UAX FP
Universidad
Alfonso X el Sabio

Sistema Centralizado de Domótica Y Almacenamiento en Red

ASIR / Presencial

Daniel Alejandro Troche Valdivia

Tutor del TFG

DEDICATORIA (OPCIONAL)

ÍNDICES

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

ABSTRACT

Este TFG presenta la planificación y ejecución de una red SOHO (Small Office Home Office) en la cual se integrará una centralita destinada a la administración de los dispositivos inteligentes del hogar junto con servicios de almacenamiento en red (NAS). Estos servicios serán accesibles mediante servicios de VPN y Proxy lo que permitirá el acceso a la red y el almacenamiento desde una red externa, y el bloqueo de contenido no solicitado y anuncios.

This TFG presents the planning and the execution of a SOHO (Small Office Home Office) network, in which it will be integrating a central hub for the management of smart home devices along network-attached storage (NAS) services. These services will be accessible through VPN (Virtual Private Network) and Proxy solutions, allowing remote access to the network and storage from an external network while enabling the blocking of undesirable content and announcements.

JUSTIFICACIÓN DEL PROYECTO

Actualmente existe un crecimiento de la digitalización de los hogares y oficinas provocando la necesidad de soluciones de automatización, seguridad, almacenamiento y otros diversos servicios orientados a cubrir esta demanda. Estos servicios ofrecidos por compañías de terceros presentan preocupaciones por la privacidad de los datos de sus usuarios, una falta de transparencia en el procesamiento de los mismo y una dependencia total de sus nubes provocando que sus sistemas queden inutilizables en caso de perdida de conexión a internet.

Este proyecto presenta una alternativa local, donde el usuario podrá interconectar y controlar sus dispositivos, acceder de manera remota a la red de forma segura y almacenar sus datos en su propia infraestructura siendo independientes de servicios y nubes de terceros donde su privacidad puede estar comprometida.

Aspectos legales para tener en cuenta:

- Anexo V del reglamento de Infraestructuras Comunes de Telecomunicaciones (ICT) (R.D. 345/2011): Es de aplicación voluntaria, este define lo que es un Hogar Digital, establece sus funcionalidades y niveles para clasificar un Hogar Digital en categorías: básico, medio y superior.[1]
- La Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, regula la manera en que los datos serán almacenados y tratados.[2]

Aspectos de Seguridad:

- Al aumentar la cantidad de dispositivos conectados a la red aumenta el riesgo de ataque por lo cual es necesario aumentar la cantidad de medidas

[1] BOE-A-2011-5834 Real Decreto 346/2011, de 11 de marzo, por el que se aprueba el Reglamento regulador de las infraestructuras comunes de telecomunicaciones para el acceso a los servicios de telecomunicación en el interior de las edificaciones.
[2] BOE-A-2018-16673 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

de seguridad como implementación de autentificación multifactor, firewalls y actualizaciones de firmware.[3]

Actualmente se encuentran disponible distintas soluciones comerciales para la domótica y el almacenamiento en red, aunque no suelen combinar estos dos servicios y pocas ofrecen un servicio sin la necesidad de conectarse a sus servidores.

Entre los sistemas de domótica existentes se encuentran:

- Google Home, Amazon Alexa, Apple HomePod, entre otros: Estos servicios dependen de los servidores de sus respectivas compañías requiriendo de conexión a internet para su normal funcionamiento.
- Home Assistant: Es una plataforma de código abierto que no depende de internet para su funcionamiento, permite controlar diversos dispositivos inteligentes.[4]

Sistemas de almacenamiento en red:

- Synology / QNAP: Son soluciones comerciales que incorporan servicios de VPN, pero dependen de su propio hardware y presentan un precio elevado.
- TrueNAS y OpenMediaVautl: Son alternativas de código abierto a Synology y QNAP, que permiten la creación de sistemas NAS.

Sistemas de acceso remoto:

- Existen diversas VPN comerciales como NordVPN, ExpressVPN, ProtonVPN, que permiten conexiones seguras, pero en dependencia de sus servidores.
- OpenVP: Son soluciones más seguras, privadas y autogestionadas.

[3] BOE-A-2018-12257 Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
[4] Home Assistant

Funcionalidades	TFG	Soluciones Comerciales	Soluciones Open Source
Control Total	Sí	No	Sí
Integración entre Domótica y NAS	Sí	No	No
Acceso Remoto sin terceros	Sí	No	Sí
Complejidad de la configuración.	Media	Baja	Media - Alta

INTRODUCCIÓN

Este proyecto propone la implementación de una red local con las siguientes funciones:

- Control y automatización de dispositivos inteligentes: Luces, Termostatos, Sensores, Cámaras de Seguridad, Puertas y electrodomésticos inteligentes.
- Almacenamiento en Red (NAS): Sistema de almacenamiento en red para copias de seguridad, archivos multimedia y otros tipos de archivos accesibles desde la red local o desde internet a través de la VPN.
- Acceso seguro con VPN: Permite a los usuarios acceder de forma segura para acceder a la red domótica y al NAS desde fuera de la red local.
- Filtrado de Contenido y Bloqueo de Anuncios con Proxy. Permite el bloqueo de anuncio y de contenido no deseado, permite una navegación más segura.

Estas funciones permiten una mayor seguridad, privacidad y permiten un control total de todos los sistemas. al no depender de servicios de compañías externas y además, acceso seguro a la red interna mediante VPN.

OBJETIVOS

Requisitos, Funciones, Tareas y Pruebas (RFTP)

R01 – Control de los dispositivos de domótica mediante Docker y Home Assistant.

- **R01F01** - La interfaz debe permitir la gestión de dispositivos inteligentes (cámaras, luces, termostato).
    - **R01F01T01** - Configurar Home Assistant en un contenedor Docker.
        - **R01F01T01P01** – Comprobar el acceso a la interfaz de Home Assistant desde distintos navegadores.
    - **R01F01T02** - Implementar la integración de dispositivos IoT compatibles.
        - **R01F01T02P01** - Realizar pruebas de conexión con diferentes dispositivos inteligentes.
        - **R01F01T02P01** - Realizar pruebas de funcionalidad con diferentes dispositivos inteligentes.

R02 - El sistema debe proporcionar almacenamiento en red (NAS).

- **R02F01** - Configuración de OpenMediaVault.
    - **R02F01T01** - Instalar y configurar OpenMediaVault en Ubuntu Server.
    - **R02F01T02** - Definir usuarios y permisos de acceso al almacenamiento.
    - **R02F01P01** - Verificar la accesibilidad a los archivos dentro y fuera de la red.
    - **R02F01P02** - Evaluar la velocidad de transferencia de archivos.

R03 - El sistema debe ofrecer acceso remoto seguro mediante VPN.

- **R03F01** - Configurar OpenVPN para el acceso remoto.

- **R03F01T01** - Implementar un servidor VPN en Ubuntu Server.
- **R03F01T02** - Generar certificados y credenciales para los clientes.
- **R03F01T03** - Configurar reglas de firewall para proteger el acceso.
- **R03F01P01** - Probar la conexión VPN desde distintos dispositivos.
- **R03F01P02** - Verificar el acceso a los recursos de la red domótica a través de la VPN.

R04 - El sistema debe proporcionar un servicio de proxy seguro.

- **R04F01** - Configurar Squid y Privoxy para filtrar y optimizar el tráfico.
  - **R04F01T01** - Instalar y configurar Squid como proxy principal.
  - **R04F01T02** - Implementar Privoxy para filtrado de contenido y anuncios.
  - **R04F01T03** - Configurar reglas de ACL para gestionar el acceso a la red.
  - **R04F01P01** - Verificar la navegación a través del proxy.
  - **R04F01P02** - Evaluar la eficacia del filtrado de contenido y bloqueo de anuncios.

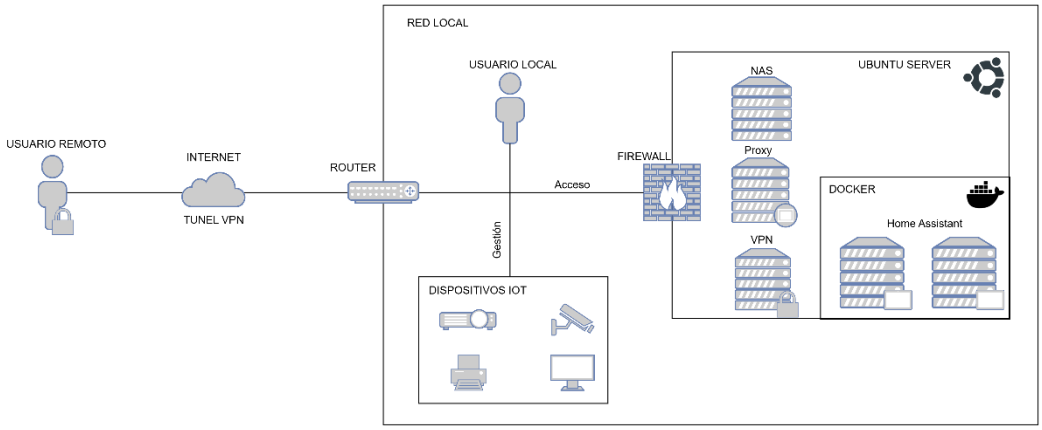
R05 - El sistema debe contar con medidas de seguridad adicionales.

- **R05F01** - Implementar firewall y protecciones contra accesos no autorizados.
  - **R05F01T01** - Configurar reglas de firewall en Ubuntu Server.
    - **R05F01T01P01** - Intentar acceder a la red mediante un puerto no autorizado.
  - **R05F01T02** - Implementar Fail2ban para mitigar ataques de fuerza bruta.
    - **R05F01T02P01** - Realizar pruebas de penetración.

- **R05F01T03** - Configurar Let's Encrypt + Certbot para certificados SSL.
    - **R05F01T03P01** - Revisar que los certificados sean válidos.
    - **R05F01T03P02** - Verificar qué los certificados se renueven automáticamente.

DESCRIPCIÓN

Arquitectura de la solución.



Casos de uso.

Caso de uso 1: Acceso a la interfaz web de Home Assistant

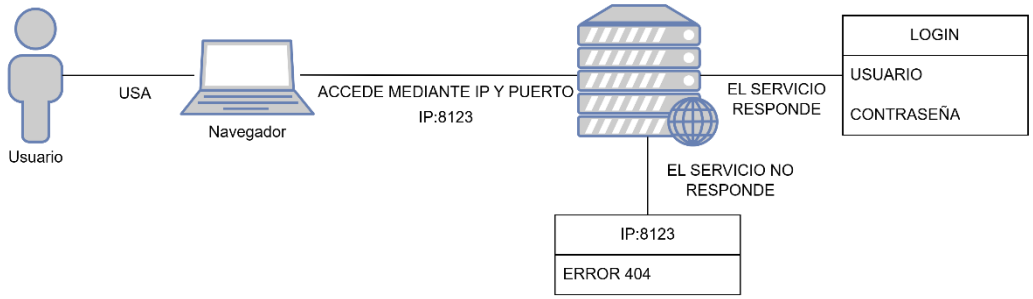


Ilustración 1: caso de uso Acceso a la interfaz web de Home Assistant

DESCRIPCIÓN: El usuario accede mediante un navegador a la interfaz web del Home Assistant mediante la IP del servidor y el puerto 8123.	
PRECONDICIONES:	**POSTCONDICIONES**:

El servidor con el servicio de Home Assistant debe de estar en ejecución. El usuario debe de conocer la IP y el Puerto del servidor. El Puerto 8123 debe de estar accesible a la red. El usuario debe de tener acceso a la red.	Si el servidor se encuentra activo aparecerá la pantalla de Login. Si el servidor no responde dará error.
DATOS ENTRADA Dirección IP del servidor. Número del puerto.	**DATOS SALIDA** Página de inicio del Home Assistant Pantalla de Error.
INTERFACES: Interfaz del Navegador Web	

Tabla 1: caso de uso Acceso a la interfaz web de Home Assistant

Caso de uso 2: Inicio de Sección del Home Assistant

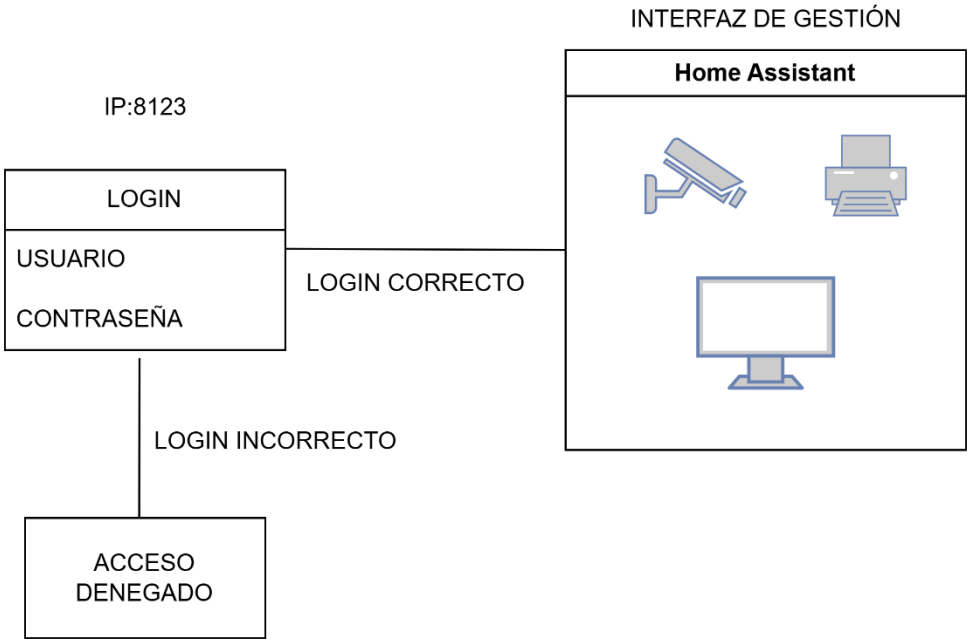


Ilustración 2: caso de uso Inicio de Sección del Home Assistant.

DESCRIPCIÓN: El usuario coloca su usuario y contraseña en la pantalla de Login.	
PRECONDICIONES: El usuario debe de conocer su usuario y su contraseña	**POSTCONDICIONES**: Pantalla de Gestión del Home Assistant. Error de Inicio de Sesión.
DATOS ENTRADA Usuario Contraseña	**DATOS SALIDA** Login Correcto. Login Incorrecto.
INTERFACES: Interfaz del Navegador Web	

Tabla 2: caso de uso Inicio de Sección del Home Assistant.

Caso de uso 3: Gestión de los dispositivos de Domótica.

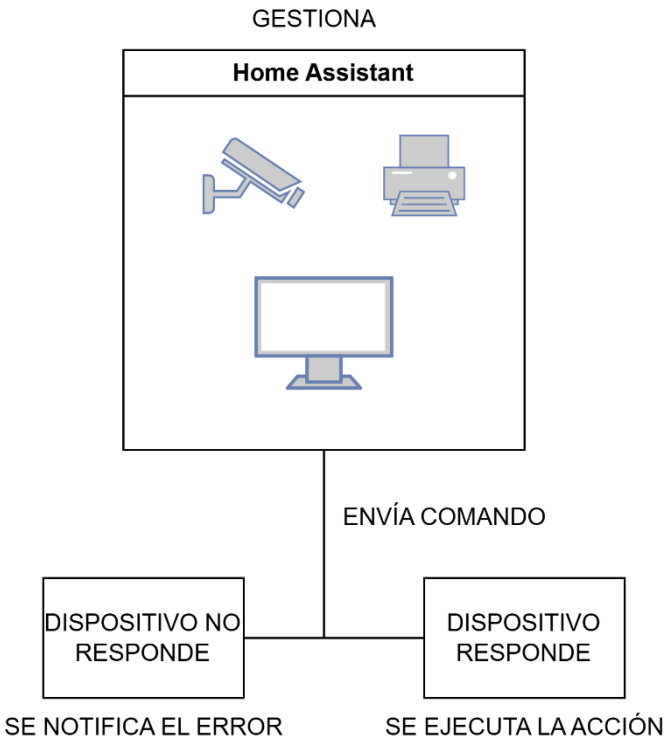


Ilustración 3: caso de uso Gestión de los dispositivos de Domótica.

DESCRIPCIÓN: El usuario realiza una acción con un dispositivo de Domótica	
PRECONDICIONES: Los dispositivos deben de estar integrados a la red de Domótica.	**POSTCONDICIONES**: El dispositivo realiza la acción. El dispositivo no responde.
DATOS ENTRADA Acción requerida (apagar, encender, etc.…)	**DATOS SALIDA** Acción realizada (apagar, encender, etc.…) Acción no realizada (error).
INTERFACES: Interfaz del Gestión del Home Assistant.	

Tabla 2: caso de uso Inicio de Sección del Home Assistant.

Caso de uso 4: El usuario accede al NAS mediante WEB o un CLIENTE SMB.

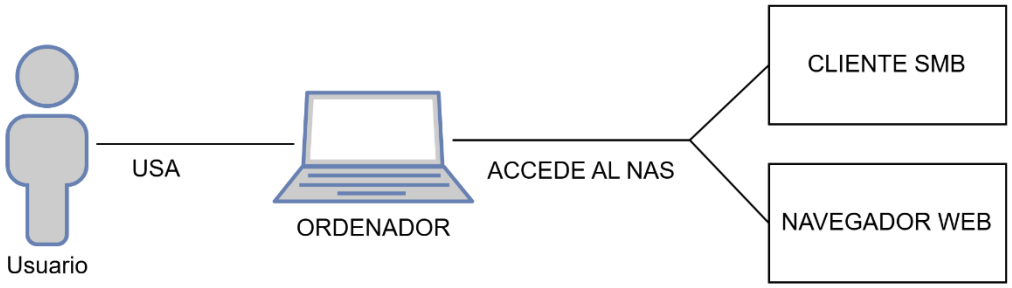


Ilustración 4: caso de uso El usuario accede al NAS.

DESCRIPCIÓN: El usuario accede al NAS mediante la utilización de un navegador web o mediante un cliente SMB.	
PRECONDICIONES: El servidor debe de estar activo y accesible desde la red. El usuario debe de tener un cliente SMB compatible.	**POSTCONDICIONES**: El cliente SMB requiere el usuario y la contraseña. Pantalla de inicio del Open Media Vault. Devuelve error al no poder conectar.
DATOS ENTRADA Dirección IP del servidor.	**DATOS SALIDA** Datos de Autentificación. Error del servidor.
INTERFACES: Interfaz web del navegador. Interfaz del cliente SMB.	

Tabla 4: caso de uso El usuario accede al NAS.

Caso de uso 5: El usuario inicia sesión en el Open Media Vault.

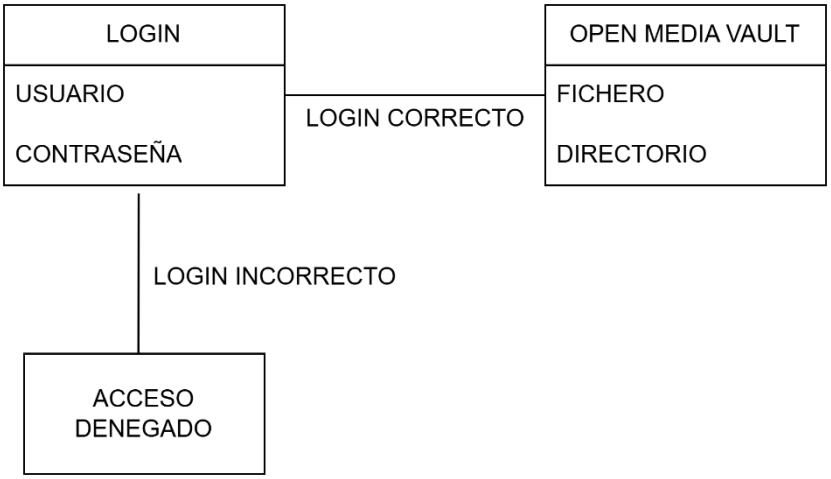


Ilustración 5: caso de uso El usuario inicia sesión en el Open Media Vault.

DESCRIPCIÓN: El usuario mediante interfaz o cliente SMB inicia sesión en el Open Media Vault.	
PRECONDICIONES: El servidor debe de estar activo y accesible desde la red. El usuario debe de conocer su usuario y contraseña del Open Media Vault.	**POSTCONDICIONES**: El cliente SMB accede al NAS. El servidor niega el acceso al cliente SMB. El navegador muestra la Interfaz del Open Media Vault. El navegador da error de inicio de sesión.
DATOS ENTRADA Usuario. Contraseña.	**DATOS SALIDA** Datos de Autentificación. Error del servidor.
INTERFACES: Interfaz web del navegador.	

Interfaz del cliente SMB.

Tabla 5: caso de uso El usuario accede al NAS.

Caso de uso 6: El usuario Navega, sube o descarga archivos.

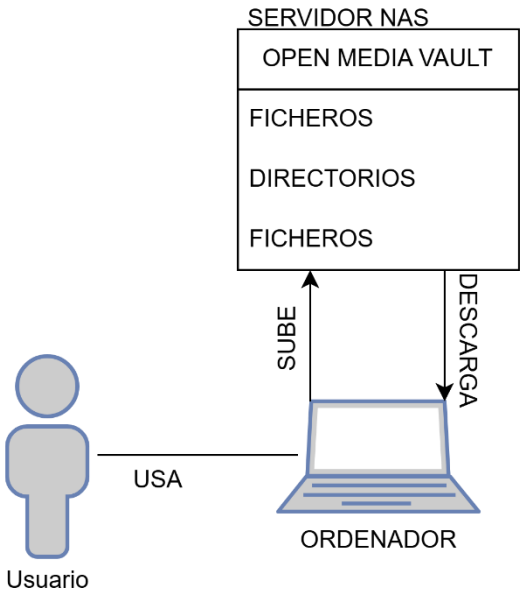


Ilustración 6: caso de uso El usuario Navega, sube o descarga archivos.

DESCRIPCIÓN: El usuario navega los directorios, los ficheros, sube sus propios ficheros o descarga las disponibles.	
PRECONDICIONES: El servidor debe de estar activo y accesible desde la red. El usuario debe de tener permisos en los ficheros.	**POSTCONDICIONES**: El fichero es subido al servidor. El fichero es descargado en el cliente. El usuario no puede subir o descargar los ficheros por no tener permisos.

DATOS ENTRADA	**DATOS SALIDA**
Ficheros. Directorios. Solicitud de descarga.	Ficheros en el servidor o cliente. Directorios en el servidor o cliente. Error de permisos.
INTERFACES: Interfaz web del navegador. Interfaz del cliente SMB.	

Tabla 6: caso de uso El usuario Navega, sube o descarga archivos.

Caso de uso 7: El usuario se conecta a la red interna mediante VPN

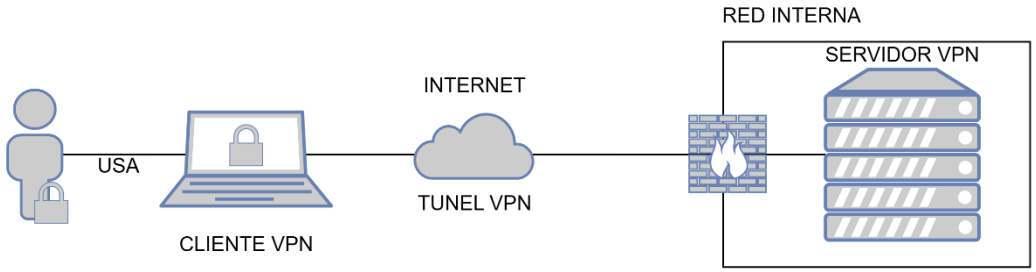


Ilustración 7: caso de uso El usuario se conecta a la red interna mediante VPN

DESCRIPCIÓN: El usuario usando un cliente VPN ingresa sus credenciales y se conecta a la red Interna.	
PRECONDICIONES: El servidor VPN debe de estar activo y ser accesible desde internet. El usuario debe de proveer las credenciales de acceso.	**POSTCONDICIONES**: El usuario accede a la red interna como si estuviera conectado localmente. El servidor rechaza la conexión.

DATOS ENTRADA	DATOS SALIDA
Usuario. Contraseña.	Acceso a la red. Acceso denegado.
INTERFACES: Interfaz del cliente VPN.	

Tabla 7: caso de uso El usuario Navega, sube o descarga archivos.

Caso de uso 8: El servidor proxy gestiona las solicitudes del usuario y bloquea los anuncios y contenidos no deseados.

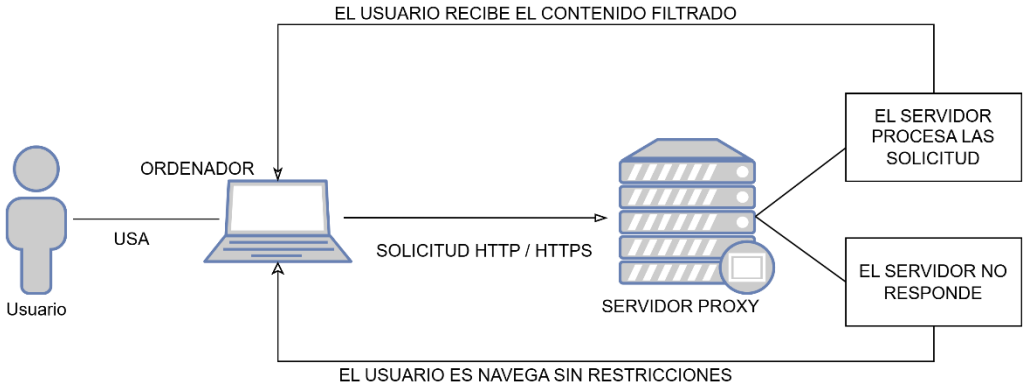


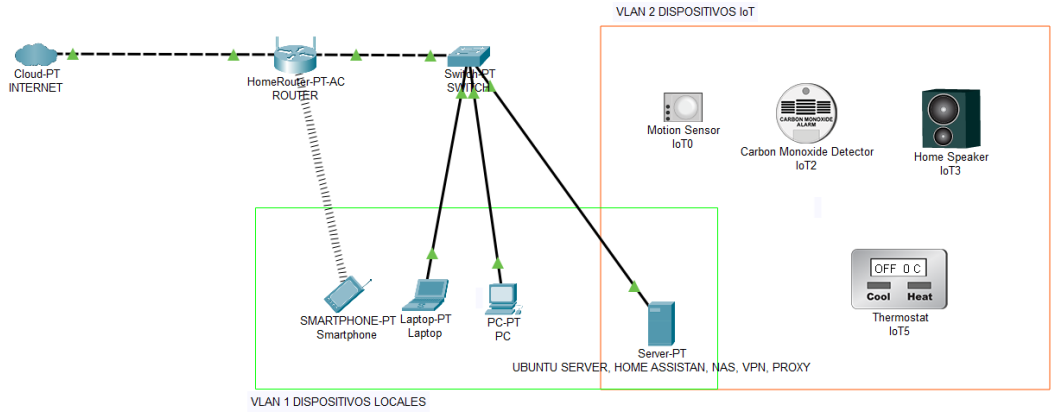
Ilustración 6: caso de uso El servidor proxy gestiona las solicitudes del usuario y bloquea los anuncios y contenidos no deseados.

DESCRIPCIÓN: El servidor proxy procesa las solicitudes del usuario y devuelve el contenido ya filtrado.	
PRECONDICIONES: El servidor proxy debe de estar activo y ser accesible desde la red.	**POSTCONDICIONES**: El servidor devuelve el contenido ya filtrado al cliente.

El usuario debe de tener configurado la IP del servidor proxy en su cliente. El servidor debe de tener una lista negra de contenido no deseado.	El servidor proxy no funciona por lo que el usuario recibe las solicitudes sin filtrar.
DATOS ENTRADA Solicitud HTTP, HTTPS	**DATOS SALIDA** Solicitud HTTP, HTTPS filtrada.
INTERFACES: Interfaz del navegador.	

Tabla 7: caso de uso El servidor proxy gestiona las solicitudes del usuario y bloquea los anuncios y contenidos no deseados.

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