos leyendo de izquierda a derecha y de arriba hacia abajo, como LAI ARFCN CGISA ROAAN ITEFT PSE. Ya para descifrarlo, se toma el cifrado y se debe de dibujar el patrón del "zig-zag". Teniendo en cuenta que debemos de tener la llave o filas para poder ubicar dicho cifrado e interpretarlo. Para así colocarlo de arriba hacia abajo y poder obtener el mensaje.

El cifrado Vernam cual puede convertir el texto plano en una cadena de bits (la cual puede ser presentada en código ASCII) de manera que esto le da una mayor robustez al cifrado. También sugiere emplear como clave una secuencia binaria aleatoria del mismo tamaño que el mensaje, y de manera relevante que la clave fuese de un solo uso. Después aplicar una operación OR Exclusiva, bit a bit con estas dos cadenas para obtener el criptograma.

Dicho procedimiento sería el siguiente:

1. Buscar el alfabeto binario para conocer todas las letras en minúsculas o mayúsculas en binario
2. Tomar la palabra que vas a encriptar y conocer su equivalente en binario.
3. Crear una clave para cada una de las letras con la misma cantidad de bits.
4. Hacer una operación de XOR entre la letra y la clave.
5. Después que tenemos el equivalente en binario. Buscamos en el internet la Tabla ASCII su equivalente en símbolo [13].

Hagamos un ejemplo para encriptar una palabra con dicho método.

- Para la palabra AZUL, puede ver su equivalente en binario en la Tabla 3. La clave de la palabra AZUL en la Tabla 4 y el resultado final en la Tabla 5.

Tabla 3
Equivalente a Binario la Palabra AZUL

Letras	Valor Binario
A	0100 0001
Z	0101 1010
U	0101 0101
L	0100 1100

Tabla 4
Valores en Binario de la Clave de las Letras

Letras	Clave
A	1011 0110
Z	1100 1001
U	1110 0010
L	0110 1101

Tabla 5

Resultado de la Palabra Encriptada AZUL

Valor hexadecimal	Operación XOR	Clave de la letra	=	Resultado en binario	Resultado en ASCII
0100 0001	⊕	1011 0110	=	1111 0111	/
0101 1010	⊕	1100 1001	=	1001 0011	“
0101 0101	⊕	1110 0010	=	1011 0111	·
0100 1100	⊕	0110 1101	=	0010 0001	!

Para descifrar el mensaje podemos hacer el mismo procedimiento, pero a la inversa. Debemos de aclarar que debemos de tener la clave de las letras que creamos para poder tener el mensaje original.

Por último, el cifrado de Playfair usa una matriz alfabética 5x5 donde se deben incluir letras del alfabeto. Todo depende si utilizamos el inglés o el español, ya que hay una diferencia de números de letras y debemos adaptarlas para que dos letras anden en la misma celda.

Los pasos para cifrar el mensaje sería el siguiente:

1. El número de caracteres debe ser par; si es impar, se añade una letra nula que no se use.
2. La palabra o texto se divide en pares de letras. Si hay letras repetidas, se inserta una letra nula entre ellas. Si al final queda un número impar de caracteres, se añade una letra nula.
3. Si dos caracteres o letras se encuentran en la misma fila de la tabla, se eligen los caracteres situados a su derecha.
4. Si están en la misma columna, se eligen los caracteres debajo de ellos.
5. Si los caracteres están en filas y columnas diferentes, se forma un rectángulo con los caracteres en las diagonales, y los extremos de la otra diagonal serán los que los sustituyan en la codificación.

Hagamos un ejemplo donde encriptamos la palabra MATEMATICAS.

Se utiliza la Tabla 6 para poder hacer la encriptación.

Primer paso: Separar las letras en pares y si se nos queda una sola le añadimos una letra nula.

MA-TE-MA-TI-CA-SX, en este caso se añadió la X

Tabla 6

Ejemplo de Cifrado Playfair

A	B	C	D	E
F	G	H	I	J
K	L	M	N/Ñ	O
P	Q	R	S	T
U	V/W	X	Y	Z

Empezamos con el cifrado:

MA: como está en filas y columnas distintas, se forma el rectángulo correspondiente y obtenemos KC.

TE: se encuentran en la misma columna, es por eso que debemos de utilizar lo que se encuentran exactamente abajo de cada una de ellas ZJ

MA: se utiliza la misma que la anterior KC

TI: como esta en filas y columnas distintas, se forma el rectángulo correspondiente y obtenemos SJ

CA: se encuentran en la misma fila, es por eso que debemos de sustituir por los que están justamente a su derecha. Por lo que tenemos DB

SX: como esta en filas y columnas distintas, se forma el rectángulo correspondiente y obtenemos RY.

Por lo tanto, el cifrado sería KCZJKCSJDBRY.

Los cifrados simétricos como lo que es el estándar de encriptado avanzado (por sus siglas en inglés AES) donde se basa en una red de sustitución-permutación donde se convierten bloques de texto planos en bloques cifrados, en el cual la clave podrá ser de 128, 192 o 256 bits. Recordando que el AES convierte el texto sin formato en un código que sólo puede descifrar quien tenga la clave. Cabe destacar que, si perdemos la llave el mensaje no puede ser descifrado. En el caso del cifrado asimétrico se basa

en que se necesita una clave pública para encriptar el mensaje, y una clave privada para descifrar dicho mensaje.

Las funciones “hash" son algoritmos matemáticos que transforman cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. En este caso, discutiremos el Algoritmo de Hash Seguro 256 (con su abreviación en inglés SHA) que normalmente es usado por los Bitcoin para garantizar la integridad de la información almacenada en un bloque. En el cual su objetivo principal es que se puedan asegurar documentos o datos informáticos frente a cualquier agente externo que desee modificarlos.

Dichos cifrados podemos accederlos a páginas de internet para hacer uso de cada uno de ellos. Sin necesidad de instalarlos en nuestros dispositivos personales. Cabe destacar que, si deseamos que nuestros códigos contengan dichos cifrados en cualquier lenguaje de programación, sería pertinente codificarlos o invocar dicha función a nuestro programa que estamos creando.

Análisis y Evaluación

Después de hacer el escenario de prueba del programa de Cisco Packet Tracer, pude llegar a los siguientes puntos sobre la eficiencia del programa:

Interface: El programa es intuitivo, permitiendo agregar dispositivos fácilmente, como computadoras, cables y servidores. Además, ofrece opciones de configuración a través de terminales y código o simplemente completando campos con información.

Documentación: Durante el proceso de configuración, existe diferentes tipos de documentación en el internet, blogs, discusiones, videos para solucionar el problema que estas enfrentando.

Accesibilidad: El programa tiene una función donde pude simular en tiempo real o simulado que ayudan a comprender cómo fluye el tráfico de la red.

En cuanto a la criptografía, es importante destacar que, al entender cómo funcionan los cifrados, se pueden implementar en cualquier entorno, buscando soluciones según sea necesario.

Finalmente, la metodología de simulaciones de redes nos permitió entender que existen herramientas para recrear redes complejas, lo cual es clave para mejorar la seguridad cibernética y proteger la información valiosa.

RESULTADOS

Los resultados sobre la simulación de una topología con una configuración de IP y cortafuegos fueron realizados con éxito. Desde la interface del programa hasta los componentes virtuales fueron posibles en completar dicha simulación.

Se empezaron a configurar las computadoras personales asignándoles direcciones IP, mascará de subred, y la puerta de enlace predeterminada. En la Tabla 7 muestra la distribución de las direcciones.

Tabla 7
Distribución de Direcciones IP en Computadoras Personales

Computadoras personales	Direcciones IP	Mascará de subred	Puerta de enlace predeterminada
PC0	192.168.15.2	255.255.255.0	192.168.15.1
PC1	192.168.15.3	255.255.255.0	192.168.15.1
PC2	192.168.15.4	255.255.255.0	192.168.15.1
Server0	223.223.223.2	255.255.255.0	

En la implementación del cortafuego, la vamos a implementar en el enrutador donde el terminal va a tener la configuración pertinente para que pueda realizar el trabajo. En la configuración debe existir el acceso negado o permitido del protocolo de comunicación que la persona desee. Por ejemplo, si desea negar la comunicación ICMP debe de contener la siguiente sintaxis “access-list 101 deny icmp” para poder restringir el acceso.

Al hacer la simulación con la restricción del protocolo de comunicación ICMP, vemos que se puede comunicar con las demás computadoras personales, pero no entra al enrutador, haciendo posible la función del cortafuego, no permitir lo que el programador de la red estableció que tipo de comunicación puede entrar a la red configurada.

En los escenarios de cifrado, pudimos comprobar la utilidad de los métodos explicados, observando cómo un mensaje podía ser cifrado siguiendo las reglas correspondientes. Es importante notar que los resultados pueden variar dependiendo del

mensaje que se encripte. Por ejemplo, un mensaje largo será más complejo de descifrar, y las llaves diferentes cambiarán el proceso de desencriptación.

Cisco Packet Tracer es una herramienta clave para estudiantes y profesionales interesados en redes de comunicación. Además, organizaciones como las fuerzas aéreas la utilizan para entrenar a su personal en la configuración de dispositivos, ya que, al ser productos de Cisco, facilita una transición rápida, efectiva y segura a los componentes reales en el entorno laboral.

Conclusión

Cisco Packet Tracer es una herramienta clave para el aprendizaje en redes, seguridad informática y criptografía. Cisco, líder en el diseño de servidores, enrutadores y conmutadores, ha consolidado su simulador como una plataforma esencial para practicar configuraciones de dispositivos de red, facilitando la adquisición de habilidades aplicables en entornos laborales.

Más allá de las conexiones físicas y configuraciones básicas, permite explorar aspectos avanzados como segmentación de redes, protocolos de seguridad y cifrado de datos. En un mundo donde la ciberseguridad es crucial, esta herramienta ayuda a garantizar la confidencialidad, integridad y autenticidad de la información.

Además, simula escenarios reales, como cortafuegos con cifrado, VPNs seguras y detección de amenazas, preparando a los usuarios para el ámbito profesional. Su uso continuo impulsa el desarrollo en ciberseguridad, diseño de redes y criptografía, posicionando a los usuarios como profesionales altamente competitivos en el mercado laboral.

Referencias

[1] Kaspersky, "¿Qué es un firewall y cómo funciona?," Kaspersky, 2024. [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/firewall. [Accedido: 10-nov-2024].

[2] Microsoft, "Generador de imágenes con IA," Microsoft Create, 2024. [En línea]. Disponible en: https://create.microsoft.com/es-es/features/ai-image-generator. [Accedido: 8-ene-2025].

[3] Secureframe, "Cybersecurity Statistics: 2024 Trends, Data, and Insights," Secureframe, 2024. [En línea]. Disponible en: https://secureframe.com/es-es/blog/cybersecurity-statistics. [Accedido: 10-ene-2025].

[4] CCNA Desde Cero, "¿Qué es Cisco? Historia y evolución," CCNA Desde Cero, 2024. [En línea]. Disponible en: https://ccnadesdecero.es/que-es-cisco-historia/. [Accedido: 30-oct-2024].

[5] Internet Engineering Task Force, RFC 791: Internet Protocol. Sep. 1981. [En línea]. Disponible en: https://datatracker.ietf.org/doc/html/rfc791 [Accedido: 11-ene-2025].

[6] Cisco Systems, "Understanding Subnet Masks," Cisco Documentation. [En línea]. Disponible en: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13790-8.html [Accedido: 11-ene-2025].

[7] Techopedia, "Default Gateway," Techopedia. [En línea]. Disponible en: https://www.techopedia.com/definition/14210/default-gateway [Accedido: 11-ene-2025].

[8] Cloudflare, "What is DNS?," Cloudflare Documentation. [En línea]. Disponible en: https://www.cloudflare.com/learning/dns/what-is-dns/ [Accedido: 11-ene-2025].

[9] E. Raffino, "Seguridad," *Enciclopedia Concepto*, 2023. [En línea]. Disponible: https://concepto.de/seguridad/ [Accedido: 24-feb-2025]

[10] E. Prieto, "¿Cuál es la historia de la ciberseguridad?," *Saint Leo University*, Jun. 21, 2024. [En línea]. Disponible: https://worldcampus.saintleo.edu/blog/historia-de-la-ciberseguridad/ [Accedido: 24-feb-2025]

[11] MSMK University, "¿Qué es una contraseña?," *MSMK University*, Sep. 10, 2024. [En línea]. Disponible: https://msmk.university/que-es-una-contrasena-msmk-university/ [Accedido: 24-feb-2025]

[12] Cisco Networking Academy, "Lab Downloads," [En línea]. Disponible en: https://www.netacad.com/resources/lab-downloads?courseLang=en-US. [Accedido: 12-ene-2025].

[13] ASCII Table, "ASCII Table and Description," https://www.asciitable.com. [En Línea]. [Accedido: 1 abr. 2025]