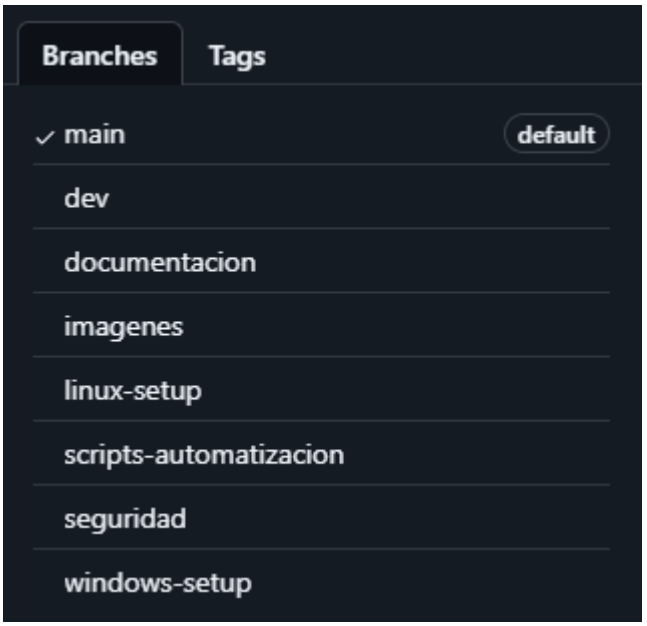
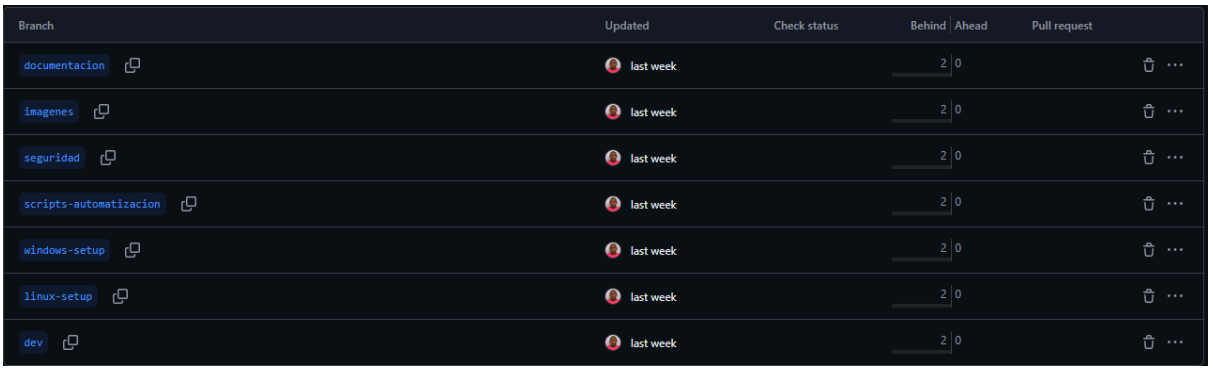
1. Github.

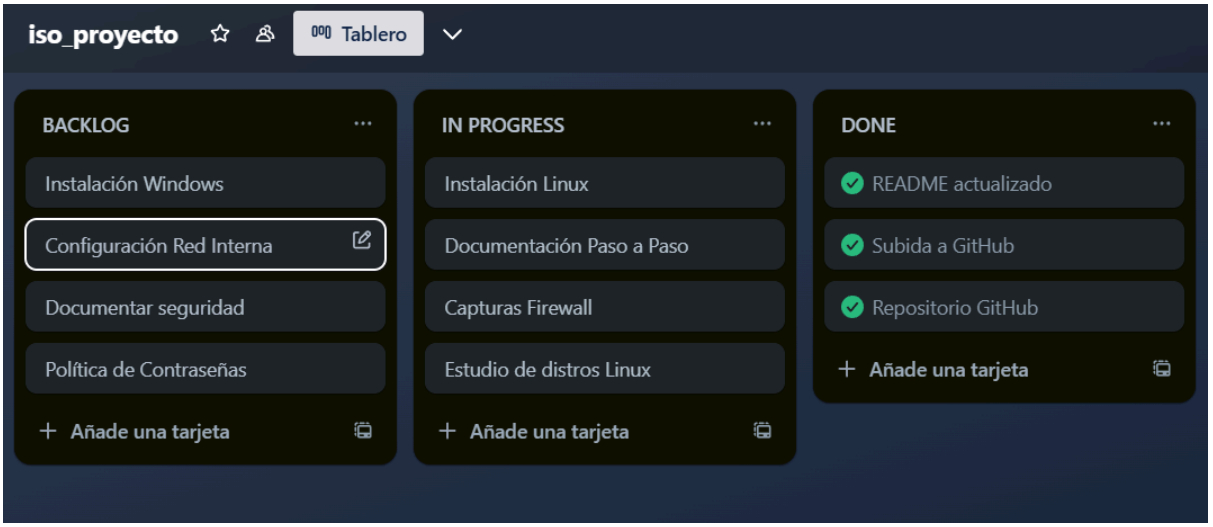
Comprueba las ramas, colaboradores, licencia, readme y insigths.
Ramas ->diseña las que consideres pero es importante una o varias ramas para el desarrollo.





2. Agile.

Diseña una pantalla KanBan en donde tienes el backlog y añades a In progress, las funcionalidades que estás trabajando hoy.
La puedes crear en Excel, Notion, Trello.... o cualquier herramienta para diseñar Kanban.



3. Análisis de necesidades

Tu defines la empresa en donde implementas la solución. De qué número de puestos hablamos, número de asistentes, ubicación, modalidad, servicios.
Tu defines el alcalce.

Empresa: TechNova Solutions S.L.
Descripción general:
TechNova Solutions S.L. es una empresa de tamaño medio dedicada al desarrollo de software libre y soluciones informáticas para centros educativos y pequeñas organizaciones. La empresa apuesta por el uso de tecnologías de código abierto, por lo que toda su infraestructura informática se basa en el sistema operativo Linux.

A. Ubicación y modalidad
Sede central: Madrid, España.

Modalidad de trabajo: Híbrida

Presencial: 25 empleados.

Remoto: 10 empleados (teletrabajo parcial o completo).

La sede principal cuenta con oficinas para desarrollo, soporte técnico, administración y salas de reuniones equipadas.

B. Número de puestos y asistentes técnicos
Total de empleados: 35

Desarrollo de software: 15 programadores

Soporte técnico (asistentes IT): 3 técnicos

Administración y RRHH: 4 personas

Departamento comercial y marketing: 5 personas

Dirección y gerencia: 2 personas

Otros (formadores y testers): 6 personas

Puestos de trabajo físicos: 25 (equipos de escritorio con Linux Ubuntu LTS).

Puestos remotos: 10 (portátiles configurados con VPN y escritorio remoto en Linux).

C. Servicios a implementar
Se identifican los siguientes servicios necesarios para el correcto funcionamiento de la empresa bajo entorno Linux:

Servidor de archivos (Samba o NFS) para compartir documentación interna.

Servidor web (Apache o Nginx) para alojar plataformas de desarrollo interno y paneles de gestión.

Servidor de correo (Postfix + Dovecot).

Servidor de base de datos (MySQL/MariaDB o PostgreSQL).

Control de versiones (Git + GitLab o Gitea en servidor propio).

VPN (OpenVPN o WireGuard) para accesos remotos seguros.

Sistema de tickets para soporte técnico interno (OTRS, GLPI o similar).

Sistema de backup automático (rsync, cronjobs y almacenamiento externo seguro).

Autenticación centralizada (LDAP o FreeIPA).

Firewall y monitorización de red (UFW/IPTables y herramientas como Nagios o Zabbix).

Clientes ligeros para terminales administrativos (si se requiere).

D. Alcance de la solución
El proyecto abarcará los siguientes puntos:

Instalación y configuración de los servicios indicados en servidores Linux.

Configuración de las estaciones de trabajo con sistemas Linux amigables para el usuario (Ubuntu, Linux Mint, etc.).

Diseño de políticas de seguridad y gestión de usuarios.

Formación básica para empleados sobre el uso del entorno Linux.

Implantación de soluciones de acceso remoto y colaboración.

Documentación técnica y operativa del sistema.

Plan de mantenimiento y escalabilidad futura.

4. Seguridad y ciberseguridad. (ya lo debes tener del borrador anterior)

Analiza posibles vulnerabilidades y medidas de corrección
(redTeam vs BlueTeam)
Escribir en borrador de memoria

La seguridad es un aspecto esencial en cualquier infraestructura IT, especialmente en una empresa como **TechNova Solutions S.L.**, que trabaja con software libre y gestiona servicios internos y remotos desde múltiples ubicaciones. La estrategia de ciberseguridad se basa en el enfoque **Red Team vs Blue Team**, permitiendo simular ataques y reforzar defensas de forma continua.

Análisis de posibles vulnerabilidades

A continuación se describen los vectores de ataque más probables según la arquitectura definida y su mitigación prevista:

Elemento	Posibles vulnerabilidades	Medidas de protección (Blue Team)
Red interna	- Escaneo de red - ARP spoofing	- Segmentación de red (VLANs) - Monitorización con IDS (Snort)
Accesos remotos (VPN)	- Robo de credenciales - Túneles no cifrados	- Autenticación multifactor (MFA) - OpenVPN con certificados y cifrado AES-256
Servidores web (Apache/Nginx)	- Inyección SQL - XSS - Acceso no autorizado	- Reglas de firewall UFW - WAF (ModSecurity) - Actualizaciones periódicas
Correo electrónico (Postfix + Dovecot)	- Phishing - Relay abierto	- SPF, DKIM y DMARC configurados - Antivirus y antispam activo
Sistema de archivos (Samba/NFS)	- Accesos no autorizados - Escalada de privilegios	- ACLs y permisos estrictos - Autenticación LDAP integrada

Bases de datos (MySQL/PostgreSQL)	- Inyecciones - Accesos no cifrados	- Acceso desde localhost o VPN - Usuarios con permisos mínimos
Autenticación (LDAP/FreeIPA)	- Robo de credenciales - Enumeración de usuarios	- Contraseñas robustas y MFA - Monitorización de intentos fallidos
Estaciones de trabajo	- Malware - Puertos abiertos	- UFW configurado por defecto - Desactivación de servicios innecesarios
Backups	- Acceso al almacenamiento - Manipulación de copias	- Backups cifrados y externos - Verificación de integridad regular
Usuarios y permisos	- Mal uso interno - Privilegios innecesarios	- Políticas de mínimo privilegio - Formación en buenas prácticas

Red Team vs Blue Team

Red Team (Equipo ofensivo):
Encargado de realizar pruebas de penetración simuladas para detectar fallos antes de que sean explotados por agentes externos. Sus acciones incluyen escaneo de puertos, ataques de ingeniería social, pruebas de inyección y análisis de vulnerabilidades de servicios abiertos.

Blue Team (Equipo defensivo):
Su objetivo es proteger, monitorear y responder a los incidentes. Implementan firewalls, antivirus, IDS/IPS, monitorización centralizada (Zabbix/Nagios), y desarrollan políticas de seguridad para minimizar riesgos.

Ambos equipos colaboran en simulacros periódicos para comprobar el estado de la red y adaptar medidas en función de nuevos vectores de ataque.

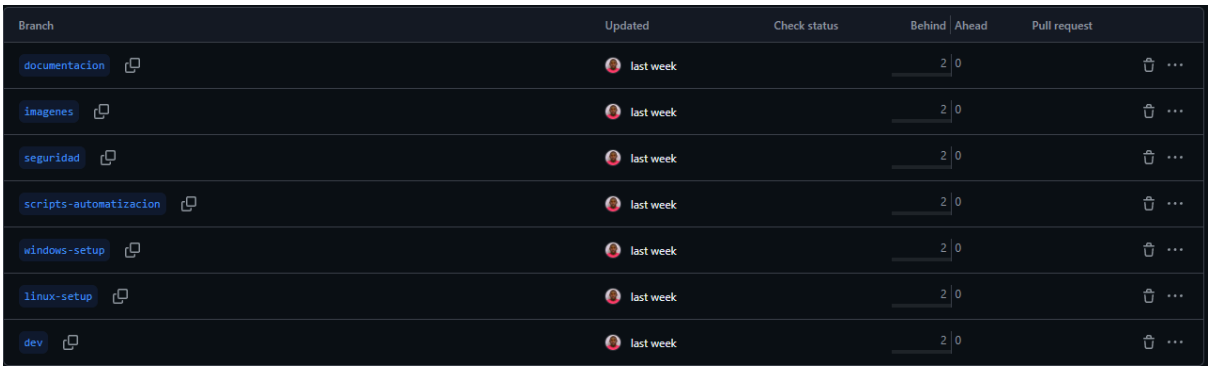
Medidas adicionales de ciberseguridad

- **Actualizaciones automáticas** y revisión semanal de paquetes críticos.
- **Registros centralizados** con análisis de logs mediante + .
- **Bloqueo automático** de IPs tras varios intentos fallidos (Fail2Ban).
- **Desactivación de servicios innecesarios** en cada estación y servidor.
- **Auditorías mensuales** de seguridad interna.

- **Concienciación del personal** mediante sesiones de formación en ciberseguridad básica y detección de amenazas comunes.

5. Anexos y capturas.

Crear una rama de imagenes en Github y subir las imágenes que luego utilizamos en memoria. kanban, alcance de proyecto, seguridad, ...



6.Instalación paso a paso

Una vez elegido el sistema operativo detalla todos los pasos para la instalación en los puestos de la empresa.

Empresa: TechNova Solutions S.L.
Descripción general:
TechNova Solutions S.L. es una empresa de tamaño medio dedicada al desarrollo de software libre y soluciones informáticas para centros educativos y pequeñas organizaciones. La empresa apuesta por el uso de tecnologías de código abierto, por lo que toda su infraestructura informática se basa en el sistema operativo Linux.

A. Ubicación y modalidad
Sede central: Madrid, España.

Modalidad de trabajo: Híbrida

Presencial: 25 empleados.

Remoto: 10 empleados (teletrabajo parcial o completo).

La sede principal cuenta con oficinas para desarrollo, soporte técnico, administración y salas de reuniones equipadas.

B. Número de puestos y asistentes técnicos
Total de empleados: 35

Desarrollo de software: 15 programadores

Soporte técnico (asistentes IT): 3 técnicos

Administración y RRHH: 4 personas

Departamento comercial y marketing: 5 personas

Dirección y gerencia: 2 personas

Otros (formadores y testers): 6 personas

Puestos de trabajo físicos: 25 (equipos de escritorio con Linux Ubuntu LTS).

Puestos remotos: 10 (portátiles configurados con VPN y escritorio remoto en Linux).

C. Servicios a implementar
Se identifican los siguientes servicios necesarios para el correcto funcionamiento de la empresa bajo entorno Linux:

Servidor de archivos (Samba o NFS) para compartir documentación interna.

Servidor web (Apache o Nginx) para alojar plataformas de desarrollo interno y paneles de gestión.

Servidor de correo (Postfix + Dovecot).

Servidor de base de datos (MySQL/MariaDB o PostgreSQL).

Control de versiones (Git + GitLab o Gitea en servidor propio).

VPN (OpenVPN o WireGuard) para accesos remotos seguros.

Sistema de tickets para soporte técnico interno (OTRS, GLPI o similar).

Sistema de backup automático (rsync, cronjobs y almacenamiento externo seguro).

Autenticación centralizada (LDAP o FreeIPA).

Firewall y monitorización de red (UFW/IPTables y herramientas como Nagios o Zabbix).

Clientes ligeros para terminales administrativos (si se requiere).

D. Alcance de la solución
El proyecto abarcará los siguientes puntos:

Instalación y configuración de los servicios indicados en servidores Linux.

Configuración de las estaciones de trabajo con sistemas Linux amigables para el usuario (Ubuntu, Linux Mint, etc.).

Diseño de políticas de seguridad y gestión de usuarios.

Formación básica para empleados sobre el uso del entorno Linux.

Implantación de soluciones de acceso remoto y colaboración.

Documentación técnica y operativa del sistema.

Plan de mantenimiento y escalabilidad futura.