DISEÑO Y DESPLIEGUE DE UN AULA TIC PARA LA INFANCIA EN HONDURAS

Nombre de los alumnos: Sofía Lacal, Elena Ballesta y Marcos Torregrosa

Grupo 3

Curso académico: 1ºDAW

Tutora/Tutor del proyecto: Carmelo Escribano

INDICE

1. Introducción y contexto proyecto

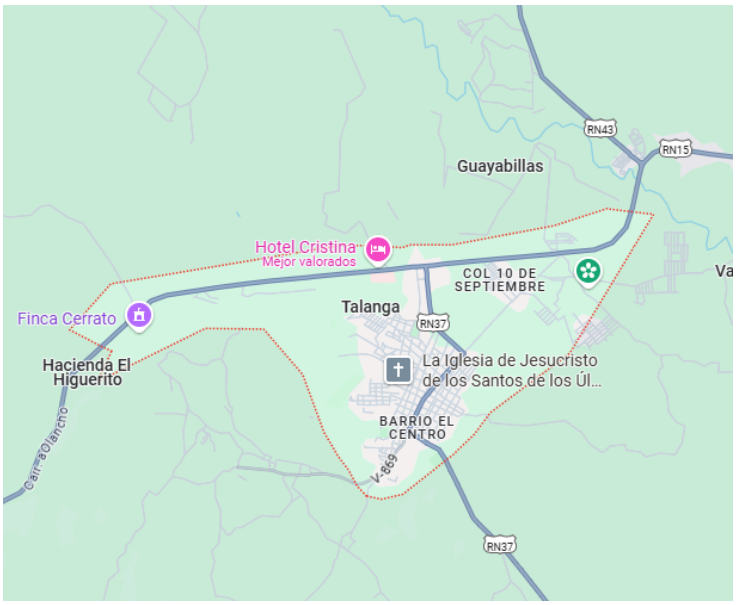
Este proyecto surge de la colaboración entre nuestro equipo (Grupo 3) del ciclo formativo de Desarrollo de Aplicaciones Web (DAW) y una organización no gubernamental (ONG) comprometida con el desarrollo educativo en zonas rurales de Honduras. La ONG ha solicitado nuestra participación para diseñar un aula de formación digital destinada a niños y niñas de entre 4 y 12 años, en una escuela con recursos limitados tanto a nivel económico como tecnológico.

El objetivo principal del proyecto es dotar a esta escuela de una infraestructura tecnológica sólida, segura y sostenible que facilite la alfabetización digital de su alumnado. Para ello, aplicaremos nuestros conocimientos en redes, sistemas, ciberseguridad y metodologías de trabajo colaborativo. Para la elección de los materiales y equipos necesarios lo más importante es saber el límite de presupuesto, ya que se puede ajustar más en función de lo que el colegio pueda gastar.

Durante el desarrollo del proyecto trabajaremos con conceptos como el direccionamiento IP, la segmentación mediante VLANs, y el diseño de topologías de red con protocolos de switching y routing. También desarrollaremos la aplicación del modelo OSI, especificando qué elementos del proyecto corresponden a cada una de sus capas. La simulación de la red se realizará utilizando la herramienta Cisco Packet Tracer.

El trabajo se organizará de forma colaborativa mediante la metodología Scrum y la distribución de tareas semanales. Todo el código, la documentación y las simulaciones se publicarán en un repositorio de GitHub, siguiendo buenas prácticas de control de versiones y fomentando la transparencia y la cultura open source.

Hemos escogido como ubicación para la escuela la ciudad de Talanga, debido a su cercanía con carreteras principales. Creemos que esto puede facilitar el acceso desde otros lugares.



2. Análisis de necesidades

Este proyecto se desarrolla en el contexto de una escuela rural ubicada en Talanga, Honduras, zona seleccionada por su fácil acceso desde carreteras principales, lo que facilita el transporte de estudiantes, docentes y recursos. La escuela atenderá a niños de entre 4 y 12 años, contará con dos aulas de formación digital y un pequeño despacho de administración.

Teniendo en cuenta que tenemos limitaciones económicas y que es una escuela, es más práctico hacer una red simple y ajustada a nuestro presupuesto.

2.1. Limitaciones y criterios de diseño

Para el diseño vamos a tener en cuenta los siguientes puntos:

- **Limitaciones económicas**: se prioriza el uso de equipos reacondicionados y una red cableada (más barata y estable que WiFi).
- **Simplicidad de mantenimiento**: la red debe ser fácil de entender y gestionar por personal no técnico.
- **Separación funcional**: es necesario que los alumnos no puedan acceder a recursos administrativos.
- **Escalabilidad**: el diseño debe permitir ampliaciones futuras con el mínimo impacto.

2.2. Distribución de espacios y necesidades específicas

2.2.1. Administración

En esta zona se ubicarían 2 PC para gestión del alumnado, archivos y coordinación

escolar. También una impresora para facilitar trámites.

Estarían conectados ambos PC con un router y un switch. Todo conectado con red cableada.

2.2.2. Aula 1

En la primera aula tendríamos 9 PC para alumnos, 1 para el profesor, un proyector conectado al PC del profesor para impartir las clases, otro router y otro switch.

2.2.3. Aula 2

En la segunda aula tendríamos la misma estructura que en la primera, 9 PC para alumnos, 1 para el profesor, el proyector, otro router y otro switch.

2.3. Equipamiento necesario

Elemento	**Cantidad**	**Función principal**
Routers	3	Uno para cada aula y uno exclusivo para administración
Switches	3	Para distribución interna en cada aula y administración
PCs	22	18 para alumnos, 2 para profesores, 2 para administración
Cableado estructurado (Cat6)	—	Conexiones estables y seguras entre todos los dispositivos
Rack y canalización	—	Para organización física, seguridad del cableado y equipos

2.4. Topología y segmentación de red

A diferencia de una red centralizada tradicional, hemos optado por una arquitectura con tres routers independientes, uno por cada segmento funcional.

Con esto se pretende separar lógica y físicamente los 3 entornos de trabajo establecidos, garantizar que la administración esté aislada para proteger datos sensibles y mantener la comunicación entre aulas para favorecer el trabajo colaborativo.

2.5. Justificación del diseño elegido

Es importante separar la información sensible, como pueden ser los registros académicos, matrículas, evaluaciones, etc., del resto de la red. Utilizando un router exclusivo sin conexión con las aulas, garantizamos una segmentación total para facilitar esa protección de los datos.

Poner dos router, uno en cada aula favorece que funcionen como entornos autónomos, garantizando menos impacto si hay errores técnicos o fallos locales y facilitando la resolución de posibles incidencias.

Con este diseño, se facilitan también los costes de mantenimiento y se reduce la carga técnica al simplificar el diseño de la red.

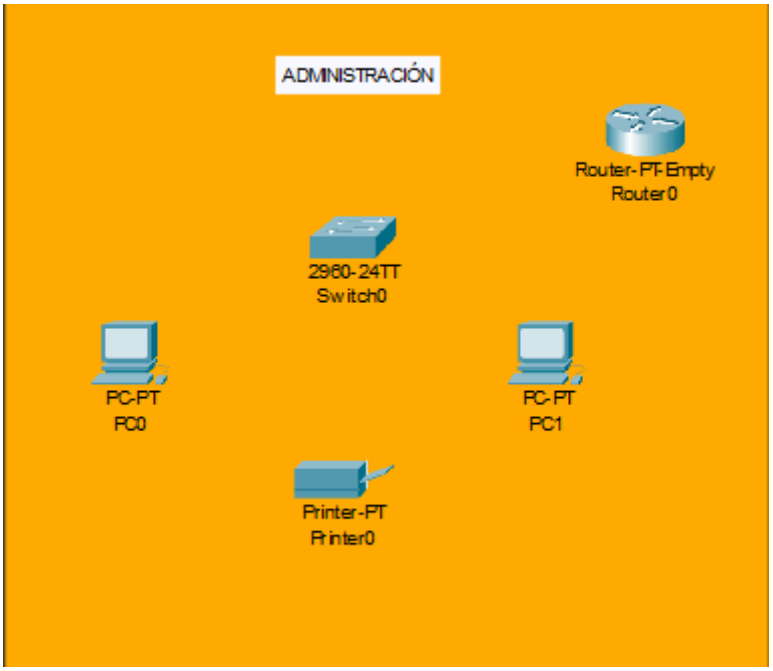
2.6. Escalabilidad y futuro

Este diseño permitiría ampliar la estructura de red o bien añadiendo más PC en cada aula o replicando la red para una tercera aula o una cuarta o las que fueran necesarias.

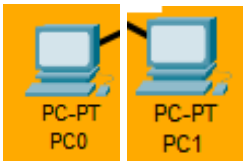
3. Diseño de red (lógico y físico)

3.1 Fase inicial del proceso:

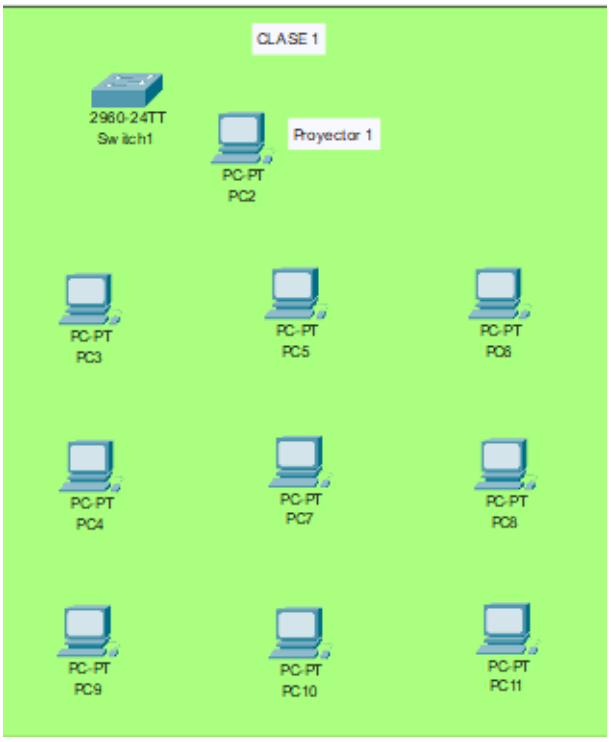
Administración de la escuela:



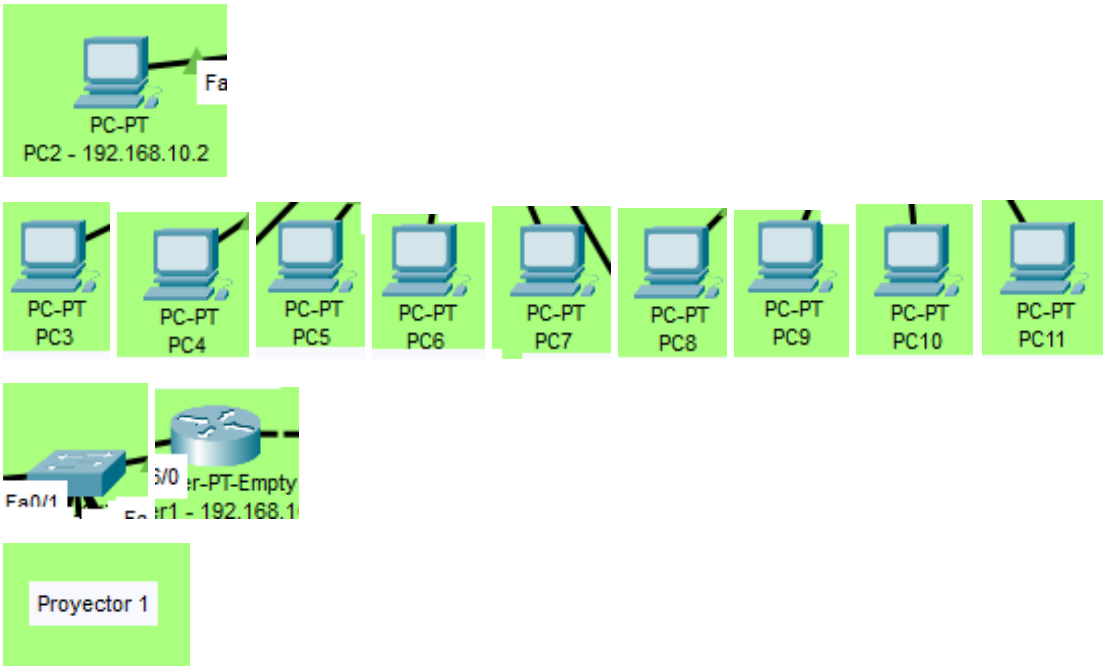
Colocamos 2PC para administración, un router, un switch y una impresora.



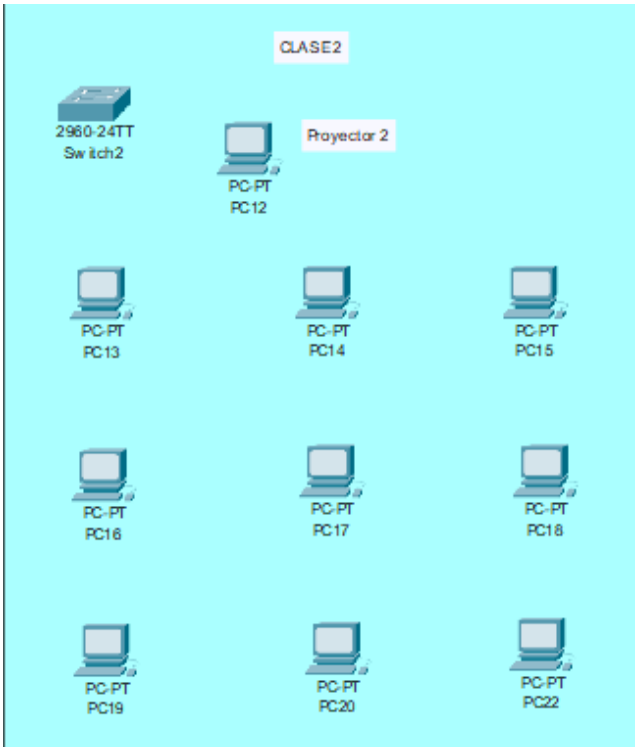
Primer aula:



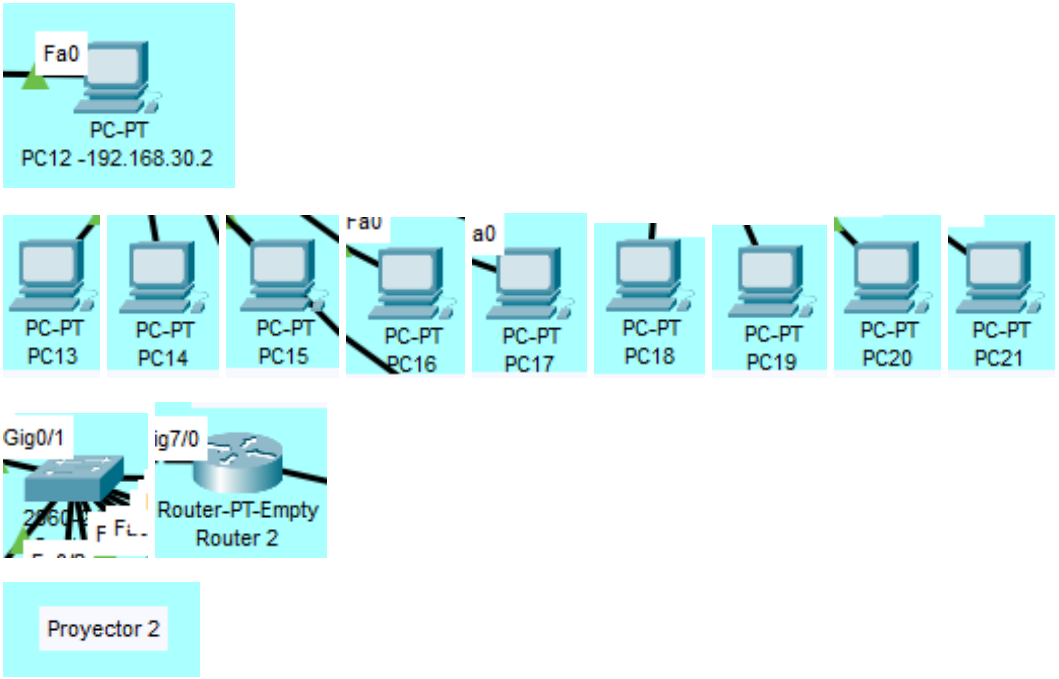
Colocamos 1PC para el profesor, 9PC para los alumnos, un router, un switch y un proyector.



Segundo aula:



Colocamos 1PC para el profesor, 9PC para los alumnos, un router, un switch y un proyector.



4. Direccionamiento y configuración

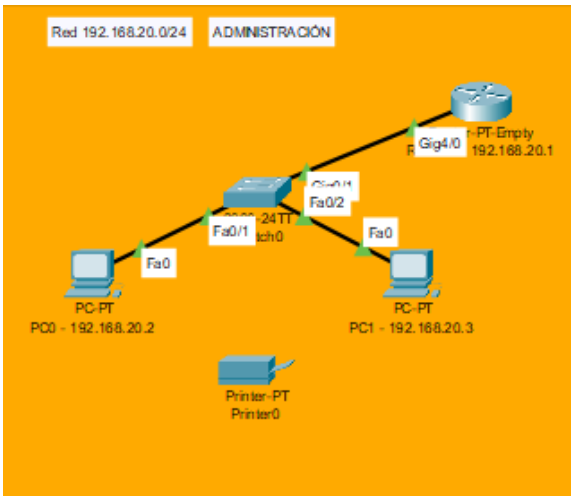
Hemos estructurado la red de la siguiente manera:

4.1 Administración

Tenemos una red de clase C (192.168.20.0/24).

En el router se ha puesto la IP (192.168.20.1)

En los ordenadores se han puesto las IP (192.168.20.2 y 192.168.20.3)

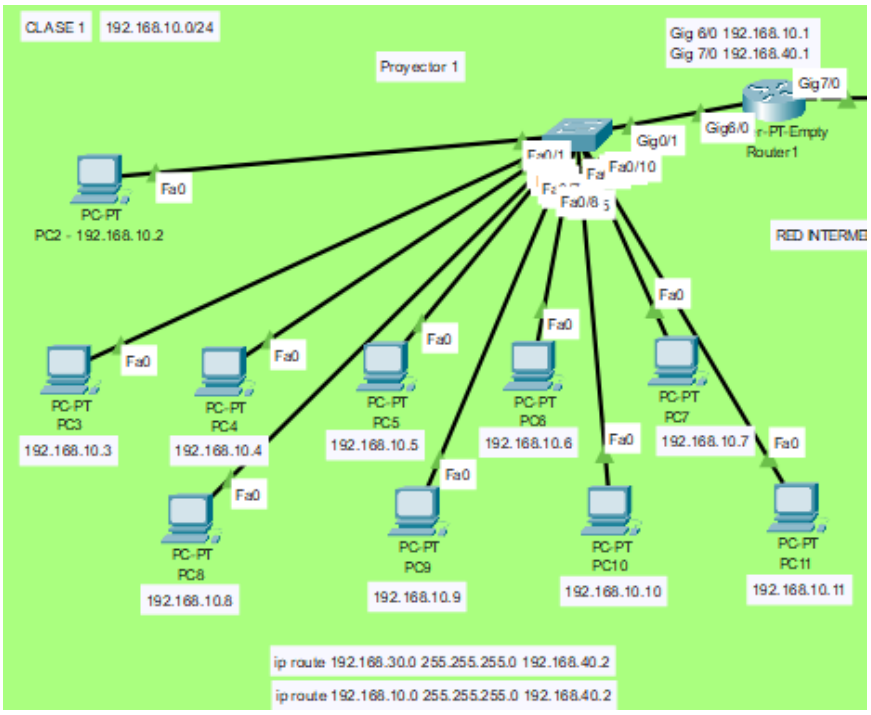


4.2 Aula 1

Tenemos una red de clase C (192.168.10.0/24).

En el router se ha puesto la IP (192.168.10.1)

En los ordenadores se han puesto las IP (192.168.10.2 / 192.168.10.3 / 192.168.10.4 / 192.168.10.5 / 192.168.10.6 / 192.168.10.7 / 192.168.10.8 / 192.168.10.9 / 192.168.10.10 / 192.168.10.11)

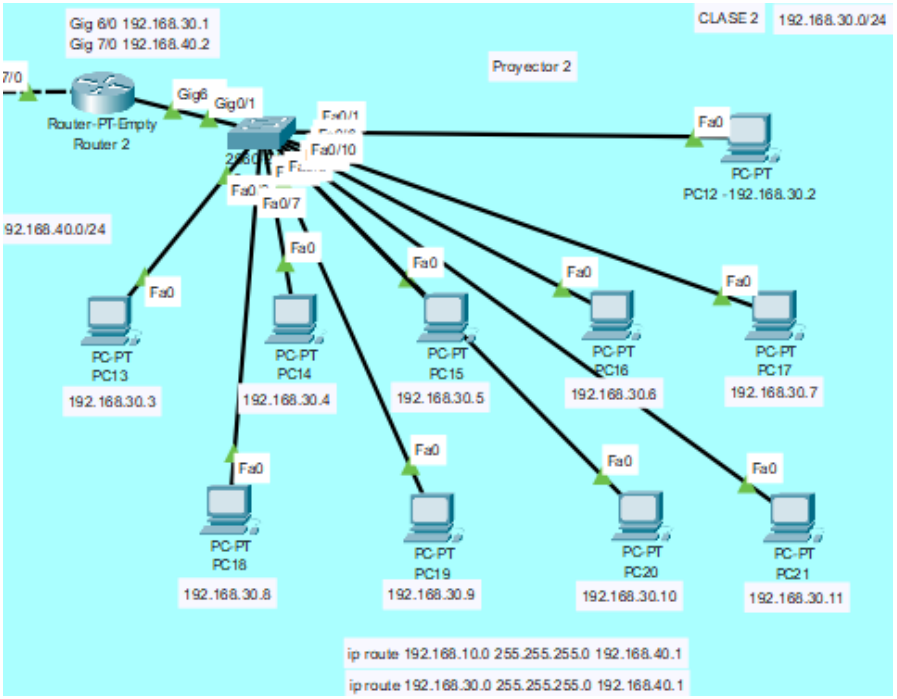


4.2 Aula 2

Tenemos una red de clase C (192.168.30.0/24).

En el router se ha puesto la IP (192.168.30.1)

En los ordenadores se han puesto las IP (192.168.30.2 / 192.168.30.3 / 192.168.30.4 / 192.168.30.5 / 192.168.30.6 / 192.168.30.7 / 192.168.30.8 /192.168.30.9 / 192.168.30.10 / 192.168.30.11)



4.3 Red intermedia

Para permitir la comunicación entre los equipos de Aula 1 y Aula 2, hemos implementado enrutamiento estático entre sus respectivos routers, utilizando una red intermedia (192.168.40.0/24) para conectarlos directamente.

La configuración utilizada ha sido la siguiente:

Router 1:

ip route 192.168.10.0 255.255.255.0 192.168.40.2

ip route 192.168.30.0 255.255.255.0 192.168.40.2

Router 2:

ip route 192.168.10.0 255.255.255.0 192.168.40.1

ip route 192.168.30.0 255.255.255.0 192.168.40.1

Hemos optado por enrutamiento estático en lugar de enrutamiento dinámico debido a que la red está compuesta por tres routers con tres redes independientes (en Administración, Aula 1 y Aula 2). Sólo queríamos permitir la comunicación entre las aulas, manteniendo aislada la red de administración.

Al ser una red pequeña, el número de rutas a configurar es reducido y un protocolo dinámico puede darle una complejidad actualmente no necesaria. En caso de una futura ampliación de la red con más aulas en la escuela u otros servicios, se podría valorar el cambio a un protocolo de routing dinámico.

En nuestro caso, el enrutamiento estático permite el control total y manual de las rutas y limita las configuraciones automáticas hacia la red de administración. También facilita la gestión del tráfico. Nos ha parecido una opción simple, segura y eficiente para la red planteada.

5. Modelo OSI y correspondencia con proyecto

El Modelo OSI (Open Systems Interconnection) es un modelo de referencia desarrollado por la ISO en los años 80 para estandarizar las comunicaciones entre sistemas de redes informáticas. Su función es hacer de guía para que distintos dispositivos y tecnologías puedan comunicarse eficazmente, independientemente de su origen o fabricante.

El modelo divide el proceso de comunicación digital en **siete capas jerárquicas**, cada una tiene una función específica y se comunica con sus capas vecinas. Esto permite simplificar el diseño y diagnóstico de redes y garantiza que todos los sistemas “hablen el mismo idioma”.

5.1 Clasificación de las capas

- **Capas de medios (de la 1 a la 3):** son las físicas, responsables del envío real de datos.

- **Capas de host (de la 4 a la 7):** son las lógicas, responsables del tratamiento y la gestión de la comunicación.

5.2 Las 7 capas del Modelo OSI

- **Capa física (physical)**: encargada de la transmisión de bits (señales eléctricas, ópticas o radioeléctricas) Define conectores, voltajes, velocidades, etc. Los dispositivos principales de esta capa son: cables, hubs, repetidores y módems.

- **Capa de enlace de datos (data link)**: Controla el acceso al medio, la detección de errores y el flujo de datos. Agrupa los bits en tramas y gestiona la transmisión libre de errores entre los nodos conectados. Incluye las subcapas LLC y MAC. Los dispositivos principales de esta capa son: switches, bridges. Tiene protocolos como: Ethernet, Wi-Fi, Bluetooth, etc.

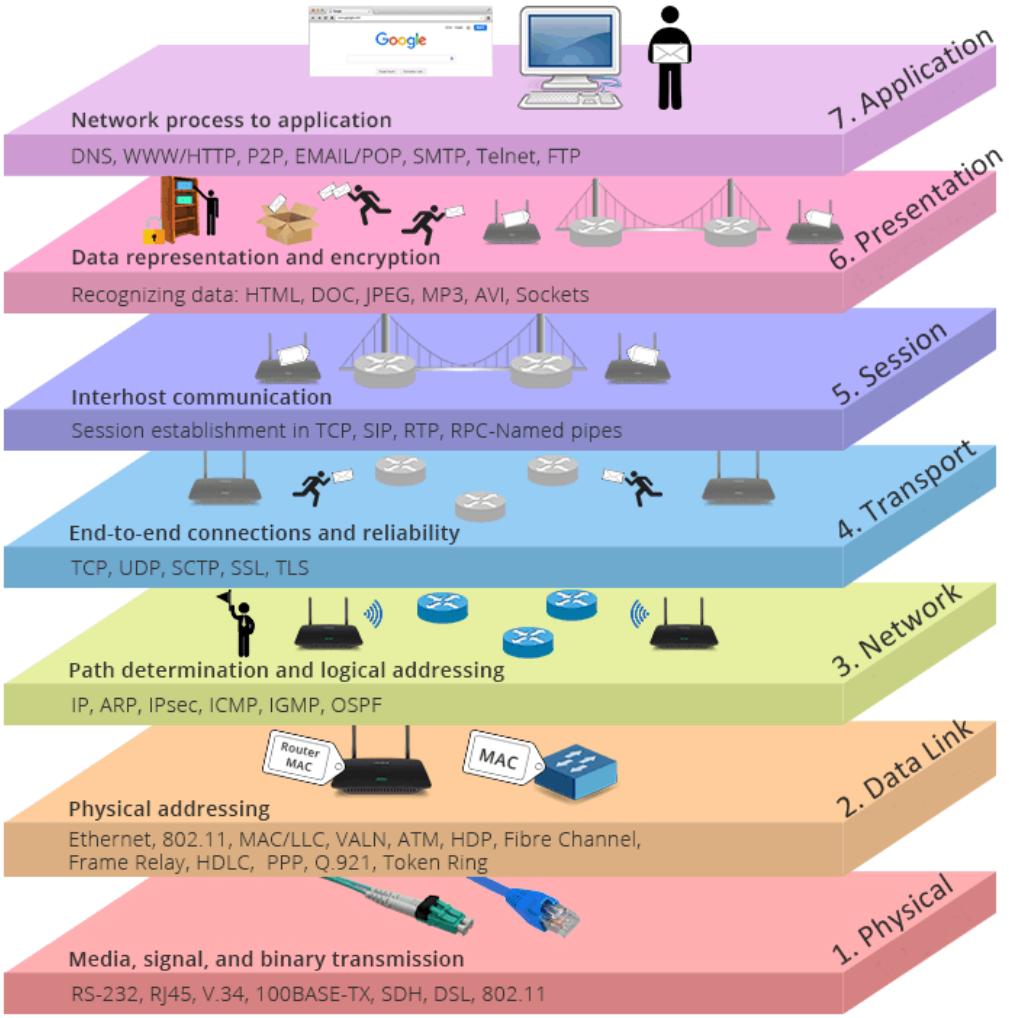
- **Capa de red (network)**: determina la ruta de envío mediante enrutamiento. Usa direcciones IP y gestiona el tráfico entre múltiples redes. Su principal dispositivo es el router. Puede aplicar los protocolos: IP, ICMP, ARP, OSPF y RIP.

- **Capa de transporte (transport)**: Asegura la entrega correcta y completa de los datos (mediante TCP/UDP, puertos), con control de errores y de flujo. Realiza multiplexación (facilita que haya varias aplicaciones en un sólo canal)

- **Capa de sesión (session)**: Establece, mantiene y cierra sesiones entre aplicaciones. Coordina el diálogo entre sistemas y permite la sincronización.

- **Capa de presentación (presentation)**: Traduce, codifica y cifra los datos para que sean entendibles por diferentes sistemas. Gestiona comprensión, formato de datos y cifrado.

- **Capa de aplicación (application)**: es el punto de contacto entre el usuario y la red. Define los protocolos (HTTP, SMTP, FTP, SNMP, etc) usados por aplicaciones como email, web o FTP.



5.3 Capas del modelo OSI aplicadas en el proyecto

- **Capa física:** Hemos utilizado un cableado estructurado Cat6 entre routers, switches y PCs; conectores RJ-45, canaletas, patch panels; e interconexiones físicas entre dispositivos de red. Se ha optado por una red completamente cableada para maximizar la estabilidad y reducir costes.

- **Capa de enlace de datos:** Hemos utilizado un switch por aula y administración, que operan en esta capa para reenviar tramas localmente y direcciones MAC gestionadas por cada interfaz de red.

- **Capa de red:** 3 routers (uno por zona), que operan en esta capa para interconectar redes diferentes y redes independientes de tipo C. Además, hemos utilizado un enrutamiento estático, configurado manualmente en R1 y R2 para permitir comunicación entre aulas, pero sin acceso a la red de administración.

- **Capa de transporte:** Aunque no se configura directamente en nuestro trabajo, esta capa es clave para asegurar que los servicios como el acceso web o el correo funcionen correctamente entre PCs y hacia internet.

- **Capa de sesión:** En nuestro proyecto, esta capa actúa en segundo plano gestionando las sesiones entre clientes y servidores (si se utilizan servicios en la nube o locales).

- **Capa de presentación:** para un posible uso de HTTPS para cifrar comunicaciones y uso de antivirus, que también inspeccionan contenido cifrado o comprimido.

- **Capa de aplicación:** Navegadores web, clientes de correo, plataformas educativas como Moodle, Google Classroom, etc.

6. Seguridad y ciberseguridad

Este apartado pretende contemplar cómo prevenir incidentes en la red así como la formación de los docentes del centro. Para ello vamos a seguir un enfoque basado en la metodología Red Team vs Blue Team.

La seguridad informática en un centro educativo no es sólo una cuestión técnica, también entran en juego la responsabilidad ética y legal. Dado que estos entornos suelen contar con recursos limitados, resulta esencial adoptar soluciones que sean tanto eficaces como asequibles.

Recomendar el uso de cursos gratuitos de INCIBE acerca de ciberseguridad y mantenimiento para los docentes y la administración del centro.

6.1. Medidas de seguridad propuestas

6.1.1 Seguridad de red

- Segmentación de tráfico por aulas: para evitar accesos no autorizados desde los puestos de los alumnos, establecemos una separación física mediante el uso de tres routers independientes.

- Configuración de contraseñas seguras en los dispositivos de red (en los routers)

- Activar el firewall en los routers para limitar el tráfico (entrante y saliente)

- Hacer uso de DNS con control parental (con OpenDNS o CleanBrowsing) para impedir el acceso a contenido no apropiado. Hemos decidido usar DNS con filtro (concretamente el 1.1.1.3 de Cloudflare) ya que nos proporciona seguridad frente a malware y filtra contenido para adultos.

6.1.2 Seguridad en los equipos

- Instalar antivirus gratuitos en todos los equipos (como Windows Defender)

- Valorar si es necesario bloquear los puertos usb para evitar entradas de malware por dispositivos externos o el robo de datos

- Crear cuentas de usuario limitadas para los alumnos y evitar así que se puedan llevar a cabo configuraciones no deseadas en el sistema

6.1.3 Seguridad física

Propondremos guardar bajo llave el equipamiento de red (routers, switches, etc) en un armario. De esta forma se limitará el acceso a aquellos que tengan la llave para hacer comprobaciones y mantenimientos.

6.1.4 Formación y concienciación

- Es bueno ofrecer una formación básica en ciberseguridad a los docentes, centrada en:
    - Reconocer correos o páginas fraudulentas (phishing)
    - Usar contraseñas seguras
    - Manejar con cuidado la información personal del alumnado
- Llevar a cabo una difusión de buenas prácticas para el uso de internet con los niños

6.2. Red Team vs Blue Team: escenarios simulados

Escenario (Red Team)	**Respuesta (Blue Team)**
Alumno intenta acceder desde su PC a la red administrativa	Aislamiento físico mediante router sin rutas entre redes
Intento de conectar un USB infectado	Política de desactivación o restricción de puertos USB
Visita a una página maliciosa	DNS con filtro parental + concienciación de docentes
Contraseñas por defecto en router	Cambio obligatorio por contraseñas robustas
Falta de actualización del antivirus	Activación de actualizaciones automáticas del software de seguridad

7. Mantenimiento y actualizaciones

Una infraestructura segura y funcional necesita también de un mantenimiento regular, especialmente en este contexto donde el acceso técnico será limitado y los recursos deben aprovecharse al máximo.

7.1 Mantenimiento preventivo

Sería recomendable llevar a cabo un mantenimiento preventivo:

- Mensual de los antivirus y el firewall de los equipos
- Trimestral del estado del cableado y los dispositivos de red (funcionamiento y aspecto de routers, switches y cables)
- Semestral del estado de los equipos

7.2. Actualización de software

Tendríamos que prestar especial atención a:

- **Antivirus**:importante activar la actualización automática en cada PC para mantener la base de datos de virus actualizada

- **Sistemas operativos**: habilitar las actualizaciones automáticas en Windows u otros sistemas utilizados

- **Aplicaciones educativas**: verificar al menos una vez por trimestre que los programas estén actualizados y funcionando correctamente

7.3. Copias de seguridad

Recomendaremos al centro educativo que realice copias de seguridad de forma periódica (semanal o cada 15 días) de la información crítica del centro (listados de alumnos, bases de datos, informes, etc).

A ser posible que se realicen en un dispositivo de almacenamiento externo seguro ((pendrive cifrado, disco duro externo)

7.4. Documentación y gestión

Es recomendable que se lleve un registro de los mantenimientos realizados, si se han encontrado incidencias y cómo se han solucionado.

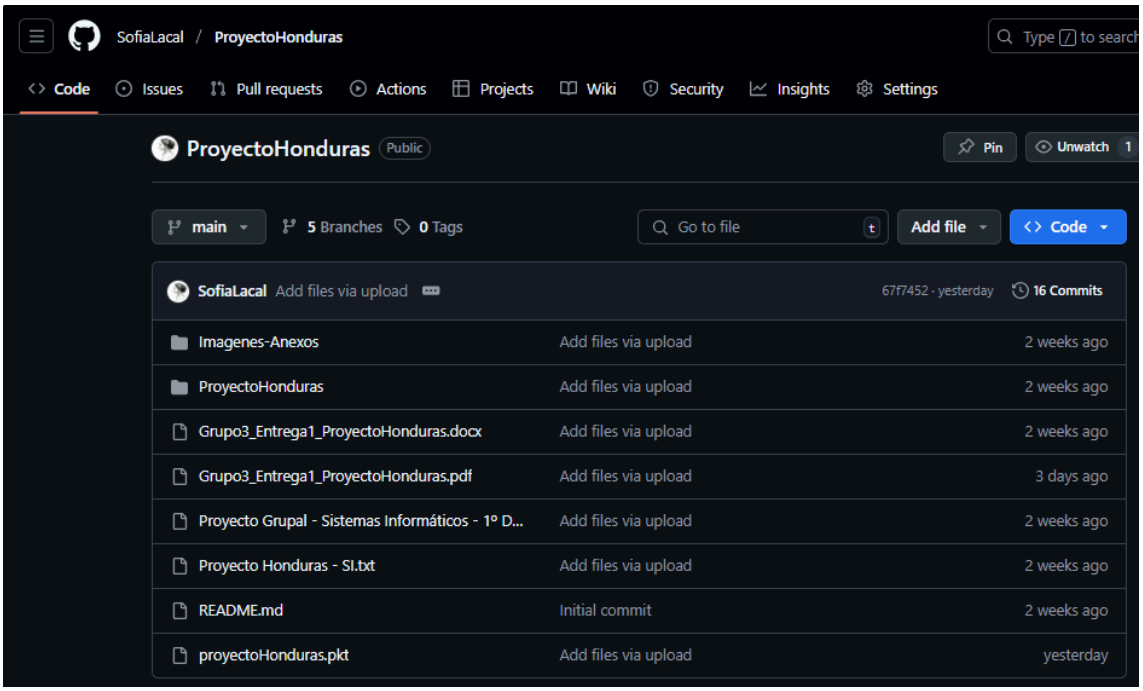
Tener designado un responsable interno para coordinar estas tareas de mantenimiento puede ser crucial para solucionar cualquier incidencia de la manera más eficaz. Puede ser un docente o un técnico que quede vinculado al centro, se tendría que valorar la posibilidad de soporte remoto en caso de necesidad.

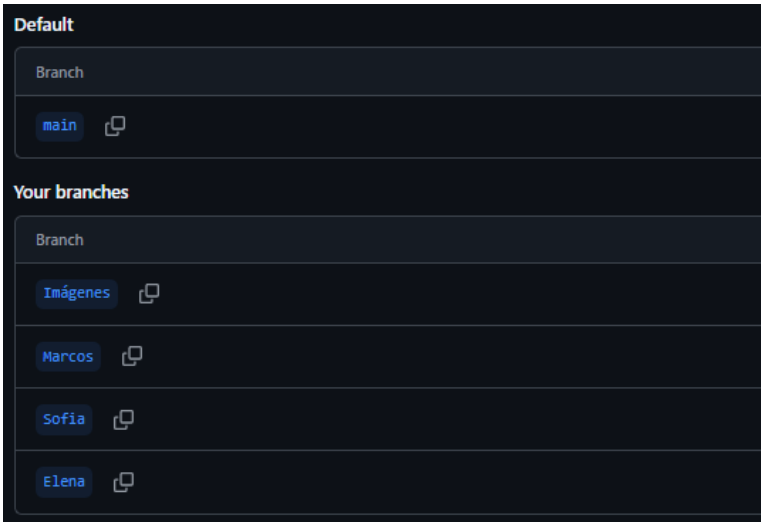
8. Gestión del proyecto (repositorio, herramientas utilizadas)

Para la gestión del proyecto y organización de tareas hemos utilizado GitHub y WhatsApp.

El enlace al repositorio de GitHub es el siguiente: [SofiaLacal/ProyectoHonduras: Proyecto SI 3T]

Para el reparto de tareas y actualización de los contenidos del repositorio hemos creado 5 ramas: una por cada miembro del equipo (Marcos, Elena y Sofía), la rama principal (main) y otra para imágenes.





9. Conclusiones

Al realizar este proyecto, hemos tenido la oportunidad de aplicar de manera práctica los conocimientos adquiridos a lo largo de nuestra formación en Sistemas Informáticos. No solo nos enfrentamos a un desafío técnico, sino también a un contexto realista en el que buscamos generar un impacto positivo en la sociedad, específicamente en comunidades subdesarrolladas. Nuestro enfoque principal ha sido mejorar el acceso a la educación tecnológica para niños, dotándolos de herramientas que les permitirán desarrollarse en un mundo cada vez más digitalizado.

Nuestro objetivo a largo plazo es seguir ampliando esta infraestructura, construyendo más aulas equipadas con ordenadores, para así poder llegar a un mayor número de niños. Además, si los resultados obtenidos son positivos y se cuenta con los recursos necesarios, no descartamos la posibilidad de abrir nuevos centros educativos en otras regiones del país, con el fin de seguir promoviendo la alfabetización digital y reducir la brecha tecnológica.

En cuanto al trabajo en equipo, la organización ha sido un factor clave para el éxito del proyecto. La correcta coordinación entre todos los integrantes nos ha permitido avanzar de manera eficiente, resolviendo problemas de forma colaborativa y optimizando los tiempos de desarrollo. Esta experiencia también nos ha enseñado la importancia de la comunicación, la planificación y la responsabilidad compartida dentro de un entorno profesional.

10. Bibliografía

- Equipo editorial, Etecé. (2023, 19 noviembre). *Modelo OSI - Concepto, cómo funciona, para qué sirve y capas*. Concepto. https://concepto.de/modelo-osi/

- Walton, A. (2024, 11 diciembre). ▷ *Qué es el Modelo OSI: Capas y Explicación » Redes*. CCNA Desde Cero. https://ccnadesdecero.es/que-es-modelo-osi/

- Admin. (s. f.-a). *Espacio Honduras*. EspacioHonduras. https://www.espaciohonduras.net/ (*La educación en Honduras: avances y retos actuales*)

- Nueva, R. C. (s. f.). *La Educación en Honduras – Focolares Ciudad Nueva*. https://www.focolaresciudadnueva.com/inicio/la-educacion-en-honduras/

- Fernández, A. J. M. (2017, 9 junio). *ACOES construye una nueva escuela en Honduras para 1000 niños*. Acoes. https://acoes.org/acoes-construye-una-nueva-escuela-en-honduras-para-1000-ninos/

- *El Observatorio Estatal de la Convivencia escolar publica unas recomendaciones para trabajar la ciberconvivencia en los centros educativos*. (s. f.). SGCTIE | Ministerio de Educación, Formación Profesional y Deportes. https://www.educacionfpydeportes.gob.es/mc/sgctie/comunicacion/blog/2022/diciembre2022/ciberconvivencia.html

- *INCIBE | INCIBE*. (s. f.). https://www.incibe.es/