**Eje 3:** **Implementando Soluciones de Seguridad en Router**

Melqui A. Romero y

Karolaine Z. Villero

Fundación Universitaria del Área Andina

Facultad De Ingeniería y Ciencias Básicas, Ingeniería en Sistemas,

Seguridad en Redes

Ing. Ricardo A. López Bulla

02 de marzo del 2025

1. Introducción

La seguridad en redes es un aspecto esencial en el diseño y administración de infraestructuras tecnológicas. En la actualidad, las redes son cada vez más complejas y vulnerables a ataques que buscan comprometer la confidencialidad, integridad y disponibilidad de la información. Por ello, la implementación de protocolos y herramientas adecuadas resulta fundamental para garantizar la protección de la red.

En este documento se desarrollará la configuración de routers utilizando el protocolo OSPF (Open Shortest Path First) con autenticación, así como la implementación de Listas de Control de Acceso (ACL) para filtrar el tráfico no deseado. La finalidad es asegurar el acceso a los dispositivos y proteger la red contra amenazas externas, brindando así una infraestructura más robusta y confiable para la comunicación de datos (Lopez, 2025)

Tabla de contenido

[1. Introducción 2](#_Toc193141410)

[2. Seguridad de Routers 6](#_Toc193141411)

[Protocolo OSPF (Open Shortest Path First): 6](#_Toc193141412)

[SSH (Secure Shell): 6](#_Toc193141413)

[Listas de Control de Acceso (ACL): 7](#_Toc193141414)

[Importancia de la Seguridad en Redes: 7](#_Toc193141415)

[3. Diseñar e implementar la configuración básica del router. 7](#_Toc193141416)

[Implementar topología física y lógica. 8](#_Toc193141417)

[4. Diseñar e implementar autenticación del protocolo de enrutamiento OSPF. 18](#_Toc193141418)

[5. Diseñar e implementar ACL estándar y ACL extendida. 22](#_Toc193141419)

[6. Análisis de seguridad de red 23](#_Toc193141420)

[7. Conclusiones 27](#_Toc193141421)

[8. Evidencias trabajo en equipo 28](#_Toc193141422)

[9. Trabajos citados 30](#_Toc193141423)

1. Tabla de Figuras

[Figura 1 Tabla de direccionamiento 8](#_Toc193141489)

[Figura 2 Ejercicio Packet Tracer 8](#_Toc193141490)

[Figura 3 Configuración Router 1 9](#_Toc193141491)

[Figura 4 Configuración Router 2 9](#_Toc193141492)

[Figura 5 Configuración servidor 1 10](#_Toc193141493)

[Figura 6 servidor 2 FUAA la Ip y default Gateway 11](#_Toc193141494)

[Figura 7 Configuración PC 0 la ip y el default Gateway 12](#_Toc193141495)

[Figura 8 Configuración PC 1 la ip y el default Gateway 13](#_Toc193141496)

[Figura 9 Configuración PC 2 la ip y el default Gateway 14](#_Toc193141497)

[Figura 10 Acceder al Router 15](#_Toc193141498)

[Figura 11 Mensaje de Alerta 15](#_Toc193141499)

[Figura 12 Configuración contraseña 16](#_Toc193141500)

[Figura 13 Configuración Router 1 ssh, crypto key con rsa a 1024 bits y vty 16](#_Toc193141501)

[Figura 14 Configuración Router 2 ssh, crypto key con rsa a 1024 bits y vty 17](#_Toc193141502)

[Figura 15 Comprobación del acceso remoto por SSH 18](#_Toc193141503)

[Figura 16 Configuración de enrutamiento OSPF en el router 1 19](#_Toc193141504)

[Figura 17 Configuración de enrutamiento OSPF en el router 2 y mensaje del proceso exitoso 19](#_Toc193141505)

[Figura 18 Configuración autenticación OSPF router 1 20](#_Toc193141506)

[Figura 19 Configuración autenticación OSPF router 1 21](#_Toc193141507)

[Figura 20 Comprobación de las tablas de direccionamiento con OSPF 21](#_Toc193141508)

[Figura 21 Configuración de las ACL Extendidas 22](#_Toc193141509)

[Figura 22 Configuración de las ACL Estándar 23](#_Toc193141510)

1. Seguridad de Routers

La seguridad en redes es un aspecto fundamental que abarca diversas técnicas y herramientas diseñadas para proteger la integridad, confidencialidad y disponibilidad de la información transmitida a través de la red. Los routers desempeñan un papel esencial en la seguridad al actuar como dispositivos que regulan el tráfico que entra y sale de la red. Las medidas de seguridad implementadas en estos dispositivos deben ser adecuadas para prevenir accesos no autorizados y garantizar la comunicación segura entre los dispositivos conectados.

Protocolo OSPF (Open Shortest Path First): OSPF es un protocolo de enrutamiento de estado de enlace que se utiliza principalmente en redes grandes y complejas debido a su capacidad para calcular rutas óptimas basadas en la menor métrica de costo. La autenticación en OSPF garantiza que sólo dispositivos autorizados puedan participar en el proceso de intercambio de información de enrutamiento, evitando ataques como la falsificación de rutas. Este protocolo es fundamental en la implementación de redes seguras, ya que su configuración adecuada permite garantizar la confiabilidad de las rutas establecidas (Netseccloud, 2025)

SSH (Secure Shell): El protocolo SSH se utiliza para asegurar la administración remota de dispositivos de red. A diferencia de Telnet, que transmite datos en texto plano, SSH proporciona un canal seguro que encripta toda la comunicación entre el cliente y el servidor. La autenticación se realiza mediante credenciales o certificados, y la integridad de la conexión se garantiza mediante el uso de algoritmos criptográficos avanzados (Microsoft Corporation. , s.f.)

Listas de Control de Acceso (ACL): Las ACL son un conjunto de reglas que permiten o deniegan el tráfico en función de criterios como direcciones IP, protocolos y puertos. Las ACL estándar se utilizan principalmente para filtrar tráfico basándose únicamente en la dirección IP de origen, mientras que las ACL extendidas permiten especificar múltiples criterios, como el tipo de tráfico (HTTP, ICMP, etc.) y la dirección IP de destino. Implementar ACL adecuadas contribuye significativamente a la protección de la red al restringir el acceso no autorizado y minimizar posibles ataques (QNAP, s.f.)

Importancia de la Seguridad en Redes: La seguridad en redes se fundamenta en la implementación de políticas adecuadas que aseguren el acceso autorizado y protejan la infraestructura contra posibles amenazas. El uso de protocolos seguros como OSPF con autenticación y SSH para acceso remoto contribuye a fortalecer la protección de la red. Además, las ACL desempeñan un papel crucial al definir reglas que permiten o bloquean ciertos tipos de tráfico, mejorando así la seguridad de la red (Lopez, 2025)

1. Diseñar e implementar la configuración básica del router.

Se configuro los routers para mejorar la protección de la red y los datos, verificando la seguridad, al asignarle contraseña y que autentifique con las bases de datos a cada usuario, enviando un mensaje de advertencia, con máximo 2 intentos de autentificación y midiendo el tiempo de inactividad el cual tiene como límite 90 segundos, gracias a configurar el acceso remoto SSH, las llaves y la configuración de la línea VTY 0 4, se comprobaran con el acceso remoto de SSH.

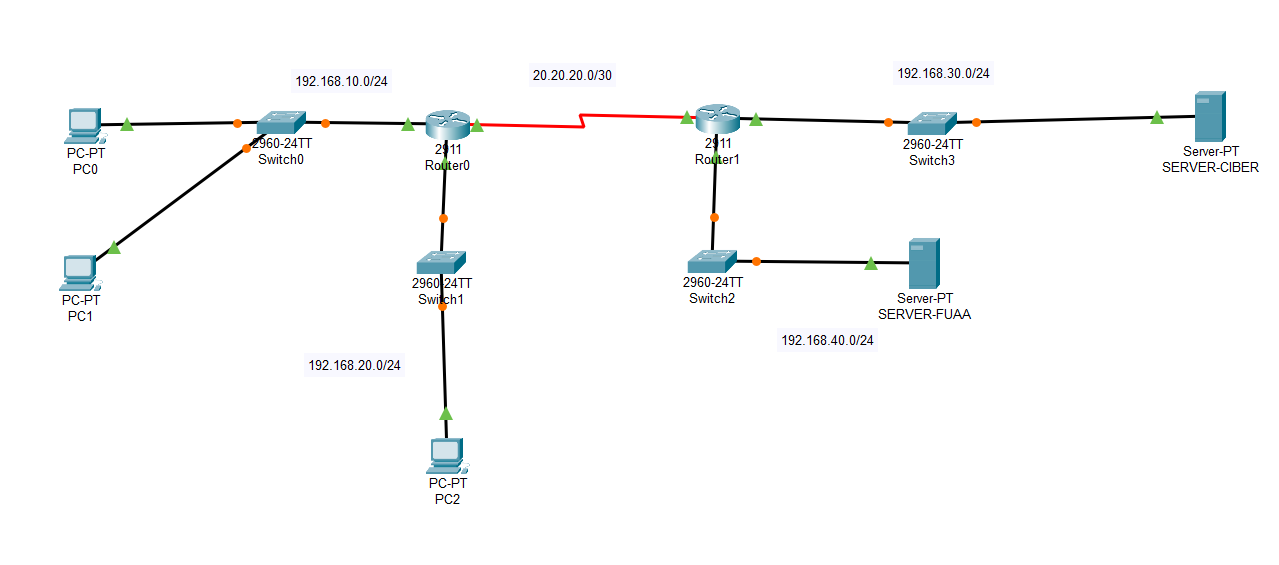
Figura 1 Tabla de direccionamiento

Con esta tabla implementaremos el Packet Tracer



Figura 2 Ejercicio Packet Tracer

Ejercicio realizado y ejecutado en Packet Tracer



Ahora configuremos los parámetros básicos del router, iniciando con asignarle los nombres con la tabla de direccionamiento:

Figura 3 Configuración Router 1

Nombre del servidor y configuración de las redes del servidor que son: G0/0 - G0/1 - S0/0/0

**Texto

El contenido generado por IA puede ser incorrecto.**

Figura 4 Configuración Router 2

nombre del servidor y configuración de las redes del servidor que son: G0/0 - G0/1 - S0/0/0

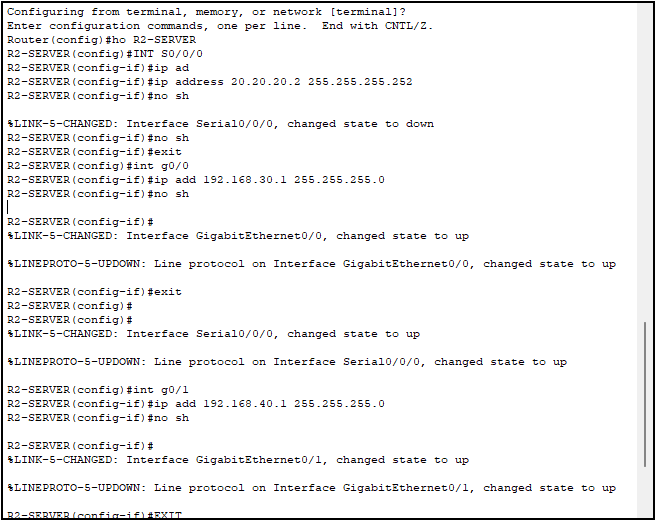


Figura Configuración servidor 1

Cibersax la Ip y default Gateway

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Figura 6 servidor 2 FUAA la Ip y default Gateway

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Figura 7 Configuración PC 0 la ip y el default Gateway

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Figura 8 Configuración PC 1 la ip y el default Gateway

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Figura 9 Configuración PC 2 la ip y el default Gateway

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Figura 10 Acceder al Router

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Configuración para que pida la contraseña al intentar acceder al router

Figura 11 Mensaje de Alerta

Texto

El contenido generado por IA puede ser incorrecto.

Creación del mensaje de alerta, creación de los usuarios y además asegure la línea de consola de manera que se autentique con las bases de datos de usuarios

Figura 12 Configuración contraseña

Texto

El contenido generado por IA puede ser incorrecto.

Configuración de contraseña en modo privilegiado, creación del mensaje de alerta, creación de los usuarios y además asegure la línea de consola de manera que se autentique con las bases de datos de usuarios

Figura 13 Configuración Router 1 ssh, crypto key con rsa a 1024 bits y vty

Texto

El contenido generado por IA puede ser incorrecto.

Figura 14 Configuración Router 2 ssh, crypto key con rsa a 1024 bits y vty

Texto

El contenido generado por IA puede ser incorrecto.

Figura 15 Comprobación del acceso remoto por SSH

Texto

El contenido generado por IA puede ser incorrecto.

1. Diseñar e implementar autenticación del protocolo de enrutamiento OSPF.

Se configuro el protocolo OSPF en los 2 router y se verificaran las tablas de rutas, así mismo comprobaremos la conexión entre las redes externas. Habilitamos la autenticación OSPF en las interfaces seriales de los routers.

Figura 16 Configuración de enrutamiento OSPF en el router 1

Texto

El contenido generado por IA puede ser incorrecto.

Figura 17 Configuración de enrutamiento OSPF en el router 2 y mensaje del proceso exitoso

Texto, Carta

El contenido generado por IA puede ser incorrecto.

Figura 18 Configuración autenticación OSPF router 1

Texto

El contenido generado por IA puede ser incorrecto.

Figura 19 Configuración autenticación OSPF router 1

Texto

El contenido generado por IA puede ser incorrecto.

Figura 20 Comprobación de las tablas de direccionamiento con OSPF

Texto

El contenido generado por IA puede ser incorrecto.

1. Diseñar e implementar ACL estándar y ACL extendida.

Figura 21 Configuración de las ACL Extendidas

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Figura 22 Configuración de las ACL Estándar

Texto, Carta

El contenido generado por IA puede ser incorrecto.

1. Análisis de Routers

La configuración de los routers y la implementación de las ACLs permitieron un control adecuado del tráfico en la red, garantizando que solo los dispositivos autorizados pudieran comunicarse. La autenticación OSPF impidió que routers externos no autorizados ingresaran al dominio de enrutamiento, mejorando así la seguridad. Además, la configuración de SSH como método exclusivo de acceso remoto aseguró que las conexiones se realizaran de manera encriptada. Las ACLs aplicadas brindaron un control granular sobre qué tráfico era permitido y cuál era bloqueado, cumpliendo con los objetivos establecidos.

<https://drive.google.com/file/d/1QhGN-0rXb84p-jzkJ1p7GYLOD2yIU5IQ/view?usp=drive_link>

Nota: Este mapa se realizó con la ayuda de (Lucidchard, s.f.)

mensajes de advertencia, autenticación SSH y dominios es esencial para evitar accesos no autorizados. Esto ayuda a establecer un control efectivo sobre quién accede al dispositivo y qué puede hacer, garantizando la seguridad de la red desde la configuración inicial.

Tabla 1 Protocolos de enrutamiento

|  |  |  |
| --- | --- | --- |
| **Categoría** | **Protocolo** | **Características** |
| **Enrutamiento Estático** | Rutas Estáticas | Configuración manual, adecuado para redes pequeñas. |
| **Enrutamiento Dinámico** | **Vector Distancia** | Envía periódicamente la tabla de rutas. |
|  | RIP (Routing Information Protocol) | Usa el número de saltos como métrica (máx. 15 saltos). |
|  | EIGRP (Enhanced Interior Gateway RP) | Propietario de Cisco, combina vector distancia y estado de enlace. |
|  | **Estado de Enlace** | Crea un mapa completo de la red. |
|  | OSPF (Open Shortest Path First) | Usa el algoritmo de Dijkstra, eficiente en redes grandes. |
|  | IS-IS (Intermediate System to IS) | Similar a OSPF, utilizado en entornos ISP y grandes redes. |
|  | **Híbrido** | Combinación de vector distancia y estado de enlace. |
|  | EIGRP (Cisco) | Utiliza múltiples métricas y optimiza rutas más rápido. |
| **Protocolos por Alcance** | **IGP (Interior Gateway Protocols)** | Usados dentro de un sistema autónomo (AS). |
|  | RIP, OSPF, EIGRP, IS-IS | Manejan el enrutamiento interno de una organización. |
|  | **EGP (Exterior Gateway Protocols)** | Usados entre diferentes sistemas autónomos. |
|  | BGP (Border Gateway Protocol) | Principal protocolo de enrutamiento en Internet. |

La autenticación garantiza que solo dispositivos autorizados puedan intercambiar información de enrutamiento. Esto previene ataques como la falsificación de rutas y asegura la integridad de las tablas de enrutamiento. La autenticación también proporciona un nivel adicional de control sobre la comunicación entre routers.

La autenticación garantiza que solo dispositivos autorizados puedan intercambiar información de enrutamiento. Esto previene ataques como la falsificación de rutas y asegura la integridad de las tablas de enrutamiento. La autenticación también proporciona un nivel adicional de control sobre la comunicación entre routers.

Tabla 2 Cuadro comparativo entre ACL estándar y ACL extendida.

|  |  |  |
| --- | --- | --- |
| **Criterio** | **ACL Estándar** | **ACL Extendida** |
| **Rango de Números** | 1 - 99 (IPv4) y 1300 - 1999 (extendido) | 100 - 199 (IPv4) y 2000 - 2699 (extendido) |
| **Filtro basado en** | Solo dirección IP de origen | Dirección IP de origen y destino, puerto y protocolo |
| **Mayor Control** | Menos específico | Más específico y flexible |
| **Protocolos Filtrados** | Solo IPv4 | IPv4, TCP, UDP, ICMP, etc. |
| **Ubicación en la Red** | Cerca del destino | Cerca del origen |
| **Ejemplo de Configuración** | access-list 10 permit 192.168.1.0 0.0.0.255 | access-list 110 permit tcp 192.168.1.0 0.0.0.255 any eq 80 |

Las políticas de seguridad propuestas buscan proteger la infraestructura de red mediante un enfoque integral que considere diferentes aspectos de seguridad. En primer lugar, es fundamental deshabilitar el uso de Telnet y permitir únicamente el acceso remoto mediante SSH versión 2, lo cual garantiza la protección de las credenciales y configuraciones críticas frente a ataques de intercepción. Asimismo, se debe implementar autenticación OSPF con claves de autenticación avanzadas como MD5 o SHA-256 en todas las interfaces seriales para prevenir la manipulación de rutas por agentes no autorizados.

También se recomienda configurar ACL estándar y extendidas para filtrar tráfico no deseado y permitir únicamente el tráfico necesario hacia redes críticas, mejorando significativamente el control sobre el flujo de datos en la red. Además, debe establecerse un sistema de monitoreo constante que registre intentos de acceso fallidos y genere alertas en tiempo real, lo cual permitirá identificar amenazas potenciales y reaccionar a tiempo.

Por otro lado, realizar auditorías periódicas de la configuración de seguridad es esencial para garantizar que las políticas implementadas se mantengan actualizadas y efectivas. Estas auditorías deben complementarse con un plan de respuesta a incidentes que incluya procedimientos específicos para la identificación, análisis, contención y recuperación de ataques. Asimismo, se debe restringir el acceso a la configuración de routers mediante usuarios autenticados y privilegios específicos, asegurando que cada usuario tenga acceso limitado a sus funciones correspondientes.

Finalmente, aplicar actualizaciones regulares de software en los dispositivos de red es crucial para protegerlos contra vulnerabilidades conocidas y emergentes. La combinación de estas políticas permitirá establecer un entorno seguro y eficiente, capaz de enfrentar las amenazas actuales y futuras con un enfoque preventivo y proactivo.

1. Conclusiones

La implementación de mecanismos de seguridad en routers mediante la autenticación de protocolos de enrutamiento OSPF y la configuración de ACLs es esencial para garantizar la integridad, disponibilidad y confidencialidad de la red. La configuración adecuada de OSPF con autenticación permite proteger el intercambio de información de enrutamiento, asegurando que solo dispositivos autorizados puedan participar en este proceso. Asimismo, el uso de SSH para acceso remoto proporciona un canal seguro que evita la exposición de credenciales y configuraciones críticas durante la gestión de la red.

Las ACLs, tanto estándar como extendidas, son herramientas efectivas para controlar el tráfico de red, permitiendo o denegando accesos específicos según criterios definidos. Su correcta implementación contribuye a la protección contra ataques comunes como ICMP no deseado o accesos no autorizados desde subredes específicas.

Además, las políticas de seguridad propuestas proporcionan un enfoque integral que incluye monitoreo continuo, auditorías periódicas, actualización de dispositivos y planes de respuesta ante incidentes, elementos fundamentales para mantener la red protegida contra amenazas conocidas y emergentes. La implementación de estas medidas permite crear una infraestructura más robusta, confiable y preparada para enfrentar desafíos de seguridad actuales y futuros.

En conclusión, asegurar la red a través de protocolos adecuados y configuraciones sólidas es un proceso continuo que requiere análisis, implementación, monitoreo y mejora constante. La adopción de buenas prácticas de seguridad permitirá garantizar un funcionamiento eficiente y seguro de la red en todo momento.La implementación de mecanismos de seguridad en routers mediante la autenticación de protocolos de enrutamiento OSPF y la configuración de ACLs es esencial para garantizar la integridad y disponibilidad de la red. El uso de SSH en lugar de Telnet proporciona un método seguro para la administración remota, mientras que las ACLs permiten controlar el tráfico no deseado y proteger áreas críticas de la red. Además, las políticas de seguridad propuestas aseguran que la infraestructura permanezca protegida ante amenazas comunes. La adopción de medidas adecuadas y la realización de auditorías periódicas permiten mantener un entorno seguro y confiable, garantizando la operación continua y eficiente de la red.

# Bibliografía

Lopez, R. A. (2025). *Seguridad en redes - Eje 2.* Obtenido de Fundación Universitaria del Área Andina.

Microsoft Corporation. . (s.f.). *Autenticación multifactor de Microsoft Entra.* Obtenido de Microsoft Corporation.: https://www.microsoft.com/es-es/security/business/identity-access/microsoft-entra-mfa-multi-factor-authentication

Netseccloud. (16 de marzo de 2025). *El impacto de las subredes y las VLAN en la seguridad de la red*. Obtenido de https://netseccloud.com/the-impact-of-subnets-and-vlans-on-network-security

QNAP. (s.f.). *Telnet/SSH.* . Obtenido de QNAP: https://docs.qnap.com/operating-system/qts/4.3.x/es-es/GUID-08E3AD8F-ADE3-4B16-85A4-F255E6F79ADB.html