

## **INSTITUTO TECNOLÓGICO SUPERIOR DEL OCCIDENTE DEL ESTADO DE HIDALGO.**

Carrera: Ingeniería en Tecnologías de la Información y  
Comunicaciones.

Materia:

Fundamentos de Redes

Reporte Técnico:

KOS System Academic

Docente:

Saul Soto Ortiz

Nombres:

22011981 Odalis Bravo Depsa.

22011435 Kaory Gissel Contreras Álvarez

22011010 Sofia Nava Cipriano

Grupo:

4ro A

Fecha de entrega:

30 /5/2024

## Tabla de contenido

Portada .....	1
Resumen Ejecutivo: .....	3
Introducción:.....	4
Problemática y la organización: .....	5
Requerimientos de la organización con respecto a la red:.....	6
Descripción y justificación de topología física y lógica:.....	7
Esquema de direccionamiento IPv4 o IPv6, con la justificación:.....	10
IMPLEMENTACIÓN DE SEGURIDAD EN LOS EQUIPOS DE RED .....	12
Importancia y la forma en que interactúan las capas red, sesión, transporte y aplicación al atender un enlace entre dos nodos; para el Modelo TCP/IP. ....	21
Fuentes: .....	23

## **Resumen Ejecutivo:**

Este proyecto integrador se enfocó en el desarrollo de un sistema académico integral para estudiantes de preescolar. Los principales objetivos fueron:

1. Implementar un sistema de gestión de matrículas y registros académicos que facilite el proceso de inscripción y seguimiento de los estudiantes.
2. Desarrollar un módulo de planificación y seguimiento del aprendizaje, que permita a los maestros diseñar y monitorear las actividades curriculares.
3. Crear una plataforma de comunicación entre la escuela, los maestros y los padres de familia, para mantener una mejor colaboración y retroalimentación.
4. Integrar todos los módulos en una solución tecnológica que mejore la eficiencia y organización de los procesos académicos en el nivel preescolar.

Para lograr estos objetivos, se utilizó una metodología de desarrollo ágil, con ciclos iterativos de análisis de requisitos, diseño de interfaces, desarrollo de funcionalidades y pruebas de usabilidad.

Los resultados obtenidos incluyen:

- Un sistema de registro y gestión de matrículas que facilita el proceso de inscripción y mantiene un historial académico de cada estudiante.
- Un módulo de planificación curricular que permite a los maestros crear y gestionar sus planes de estudio, actividades y evaluaciones.
- Una plataforma de comunicación que conecta a la escuela, los maestros y los padres de familia, permitiendo el intercambio de información, notificaciones y comentarios.
- Una interfaz de administración que integra todos los módulos y brinda a los directivos una visión general del desempeño académico y la gestión escolar.

En conclusión, este proyecto integrador ha logrado desarrollar una solución tecnológica adaptada a las necesidades específicas de las escuelas preescolares, mejorando la eficiencia de los procesos académicos y fortaleciendo la comunicación entre todos los actores involucrados.

## **Introducción:**

El presente proyecto integrador se enfoca en el desarrollo de un sistema académico integral para estudiantes de nivel preescolar. Esta solución tecnológica tiene como objetivo mejorar la eficiencia y organización de los procesos académicos en las escuelas de educación inicial, impactando de manera positiva en la experiencia de los maestros.

En la actualidad, muchas instituciones preescolares enfrentan desafíos en la gestión de sus actividades académicas, administrativas y de comunicación. La falta de herramientas digitales adecuadas dificulta el registro y seguimiento de los estudiantes, la planificación y ejecución de las actividades curriculares, así como la colaboración entre la escuela, los maestros y los padres de familia.

Esta problemática tiene implicaciones relevantes para la sociedad, ya que una educación preescolar de calidad es fundamental para el desarrollo integral de los niños y niñas. Una gestión eficiente de los procesos académicos en este nivel educativo puede contribuir a mejorar los índices de retención, aprendizaje y bienestar de los estudiantes, sentando las bases para su futura trayectoria académica y desarrollo personal.

El proyecto integrador será implementado por una empresa de desarrollo de software especializada en soluciones para el sector educativo. Su objetivo es proporcionar a las escuelas preescolares una herramienta tecnológica que les permita optimizar sus operaciones académicas, fortalecer la comunicación con la comunidad educativa y, en última instancia, brindar una experiencia de aprendizaje más enriquecedora para las profesoras.

**Problemática y la organización:**

Existen dificultades en la gestión del jardín de niños “Emiliano Zapata”, dado que toda la información de los alumnos y sus tutores se registra en una agenda física.

Este método complica la consulta y actualización de datos, además de que la dependencia de registros físicos puede conllevar la pérdida de información importante, demoras en la comunicación y una administración tardía.

**Impacto en la comunicación y administración:**

Estas dificultades en la gestión de la información también se reflejan en otros aspectos clave del jardín de niños:

**Demoras en la comunicación:** La ausencia de un sistema digital para almacenar y acceder a la información de contacto de los tutores dificulta una comunicación ágil y oportuna entre la escuela y las familias.

**Administración tardía:** La dependencia de registros físicos ralentiza los procesos administrativos, como la generación de reportes, el seguimiento del desempeño de los alumnos y la toma de decisiones basada en datos.

## Requerimientos de la organización con respecto a la red:

Requerimiento de red	Descripción
Ancho de banda	Se requiere un ancho de banda mínimo de 100 Mbps para soportar las necesidades actuales y futuras de la institución. Esto permitirá una transferencia de datos eficiente durante el acceso a la plataforma web, la carga y descarga de archivos, y la comunicación entre los diferentes usuarios.
Cantidad de usuarios	Se estima que la red deberá dar soporte a un total de 150 usuarios, incluyendo maestros, personal administrativo y directivos. Esta cantidad podría aumentar en el futuro a medida que la matrícula del jardín de niños crezca.
Seguridad	La red debe implementar medidas de seguridad robustas, como un firewall, autenticación de usuarios, cifrado de comunicaciones y políticas de control de acceso. Esto con el fin de proteger la confidencialidad e integridad de la información académica y administrativa del jardín de niños.
Disponibilidad	La red debe garantizar una disponibilidad mínima del 99% durante el horario de funcionamiento del jardín de niños, de modo que los usuarios puedan acceder a los servicios y recursos de manera confiable.
Escalabilidad	La solución de red debe ser escalable, de manera que pueda adaptarse a un crecimiento futuro en términos de usuarios, ancho de banda y nuevos requerimientos sin necesidad de una reestructuración completa.
Redundancia	Para asegurar la continuidad operativa, la red debe contar con mecanismos de redundancia, como enlaces de red redundantes y servidores de respaldo, que permitan mantener el servicio en caso de fallos o interrupciones.

## Descripción y justificación de topología física y lógica:

### Topología Física:

Para el diseño de la red de esta organización, se ha optado por utilizar una topología física tipo Estrella, la cual se considera la más adecuada para este tipo de proyecto. Esta configuración permite una mejor escalabilidad, gestión y control de la red, al tener un punto central de administración, como un switch principal.

La topología lógica utilizada será de tipo Jerarquizada, con tres capas principales:

**Capa de Núcleo:** Conformada por un switch de alto rendimiento que actuará como backbone de la red y se encargará de enrutar el tráfico entre las diferentes subredes.

**Capa de Distribución:** Compuesta por switches de acceso que se conectan al switch de núcleo y se encargan de la segmentación de la red, implementación de políticas de control de acceso y administración del tráfico.

**Capa de Acceso:** Formada por los switches que brindan conectividad directa a los usuarios finales y dispositivos de la red local.

Esta estructura jerarquizada permite una mejor organización del tráfico, facilita la implementación de medidas de seguridad y simplifica la administración y resolución de problemas en la red.

### Listado de Protocolos y Estándares Empleados

#### VIII. Protocolos y Estándares

La red utilizará los siguientes protocolos y estándares:

Capa OSI	Protocolo/Estándar	Descripción
----------	--------------------	-------------

Física	Ethernet IEEE 802.3	Estándar para redes LAN cableadas que define las características físicas y de enlace de datos.
--------	---------------------	--

Wi-Fi IEEE 802.11 Estándar para redes LAN inalámbricas que permite la conectividad de dispositivos móviles.

Enlace de Datos VLANs IEEE 802.1Q Permite la segmentación lógica de la red en múltiples dominios de difusión.

Spanning Tree Protocol (STP) Evita la formación de bucles en la topología de la red y permite la redundancia.

Red IPv4 / IPv6 Protocolos de direccionamiento y enrutamiento para la comunicación entre dispositivos.

DHCP Asignación dinámica de direcciones IP a los dispositivos de la red.

Transporte TCP / UDP Protocolos de transporte de datos extremo a extremo.

Aplicación HTTP/HTTPS Protocolos de comunicación web para el acceso a aplicaciones y servicios.

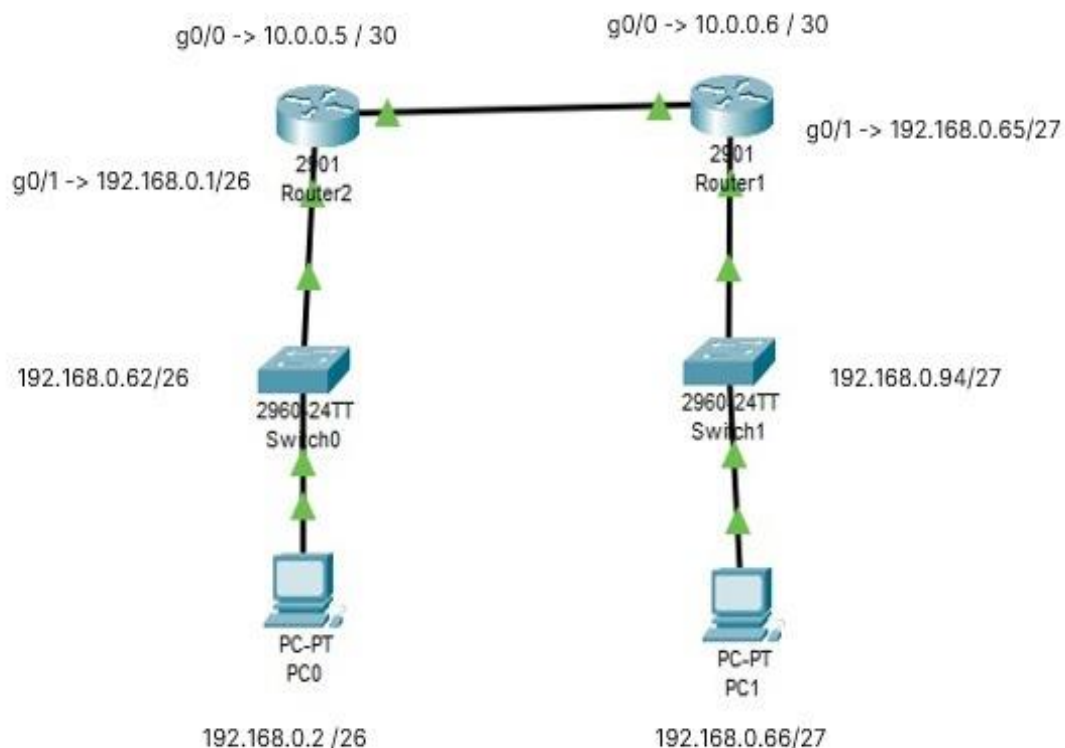
DNS Resolución de nombres de dominio a direcciones IP.

SSH / SFTP Protocolos seguros para la administración remota y transferencia de archivos.

Estos protocolos y estándares, en conjunto con la topología física y lógica diseñada, permitirán una red robusta, escalable y segura que cumpla con los requerimientos de la organización.

## **Topología Lógica.**





Para el diseño de la red de esta organización, se ha optado por utilizar una topología física tipo estrella, la cual se considera la más adecuada para este tipo de proyecto. Esta configuración permite una mejor escalabilidad, gestión y control de la red, al tener un punto central de administración, como un switch principal.

La topología lógica utilizada será de tipo jerarquizada, con tres capas principales:

Capa de núcleo: conformada por un switch de alto rendimiento que actuará como backbone de la red y se encargará de enrutar el tráfico entre las diferentes subredes.

Capa de distribución: compuesta por switches de acceso que se conectan al switch de núcleo y se encargan de la segmentación de la red, implementación de políticas de control de acceso y administración del tráfico.

Capa de acceso: formada por los switches que brindan conectividad directa a los usuarios finales y dispositivos de la red local.

Esta estructura jerarquizada permite una mejor organización del tráfico, facilita la implementación de medidas de seguridad y simplifica la administración y resolución de problemas en la red.

## Esquema de direccionamiento IPv4 o IPv6, con la justificación:

Para el diseño de la red de esta organización, se ha optado por utilizar el protocolo de direccionamiento IPv4, ya que es el protocolo más ampliamente implementado y compatible con la mayoría de los dispositivos y aplicaciones existentes. Además, IPv4 sigue siendo la opción preferida en la mayoría de los entornos empresariales y de pequeña a mediana escala.

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MÁSCARA DE SUBRED	GATEWAY PREDETERMINADO
ROUTER 1	G0/0	10.0.0.5	255.255.255.252	
	G0/1	192.168.0.1	255.255.255.192	
ROUTER 2	G0/0	10.0.0.6	255.255.255.252	
	G0/1	192.168.0.65	255.255.255.224	
SWITCH 1	VLAN1	192.168.0.62	255.255.255.192	192.168.0.1
SWITCH 2	VLAN1	192.168.0.94	255.255.255.224	192.168.0.65
LAPTOP 1	f0/1	192.168.0.2	255.255.255.192	
LAPTOP 2	f0/1	192.168.0.66	255.255.255.224	

El esquema de direccionamiento IPv4 implementado en la red se basa en la utilización de redes privadas con la siguiente distribución:

La justificación de este esquema de direccionamiento se basa en los siguientes puntos:

Utilización de redes privadas: Esto permite un mayor control y seguridad de la red, ya que los dispositivos dentro de la organización no serán accesibles desde Internet.

Segmentación de la red por VLAN: La división de la red en múltiples VLAN (redes virtuales) permite una mejor organización del tráfico, implementación de políticas de seguridad y escalabilidad de la red.

Asignación de direcciones IP: Se han reservado bloques de direcciones IP para cada segmento de la red, lo que facilita la administración y la expansión futura.

Gateway predeterminado: Todos los dispositivos de usuario y servidores tienen configurado el switch de núcleo como su gateway predeterminado, lo que permite el enrutamiento adecuado del tráfico entre las diferentes subredes.

Este esquema de direccionamiento IPv4 se considera adecuado para las necesidades actuales y futuras de la organización, ya que proporciona una estructura ordenada y escalable para la red.

# IMPLEMENTACIÓN DE SEGURIDAD EN LOS EQUIPOS DE RED

**enable password cisco:** Este comando establece la contraseña que se necesita para entrar en el modo privilegiado (modo EXEC) en un dispositivo Cisco. La contraseña en este caso es "cisco". Sin embargo, este método no es seguro porque la contraseña se guarda en texto claro.

**enable secret tics:** Este comando también establece una contraseña para acceder al modo privilegiado, pero la diferencia es que la contraseña "tics" se almacena encriptada utilizando un algoritmo MD5, lo que ofrece mayor seguridad comparado con el comando enable password.

**service password-encryption:** Este comando habilita la encriptación de todas las contraseñas en el archivo de configuración del dispositivo. Esto incluye contraseñas de consolas, líneas VTY, y cualquier otra contraseña que pueda ser configurada. Utiliza una encriptación simple (tipo 7) que no es muy fuerte, pero ayuda a evitar que las contraseñas se muestren en texto claro.

**banner login "Dispositivo permitido":** Este comando configura un mensaje de bienvenida que se muestra a los usuarios antes de iniciar sesión en el dispositivo. En este caso, el mensaje sería "Dispositivo permitido".

**banner motd "Acceso restringido":** Este comando configura el mensaje del día (Message Of The Day), que se muestra a todos los usuarios cuando se conectan al dispositivo. En este caso, el mensaje sería "Acceso restringido".

**username admin password admin:** Este comando crea un usuario con el nombre "admin" y la contraseña "admin". Este usuario puede ser utilizado para autenticarse en el dispositivo, y la contraseña se guarda en texto claro.

**crypto key generate rsa 1024:** Este comando genera un par de claves RSA con una longitud de 1024 bits. Este par de claves es utilizado para cifrar datos y para autenticación, comúnmente en configuraciones de SSH para permitir conexiones seguras al dispositivo.

## Descripción de las configuraciones básicas en los equipos de red:

DISPOSITIVO	COMANDOS	COMENTARIOS
ROUTER	<pre> hostname R1 enable password cisco enable secret tics service password-encryption line console 0 password tics login exit interface g0/1 ip add 192.168.0.1 255.255.255.192 description "R1toS1" no shut interface g0/0 ip add 10.0.0.5 255.255.255.252 description "R1toS1" no shut exit ip route 192.168.0.64 255.255.255.224 10.0.0.6 ip domain-name itsoeh.edu username admin password admin crypto key generate rsa 1024 line vty 0 15 transport input ssh login local exit banner login "Dispositivo permitido" banner motd "Acceso restringido" </pre>	<p><b>enable:</b> Cambia al modo privilegiado (EXEC) del dispositivo.</p> <p><b>configure terminal:</b> Entra en el modo de configuración global, donde se pueden realizar cambios en la configuración del dispositivo.</p> <p><b>hostname R1:</b> Establece el nombre del dispositivo a "R1". El nombre del host es utilizado para identificar el dispositivo en la red.</p> <p><b>enable password cisco:</b> Configura la contraseña "cisco" para acceder al modo privilegiado. Este método no es muy seguro ya que la contraseña se guarda en texto claro.</p> <p><b>enable secret tics:</b> Establece una contraseña "tics" encriptada para acceder al modo privilegiado. Es más seguro que enable password ya que usa una encriptación MD5.</p> <p><b>service password-encryption:</b> Habilita la encriptación de todas las contraseñas en el archivo de configuración del dispositivo. Utiliza una encriptación simple (tipo 7) para evitar que las contraseñas se muestren en texto claro.</p> <p><b>line console 0:</b> Entra en el modo de configuración de la línea de consola.</p> <p><b>password console:</b> Establece la contraseña "tics" para la línea de consola.</p> <p><b>login:</b> Requiere una contraseña para iniciar sesión en la consola.</p> <p><b>exit:</b> Sale del modo de configuración de la línea de consola.</p> <p><b>interface g0/1:</b> Entra en el modo de configuración de la interfaz.</p> <p><b>ip add 192.168.0.1 255.255.255.192:</b> Asigna la dirección IP 192.168.0.1 con una máscara de subred 255.255.255.192.</p> <p><b>description "R1toS1":</b> Añade una descripción a la interfaz.</p> <p><b>no shut:</b> Activa (levanta) la interfaz.</p> <p><b>interface g0/0:</b> Entra en el modo de configuración de la interfaz.</p> <p><b>ip add 10.0.0.5 255.255.255.252:</b></p>

		<p>Asigna la dirección IP 10.0.0.5 con una máscara de subred 255.255.255.252 a la interfaz.</p> <p><b>description "R1toS1":</b> Añade una descripción a la interfaz.</p> <p><b>no shut:</b> Activa (levanta) la interfaz</p> <p><b>exit:</b> Sale del modo de configuración de la interfaz.</p> <p><b>ip route 192.168.0.64 255.255.255.224 10.0.0.6:</b> Añade una ruta estática en la tabla de enrutamiento. El tráfico destinado a la red 192.168.0.64/27 será enviado a la dirección IP 10.0.0.6.</p> <p><b>ip domain-name itsoeh.edu:</b> Configura el nombre de dominio del dispositivo como "itsoeh.edu".</p> <p><b>username admin password admin:</b> Crea un usuario con nombre "admin" y contraseña "admin".</p> <p><b>crypto key generate rsa 1024:</b> Genera un par de claves RSA de 1024 bits, necesarias para la configuración de SSH.</p> <p><b>line vty 0 15:</b> Entra en el modo de configuración de las líneas VTY (líneas virtuales de terminal, que son las líneas para las sesiones remotas como Telnet o SSH).</p> <p><b>transport input ssh:</b> Configura las líneas VTY para aceptar solo conexiones SSH, mejorando la seguridad.</p> <p><b>login local:</b> Requiere que los usuarios se autenticuen utilizando las credenciales configuradas localmente (como el usuario "admin" configurado anteriormente).</p> <p><b>exit:</b> Sale del modo de configuración de las líneas VTY.</p> <p><b>banner login "Dispositivo permitido":</b> Configura un mensaje de bienvenida que se muestra antes de iniciar sesión.</p> <p><b>banner motd "Acceso restringido":</b> Configura el mensaje del día (Message Of The Day) que se muestra a todos los usuarios al conectarse al dispositivo.</p>
--	--	--

## SWITCH

```
enable
configure terminal
hostname S1
enable password cisco
enable secret tics
service password-encryption
line console 0
password console
login
exit
interface vlan1
ip add 192.168.0.62
255.255.255.192
description "toAdmin"
no shut
exit
ip default-gateway 192.168.0.1
ip domain-name itsoeh.edu
username admin password
admin
crypto key generate rsa
1024
line vty 0 15
transport input ssh
login local
banner login "Dispositivo
permitido"
banner motd "Acceso
restringido"
```

**Switch>enable:** Este comando permite ingresar al modo de configuración privilegiado del switch, lo que otorga acceso a comandos y configuraciones avanzadas.

**Switch#configure terminal:** Con este comando, se accede al modo de configuración global del switch, lo que permite realizar cambios en la configuración general del dispositivo.

**Switch(config)#hostname sw1:** Este comando cambia el nombre del switch

**Sw1(config)#enable password cisco:** Este comando establece una contraseña de acceso para el modo de configuración privilegiado.

**Sw1(config)#enable secret tics:** Este comando establece una contraseña cifrada para el modo de configuración privilegiado.

**Sw1(config)#service password-encryption:** Este comando habilita la encriptación de las contraseñas almacenadas en la configuración del switch, lo que mejora la seguridad al ocultar las contraseñas en texto claro.

**Sw1(config)#line console 0:** Con este comando, se accede a la configuración de la línea de consola del switch.

**Sw1(config-line)#password console:** Este comando establece una contraseña de acceso para la línea de consola del switch.

**Sw1(config-line)#login:** Con este comando, se habilita el proceso de inicio de sesión para la línea de consola del switch, lo que requiere una contraseña para acceder.

**Sw1(config-line)#exit:** Este comando permite salir del modo de configuración de la línea de consola y volver al modo de configuración global.

**Sw1(config)#interface vlan1:** Con este comando, se accede a la configuración de la interfaz de la VLAN1 en el switch.

**Sw1(config-if)#ip address 192.168.1.1 255.255.255.0:** Este comando asigna una dirección IP y

		<p>una máscara de subred a la interfaz de la VLAN1.</p> <p><b>Sw1(config-if)#description to admin:</b> Con este comando, se proporciona una descripción a la interfaz de la VLAN1, indicando que está destinada a la administración.</p> <p><b>Sw1(config-if)#no shutdown:</b> Este comando habilita la interfaz de la VLAN1, lo que permite que esté activa y funcional.</p> <p><b>Sw1(config)#ip default-gateway 192.168.1.254:</b> Con este comando, se establece la puerta de enlace predeterminada para el switch, lo que permite la conectividad con redes externas.</p> <p><b>Sw1(config)#ip domain-name itsoeh.edu:</b> Este comando define el nombre de dominio para el switch, en este caso "itsoeh.edu". Es importante para la resolución de nombres en la red.</p> <p><b>Sw1(config)#crypto key generate rsa:</b> Con este comando, se genera un par de claves RSA para el switch, necesario para habilitar servicios de seguridad como SSH.</p> <p><b>Sw1(config)#username admin password admin:</b> Este comando crea un usuario llamado "admin" con la contraseña "admin", que se utilizará para iniciar sesión en el switch.</p> <p><b>Sw1(config)#line vty 0 15:</b> Con este comando, se accede a la configuración de las líneas virtuales (VTY) del switch.</p> <p><b>Sw1(config-line)#transport input ssh:</b> Este comando configura el protocolo de transporte para las conexiones de línea virtual como SSH, lo que permite la conexión segura al switch.</p> <p><b>Sw1(config-line)#login local:</b> Con este comando, se especifica que el switch debe autenticar las conexiones de línea virtual utilizando la base de datos local de usuarios.</p> <p><b>Sw1(config-line)#exit:</b> Este comando permite salir del modo de configuración de la línea virtual y volver al modo de configuración global.</p>
--	--	---



		<p><b>Sw1(config)#banner motd "solo personal autorizado":</b> Con este comando, se establece un mensaje de bienvenida que se mostrará a los usuarios al iniciar sesión en el switch. El mensaje indica que solo el personal autorizado puede acceder.</p>
LAPTOP		<p>En la parte de la laptop se le pone en conexiones de internet, elegimos la IPv6, en donde agregamos la IP, máscara de subred y la puerta de enlace determinada, y así mismo en la laptop 2.</p>

## Pruebas de conectividad de la red

```
C:\>ping 192.168.0.1
```

```
Pinging 192.168.0.1 with 32 bytes of data:
```

```
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
```

```
Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
Pinging 192.168.0.65 with 32 bytes of data:
```

```
Reply from 192.168.0.65: bytes=32 time<1ms TTL=255
Reply from 192.168.0.65: bytes=32 time<1ms TTL=255
Reply from 192.168.0.65: bytes=32 time<1ms TTL=255
Reply from 192.168.0.65: bytes=32 time<1ms TTL=255
```

```
Ping statistics for 192.168.0.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 192.168.0.62
```

```
Pinging 192.168.0.62 with 32 bytes of data:
```

```
Reply from 192.168.0.62: bytes=32 time<1ms TTL=255
Reply from 192.168.0.62: bytes=32 time<1ms TTL=255
Reply from 192.168.0.62: bytes=32 time<1ms TTL=255
Reply from 192.168.0.62: bytes=32 time<1ms TTL=255
```

```
Ping statistics for 192.168.0.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 192.168.0.94
```

```
Pinging 192.168.0.94 with 32 bytes of data:
```

```
Reply from 192.168.0.94: bytes=32 time<1ms TTL=255
Reply from 192.168.0.94: bytes=32 time<1ms TTL=255
Reply from 192.168.0.94: bytes=32 time<1ms TTL=255
Reply from 192.168.0.94: bytes=32 time<1ms TTL=255
```

```
Ping statistics for 192.168.0.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
COM4 - PuTTY

--- System Configuration Dialog ---

Enable secret warning
-----
In order to access the device manager, an enable secret is required
If you enter the initial configuration dialog, you will be prompted for the enable secret
If you choose not to enter the initial configuration dialog, or if you exit setup
without setting the enable secret, please set an enable secret using the following CLI in configuration mode-
enable secret 0 <cleartext password>
-----
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch
*Mar 1 00:14:48.059: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively down
*Mar 1 00:14:48.068: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
Switch#enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable password cisco
S1(config)#enable secret tics
S1(config)#line con 0
S1(config-line)#password console
S1(config-line)#login
S1(config-line)#exit
S1(config)#interface Vlan1
S1(config-if)#ip address 172.168.0.62 255.255.255.192
S1(config-if)#description "toAdmin"
S1(config-if)#no shut
S1(config-if)#
*Mar 1 00:19:19.951: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Mar 1 00:19:19.959: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)#exit
S1(config)#ip default-gateway 172.168.0.61
S1(config)#ip domain-name itsoeh.edu
S1(config)#crypto key generate rsa
The name for the keys will be: S1.itsoeh.edu
Choose the size of the key modulus in the range of 360 to 4096 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
```

## **Inventarios de equipos de red**

Switches Cisco de 24 puertos:

### **1.- Cisco Catalyst 2960-X Series**

- Modelo: WS-C2960X-24TS-L
- Marca: Cisco
- Características:
- 24 puertos Gigabit Ethernet (10/100/1000)
- 4 puertos SFP uplink
- Capacidad de switching: 216 Gbps
- Memoria DRAM: 512 MB
- Capacidad de forwarding: 108 Mpps
- Soporte para VLANs
- QoS (Calidad de Servicio)
- Seguridad avanzada con 802.1x y ACLs
- Gestión a través de Cisco IOS

### **2.- Cisco Catalyst 9200 Series**

- Modelo: C9200L-24T-4G-E
- Marca: Cisco
- Características:
- 24 puertos Gigabit Ethernet (10/100/1000)
- 4 puertos SFP uplink
- Capacidad de switching: 56 Gbps
- Memoria DRAM: 2 GB
- Capacidad de forwarding: 83.3 Mpps
- Soporte para VLANs y routing estático
- QoS avanzado
- Seguridad con TrustSec
- Gestión a través de Cisco IOS XE

Routers Cisco

### **1.- Cisco ISR 4000 Series:**

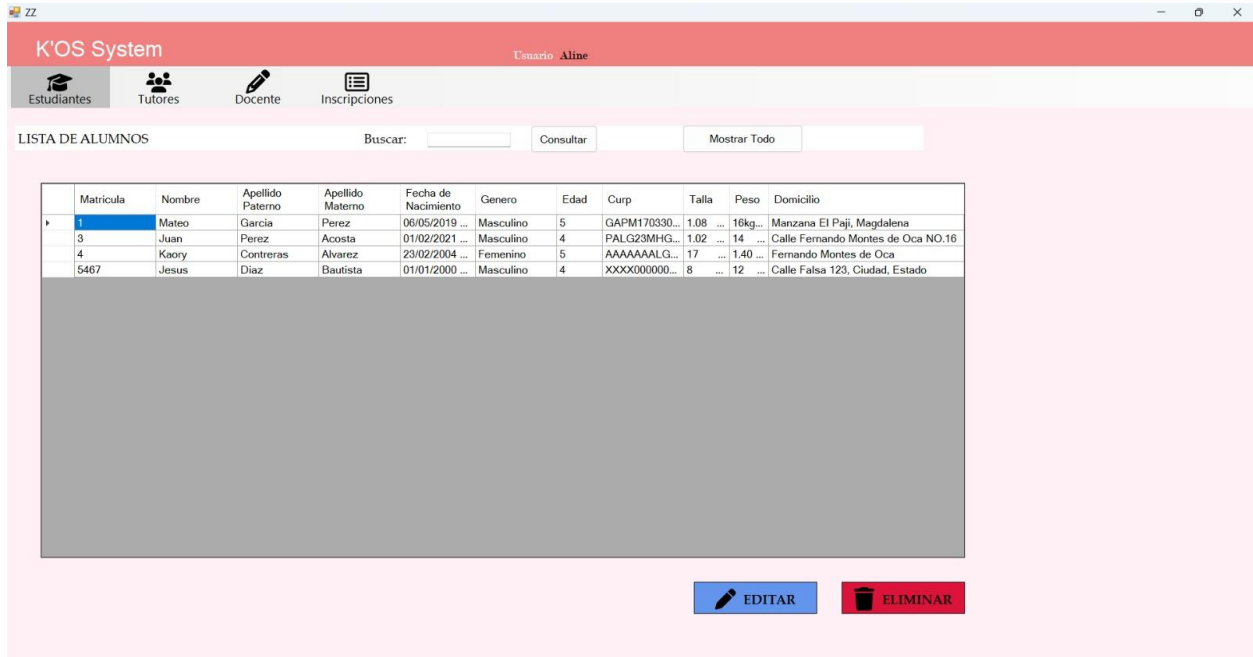
- Modelo: ISR4321/K9
- Marca: Cisco
- Características:
- 2 interfaces integradas Gigabit Ethernet
- Capacidad de rendimiento hasta 50 Mbps (con servicios)
- Memoria DRAM: 4 GB (expandible)
- Almacenamiento flash: 4 GB (expandible)

- Soporte para WAN: ADSL2/2+, VDSL2, T1/E1, 4G LTE
- Funciones de seguridad: VPN, firewall, IPS
- Gestión a través de Cisco IOS XE
- Soporte para Voice and Video

## 2.- Cisco ASR 1000 Series:

- Modelo: ASR1001-X
- Marca: Cisco
- Características:
  - 6 interfaces integradas Gigabit Ethernet (con opción de 10 Gigabit)
  - Capacidad de rendimiento hasta 20 Gbps
  - Memoria DRAM: 8 GB (expandible)
  - Almacenamiento flash: 8 GB (expandible)
- Soporte para múltiples tipos de WAN y servicios avanzados
- Funciones de seguridad: VPN, firewall, IPS
- Gestión a través de Cisco IOS XE
- Soporte para servicios avanzados como QoS y MPLS

## Resultados:



The screenshot shows a web application titled "K'OS System" with a user "Aline". The interface includes navigation tabs for "Estudiantes", "Tutores", "Docente", and "Inscripciones". Below these is a section titled "LISTA DE ALUMNOS" with a search bar and buttons for "Consultar" and "Mostrar Todo". A table displays student information, with the first row highlighted in blue. Below the table are buttons for "EDITAR" and "ELIMINAR".

Matricula	Nombre	Apellido Paterno	Apellido Materno	Fecha de Nacimiento	Genero	Edad	Curp	Talla	Peso	Domicilio
1	Mateo	Garcia	Perez	06/05/2019 ...	Masculino	5	GAPM170330...	1.08 ...	16kg...	Manzana El Paji, Magdalena
3	Juan	Perez	Acosta	01/02/2021 ...	Masculino	4	PALG23MHG...	1.02 ...	14 ...	Calle Fernando Montes de Oca NO.16
4	Kaory	Contreras	Alvarez	23/02/2004 ...	Femenino	5	AAAAAALG...	17 ...	1.40 ...	Fernando Montes de Oca
5467	Jesus	Diaz	Bautista	01/01/2000 ...	Masculino	4	XXXX000000...	8 ...	12 ...	Calle Falsa 123, Ciudad, Estado

## Trabajos Futuros:

Se tiene planeado implementar las redes para que en un futuro nuestro prototipo sea para más jardines de niños, y se pueda expandir la red.

## Conclusiones:

Hemos explorado varios aspectos de la configuración y administración de dispositivos de red Cisco, incluyendo comandos esenciales para configurar contraseñas, interfaces de red, rutas estáticas y métodos de autenticación segura, proporcionando un marco básico para la implementación y gestión de una red eficiente.

En el contexto de nuestro proyecto, nuestro prototipo de aplicación espera ser útil para el registro y consulta de alumnos y tutores, permitiendo obtener los datos de una manera más rápida. Se espera que esta herramienta ayude a las maestras a tener los registros más ordenados, minimizando la probabilidad de pérdida de información. La integración de soluciones de red robustas y seguras es fundamental en nuestro proyecto, ya que una red bien configurada garantiza el acceso rápido y seguro a la información, lo cual es crucial para la eficiencia y fiabilidad del sistema.

## Importancia y la forma en que interactúan las capas red, sesión, transporte y aplicación al atender un enlace entre dos nodos; para el Modelo TCP/IP.

CAPA OSI	PROTOCOLO/ESTÁNDAR	DESCRIPCIÓN
Física	Ethernet IEEE 802.3	Estándar para redes LAN cableadas que define las características físicas y de enlace de datos.
	Wi-fi IEEE 802.11	Estándar para redes LAN inalámbricas que permite la conectividad de dispositivos móviles.
Enlace de datos	Vlans IEEE 802.1q	Permite la segmentación lógica de la red en múltiples dominios de difusión.
	Spanning tree protocol (STP)	Evita la formación de bucles en la topología de la red y permite la redundancia.
Red	ipv4 / ipv6	Protocolos de direccionamiento y enrutamiento para la comunicación entre dispositivos.
	DHCP	Asignación dinámica de direcciones IP a los dispositivos de la red.

<b>Transporte</b>	TCP / UDP	Protocolos de transporte de datos extremo a extremo.
<b>Aplicación</b>	HTTP/HTTPS	Protocolos de comunicación web para el acceso a aplicaciones y servicios.
	DNS	Resolución de nombres de dominio a direcciones IP.
	SSH / SFTP	Protocolos seguros para la administración remota y transferencia de archivos.

## **Fuentes:**

**[1] G. Sánchez-Pérez, G. Hernández-Peñaloza, y A. Monroy-Ríos, "Implementación de Políticas de Seguridad en Redes Locales Utilizando Firewall y Antivirus," Pist. Educ., vol. 33, n.o 94, pp. 41–52, ene. 2021.**

**[2] J. D. Ríos-Páez, J. A. Reyes-Restrepo, y J. D. Acosta-Gómez, "Mejores prácticas de seguridad en la implementación de redes inalámbricas en entornos empresariales," Inge Cuc, vol. 15, n.o 2, pp. 61–72, jul. 2019.**

**[3] D. Calvo-Palomino, M. Moreira-Segura, y J. Segarra-Bonet, "Propuesta de un modelo de gestión de seguridad de la información para pequeñas y medianas empresas," Rev. Tecnol. Inf. Comun. Tic, vol. 10, n.o 1, pp. 17–27, ene. 2021.**

**[4] F. J. Herrera-Galán y J. A. Gutiérrez-Tovar, "Implementación de Políticas de Seguridad en Redes de Datos Utilizando Técnicas de Virtualización," Ing. Investig. Tecnol., vol. 22, n.o 2, pp. 1–11, abr. 2021.**

**[5] S. Gajek, M. Manulis, A. Sadeghi, and J. Schwenk, "Provably Secure Browser-Based User-Aware Mutual Authentication over TLS," in Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, New York, NY, USA, 2008, pp. 300–311. doi: 10.1145/1368310.1368352.**