

## PORTADA



### Proyecto Final Grupo 3

---

Sistemas informáticos

#### Nombre de los integrantes:

Pablo Roncero Pizarro

Álvaro Cabada Illescas

Víctor Martínez García **SM**

Alejandro Menéndez Pazo

**Curso académico:** 1ºDAM G2

**Tutora/Tutor del proyecto:** Carmelo Escribano López

Repositorio GitHub: [https://github.com/vicma06/proyectoFinal\\_SI](https://github.com/vicma06/proyectoFinal_SI)

## ÍNDICE PAGINADO

## **ANÁLISIS DE NECESIDADES Y CONFIGURACIÓN DE LA ESCUELA**

### **DEFINICIÓN DEL PROYECTO EDUCATIVO**

- **TIPO DE INSTITUCIÓN:** ESCUELA PRIMARIA CON ENFOQUE EN INNOVACIÓN TECNOLÓGICA Y DESARROLLO SOCIOEMOCIONAL.

- **EDAD DE LOS ESTUDIANTES:** DE 6 A 12 AÑOS.

- **CAPACIDAD:** 300 ESTUDIANTES (50 POR GRADO).

- **UBICACIÓN:** ZONA SEMIURBANA, ACCESIBLE Y CON DISPONIBILIDAD DE SERVICIOS PÚBLICOS.

- **MODALIDAD EDUCATIVA:** PRESENCIAL, COMPLEMENTADA CON RECURSOS DIGITALES.

- **SERVICIOS DISPONIBLES:**

- EDUCACIÓN BÁSICA (MATEMÁTICAS, CIENCIAS, LENGUA, ETC.)

- AULA DIGITAL CON RECURSOS MULTIMEDIA Y ROBÓTICA

- BIBLIOTECA FÍSICA Y DIGITAL

- ATENCIÓN PSICOPEDAGÓGICA

- COMEDOR ESCOLAR

- ACTIVIDADES EXTRACURRICULARES (DEPORTES, CLUBES, TALLERES CREATIVOS)

### **ALCANCE Y CONFIGURACIÓN TECNOLÓGICA**

- **INFRAESTRUCTURA FÍSICA:**

- AULAS CON PIZARRAS DIGITALES Y PROYECTORES INTERACTIVOS

- LABORATORIO DE COMPUTACIÓN CON 30 EQUIPOS CONECTADOS

- RESPALDO ENERGÉTICO CON SAI (UPS)

- **INFRAESTRUCTURA DIGITAL:**

- o PLATAFORMA EDUCATIVA BASADA EN LA NUBE (MOODLE O GOOGLE WORKSPACE)
  - o GESTIÓN ACADÉMICA DIGITALIZADA (ASISTENCIA, NOTAS, COMUNICACIÓN CON FAMILIAS)
  - o CONTROL DE ACCESO A RED SEGÚN PERFIL (ESTUDIANTE, DOCENTE, ADMINISTRACIÓN) o DISPOSITIVOS MÓVILES DISPONIBLES PARA PRÉSTAMO
- 

## SEGURIDAD Y CIBERSEGURIDAD ANÁLISIS DE VULNERABILIDADES

- **RED INTERNA:**

- o WI-FI SIN SEGMENTACIÓN ADECUADA PUEDE PERMITIR ACCESOS NO AUTORIZADOS
- o CONTRASEÑAS DÉBILES O COMPARTIDAS

- **CUENTAS Y DISPOSITIVOS:**

- o USUARIOS SIN AUTENTICACIÓN MULTIFACTOR (MFA)
- o EQUIPOS SIN CIFRADO NI POLÍTICAS DE BLOQUEO AUTOMÁTICO

- **PLATAFORMA LMS:**

- o RIESGO DE FILTRACIÓN DE DATOS PERSONALES
- o PERMISOS MAL CONFIGURADOS

- **RIESGOS FÍSICOS:**

- o ACCESO SIN CONTROL A LABORATORIOS
- o ROBO DE EQUIPOS PORTÁTILES MEDIDAS DE CORRECCIÓN (BLUE TEAM)

- **INFRAESTRUCTURA DE RED:**

- o IMPLEMENTACIÓN DE VLANS POR TIPO DE USUARIO

- o WI-FI CON CIFRADO WPA3 Y ROTACIÓN PERIÓDICA DE CLAVES

- **GESTIÓN DE CUENTAS:**

- o MFA OBLIGATORIO EN CUENTAS DE DOCENTES Y ADMINISTRACIÓN

- o POLÍTICAS DE CONTRASEÑAS FUERTES Y ROTACIÓN CADA 90 DÍAS

- o CIFRADO DE DISCOS EN LAPTOPS Y TABLETS

- **CONCIENCIACIÓN Y MONITOREO:**

- o FORMACIÓN ANUAL EN CIBERSEGURIDAD PARA EL PERSONAL

- o SIMULACIONES DE ATAQUES DE PHISHING

- o SIEM BÁSICO PARA MONITOREO DE INCIDENTES

- o **BACKUPS AUTOMÁTICOS EN LA NUBE RED TEAM VS. BLUE TEAM**

EN EL ENTORNO ESCOLAR RED TEAM (EQUIPO DE ATAQUE / SIMULACIÓN DE AMENAZAS) EL RED TEAM ADOPTA EL ROL DE ATACANTE ÉTICO,

SIMULANDO AMENAZAS REALES PARA PONER A PRUEBA LA SEGURIDAD DEL SISTEMA ESCOLAR. SUS ACCIONES ESTÁN DISEÑADAS PARA DESCUBRIR DEBILIDADES ANTES DE QUE LO HAGAN ACTORES MALICIOSOS REALES.

## **FUNCIONES Y ACTIVIDADES:**

- REALIZAR PRUEBAS DE PENETRACIÓN (PENTESTING) PARA EVALUAR VULNERABILIDADES EN LA RED ESCOLAR, SERVIDORES Y EQUIPOS.
- SIMULAR ATAQUES DE PHISHING DIRIGIDOS A PERSONAL DOCENTE Y ADMINISTRATIVO.
- EVALUAR LA RESPUESTA ANTE INCIDENTES FÍSICOS (INTENTOS DE ACCESO A ZONAS RESTRINGIDAS SIN CREDENCIALES).
- ANÁLISIS DE INGENIERÍA SOCIAL PARA DETECTAR QUÉ TAN FÁCILMENTE SE PODRÍAN VULNERAR PROTOCOLOS HUMANOS.

**BLUE TEAM (EQUIPO DE DEFENSA / PROTECCIÓN ACTIVA) EL BLUE TEAM SE ENCARGA DE PROTEGER, DETECTAR Y RESPONDER ANTE LOS INCIDENTES DE SEGURIDAD.**

**A DIFERENCIA DEL RED TEAM, SU FUNCIÓN ES CONTINUA Y PREVENTIVA.**

## **FUNCIONES Y ACTIVIDADES:**

- CONFIGURACIÓN DE CORTAFUEGOS (FIREWALLS) Y SEGMENTACIÓN DE REDES (VLANS) PARA LIMITAR MOVIMIENTOS LATERALES DENTRO DEL SISTEMA.
- IMPLEMENTACIÓN DE AUTENTICACIÓN MULTIFACTOR (MFA) Y GESTIÓN CENTRALIZADA DE CONTRASEÑAS.
- INSTALACIÓN DE SISTEMAS DE MONITOREO (SIEM) PARA DETECTAR COMPORTAMIENTOS ANÓMALOS.
- GESTIÓN DE BACKUPS AUTOMÁTICOS Y ENCRİPTADOS.
- CAPACITACIÓN CONTINUA A USUARIOS EN BUENAS PRÁCTICAS DE CIBERSEGURIDAD.
- APLICACIÓN DE PARCHES DE SEGURIDAD PERIÓDICAMENTE EN LOS SISTEMAS.

**AMBOS EQUIPOS COLABORAN EN UN CICLO CONTINUO DE MEJORA:**

1. RED TEAM SIMULA ATAQUES
2. BLUE TEAM RESPONDE Y CORRIGE FALLOS
3. SE DOCUMENTAN RESULTADOS Y SE AJUSTAN POLÍTICAS
4. SE REPITE EL CICLO PARA REFORZAR LA SEGURIDAD GLOBAL.

## **1. MODELO OSI**

### **1. CAPA FÍSICA**

- **FUNCIÓN:** TRANSMISIÓN DE BITS SIN ESTRUCTURA POR MEDIOS FÍSICOS.

- **DISPOSITIVOS:**

o CABLES (UTP, FIBRA ÓPTICA, COAXIAL)

o CONECTORES (RJ45, LC, ETC.)

o REPETIDORES O HUBS O MÓDEMS (A NIVEL DE SEÑAL)

---

### **2. Capa de Enlace de Datos**

- **Función:** Transmisión de tramas entre nodos conectados directamente; detección y posible corrección de errores.

- **Dispositivos:**

o Switches (nivel 2)

o Tarjetas de red (NIC)

o Puentes (bridges)

---

### 3. Capa de Red

- **Función:** Enrutamiento de paquetes entre redes distintas.

- **Dispositivos:**

- o Routers

- o Switches multicapa (nivel 3)

- o Gateways (en parte)

---

### 4. Capa de Transporte

- **Función:** Control de flujo, segmentación, control de errores extremo a extremo.

- **Dispositivos:**

- o Firewalls (nivel de puertos)

- o Dispositivos intermedios con funciones de balanceo de carga o Software (TCP/UDP en sistemas operativos)

---

### 5. Capa de Sesión

- **Función:** Gestión de sesiones de comunicación (establecimiento, mantenimiento y terminación).

- **Dispositivos:**

- o No hay dispositivos físicos específicos, pero:

- o Servidores de autenticación

- o Software de comunicación (como RDP, NetBIOS)

---



## 6. Capa de Presentación

- **Función:** Traducción, cifrado y compresión de datos.
  - **Dispositivos:**
    - o Tampoco hay dispositivos físicos concretos, pero:  
Sistemas operativos (códecs, cifrado SSL/TLS)  
Software de compresión y conversión de formatos
- 

## • 7. Capa de Aplicación

- **Función:** Interacción directa con el usuario final, aplicaciones y servicios.
- **Dispositivos:**
  - o PCs, smartphones, servidores
  - o Servidores web, de correo, FTP, DNS, etc.
  - o Dispositivos IoT

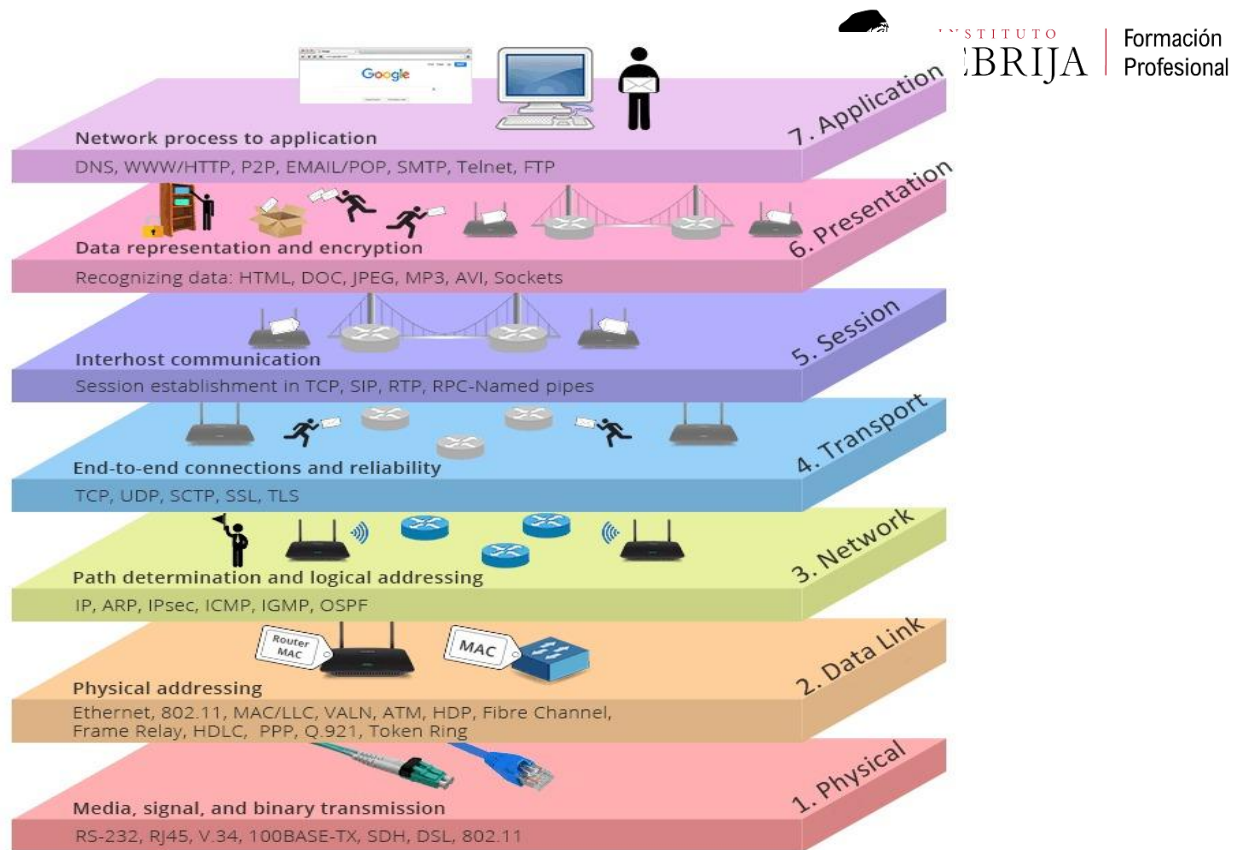


Fig 1. Imagen modelo OSI

## Configuración de un Servidor DHCP en una Red de Clase C

Fecha: 27 de mayo de 2025

En el marco del desarrollo y la gestión eficiente de redes informáticas dentro del entorno educativo, se ha llevado a cabo la incorporación de un servidor DHCP (Protocolo de Configuración Dinámica de Host) en una red de clase C. Esta implementación se realizó utilizando el software de simulación Cisco Packet Tracer, el cual permite diseñar, configurar y probar redes de forma virtual antes de aplicar los cambios en un entorno físico real.

El principal objetivo de esta configuración es automatizar la asignación de direcciones IP a cada uno de los dispositivos (ordenadores) conectados a la red de la escuela. En lugar de realizar



una asignación manual —la cual resulta más propensa a errores—, el servidor DHCP se encarga de distribuir direcciones IP de manera dinámica a cada equipo cuando estos se conectan a la red.

Al tratarse de una red de clase C, se cuenta con un rango específico de direcciones IP privadas que permiten conectar hasta 254 dispositivos únicos. El servidor DHCP ha sido configurado para operar dentro de este rango, definiendo parámetros como:

- Dirección IP del servidor DHCP
- Rango de direcciones IP asignables
- Máscara de subred
- Puerta de enlace predeterminada (gateway)
- Servidor DNS (opcional)

Esta configuración garantiza una administración más eficiente de los recursos de red, reduce la posibilidad de conflictos por direcciones IP duplicadas y permite una escalabilidad más sencilla en caso de que se agreguen nuevos dispositivos a la red.

Además, al trabajar con Cisco Packet Tracer, los estudiantes y administradores de red pueden observar en tiempo real el proceso de solicitud y asignación de direcciones IP mediante el protocolo

DHCP, lo que también representa una valiosa herramienta educativa para la comprensión de los principios fundamentales de redes.

**En resumen**, la integración de un servidor DHCP en esta red de clase C representa un avance importante en la modernización de la infraestructura tecnológica de la escuela, contribuyendo no solo a una mejor gestión de los dispositivos conectados, sino también al fortalecimiento del aprendizaje práctico en materia de redes de datos.

## 1. INTRODUCCIÓN

Vamos a tener una red de administración, alumnos y profesores, también vamos a tener un servicio de correo.

Vamos a dividir las redes de los alumnos en 4 aulas con un switch y router cada aula.

## Descripción General

Se diseñará una red institucional para un centro educativo que incluye tres tipos de usuarios: **administración, profesores y alumnos**. La red contará con:

- Segmentación por VLAN o subredes.
  - Cuatro aulas para alumnos, cada una con su propio switch y router.
  - Un servidor de correo electrónico institucional.
  - Políticas de red separadas y seguras para cada grupo.
  - Implementación y simulación con **Cisco Packet Tracer**.
- 

## Topología de Red Propuesta

### Segmentos de Red:

1. **Red Administración** (Oficinas administrativas)
2. **Red Profesores**
3. **Red Alumnos** (dividida en 4 aulas):
  - Aula 1: Switch + Router
  - Aula 2: Switch + Router
  - Aula 3: Switch + Router
  - Aula 4: Switch + Router

#### 4. Red Servidor

#### Dispositivos Utilizados

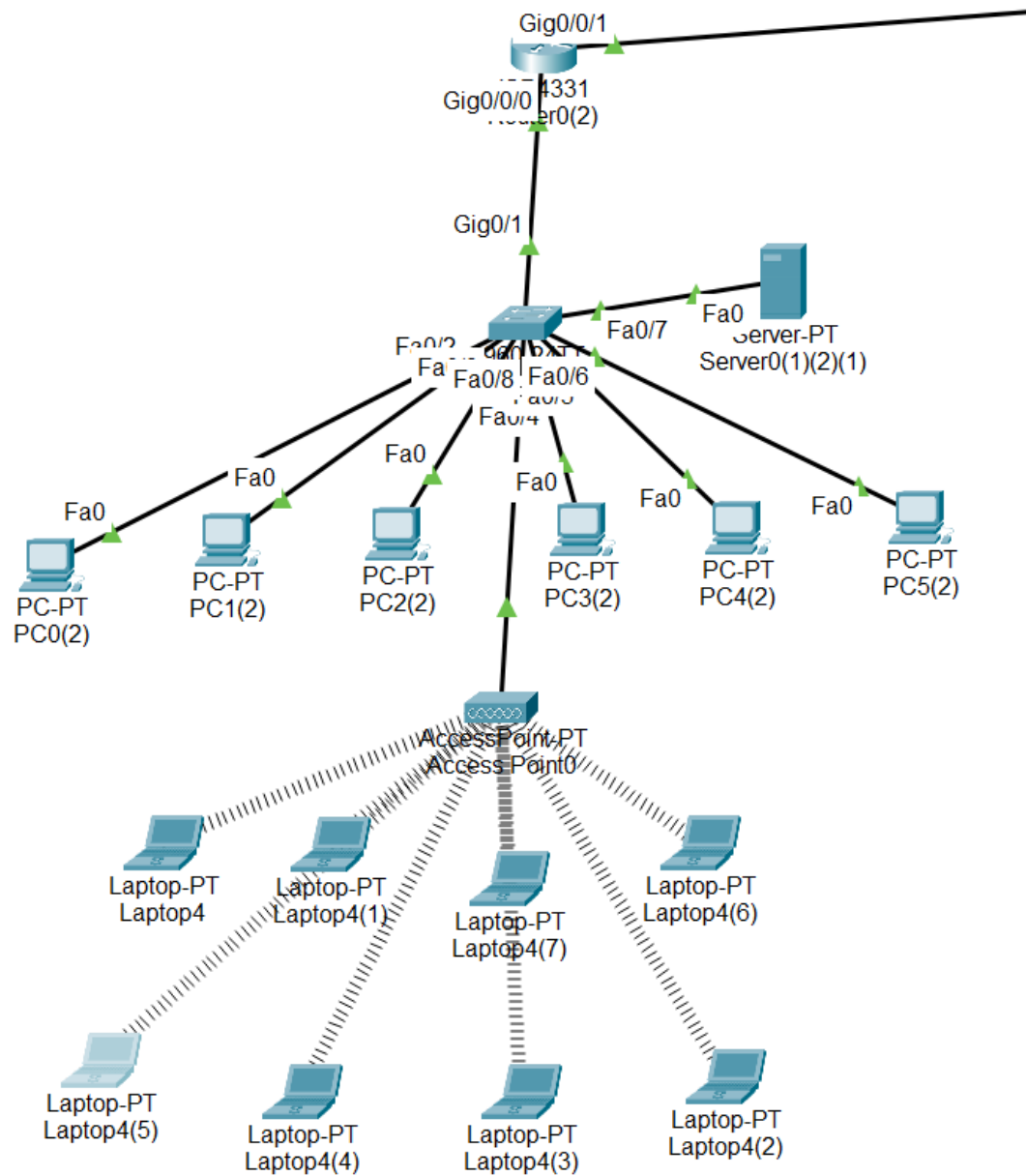
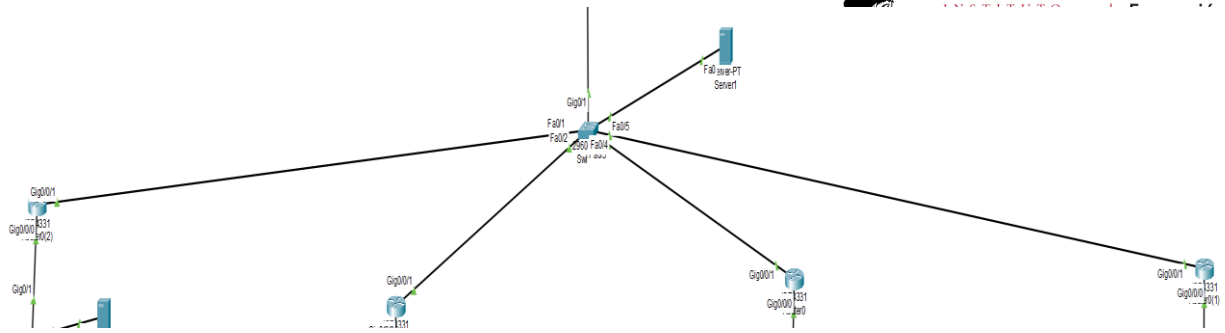
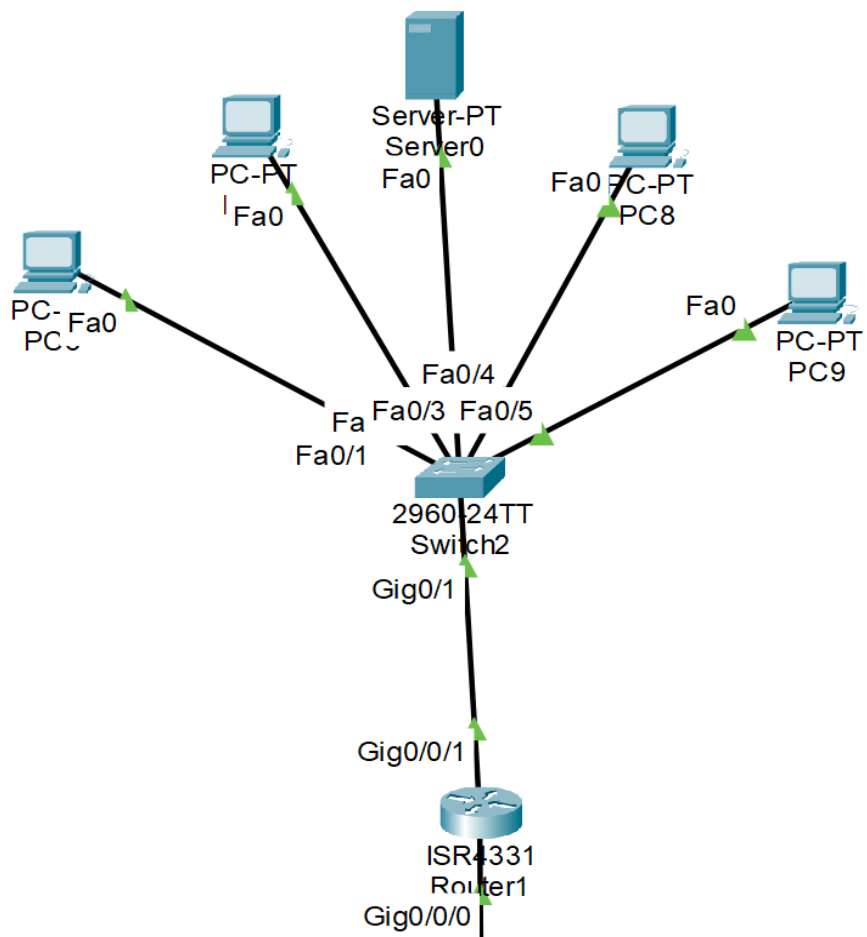


Fig 2. Estructura del aula



**Fig 3. Estructura entre routers**



**Fig 4. Estructura Administración**



**Estaciones de Trabajo (PCs):**

- **Administración:** 5 PCs
- **Profesores:** 1 PC por aula
- **Alumnos:** 5 PCs por aula + 8 portátiles (conexión vía WIFI gracias a Access Point)

**Total de PCs:** 50

---

**Switches:**

- 4 switches para Aulas (uno por aula)
- 1 switch para conexión entre routers
- 1 switch conexión administración

**Total de switches:** 6

---

**Routers:**

- 4 routers para cada aula (redes privadas de clase C)
- 1 router principal para administración (red privada de clase B)
- Conexión entre routers (red privada de clase A con subnetting para 6 dispositivos)

**Total de routers:** 5

---

**Servidores:**

Servidor DHCP para distribución de IPs dinámicas

**Total de servidores:** 5

---

**Licencias y Tipos de Dispositivo**

### Licencias OEM (Original Equipment Manufacturer):

- Licencias preinstaladas en PCs, no transferibles.
- PCs de alumnos, profesores y administración pueden tener licencias OEM de:
  - **Windows 11 Education (Versión 24h2)**
  - Licencia de uso individual

### Switches y Routers (Cisco):

- En Cisco Packet Tracer, puedes usar dispositivos como:
    - **Switch 2960** (suficiente para práctica)
    - **Router 2911 o 1941** (para conexiones por aula)
- 

### Servicio de Correo

- **Servidor SMTP/POP3/IMAP** (puede ser simulado con un servidor predefinido en Packet Tracer)
  - Dominios internos como @instituto.edu
  - Usuarios: alumnos, profesores y administración tendrán cuentas diferentes.
  - Pruebas de envío y recepción con clientes de correo en PCs.
-

Elemento	Cantidad
PCs	50
Switches	6
Routers	5
Servidores	6 (5 DHCP y 1 DNS)
VLAN/Subredes	5
Licencias OEM	Para cada PC

## 2. OBJETIVOS

### A. OBJETIVO GENERAL

El objetivo general de nuestro proyecto es diseñar y poner en marcha un instituto educativo en Honduras que cuente con una infraestructura de red sólida, moderna y eficiente. Este instituto estará dotado de una red de comunicaciones bien estructurada, basada en la implementación de múltiples routers y switches estratégicamente distribuidos para garantizar una conectividad óptima en todas sus áreas.

Buscamos que la configuración de la red sea lo más dinámica, flexible y escalable posible, permitiendo una administración sencilla, una rápida adaptación a nuevas necesidades y un uso intuitivo tanto para el personal administrativo como para los docentes y estudiantes. Además, se priorizará la seguridad, el rendimiento y la facilidad de mantenimiento, con el fin de asegurar una experiencia tecnológica fluida que respalde los procesos educativos y administrativos del instituto.

### B. OBJETIVOS ESPECÍFICOS

2. **?** **Diseñar una infraestructura de red eficiente** que permita una conectividad estable y segura en todo el instituto, utilizando routers y switches de manera estratégica para cubrir todas las áreas necesarias.
3. **?** **Implementar configuraciones dinámicas y flexibles** que faciliten la gestión de la red, permitiendo adaptaciones rápidas ante futuras ampliaciones o cambios en la infraestructura tecnológica.
4. **?** **Optimizar los recursos económicos disponibles**, seleccionando equipos y soluciones tecnológicas que ofrezcan una excelente relación entre costo y beneficio, sin comprometer la calidad ni el rendimiento del sistema.
5. **?** **Garantizar una red intuitiva y fácil de utilizar**, especialmente para los usuarios no técnicos, asegurando que el acceso a los servicios y recursos digitales sea sencillo y accesible para toda la comunidad educativa.
6. **?** **Fomentar la sostenibilidad y el mantenimiento a largo plazo** mediante el uso de componentes duraderos y configuraciones que minimicen la necesidad de intervención constante o especializada.

### **3 . DESARROLLO**

#### **1.FUNDAMENTACIÓN-TEÓRICA:**

**DISEÑO DE RED, SEGMENTACIÓN POR VLAN, IMPLEMENTACIÓN DE DHCP, SERVIDOR DE CORREO Y PROTOCOLOS OSI.**

#### **2. MATERIALES Y MÉTODOS:**

**ESTRATEGIAS DE BÚSQUEDA EN FUENTES TÉCNICAS**

**METODOLOGÍA BASADA EN SIMULACIÓN CON CISCO PACKET TRACER**

**ANÁLISIS TÉCNICO Y EVALUACIÓN DE RESULTADOS**

#### **3.RESULTADOS Y ANÁLISIS:**

**SE IDENTIFICARON DEBILIDADES CORREGIBLES EN LA RED. EL SISTEMA FUNCIONA CORRECTAMENTE CON ASIGNACIÓN DINÁMICA DE IPS, SIMULACIÓN DE SERVICIOS Y UNA TOPOLOGÍA CLARA.**

## 5. CONCLUSIONES

- La infraestructura diseñada es viable y educativa
- El uso de VLANs mejora la seguridad y gestión
- La ciberseguridad debe ser tratada como proceso continuo
- La integración tecnológica apoya el desarrollo integral de los alumnos

## **6. LÍNEAS DE INVESTIGACIÓN FUTURAS**

**(No son obligatorios, pero pueden aparecer)**

**Integración de inteligencia artificial para detección de amenazas**

**Virtualización de laboratorios y uso de contenedores**

**Análisis forense y respuesta ante incidentes educativos**

# Reforzamiento de Seguridad Informática y Ampliación de Infraestructura

## Implementación de Antivirus y Cortafuegos

Como medida complementaria a las políticas de ciberseguridad, se propone la instalación de un antivirus y un cortafuegos (firewall) en todos los equipos del centro educativo. La propuesta incluye:

- **Antivirus propuesto:** *ESET Endpoint Security*
  - Coste aproximado: 25 € por dispositivo/año (con descuentos por volumen disponibles)
  - Características: Protección en tiempo real, control de dispositivos USB, escaneo en la nube y bajo consumo de recursos.
  - Sistema de actualización: Automática a través de consola de administración remota.
- **Cortafuegos propuesto:** *pfSense (open source) + hardware dedicado por red segmentada*
  - Coste: Gratuito el software; coste aproximado del hardware: 250 € por unidad.
  - Sistema de actualización: Manual o programado desde la interfaz web administrativa; posibilidad de automatización por script en la red.

Esta medida fortalece la defensa frente a amenazas como malware, accesos no autorizados o vulnerabilidades críticas.



Además, se solicita la creación de una nueva aula equipada con aproximadamente 15 puestos de trabajo. Las especificaciones preliminares **incluyen:**

- 15 PCs con características similares a las del laboratorio actual
- 1 switch adicional
- Conexión WiFi y cableada
- Integración en la topología de red existente
- VLAN específica y políticas de seguridad adaptadas

Esta ampliación responde al crecimiento de la demanda educativa y permitirá distribuir mejor los recursos tecnológicos entre los grupos escolares.

## 7. BIBLIOGRAFÍA

[Cisco Networking Academy](#)

[Documentación oficial de Cisco Packet Tracer](#)

[Guías oficiales de seguridad de Microsoft y Google Workspace](#)

[Manuales OSI y fundamentos de redes](#)

Artículos de IEEE sobre redes escolares seguras

## 8. ANEXOS

- Capturas de simulación en Packet Tracer
- Tablas de asignación de IPs
- Capturas de configuración DHCP y VLANs
- Planos de topología