


Memorias del Proyecto:

Automatización de Infraestructura de Servicios de Red con Ansible

Francisco José Rodríguez Muñoz

12 de mayo del 2025

1. DEFINICIÓN Y ANÁLISIS CONTEXTUAL.....	3
1.1 Contexto y justificación.....	3
1.1.2 Clasificación de empresas del sector.....	4
1.1.3 Caracterización de las empresas tipo.....	5
1.1.4 Necesidades más demandadas y oportunidades del sector.....	5
1.1.5 Tipo de proyecto requerido y características específicas.....	6
1.1.6 Obligaciones fiscales, laborales y de prevención de riesgos.....	6
1.1.7 Ayudas y subvenciones para digitalización y tecnología.....	8
1.2 Marco Legal.....	9
1.2.1 Legislación en materia de protección de datos y seguridad informática.....	9
1.2.2 Subvenciones y ayudas públicas (España y UE).....	12
1.2.3 Obligaciones fiscales y laborales.....	13
1.3 Alcance del Proyecto.....	14
1.3.1 Objetivos del proyecto.....	14
1.3.2 Límites del proyecto.....	15
1.4 ALTERNATIVAS Y PROPUESTA DE SOLUCIÓN.....	15
2. ANÁLISIS DE REQUISITOS.....	16
2.1 Recursos necesarios.....	16
2.1.1 Recursos Humanos.....	16
2.1.2 Administrador de redes.....	16
2.1.3 Especialista en automatización (DevOps).....	16
2.1.4 Técnico en ciberseguridad.....	16
2.1.5 Documentalista técnico.....	16
2.2 Recursos Legales.....	16
2.3 Hardware.....	17
2.4 Software.....	17
2.5 Otros Requisitos Técnicos.....	17
3. TEMPORALIZACIÓN.....	17
3.1 Identificación de fases y tareas.....	18
3.1.1 Inicio (Semana 1).....	18
3.1.2 Planificación (Semana 2).....	18
3.1.3 Ejecución (Semanas 3 a 6).....	18
3.1.4 Control y pruebas (Semanas 7 y 8).....	18
3.1.5 Cierre (Semana 9).....	18
3.2 SECUENCIACIÓN.....	18
4. DOCUMENTACIÓN TÉCNICA.....	19
4.1 Elementos documentales.....	19



5. ANÁLISIS ECONÓMICO.....	19
5.1 Presupuesto estimado.....	19
5.2 Financiación.....	20
5.3 Retorno de Inversión.....	20
5.4 Evaluación de Viabilidad Económica.....	21
6. SEGUIMIENTO Y CONTROL.....	21
6.1 Indicadores de Seguimiento.....	21
6.2 Evaluación General (DAFO).....	22
6.2.1 Fortalezas.....	22
6.2.2 Debilidades.....	22
6.2.3 Oportunidades.....	22
6.2.4 Amenazas.....	22
7. FUENTES DE DOCUMENTACIÓN.....	22
8. ANEXOS.....	24



1. DEFINICIÓN Y ANÁLISIS CONTEXTUAL

1.1 Contexto y justificación

En la actualidad, la mayoría de las organizaciones dependen cada vez más de infraestructuras de red sólidas, seguras y escalables para garantizar la disponibilidad continua de sus servicios digitales. Esta dependencia se intensifica con el crecimiento exponencial del uso de tecnologías basadas en la nube, la virtualización y la digitalización generalizada de procesos empresariales. En este contexto, la gestión manual de la infraestructura de red se ha vuelto insostenible, debido a su propensión a errores humanos y su falta de escalabilidad.

La automatización de la infraestructura TI, especialmente de los servicios de red, se presenta como una solución estratégica para afrontar estos retos. Herramientas como Ansible, de código abierto, han ganado gran popularidad por su simplicidad y eficacia en la administración automatizada de configuraciones y despliegues de servicios. Ansible permite gestionar una gran variedad de dispositivos de red y servidores desde un único punto de control, garantizando coherencia, repetibilidad y rapidez en las operaciones.

Este proyecto se desarrolla en un contexto de creciente necesidad empresarial por optimizar procesos operativos, reducir costos y aumentar la confiabilidad de sus infraestructuras. El objetivo principal es automatizar la configuración y gestión de servicios de red fundamentales como DNS, DHCP, VPN entre otros, mediante el uso de Ansible, abordando así la necesidad productiva clave: minimizar el tiempo dedicado a tareas repetitivas y propensas a errores humanos, al tiempo que se garantiza la seguridad y el cumplimiento de políticas operativas.

El ámbito de aplicación de este proyecto abarca tanto entornos empresariales medianos y grandes como laboratorios educativos y de pruebas, donde la gestión de redes y servicios suele requerir intervenciones frecuentes y controladas.

En resumen, este proyecto responde a una demanda concreta del sector TI: la necesidad de gestionar infraestructuras de red de forma ágil, eficiente y segura, contribuyendo así a una mejora significativa en la calidad del servicio y la productividad operativa de las organizaciones.

1.1.2 Clasificación de empresas del sector

En el ámbito autonómico, concretamente en comunidades como Madrid, Cataluña o la Comunidad Valenciana, existen diversas empresas que ofrecen servicios tecnológicos vinculados al despliegue, gestión y automatización de infraestructuras de red. Estas empresas pueden clasificarse en tres grandes grupos según sus características organizativas y el tipo de servicio que ofrecen:

- **Empresas integradoras de sistemas y redes:** Entre ellas destacan **Axians**, **Sothis** o **Nunsys**, las cuales trabajan en la implantación de soluciones de red, servidores, seguridad y cloud, para medianas y grandes organizaciones. Estas compañías cuentan con departamentos técnicos especializados y se enfocan mayormente en clientes corporativos o institucionales.
- **Empresas de servicios gestionados (MSP):** **Gigas**, **Inycom** o **Inetum** son empresas que suelen ser contratadas para gestión de servicios, proporcionando administración remota de redes, seguridad y soporte. Su modelo de negocio se basa en contratos de mantenimiento y disponibilidad 24/7.
- **Empresas tecnológicas orientadas a PYMEs:** Algunas startups y cooperativas tecnológicas como **Neodoo Microsystems** desarrollan soluciones a medida para pequeñas empresas, centrándose en automatización, virtualización y servicios adaptados a entornos con menor presupuesto, pero con alta demanda técnica.

Todas estas organizaciones demandan soluciones que permitan una implantación rápida, segura y automatizada de servicios críticos como DNS, DHCP, VPN, gestión de usuarios o monitorización, especialmente a través de herramientas como Ansible, Docker, o monitorización como Prometheus o Grafana.

1.1.3 Caracterización de las empresas tipo

La empresa tipo del sector suele ser una PYME tecnológica de entre 15 y 50 empleados, con una estructura organizativa relativamente horizontal pero funcionalmente especializada. Estas empresas suelen dividirse en cinco departamentos principales:

- **Dirección General:** Encargada de la estrategia, visión, alianzas y viabilidad económica. Toma decisiones sobre inversión y expansión.
- **Departamento Técnico:** Se divide normalmente en Infraestructura, Desarrollo de software y Soporte, siendo el núcleo de la empresa. Aquí se diseñan e implementan soluciones de red, servidores, automatización y virtualización. También se realizan pruebas de integración y mantenimiento correctivo y preventivo.

- **Departamento de Sistemas y Seguridad:** Responsable de la administración de sistemas, copias de seguridad, cumplimiento de políticas de seguridad y respuesta ante incidentes.
- **Departamento Comercial:** Orientado a la captación de clientes, diseño de propuestas comerciales, gestión de licitaciones y atención postventa. Suele trabajar en conjunto con los técnicos para asegurar que la solución ofertada se adapta al cliente.
- **Departamento de Formación y Documentación:** Elabora guías, documentación técnica, y cursos de capacitación para el personal del cliente o alumnado.

Estas empresas, aunque pequeñas, requieren alta especialización técnica y procesos muy eficientes para mantenerse competitivas, lo que justifica la necesidad de herramientas automatizadas que minimicen tiempos de despliegue, errores y costes operativos.

1.1.4 Necesidades más demandadas y oportunidades del sector

El sector de redes y servicios IT presenta una necesidad creciente de automatización de tareas repetitivas, gestión centralizada de servicios (DNS, DHCP, VPN, web) y monitorización eficiente. Las empresas buscan reducir tiempos de provisión, mejorar la seguridad y cumplir normativas. En especial, se demandan soluciones modulares y adaptables para entornos educativos, donde cada curso requiere configurar múltiples veces los mismos servicios. Esta realidad abre una gran oportunidad de negocio para proyectos que automaticen y documentan todo el proceso de la infraestructura con herramientas de código abierto.

1.1.5 Tipo de proyecto requerido y características específicas

El proyecto desarrollado responde directamente a estas demandas con un sistema basado en Ansible que automatiza el despliegue de servicios como DNS, DHCP, VPN, Nginx, etc., con una estructura modular, reutilizable y segura. La solución permite que cualquier empresa, centro educativo o profesional IT pueda desplegar en minutos una infraestructura funcional, robusta y monitorizable (mediante integración con Prometheus).

- Las características diferenciales frente a otras soluciones del mercado incluyen:
- Código abierto y sin costes de licencia.
- Documentación exhaustiva, orientada a usuarios técnicos y docentes.
- Despliegue rápido y seguro, con scripts verificados.
- Adaptabilidad a múltiples entornos (educativos, empresariales, laboratorios).

- Atención más personalizada y enfoque pedagógico, especialmente útil para la formación técnica.

Frente a soluciones cerradas o complejas, este proyecto representa una opción accesible, flexible y profesional, adaptada a las necesidades reales del entorno autonómico.

1.1.6 Obligaciones fiscales, laborales y de prevención de riesgos

Pasos para constituir una Sociedad Limitada (S.L.)

- Certificar el nombre en el Registro Mercantil Central (para asegurarte de que no esté cogido).
- Abrir una cuenta bancaria a nombre de la empresa y hacer el ingreso del capital mínimo (3.000 €).
- Redactar los estatutos sociales (normas internas de la empresa).
- Firmar la escritura pública de constitución ante notario.
- Obtener el NIF provisional en la Agencia Tributaria.
- Inscribir la empresa en el Registro Mercantil Provincial.
- Solicitar el NIF definitivo y darse de alta en el censo de empresarios (modelo 036).
- Alta en el Impuesto de Actividades Económicas (IAE) y en la Seguridad Social como empresa.

Calendario fiscal básico para la empresa

Impuesto	Periodicidad	Cuándo se paga/declara
IAE (Impuesto Actividades Económicas)	Anual	Septiembre-Diciembre
IVA (Impuesto sobre el Valor Añadido)	Trimestral	Enero, abril, julio, octubre
IRPF (retenciones si hay empleados)	Trimestral	Igual que el IVA
IBI (Impuesto de Bienes Inmuebles)	Anual	Mayo-Junio (aprox.)

Prevención de riesgos laborales (PRL)

Aunque sea una empresa tecnológica o de servicios IT, es obligatorio aplicar medidas de PRL. Algunas acciones clave:

- Realizar una evaluación de riesgos del entorno laboral (espacios, pantallas, electricidad).
- Formar al equipo en ergonomía y seguridad informática (evitar lesiones posturales, proteger datos).
- Contar con un servicio de prevención ajeno (empresa externa especializada).
- Tener un botiquín, plan de evacuación y extintores accesibles.
-

Obligaciones con la Seguridad Social (empleados)

Cuando contratamos personal, debemos:

- Dar de alta la empresa en la Seguridad Social como empleadora.
- Dar de alta a cada trabajador.
- Comunicar el contrato al SEPE.
- Cotizar mensualmente por ellos con los modelos correspondientes).
- Gestionar bajas, altas, vacaciones y nóminas cumpliendo normativa laboral.

1.1.7 Ayudas y subvenciones para digitalización y tecnología

Subvenciones identificadas

Kit Digital (Red.es): hasta 12.000 € para pymes y autónomos, para software de gestión, web, ciberseguridad o automatización.

Industria Conectada 4.0: subvenciones para modernizar procesos con tecnologías como Ansible, IoT o monitorización.

Horizonte Europa - Innovación Digital: fondos europeos para startups tecnológicas o proyectos que propongan automatización de servicios.

Subvenciones autonómicas: muchas ofrecen programas específicos de digitalización para jóvenes emprendedores.

Financiación externa para constituir la empresa

Una empresa S.L. necesita un capital social mínimo de 3.000 €. Si no lo tienes de forma personal, puedes recurrir a:

- **Préstamos ENISA (jóvenes emprendedores):** sin avales, hasta 75.000 €.
- **ICO (Instituto de Crédito Oficial):** para financiar la inversión inicial, compra de equipos etc...
- **Microcréditos para jóvenes emprendedores (CaixaBank en mi caso):** fáciles de obtener si tienes un plan sólido.

1.2 Marco Legal

1.2.1 Legislación en materia de protección de datos y seguridad informática

RGPD (Reglamento General de Protección de Datos - UE 2016/679)

¿Qué es?

Es el Reglamento Europeo que regula el tratamiento de datos personales de ciudadanos de la Unión Europea (UE).

¿Qué regula dicho reglamento?

- Consentimiento y derechos de los usuarios.
- Seguridad en el tratamiento de datos personales.
- Obligaciones del responsable del tratamiento.

Relación con el proyecto:

Si se automatizan servicios que manejan datos de usuarios (por ejemplo, autenticaciones, logs o direcciones IP), es esencial garantizar que la automatización no vulnere derechos ni exponga información personal.

LOPDGDD (Ley Orgánica 3/2018 – España)

¿Qué es?

Norma española que adapta y complementa el RGPD al ordenamiento jurídico nacional.

¿Qué regula?

- Derechos digitales.
- Control de dispositivos y vigilancia laboral.
- Limitaciones en el uso automatizado de datos.

Relación con el proyecto:

Refuerza las obligaciones de seguridad y control sobre los datos procesados automáticamente, incluyendo registros y trazabilidad que pueden generarse con Ansible.

ISO/IEC 20000-1 – Gestión de Servicios TI

¿Qué es?

Norma que define las mejores prácticas para la gestión y entrega de servicios de TI de calidad.

¿Qué regula?

- Gestión de incidentes, problemas y cambios.
- Diseño y entrega de servicios eficientes.
- Evaluación del desempeño del servicio.

Relación con el proyecto:

Automatizar con Ansible permite mejorar la eficiencia y trazabilidad de los servicios de red. Esta norma garantiza que esas mejoras se integren dentro de una gestión de servicios estructurada y profesional.

Esquema Nacional de Seguridad (ENS) – Real Decreto 311/2022

¿Qué es?

Marco normativo obligatorio para sistemas que manejan información del sector público en España.



¿Qué regula?

- Clasificación de sistemas según nivel de seguridad.
- Requisitos técnicos y organizativos.
- Auditorías y certificación de sistemas.

Relación con el proyecto:

Si el sistema automatizado se implementa en organismos públicos o trabaja con su infraestructura, debe cumplir con el ENS. Ansible puede configurarse para documentar y controlar cambios, cumpliendo con este estándar.

Ley 43/2021 – Medidas para la ciberseguridad en redes 5G

¿Qué es?

Norma española que establece medidas para asegurar la integridad de redes de nueva generación.

¿Qué regula?

- Requisitos de seguridad para proveedores de red.
- Evaluación de riesgos en infraestructuras críticas.
- Registro y control de actividades automatizadas.

Relación con el proyecto:

Aunque orientada a redes de nueva generación, esta ley promueve prácticas de ciberseguridad que también aplican a redes tradicionales, especialmente si se automatizan con herramientas como Ansible.

Ley 9/2014 – Ley General de Telecomunicaciones

¿Qué es?

Norma española que regula el despliegue, operación y gestión de redes de comunicaciones electrónicas.



¿Qué regula?

- Derechos y deberes de operadores de red.
- Condiciones técnicas y de seguridad.
- Infraestructura física y servicios públicos.

Relación con el proyecto:

Aplica si el sistema automatizado se integra en redes empresariales, de proveedores o en telecomunicaciones. La automatización debe respetar los estándares de trazabilidad y disponibilidad.

Ley 31/1995 – Prevención de Riesgos Laborales (PRL)

¿Qué es?

Norma española que regula la prevención de riesgos en el entorno de trabajo.

¿Qué regula?

- Evaluación de riesgos en el puesto.
- Ergonomía en el uso de ordenadores.
- Riesgos psicosociales y tecnológicos.

Relación con el proyecto:

Si hay personas trabajando en la automatización como programadores o administradores, se deben adoptar medidas para proteger la salud laboral, tanto física como mental.

Licencia GPLv3 (GNU General Public License v3) – Software libre

¿Qué es?

Licencia que regula el uso, modificación y distribución de software libre, como Ansible.

¿Qué regula?

- Uso libre del software.
- Modificación y reutilización con atribución.
- Obligación de mantener la licencia en derivados.

Relación con el proyecto:

Al usar Ansible en un entorno automatizado, se deben respetar los términos de la GPLv3, especialmente si se redistribuyen scripts o soluciones basadas en él.

1.2.2 Subvenciones y ayudas públicas (España y UE)

¿Qué son?

Programas públicos para fomentar la digitalización y automatización empresarial.

¿Ejemplos aplicables al proyecto?

- **Kit Digital:** Ayuda a pymes para implementar soluciones de automatización.
- **Industria Conectada 4.0:** Subvenciones para digitalización industrial.
- **Horizonte Europa / Horizonte PYME:** Financiación para innovación tecnológica.
- **Programas autonómicos:** Subvenciones regionales para modernización TI.

Relación con el proyecto:

Este proyecto puede ser parcial o totalmente financiado si se orienta a mejorar la eficiencia digital de una empresa, especialmente una pyme o startup.

1.2.3 Obligaciones fiscales y laborales

¿Qué son?

Normas que rigen la actividad profesional o empresarial en el desarrollo del proyecto.

¿Qué incluyen?

- Alta en la Agencia Tributaria (IVA, IRPF, IS).
- Alta en la Seguridad Social y cumplimiento de cotizaciones.
- Contratación conforme al Estatuto de los Trabajadores.

Relación con el proyecto:

Si se desarrolla como freelance o en empresa, debe cumplir con los requisitos fiscales y laborales vigentes. Esto incluye el pago de impuestos y aseguramiento de condiciones de trabajo dignas para cualquier persona involucrada.

1.3 Alcance del Proyecto

Este proyecto tiene como finalidad mejorar la eficiencia, seguridad y escalabilidad en la gestión de servicios de red mediante el uso de Ansible como herramienta principal de automatización. Se dirige tanto a pequeñas como medianas empresas tecnológicas que necesiten optimizar sus procesos de configuración, mantenimiento y despliegue de servicios de red con recursos limitados y sin depender de soluciones propietarias o costosas.

A partir de la recopilación de información técnica y normativa (mencionadas en secciones anteriores), y del análisis de necesidades operativas en entornos TI reales, se han definido los siguientes objetivos específicos y realistas, que determinan el alcance del proyecto:

1.3.1 Objetivos del proyecto

- ☐ **Automatizar** la configuración inicial de servicios de red fundamentales como DNS, DHCP, servicio web y VPN, mediante playbooks de Ansible.
- ☐ **Diseñar** una arquitectura de automatización reproducible, segura y adaptable a distintos entornos (laboratorio, producción, cloud).
- ☐ **Implementar** un sistema de gestión centralizada que permita aplicar configuraciones de red de forma consistente.
- ☐ **Documentar** de forma detallada cada componente del sistema automatizado para facilitar su mantenimiento y escalabilidad.
- ☐ **Verificar** la integridad y operatividad del sistema tras cada despliegue automático mediante pruebas funcionales integradas.
- ☐ **Reducir** la intervención manual y los errores humanos en tareas repetitivas relacionadas con servicios de red.
- ☐ **Optimizar** el tiempo de provisión y recuperación de servicios ante fallos o cambios de configuración.
- ☐ **Asegurar** el cumplimiento normativo en materia de seguridad, trazabilidad y gestión de cambios en redes TI.

Resumen del alcance:

Este proyecto se enfoca en diseñar, automatizar, probar y documentar una infraestructura de servicios de red con Ansible, aplicando buenas prácticas de seguridad y cumplimiento normativo. Está orientado a facilitar la gestión de redes en entornos reales mediante herramientas de código abierto, garantizando resultados reproducibles, mantenibles y escalables.

1.4 ALTERNATIVAS Y PROPUESTA DE SOLUCIÓN

Alternativa 1: Automatización con scripts Bash personalizados

Consistía en desarrollar scripts manuales en Bash para configurar servicios de red en diferentes nodos del sistema.

Ventajas:

- Total control del proceso.
- No requiere software externo adicional.

Inconvenientes:

- Difícil de mantener y escalar.
- Carece de gestión de inventario y estructura modular.
- Mayor posibilidad de errores humanos y menor reutilización.

Alternativa 2: Uso de Ansible como solución

Ansible es una herramienta de automatización ligera y sin agentes, basada en SSH, ideal para gestionar configuraciones en nodos Linux de forma sencilla, segura y reutilizable mediante playbooks.

Ventajas:

- Fácil de aprender y desplegar.
- No requiere agentes (usa SSH).
- Modular, escalable y ampliamente soportada.
- Excelente documentación y comunidad activa.

Inconvenientes:

- Puede requerir adaptación en entornos Windows o híbridos.
- Menor control de estado frente a soluciones como Puppet (aunque se puede mitigar con buenas prácticas).

2. ANÁLISIS DE REQUISITOS

El éxito del proyecto de automatización de servicios de red con Ansible depende directamente de la correcta identificación y planificación de los recursos necesarios. Este apartado detalla los requerimientos clave desde distintas perspectivas: humana, técnica, legal y operativa.

2.1 Recursos necesarios

2.1.1 Recursos Humanos

Para la ejecución adecuada del proyecto se requerirá la intervención de varios perfiles profesionales, entre ellos:

2.1.2 Administrador de redes

Responsable de diseñar y supervisar la infraestructura de red, identificar necesidades de configuración y verificar la integración de servicios.

2.1.3 Especialista en automatización (DevOps)

Encargado de desarrollar los playbooks de Ansible, validar su funcionamiento y garantizar su modularidad y escalabilidad.

2.1.4 Técnico en ciberseguridad

Asegura que las configuraciones automatizadas cumplan con las normativas de seguridad, y gestiona el control de accesos y auditorías.

2.1.5 Documentalista técnico

Redacta y mantiene la documentación del sistema, facilitando futuras tareas de mantenimiento, formación y escalabilidad.

2.2 Recursos Legales

- Es fundamental respetar el marco jurídico aplicable, incluyendo:
- Cumplimiento del RGPD y la LOPDGDD en el tratamiento de datos personales.
- Aplicación de estándares como ISO/IEC 20000-1, ENS y normativa de ciberseguridad (Ley 43/2021).
- Respeto a la licencia GPLv3 al utilizar Ansible y reutilizar sus componentes.
- Observancia de las obligaciones laborales y fiscales, especialmente si el proyecto se desarrolla en un entorno empresarial o freelance.

2.3 Hardware

- Servidor principal de automatización: Procesador Intel Xeon o AMD EPYC, mínimo 32GB RAM, almacenamiento SSD \geq 1TB.
- Servidores de destino (nodos): Equipos con sistemas Linux compatibles (Ubuntu, Debian, CentOS), configurados para permitir conexiones SSH seguras.
- Equipos de red: Switches y routers gestionables, compatibles con VLANs y con soporte para configuración remota.
- Firewall físico o virtual: Para asegurar segmentación y políticas de acceso.

2.4 Software

- Ansible (última versión estable).
- Sistemas operativos Linux (Ubuntu Server preferentemente).
- Herramientas complementarias: Git para control de versiones, herramientas de monitoreo (como Zabbix o Nagios), y editores de texto como Visual Studio Code.
- Sistemas de control de acceso y autenticación (por ejemplo, FreeIPA o servicios LDAP, si aplica).

2.5 Otros Requisitos Técnicos

- Seguridad: Toda comunicación entre nodos se realizará mediante canales cifrados (SSH), con autenticación por claves.
- Escalabilidad: La arquitectura estará preparada para añadir nuevos nodos y servicios sin rediseñar los playbooks.
- Calidad y rendimiento: Las tareas automatizadas deberán ejecutarse en menos de 5 minutos en entornos de prueba, garantizando eficiencia y fiabilidad.
- Prevención de riesgos laborales: Se tendrán en cuenta aspectos ergonómicos, carga de trabajo digital y desconexión laboral para el personal involucrado en entornos intensivos de programación.

3. TEMPORALIZACIÓN

Una correcta planificación temporal es esencial para garantizar el cumplimiento de los plazos y objetivos del proyecto. Se identifican las fases secuenciales con sus respectivas tareas, recursos implicados y estimación temporal.



3.1 Identificación de fases y tareas

3.1.1 Inicio (Semana 1)

- Análisis del problema.
- Estudio de viabilidad técnica y económica.
- Revisión legal inicial y recopilación de requisitos normativos.
- Reunión de lanzamiento del equipo de trabajo.

3.1.2 Planificación (Semana 2)

- Definición de la arquitectura de red objetivo.
- Identificación de recursos técnicos y humanos.
- Elaboración de plan de trabajo y cronograma detallado.
- Revisión de permisos, riesgos laborales y compliance.

3.1.3 Ejecución (Semanas 3 a 6)

- Desarrollo de playbooks de Ansible para cada servicio (DNS, DHCP, servidor web).
- Despliegue de entornos de prueba controlados.
- Validación funcional de configuraciones.
- Ajuste de parámetros y pruebas de escalabilidad.

3.1.4 Control y pruebas (Semanas 7 y 8)

- Ejecución de pruebas de seguridad, rendimiento y recuperación ante fallos.
- Verificación del cumplimiento normativo.
- Análisis de trazabilidad y generación de logs automáticos.

3.1.5 Cierre (Semana 9)

- Documentación técnica completa (manual de instalación, guía de mantenimiento, inventario de nodos y configuraciones).
- Evaluación del proyecto y presentación de resultados.
- Retroalimentación y cierre formal con stakeholders.

3.2 SECUENCIACIÓN

Fase	Semana	Actividades principales
Inicio	1	Análisis, viabilidad, requisitos legales
Planificación	2	Arquitectura, recursos, planificación
Ejecución	3–6	Desarrollo y pruebas de playbooks
Control	7–8	Validaciones, seguridad, rendimiento
Cierre	9	Documentación, presentación y entrega final

4. DOCUMENTACIÓN TÉCNICA

Durante el proyecto se generará documentación técnica detallada para garantizar la reproducibilidad, mantenimiento y escalabilidad del sistema automatizado.

4.1 Elementos documentales

Diagramas de arquitectura de red: Segmentación lógica, roles de cada nodo, políticas de acceso y zonas de seguridad.

Diagrama de flujo de procesos Ansible: Secuencia de ejecución de playbooks, lógica condicional, gestión de errores.

Fragmentos de código Ansible: Roles definidos, variables de entorno, configuraciones YAML comentadas.

Ejemplo de playbook: Configuración automática de servidor DNS Bind9.

Manual de instalación y uso: Pasos para desplegar la solución desde cero, incluyendo requisitos previos.

Registro de pruebas funcionales: Resultado de ejecuciones, logs generados, incidencias y soluciones aplicadas.

5. ANÁLISIS ECONÓMICO

El análisis económico contempla tanto costes directos como indirectos, identificando las posibles fuentes de financiación disponibles.

5.1 Presupuesto estimado

Concepto	Detalle	Coste Aprox.
Hardware	Servidor dedicado (Xeon, 32GB RAM, SSD)	2.500 €
	Switches gestionables compatibles con VLAN	600 €
	UPS y protección eléctrica	400 €
Software / Herramientas	Sistema operativo libre (Ubuntu Server)	0 €
	Herramientas de automatización (Ansible)	0 €
	Prometheus + Grafana (código abierto)	0 €
	Costes asociados a soporte profesional opcional	300 €
Implementación	Playbooks, pruebas y documentación	2.000 €
	Instalación de servicios y pruebas funcionales	1.000 €
	Formación interna al personal	500 €
Mantenimiento y soporte	Supervisión técnica semestral (opcional)	500 €
Documentación y manuales	Redacción técnica, licencias, plan de seguridad	200 €
Costes indirectos	Consumo eléctrico estimado por año	300 €
TOTAL ESTIMADO		8.300 €

Nota: Estos valores son estimaciones y pueden variar en función del proveedor, volumen de la infraestructura y tarifas locales.

5.2 Financiación

Este proyecto puede acogerse a ayudas como:

Kit Digital: Financiación de hasta 12.000 € para pymes.

Industria Conectada 4.0: Apoyo a proyectos de automatización industrial.

Horizonte Europa / Horizonte PYME: Subvenciones orientadas a la innovación digital.

Programas regionales (CCAA): Apoyo a la transformación digital de empresas locales.

5.3 Retorno de Inversión

Aunque el coste inicial se estima en 8.300 €, los beneficios esperados permiten recuperar la inversión en un plazo aproximado de 12 a 18 meses, gracias a:

- Reducción del 60–70% en el tiempo de despliegue y configuración de servicios.
- Minimización de errores humanos y costes asociados a fallos en producción.
- Mejor gestión del tiempo del personal técnico, con ahorro en horas hombre.
- Mayor fiabilidad y continuidad del servicio, reduciendo pérdidas operativas.

Por ejemplo: Si antes un técnico dedicaba 15 horas mensuales a tareas repetitivas que ahora se automatizan, se liberan aproximadamente 180 horas al año. Con un coste medio de 25 €/hora, el ahorro directo es de 4.500 € anuales.

5.4 Evaluación de Viabilidad Económica

El proyecto es viable económicamente desde una perspectiva técnica y estratégica:

- Inversión moderada comparada con soluciones comerciales propietarias.
- Costes de mantenimiento reducidos gracias al uso de herramientas de código abierto.
- Mejor aprovechamiento de los recursos humanos, que podrán centrarse en tareas más críticas.
- Escalabilidad sin penalizaciones económicas: no existen licencias por nodo ni costes adicionales al crecer la infraestructura.

6. SEGUIMIENTO Y CONTROL

Para garantizar el cumplimiento de objetivos, se establecerá un sistema de control basado en indicadores técnicos y evaluaciones periódicas.

6.1 Indicadores de Seguimiento

Indicador	Objetivo
Tiempo de provisión	< 5 minutos por servicio
Disponibilidad	99.9% en entornos de prueba
Tasa de error	< 1% en ejecuciones de playbook
Cumplimiento normativo	100% conforme a RGPD y ENS
Seguridad de accesos	100% autenticación mediante clave

6.2 Evaluación General (DAFO)

6.2.1 Fortalezas

- Uso de software libre y ampliamente soportado.
- Automatización sin agentes, reduciendo sobrecarga.
- Escalabilidad y modularidad de la arquitectura.

6.2.2 Debilidades

- Requiere personal cualificado en Ansible y redes.
- Menor integración con entornos Windows.

6.2.3 Oportunidades

- Elegible para subvenciones y ayudas públicas.
- Aplicabilidad en sectores educativos y empresariales.

6.2.4 Amenazas

- Rápida obsolescencia tecnológica.
- Posibles brechas de seguridad si no se actualiza el sistema.

7. FUENTES DE DOCUMENTACIÓN

Herramientas y tecnologías utilizadas

Red Hat. (2023). Ansible Automation Platform documentation. <https://docs.ansible.com>

Git. (2024). Git documentation. <https://git-scm.com/doc>

Docker Inc. (2024). Docker Documentation. <https://docs.docker.com>

Prometheus Authors. (2024). Prometheus Documentation. <https://prometheus.io/docs/>

Grafana Labs. (2024). Grafana Documentation. <https://grafana.com/docs/>

Legislación y normativa

Agencia Española de Protección de Datos (AEPD). (2019). Guía para el cumplimiento del RGPD. <https://www.aepd.es>

BOE. (2018). Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). <https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673>

Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (RGPD). <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679>

BOE. (2022). Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad (ENS). <https://www.boe.es/eli/es/rd/2022/05/03/311>

BOE. (2021). Ley 43/2021, de medidas urgentes en materia de ciberseguridad de las redes 5G. <https://www.boe.es/eli/es/l/2021/12/29/43>

BOE. (2014). Ley 9/2014, General de Telecomunicaciones. <https://www.boe.es/buscar/doc.php?id=BOE-A-2014-4950>

BOE. (1995). Ley 31/1995, de Prevención de Riesgos Laborales. <https://www.boe.es/buscar/act.php?id=BOE-A-1995-24292>

ISO. (2018). ISO/IEC 20000-1:2018 – Information technology – Service management. <https://www.iso.org/standard/70636.html>



Licencias y software libre

Free Software Foundation. (2007). GNU General Public License version 3 (GPLv3).

<https://www.gnu.org/licenses/gpl-3.0.html>

Empresas y mercado TI en España

Axians España. (2024). Servicios y soluciones de redes e infraestructura. <https://www.axians.es>

Nunsys. (2024). Transformación digital para empresas. <https://www.nunsys.com>

Gigas Hosting. (2024). Servicios cloud y soluciones IT para empresas. <https://www.gigas.com>

Sothis. (2024). Soluciones tecnológicas empresariales. <https://www.sothis.tech>

Imagina Formación. (2024). Formación técnica en redes y automatización.

<https://www.imaginaformacion.com>

Instituto Nacional de Ciberseguridad (INCIBE). (2023). Informe de necesidades y tendencias del sector TI. <https://www.incibe.es>

Ayudas y subvenciones

Red.es. (2024). Kit Digital para PYMEs. <https://www.acelerapyme.gob.es/kit-digital>

Ministerio de Industria, Comercio y Turismo. (2024). Programa Industria Conectada 4.0.

<https://www.industriaconectada40.gob.es>

Comisión Europea. (2024). Horizonte Europa: Programa de financiación de I+D.

<https://ec.europa.eu/programmes/horizon2020/>

8. ANEXOS