UAX FP
Universidad
Alfonso X el Sabio

Integración de sistemas de control de acceso a redes (NAC) con inteligencia artificial para la detección proactiva de amenazas

ASIR / Presencial

Vladimir Edgar Carpio Morales

Tutor del TFG

UAX FP
Universidad
Alfonso X el Sabio

DEDICATORIA (OPCIONAL)

ÍNDICES

De contenido, tablas e ilustraciones. Se recomienda realizarlos de manera automática.

ABSTRACT

Con este proyecto se pretende integrar sistemas de Control de Acceso a la Red (NAC) con inteligencia artificial. La IA analizará los datos de acceso en tiempo real, reaccionará y se adaptará ante amenazas emergentes. A su vez, detectará posibles comportamientos anómalos, modificando las reglas de política de seguridad.

Para la integración, se utilizan las APIs de los sistemas de Control de Acceso a la Red (NAC). La diferenciación respecto a las soluciones tradicionales radica en la capacidad de modificar dinámicamente las políticas de seguridad, permitiendo una respuesta automatizada.

This project aims to integrate Network Access Control (NAC) systems with artificial intelligence. The AI will analyze access data in real time, react, and adapt to emerging threats. Additionally, it will detect anomalous behaviors and modify security policy rules accordingly.

For the integration, the APIs of NAC systems will be used. The key differentiation from traditional solutions lies in the ability to dynamically modify security policies, enabling an automated response.

JUSTIFICACIÓN DEL PROYECTO

Motivación principal del proyecto

A medida que crece la cantidad de dispositivos conectados a la red, la gestión del acceso a redes corporativas se vuelve más compleja. Actualmente las soluciones de Control de Acceso a la Red (NAC) cuentan con políticas de acceso basadas en reglas estáticas que limitan su capacidad en adaptarse a amenazas emergentes.

Este proyecto solventa la necesidad de implementar una solución que utilice inteligencia artificial que analizara patrones de comportamiento, detección de anomalías en tiempo real y la solución que actúe de forma dinámica modificando las políticas de acceso.

Las principales soluciones de Control de Acceso a la Red (NAC) actuales que existen en el mercado son Cisco ISE, Aruba ClearPass y FortiNAC, las cuales permiten la gestión de accesos y segmentación de redes. Sin embargo, estas soluciones dependen no cuentan con un aprendizaje adaptativo basado en IA.

Con respecto a mi proyecto existen soluciones similares en el mercado que utilizan inteligencia artificial para el análisis pero con enfoques diferentes:

Característica	Aruba AI Insights	Cisco AI Endpoint Analytics	Fortinet FortiAI	Aportación del Proyecto Propuesto
Análisis con IA	Detecta anomalías en redes WiFi.	Identifica y clasifica dispositivos en la red.	Analiza y detecta malware y anomalías.	Aprende patrones de comportamiento en la red y detecta amenazas.
Modificación de políticas NAC	No modifica políticas.	No modifica políticas.	No modifica accesos.	Modifica dinámicamente las reglas de acceso según el análisis de IA. Aplica acciones correctivas

Compatibilidad con NACs	Solo Aruba.	Solo Cisco.	Independiente de NACs.	Open-source y compatible con múltiples NACs.

Marcos normativos y legales:

Proyecto debe cumplir con las siguientes normativas de seguridad y protección de datos:

- Reglamento General de Protección de Datos (GDPR) para garantizar el cumplimiento de la privacidad y protección de datos personales.
- Normativas ISO 27001 las cuales implementan normativas sobre las buenas prácticas de seguridad en la gestión de la información.
- Cifrado y copias de seguridad, para los datos manejados por el sistema sean encriptados y se establecerán mecanismos de respaldo para evitar pérdidas o accesos no autorizados.

INTRODUCCIÓN

Problemas que resuelve

- El proyecto tiene como objetivo mejorar la seguridad del acceso en redes corporativas mediante el uso de inteligencia artificial. Los principales problemas que resuelve son:
- Las reglas de acceso de los sistemas de Control de Acceso a la Red (NAC) actuales son rígidas y no pueden adaptarse automáticamente a nuevas amenazas y requieren de ajustes manuales.
- Tiempos de respuesta a incidentes de seguridad lentos, debido a que los cambios en las políticas deben hacerse manualmente.
- La dificultad en la detección de comportamientos anómalos y amenazas emergentes, en el acceso a la red sin una herramienta que analice patrones en tiempo real.

Requisitos generales del cliente

Desde la perspectiva del cliente, la solución debe cumplir con los siguientes requisitos:

- Análisis de datos en tiempo real provenientes de los sistemas NAC.
- Detección de anomalías.
- Modificación dinámica de políticas de acceso basadas en el análisis de la IA.
- Generación de alertas automáticas sobre amenazas detectadas.
- Presenta listados y rankings de riesgo a través de un dashboard que el sistema clasifica y ordena los dispositivos o eventos.

OBJETIVOS

Listado de objetivos que se plantean resolver. Requisitos.

Se debe presentar un **RFTP** inicial para acompañar a la propuesta.

R – Requisitos: Lo que debe hacer el programa expresado en lenguaje coloquial.

F – Funciones: Desglose de las características asociadas o subrequisitos de cada requisito. Expresado en leguaje técnico.

T – Tareas asociadas a cada funcionalidad. Deben describir completamente su alcance.

P – Pruebas. Demostración o prueba planificada para cumplir cada tarea.

Ejemplo:

R01 – El programa debe solo debe permitir entrar a las personas que han dado sus datos.

R01F01 – El usuario debe registrarse en el sistema.

R01F01T01 – Crear una tabla usuarios en la base de datos.

R01F01T01P01 – Introducir un dato de prueba.

R01F01T02 - Diseñar un html que permita rellenar los campos de registro.

R01F01T02P01 – Visualizar la pantalla login.html

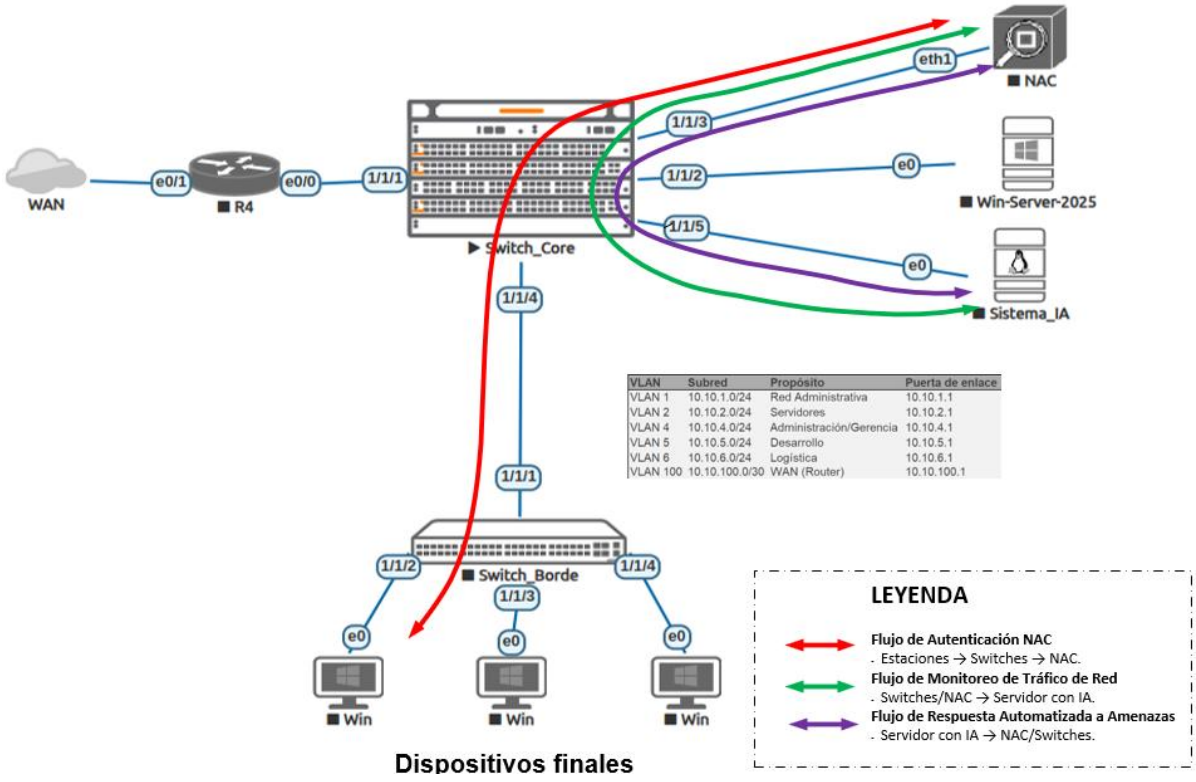
...

R01F02 - El usuario debe introducir nombre y clave para poder entrar

...

DESCRIPCIÓN

Arquitectura de la solución.



VLAN	Subred	Propósito	Puerta de enlace
VLAN 1	10.10.1.0/24	Red Administrativa	10.10.1.1
VLAN 2	10.10.2.0/24	Servidores	10.10.2.1
VLAN 4	10.10.4.0/24	Administración/Gerencia	10.10.4.1
VLAN 5	10.10.5.0/24	Desarrollo	10.10.5.1
VLAN 6	10.10.6.0/24	Logística	10.10.6.1
VLAN 100	10.10.100.0/30	WAN (Router)	10.10.100.1

Diagrama de Arquitectura de la Solución:

- **WAN**
  - **Función:** Conectividad a redes externas, como Internet.

- **Router R4 (IP: 10.10.100.2):**
  - **Función:** Enruta el tráfico entre la red local y la WAN, y realiza NAT.

- **Switch Core (IP: 10.10.100.1):**
  - **Función:** Gestiona el tráfico interno de la red, administra las VLANs y enruta el tráfico hacia la WAN.

- **NAC (IP: 10.10.2.100):**
  - **Función:** Gestiona autenticación, políticas NAC, controla el acceso a la red, autentica dispositivos y aplica políticas de seguridad, y envía datos al servidor con IA.

- **Windows Server (IP: 10.10.2.10):**
  - **Función:** Es el servidor DHCP para las VLANs, servidor DNS, servidor AD (Active Directory) y servidor de certificados, políticas de GPO, grupos, usuarios del dominio y se integra con el NAC.

- **Sistema IA** (Ubuntu Server 24.04, IP: 10.10.2.20).
  - **Función:** Aloja la inteligencia artificial (IA), gestiona conexiones con la API de NAC vía API REST, analiza resultados y devuelve respuestas.

- **Switch Borde (IP: 10.10.100.1):**
  - **Función:** Punto de conexión de los dispositivos finales (estaciones de trabajo, dispositivos IoT, cámaras, teléfonos IP, etc.) gestiona el tráfico interno de la red y transporta vlans.

- **Dispositivos finales** (estaciones de trabajo, dispositivos IoT, cámaras, teléfonos IP, etc.)
  - **Función:** Acceder a la red.

Casos de uso. Incluye diagrama y tabla con:

- Descripción.
- Precondiciones
- Postcondiciones
- Datos de entrada
- Datos de salida
- Tablas
- Clases
- Interfaces

Ejemplo:

Caso de uso: Pedir ayuda

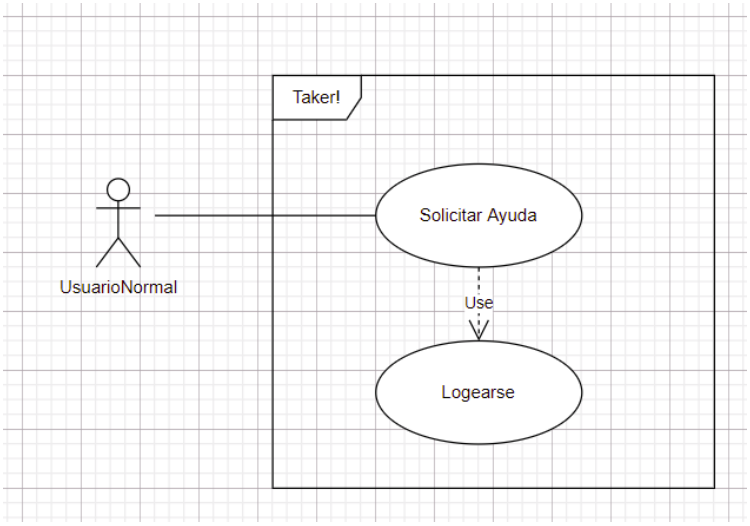


Ilustración 1: caso de uso Pedir Ayuda

DESCRIPCIÓN: Solicitar ayuda al especialista	
PRECONDICIONES: Usuario logado	**POSTCONDICIONES**: Solicitud en espera Se inicia el chat
DATOS ENTRADA Nombre especialista	**DATOS SALIDA** Nombre especialista

Id usuario Id especialista	Id usuario Id especialista Idchat Valoración fecha/hora
TABLAS: USUARIOS CHAT	**CLASES**: ESPECIALISTA.PHP USUARIO NORMAL.PHP CHAT.PHP
INTERFACES: PERFILUSUARIO.HTML CHAT.HTML	

Tabla 1: caso de uso Pedir Ayuda

DISEÑOS (Los que procedan según el tipo de proyecto)

Diagrama de clases.

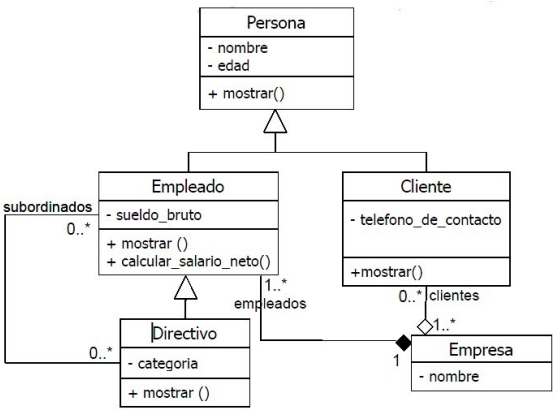


Diagrama E/R (Entidad - Relación)

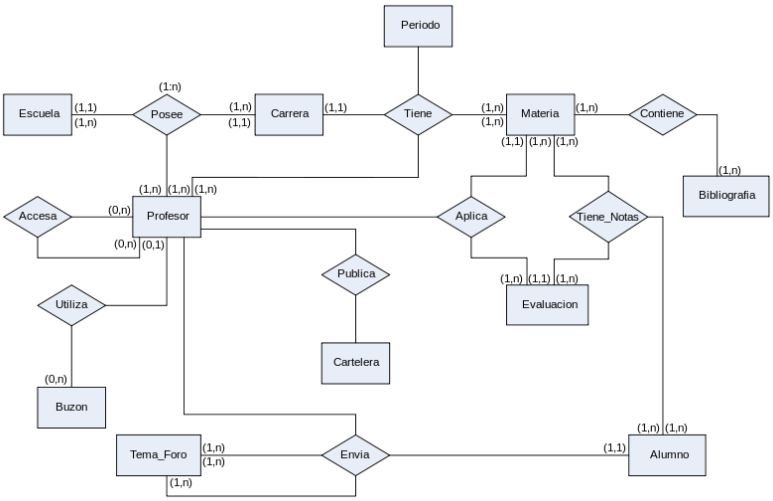


Diagrama de la base de datos. Con detalle de campos.

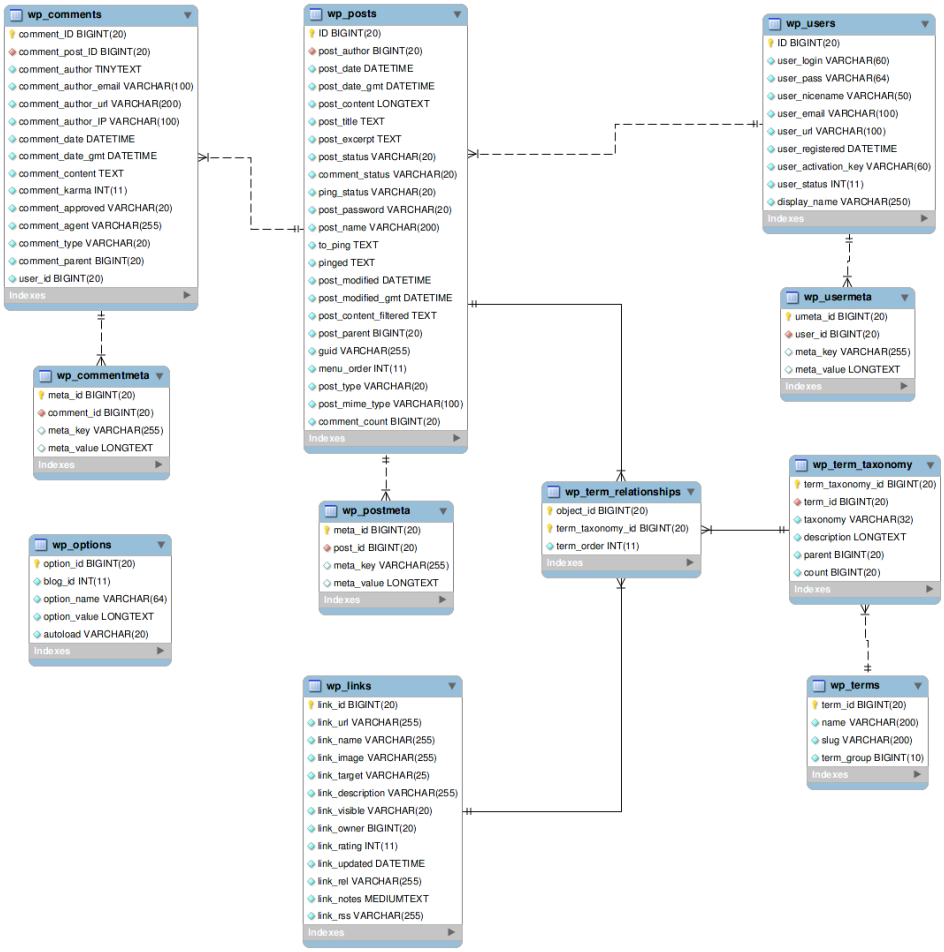
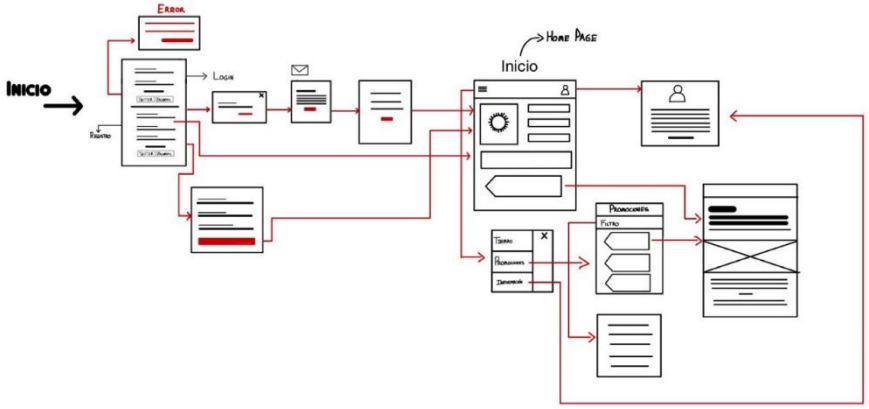


Diagrama de flujo de navegación. Esquemático. Debe incluirse en la propuesta.



Interfaces. Interesa ver la solución en diferentes tamaños o dispositivos.

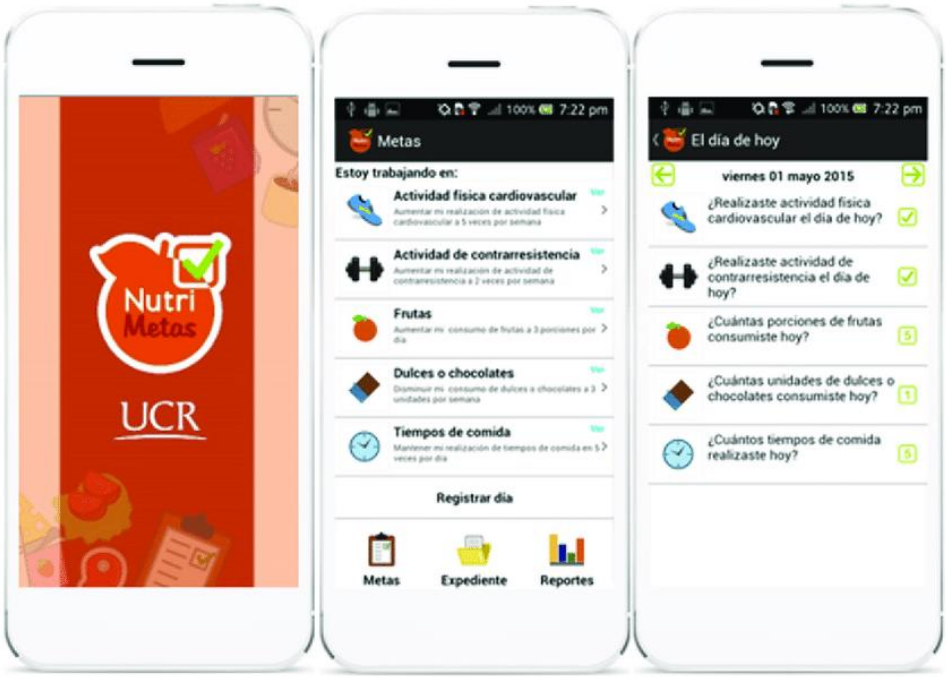
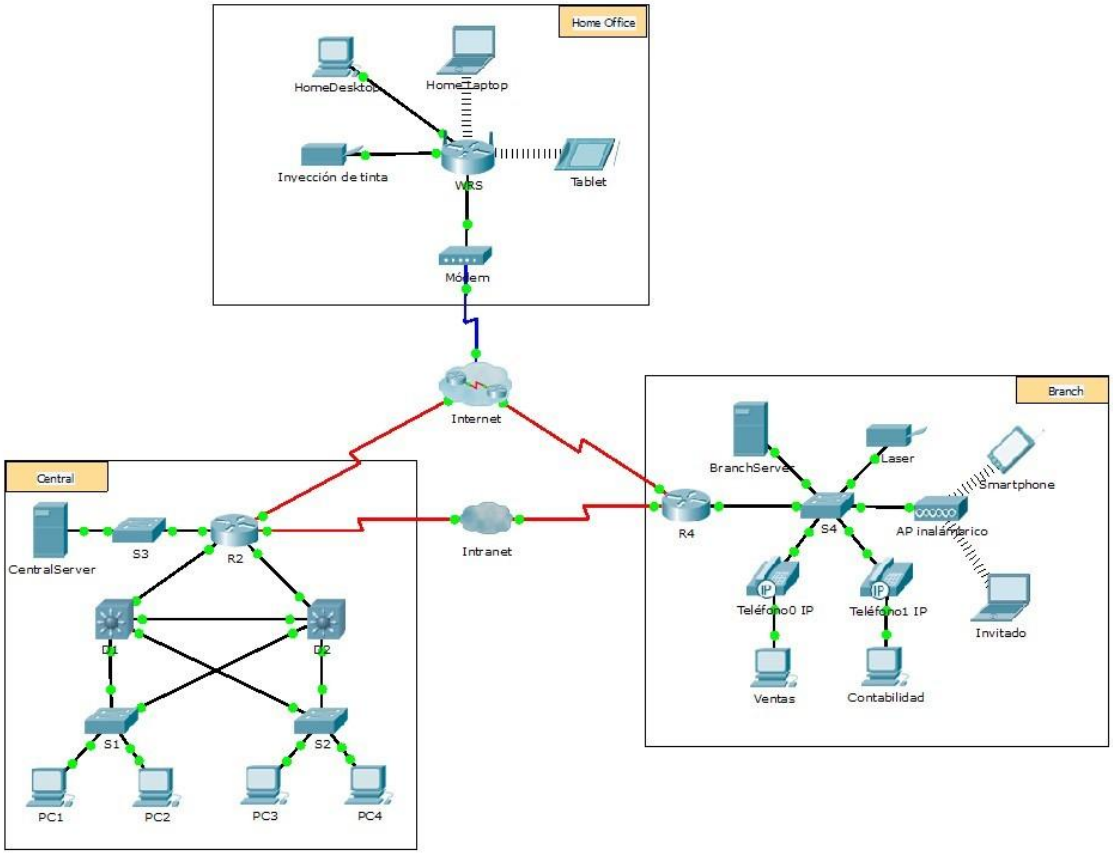


Diagrama de red.



TECNOLOGÍA

Las tecnologías y herramientas utilizadas para este proyecto. Por ejemplo:

Java.
Descripción de la herramienta.
Descripción del uso de la herramienta en el proyecto.

METODOLOGÍA

Metodología usada y justificación de la misma.

Se presentarán dos planificaciones, una valoración inicial y previa a la implementación del proyecto y otra final con el tiempo real dedicado a cada parte del RFTP. Se analizarán las desviaciones.
El tiempo se expresará en horas. Debe existir una totalización final.

Diagrama de Gantt (Microsoft Project o similar). Real, contrastable con GIT, RFTP y Casos de uso.

ID	Task	Start	Finish	Duration	Progress	Priority	Resources
1	**Analysis**	**2018-10-01 08:00**	**2018-10-10 16:00**	**8 d**	**98.9%**	1	**Rita; William; Tyler; Wenger; Steve**
2	Requirement Meetings	2018-10-01 08:00	2018-10-04 16:00	4 d	100%	1	Rita; William
3	Communication with Stakeholders	2018-10-05 08:00	2018-10-08 16:00	2 d	95.5%	3	Rita; William; Tyler; Wenger; Steve
4	Document Current System	2018-10-09 08:00	2018-10-10 16:00	2 d	100%	3	William
5	Analysis Finished	2018-10-10 08:00	2018-10-10 16:00	1 d	0%	1	
6	**Design**	**2018-10-11 08:00**	**2018-11-05 16:00**	**18 d**	**14.9%**	2	**Steve; Yvette; Zoe**
7	Design Database	2018-10-11 08:00	2018-10-17 16:00	5 d	62.4%	1	Steve
8	Software Design	2018-10-18 08:00	2018-10-25 16:00	6 d	0%	2	Yvette
9	Interface Design	2018-10-26 08:00	2018-10-30 16:00	3 d	0%	4	Zoe
10	Create Design Specifications	2018-10-26 08:00	2018-11-05 16:00	7 d	0%	2	Steve
11	Design Finished	2018-11-05 08:00	2018-11-05 16:00	1 d	0%	2	
12	**Development**	**2018-10-11 08:00**	**2018-11-09 16:00**	**22 d**	**22.5%**	3	**Tyler; Wenger**
13	Develop System Module	2018-10-11 08:00	2018-10-26 16:00	12 d	41.2%	1	Tyler; Wenger
14	Integrate System Module	2018-10-29 08:00	2018-11-06 16:00	7 d	0%	1	Tyler
15	Perform Initial Testing	2018-11-07 08:00	2018-11-09 16:00	3 d	0%	2	Wenger
16	Development Finished	2018-11-09 08:00	2018-11-09 16:00	1 d	0%	3	
17	**Testing**	**2018-10-29 08:00**	**2018-11-20 16:00**	**17 d**	**29.4%**	4	**Vicky; Mike**
18	Perform System Testing	2018-10-29 08:00	2018-11-07 16:00	8 d	62.5%	3	Vicky
19	Document Issues Found	2018-11-08 08:00	2018-11-15 16:00	6 d	0%	4	Mike
20	Correct Issues Found	2018-11-16 08:00	2018-11-20 16:00	3 d	0%	1	Mike
21	Testing Finished	2018-11-20 08:00	2018-11-20 16:00	1 d	0%	3	
22	**Implementation**	**2018-11-20 08:00**	**2018-12-10 16:00**	**15 d**	**0%**	1	**Tyler; Mike**
23	On-Site Installation	2018-11-20 08:00	2018-11-20 16:00	1 d	0%	5	Tyler
24	Support Plan for the System	2018-11-20 08:00	2018-12-10 16:00	15 d	0%	4	Mike
25	**Completion**	**2018-11-21 08:00**	**2018-12-03 16:00**	**9 d**	**0%**	2	**Rita; William**
26	System Maintenance	2018-11-21 08:00	2018-12-03 16:00	9 d	0%	3	Rita
27	Evaluation	2018-11-21 08:00	2018-12-03 16:00	9 d	0%	1	William

Presupuesto. Con detalle de horas, indispensable si se realiza en grupo, y coste total del desarrollo por cada requisito.

README y GIT.

TRABAJOS FUTUROS

Trabajos de ampliación y mejora proyectados.

CONCLUSIONES

Conclusión profesional del proyecto.

REFERENCIAS

Según las normas APA.

Cada referencia se acompañará de un texto descriptivo con el apartado del proyecto asociado.

Formato:

Autor, A. A. (Año de publicación). Título de la página. Recuperado de URL

Ejemplo:

Aplicado en la investigación del tema de la web.

Smith, J. (2023). La importancia del reciclaje en la conservación del medio ambiente. Recuperado de https://www.ejemplodepagina.com/

Otro ejemplo:

Aplicado para realizar las vistas de la base de datos.

Oracle Corporation. (s. f.). Oracle Database 19c Documentation. Recuperado de https://docs.oracle.com/en/database/oracle/oracle-database/index.html