INSTITUTO NEBRIJA | Formación Profesional

PORTADA

"Red Solidaria: Diseño y despliegue de un aula TIC para la infancia en Honduras"

Proyecto final – sistemas informáticos

- **Nombre del alumno o de la alumna:**
- Daniel Arévalo
- Daniel Sanz
- Rui Qian
- Guillermo Pinilla
- Scrum Master: Rui Qian

Curso académico: 1º DAM

Tutora/Tutor del proyecto: Carmelo

ÍNDICE PAGINADO

INTRODUCCIÓN

Escenario del proyecto Una ONG ha contactado con tu equipo para diseñar un aula de formación digital para niños y niñas en una zona rural de Honduras. El objetivo es dotar de infraestructura y recursos digitales a una escuela con limitaciones económicas ytecnológicas. Como estudiantes del ciclo superior de DAM, deberéis aplicar vuestros conocimientos sobre redes, sistemas, ciberseguridad y trabajo colaborativo para llevar a cabo este proyecto.

Github repositorio:

https://github.com/Theshy520-spec/Proyecto-sistema.github.io.git

Entregable:

Memoria del proyecto en PDF (mínimo 50 páginas) con los siguientes apartados:

- Introducción y contexto
- Análisis de necesidades
- Diseño de red (lógico y físico)
- Subnetting y direccionamiento
- Configuración de dispositivos (routers, switches, puntos de acceso)
- Correspondencia con el modelo OSI
- Seguridad y ciberseguridad
- Mantenimiento y actualizaciones
- Gestión del proyecto (Scrum, Kanban)
- Repositorio GitHub
- Conclusiones
- Anexos (capturas, simulaciones)

OBJETIVOS

1. ● Aplicar conocimientos de redes, direccionamiento IP, VLANs, switching y routing.
2. ● Documentar y aplicar el modelo OSI en un entorno realista.
3. ● Diseñar una red segura y sostenible.
4. ● Simular la red con herramientas como Cisco Packet Tracer o GNS3.
5. ● Colaborar en equipo usando metodología Scrum y gestión visual con Kanban.
6. ● Publicar el trabajo en GitHub, fomentando la cultura open source.
7. ●Vinculación con la LOMLOE Resultados de aprendizaje (RA) y criterios de evaluación (CE):

RA	Descripción	Criterios vinculados
RA1	Reconoce la estructura de redes	CE1.1, CE1.3
RA2	Instala y configura sistemas operativos en red	CE2.2, CE2.4
RA3	Aplica procedimientos de conexión a redes	CE3.1, CE3.3
RA4	Implementa medidas de seguridad	CE4.1, CE4.2
RA5	Gestiona la documentación técnica	CE5.2, CE5.3

OBJETIVO GENERAL:

Alfabetización digital: Iniciar a los alumnos en el uso básico del ordenador y herramientas ofimáticas.

Aprendizaje interactivo: Usar recursos educativos multimedia (vídeos, juegos educativos, simuladores).

Acceso a contenidos en línea: Fomentar la investigación en Internet bajo supervisión.

Formación docente: Proporcionar herramientas para que el profesorado integre TIC en sus clases.

Creación de contenidos: Permitir que estudiantes y docentes creen textos, presentaciones y recursos educativos simples.

Mantenimiento autónomo: Permitir que el centro pueda operar el sistema con mínima intervención técnica externa.

OBJETIVOS ESPECÍFICOS:

Análisis de necesidades:

Infraestructura: La escuela cuenta con energía eléctrica limitada, espacios reducidos y sin acceso a Internet confiable.

Conectividad: No hay red local ni conexión a Internet estable. Se contempla el uso de conexión satelital o redes móviles.

Equipamiento: No hay computadoras disponibles actualmente. Se prevé dotar el aula con al menos 10 equipos básicos (ordenadores o portátiles reacondicionados).

Usuarios: Niños y niñas de entre 8 y 14 años, así como el personal docente, con conocimientos tecnológicos limitados.

Soporte técnico: No hay personal técnico especializado en la zona, por lo que se prioriza el uso de tecnologías fáciles de mantener.

Necesidades identificadas:

1. Establecer una red local segura (LAN).
2. Acceso a Internet, incluso con conectividad intermitente.
3. Equipos informáticos con software educativo y herramientas ofimáticas.
4. Sistema operativo libre o de bajo coste (Linux, por ejemplo).
5. Formación básica en competencias TIC para alumnado y profesorado.
6. Políticas de seguridad y control de contenidos.

Tareas principales a implementar:

Ofimática básica: uso de procesador de texto, presentaciones y hojas de cálculo.

Navegación web educativa: uso de navegadores con acceso controlado a plataformas educativas.

Aplicaciones interactivas offline: juegos educativos y software de aprendizaje sin conexión.

Creación de recursos educativos simples: audios, presentaciones, imágenes o infografías.

Gestión de archivos y almacenamiento: organización de trabajos, tareas y proyectos en carpetas locales.

Capacitación TIC básica para docentes: correo electrónico, creación de materiales, control de aulas digitales.

DESARROLLO

Seguridad y ciberseguridad

1. Infraestructura Física

***Red Team (Vulnerabilidades)*:**

- Acceso físico fácil a los equipos (robo o manipulación).
- Equipos sin protección contra sobrecargas o apagones.
- No hay cerraduras o control de acceso físico.

***Blue Team (Medidas de Corrección)*:**

- Guardar equipos en muebles con cerradura.
- Uso de regletas con protección contra sobretensiones.
- Ubicar el router y el switch en una caja cerrada o armario.
- Desconectar o asegurar físicamente puertos USB si no se necesitan

2.Red Local (LAN)

***Red Team (Vulnerabilidades)*:**

- Switch sin protección o configuración por defecto.
- Todos los dispositivos en la misma red (sin segmentación).
- Posibilidad de ataques tipo ARP spoofing o sniffing.

***Blue Team (Medidas de Corrección)*:**

- Configurar VLANs para separar tráfico de alumnos y docentes.
- Cambiar contraseñas predeterminadas del switch.
- Aplicar reglas de firewall en dispositivos (por ejemplo, en Raspberry Pi o router).
- Monitorizar el tráfico básico (usando herramientas como ntopng o Wireshark en auditorías).

3. Acceso a Internet

***Red Team (Vulnerabilidades)*:**

- Acceso sin control al router (configuración abierta).
- DNS no filtrados, posibilidad de phishing.
- Ausencia de VPN o túneles seguros.

***Blue Team (Medidas de Corrección)*:**

- Cambiar contraseña de administrador del router.
- Activar control parental y firewall en el router.
- Usar **DNS filtrado** como CleanBrowsing o AdGuard DNS.
- Enlace de acceso satelital o móvil con cifrado (VPN si es posible).

4.Software

Red Team (Vulnerabilidades):

- Utilizar sistemas operativos o software desactualizado aumenta el riesgo de vulnerabilidades sin parches de seguridad.
- No instalar software antivirus deja los equipos expuestos a malware.
- No configurar firewalls en los equipos permite que los atacantes accedan a ellos desde la red.

Blue Team (Medidas de Corrección):

- Instalar sistemas operativos open-source como linux para mantener actualizado el SO
- Instalar antivirus gratis como Avast Free para tener un mínimo de seguridad
- Activar el firewall integrado en el sistema operativo de cada equipo.
- Configurar reglas de firewall para permitir solo el tráfico necesario y bloquear el resto.

CONCLUSIONES

6. LÍNEAS DE INVESTIGACIÓN FUTURAS

(No son obligatorios, pero pueden aparecer)

7. BIBLIOGRAFÍA

8. ANEXOS

9. OTROS PUNTOS

(No son obligatorios, pero pueden aparecer)

- Aportaciones personales
- Retos profesionales
- Restos personales
- Agradecimientos