TRABAJO FIN DE GRADO

UCAM
UNIVERSIDAD CATÓLICA
DE MURCIA

ESCUELA POLITÉCNICA SUPERIOR

Grado en Ingeniería Informática

SOLUCIÓN PARA LA GESTIÓN Y CUMPLIMIENTO DE LA NORMA ISO 27001 CON SOPORTE DE IA

Autor:

Jaime Dionisio Burillo

Directora:

Dra.Dña. Magdalena Cantabella Sabater

Murcia, junio de 2025

TRABAJO FIN DE GRADO

UCAM
UNIVERSIDAD CATÓLICA DE MURCIA

ESCUELA POLITÉCNICA SUPERIOR

Grado en Ingeniería Informática

SOLUCIÓN PARA LA GESTIÓN Y CUMPLIMIENTO DE LA NORMA ISO 27001 CON SOPORTE DE IA

Autor:

Jaime Dionisio Burillo

Directora:

Dra. Dña. Magdalena Cantabella Sabater

Murcia, junio de 2025

https://youtu.be/Me77dglpTmI

Agradecimientos

Quiero dar las gracias, en primer lugar, a mi mujer y a mis hijos, por haberme permitido sacar tiempo para estudiar, asistir a clases y trabajar en este proyecto. Mi mujer, además, ha sido quien más me ha animado a seguir adelante, convenciéndome más de una vez de que valía la pena intentarlo. Su apoyo ha sido clave para que pudiera llegar hasta aquí.

También quiero agradecer a Francisco Manuel Moreno y a mi hermano Alejandro Dionisio, que nunca me han dejado solo en este camino. Siempre han estado ahí para ayudarme y compartir su conocimiento cuando más lo he necesitado, y su apoyo ha sido clave para que hoy pueda estar cerrando esta etapa.

Agradezco especialmente a la catedrática Esperanza Marcos, con quien coincidí en un momento de cambio. Gracias a su confianza, hoy tengo la oportunidad de trabajar a su lado en el ámbito de la investigación, y confío en que podremos desarrollar juntos proyectos relevantes en ingeniería de servicios.

Gracias también a Magdalena Cantabella Sabater, directora de este TFG, por su guía, disponibilidad y apoyo durante el desarrollo del trabajo.

Y, por último, quiero reconocer el esfuerzo personal que me ha llevado hasta aquí. Retomar los estudios a estas alturas de mi vida no era fácil, y durante mucho tiempo pensé que quizá no llegaría a conseguirlo. Sin embargo, con trabajo y constancia, este sueño que llevaba tanto tiempo persiguiendo hoy por fin se ha hecho realidad. Ha sido un reto enorme, pero también una satisfacción personal que sin duda ha merecido la pena.

Listado de Abreviatura

IA, Inteligencia Artificial

ISO, Internacional Organization for Standardization

SGSI, Sistema de Gestión de Seguridad de la Información

TFG Trabajo Fin de Grado

PYME, Pequeña y Mediana Empresa

CIO, Chief Information Officer or IT manager

AWS, Amazon Web Services

CI/CD, Integración Continua (Continuous Integration, CI) y Despliegue Continuo (Continuous Deployment, CD)

BBDD Base de datos.

UI/UX: User Interface / User Experience

API: Application Programming Interface

E/R: Entidad-Relación

ÍNDICE

ÍNDICE DE ELEMENTOS GRÁFICOS

TABLA

GRÁFICO

RESUMEN

Introducción: Este Trabajo Fin de Grado presenta el diseño y desarrollo de una aplicación web destinada a facilitar el proceso de auditoría y gestión del cumplimiento de la norma ISO 27001, enfocándose específicamente en los controles de seguridad de la información. **Objetivos:** El objetivo principal es ayudar a las pequeñas y medianas empresas (PYMES) a justificar y evidenciar el cumplimiento de los controles de seguridad exigidos por la norma ISO 27001, sin depender continuamente de un auditor experto. La aplicación incorpora inteligencia artificial (ChatGPT) para ofrecer recomendaciones automáticas y sugerencias de mejora. **Metodología:** Para la gestión del proyecto se ha seguido una metodología híbrida Water-Scrum-Fall, aplicando el modelo Waterfall en la planificación inicial y el cierre, y utilizando SCRUM en la fase de desarrollo de funcionalidades. **Resultado**: El desarrollo ha dado lugar a una herramienta web funcional, con gestión de roles, carga de evidencias, categorización de controles y visualización gráfica del grado de cumplimiento global y por áreas. Es útil tanto para auditores como para empresas auditadas. **Conclusiones:** En síntesis, el proyecto ofrece una solución práctica, asequible y autónoma para que las PYMES puedan abordar el cumplimiento de la ISO 27001 con mayor facilidad y eficiencia, haciendo uso de tecnologías actuales como la inteligencia artificial.

Palabras claves:

ISO 27001, auditoría, seguridad de la información, inteligencia artificial, Water-Scrum-Fall, PYMES, cumplimiento normativo, herramienta web.

ABSTRACT

Introduction: This Final Degree Project presents the design and development of a web application aimed at facilitating the audit and compliance management process for the ISO 27001 standard, specifically focusing on information security controls. **Objectives:** The main objective is to assist small and medium-sized enterprises (SMEs) in justifying and demonstrating compliance with the security controls required by ISO 27001, without the constant need for an expert auditor. The application incorporates artificial intelligence (ChatGPT) to provide automatic recommendations and improvement suggestions. **Methodology:** A hybrid Water-Scrum-Fall methodology was followed for project management, applying the Waterfall model during the initial planning and closing phases, and using SCRUM for the functional development stage. **Result:** The result is a functional web-based tool that includes role management, evidence uploading, control categorization, and graphical visualization of compliance levels both globally and by thematic areas. It is useful for both auditors and audited companies. **Conclusions:** In summary, the project delivers a practical, affordable, and autonomous solution that enables SMEs to approach ISO 27001 compliance more easily and efficiently, leveraging modern technologies such as artificial intelligence.

Keywords:

ISO 27001, auditing, information security, artificial intelligence, Water-Scrum-Fall, SMEs, regulatory compliance, web tool

1. INTRODUCCIÓN

1.1. Motivación

En los entornos empresariales actuales, proteger la información y garantizar la confianza son uno de los pilares fundamentales. La norma ISO 27001 (International Organization for Standardization [ISO], 2022) se ha posicionado como un pilar fundamental en todas aquellas empresas donde su información es uno de los activos más valiosos que poseen.

A pesar de que este marco sirve para proporcionar una guía integral que permite identificar los riesgos, aplicar los controles adecuados y cumplir con todas las normativas vigentes, el proceso de auditar esta norma no está exento de desafíos ya que suele ser mucho más complejo, caro y, en muchos casos, depende casi siempre de consultores externos. Para muchas empresas, esto supone un obstáculo significativo haciendo muy difícil su ejecución en pequeñas y medianas empresas.

La motivación principal para hacer este Trabajo Fin de Grado surge de la necesidad observada durante mi experiencia laboral donde pude comprobar que era muy complicado de forma autónoma abordar estas auditorías y el coste de una empresa auditora externa no era fácilmente asumible por pequeñas y medianas empresas. Pude comprobar de primera mano que hasta que mi empresa no pasó de PYME a gran empresa no pudo permitirse incluir en los presupuestos de IT y Ciberseguridad, el coste de una empresa auditora externa.

En varias ocasiones, me he enfrenté a las dificultades que conlleva evaluar y documentar de manera efectiva el cumplimiento de los 93 controles de la ISO 27001 incluso con la ayuda de empresas externas. Entre los problemas más comunes que me encontré se encuentran la gran dependencia de auditores, la falta de herramientas específicas que ayuden con el seguimiento y gestión de los controles de la norma y, por último, la necesidad de personal capacitado dentro del departamento con roles no solo de IT sino con conocimiento de negocio para poder interpretar tanto los requerimientos como los resultados de las auditorías.

Esta necesidad en mi entorno laboral es la que me llevó a pensar en una solución que pudiera automatizar parte de estos procesos. Con el auge de tecnologías emergentes como la inteligencia artificial generativa, vi una oportunidad única para transformar el enfoque tradicional de las auditorías. La implementación de un módulo de IA Generativa basada en ChatGPT tiene el potencial de revolucionar el proceso, actuando como un "auditor digital" que proporcionará recomendaciones personalizadas, reduciendo los costos y aumentando la autonomía de las empresas.

Como se explica en el artículo de la web secureframe.com (Secureframe, 2025), las empresas pueden esperar pagar más de 15.000 USD por la auditoría de certificación inicial realizada por un organismo certificador acreditado. Y, además, se deben considerar auditorías de seguimiento anuales para mantener la certificación, con un costo aproximado de 10.000 USD por año

A esto hay que añadir los costos internos: Es fundamental considerar el tiempo y los recursos que el personal dedicará a la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI). (Advisera, 2011)

1.2. Definición

Este Trabajo Fin de Grado (TFG) trata sobre el diseño y desarrollo de una herramienta web que busca facilitar la gestión y auditoría del cumplimiento de la norma ISO 27001. Esta norma es un estándar internacional muy reconocido en seguridad de la información (GlobalSuite Solutions, 2023). La herramienta está orientada para que la puedan usar tanto empresas como auditores. Sirve para llevar un seguimiento detallado (y más organizado) del nivel de cumplimiento de los 93 controles que exige la norma.

Actualmente, hay bastantes empresas que tienen problemas para cumplir con ISO 27001 (ISOTools, 2018). La mayoría de estos problemas son debidos a que a pesar de que hay herramientas especializadas que puedan simplificar el proceso, a menudo es necesario depender en exceso de consultores externos, lo que, además de ser caro, reduce bastante su autonomía en la implementación.

Aunque ya existen sistemas que organizan toda la información necesaria (Ver apartado 2.2. Relación con proyectos con la misma funcionalidad), muchas veces es difícil hacer un seguimiento claro de cada control mientras se va aplicando. Esto suele provocar retrasos en la certificación. O incluso podría aumentar el riesgo de que no cumplan con algunos requisitos importantes.

Por estas razones, surge la idea de desarrollar esta herramienta. Una solución que permita a las empresas gestionar mejor todo lo relacionado con la norma y tener más independencia en el proceso.

El proyecto se fundamenta en dos pilares principales:

1. **Automatización y eficiencia en las auditorías:**

   A través de una interfaz intuitiva y funcionalidades específicas, se busca simplificar el proceso de auditoría, reduciendo la carga administrativa y mejorando la trazabilidad de las evaluaciones realizadas. Esto incluye la capacidad de registrar evidencia, generar informes consolidados y realizar un seguimiento continuo de las acciones correctivas.

2. **Integración de Inteligencia Artificial Generativa:**

   Uno de los elementos diferenciadores del proyecto es la incorporación de un módulo de IA Generativa basado en ChatGPT. Este módulo actúa como un "auditor digital", analizando las respuestas proporcionadas por el usuario para cada control y generando recomendaciones personalizadas. Estas recomendaciones incluyen:

   - Identificación de fortalezas y debilidades en las medidas implementadas.
   - Detección de información faltante para una correcta evaluación.
   - Propuestas de mejora concretas para alcanzar o mantener el cumplimiento.

En conjunto, esta herramienta no solo busca optimizar los procesos de auditoría, sino también fortalecer a las empresas, permitiéndoles una mayor autonomía en la gestión de la seguridad de la información y una reducción significativa de costos asociados. La aplicación destaca por su enfoque innovador que integra tecnologías de gran actualidad (IA) para abordar problemas reales en el cumplimiento de la norma ISO 27001.

1.3. Objetivos propuestos

1.3.1. Objetivo general

Diseñar y desarrollar una herramienta web que facilite la gestión y auditoría del cumplimiento de la norma ISO 27001. Permitiendo tanto a empresas como a auditores realizar evaluaciones detalladas y a su vez poder recibir recomendaciones automáticas mediante un módulo de inteligencia artificial generativa basado en el uso de ChatGPT.

1.3.2. Objetivos específicos

1. **Diseñar un sistema de gestión de auditorías por empresa y año.**

   Diseñar un sistema de gestión de auditorías por empresa y año. Implementar una funcionalidad que permita registrar y organizar auditorías de acuerdo con cada empresa y su correspondiente año, ofreciendo vistas personalizadas según el perfil del usuario. Los auditores tendrán acceso a todas las empresas, mientras que los usuarios internos de cada empresa podrán consultar únicamente la información que les concierne.

2. **Crear una interfaz intuitiva que permita un fácil seguimiento de los controles**

   Desarrollar una interfaz amigable, que facilite la navegación y búsqueda entre los controles auditados, mostrando rápidamente el estado actual de cada uno. Los controles se mostrarán organizados por las 4 categorías de la norma.

3. **Integrar inteligencia artificial para apoyar el análisis de auditorías** Incorporar un módulo basado en IA que proporcione recomendaciones específicas para cada control, incluyendo sugerencias de mejora y análisis automatizado de las acciones realizadas. Este módulo junto con la ayuda contextual sobre cada control, ayudarán a los usuarios a comprender mejor las acciones necesarias para alcanzar el cumplimiento normativo y el grado de cumplimiento al que han llegado.

4. **Generar informes detallados sobre el estado de las auditorías** Diseñar un sistema de generación de informes que resuma el progreso de las auditorías, incluyendo gráficos, indicadores visuales y un análisis del estado de cumplimiento de los controles. Los informes estarán enfocados para que tanto un CIO o un auditor dispongan de un Dashboard en tiempo real del estado de la auditoría.

5. **Permitir por cada control adjuntar información y documentos asociados al cumplimiento de cada uno de los controles.** Permitir que los usuarios registren documentación y pruebas detalladas sobre las acciones realizadas en cada control y adjunten documentos relevantes como evidencias de cumplimiento.

6. **Desarrollar una interfaz de gestión para administradores** Crear una plataforma de exclusiva para administradores que permita gestionar el conjunto de operaciones básicas (crear, leer, actualizar y eliminar) para gestionar la configuración global del sistema, como la creación de empresas, la asignación de auditorías por año, y la gestión usuarios, roles, controles y auditorías.

2. ESTUDIO DEL MERCADO

2.1. Conceptos relevantes del dominio de aplicación.

La gestión de la seguridad de la información se basa en la identificación, evaluación y mitigación de riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de los datos.

La norma ISO 27001 actúa como un estándar internacional que define las mejores prácticas para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI).

Un SGSI permite a las organizaciones gestionar sus activos de información de manera segura a través de:

- **Análisis de riesgos:** Identificar y evaluar amenazas y vulnerabilidades.
- **Controles de seguridad:** Implementar medidas técnicas, organizativas y administrativas para mitigar riesgos.
- **Cumplimiento normativo:** Asegurar que las prácticas de seguridad estén alineadas con regulaciones aplicables, como el RGPD u otras normas de aplicación.

Los 93 controles de la norma ISO 27001 se agrupan en **4 categorías principales:**

1. **Controles Organizacionales (37 controles):** Estos controles se enfocan en las políticas, procedimientos, roles y responsabilidades dentro de la organización.
    a. Políticas de seguridad de la información.
    b. Gestión de la seguridad de la información.
    c. Clasificación y manejo de información.
    d. Gestión de terceros.
    e. Gestión de riesgos de seguridad de la información.

f. Continuidad del negocio relacionada con la seguridad.

g. Concienciación y formación en seguridad.

h. Revisión independiente de la seguridad de la información.

i. Otros controles relacionados con la gestión organizacional.

2. **Controles de Personas (8 controles):** Estos se centran en las personas, desde la gestión de recursos humanos hasta la capacitación y concienciación.

    a. Proceso de contratación seguro.

    b. Capacitación en seguridad.

    c. Responsabilidades relacionadas con la seguridad de los empleados y contratistas.

3. **Controles Físicos (14 controles):** Enfocados en la protección del entorno físico y las instalaciones.

    a. Seguridad de oficinas y sitios.

    b. Protección contra riesgos ambientales.

    c. Restricciones físicas de acceso.

    d. Equipamiento y mantenimiento físico.

4. **Controles Tecnológicos (34 controles):** Relacionados con la seguridad de sistemas, redes, aplicaciones y datos.

    a. Gestión de accesos.

    b. Protección contra malware.

    c. Gestión de vulnerabilidades.

    d. Seguridad en el desarrollo de sistemas y software.

    e. Controles criptográficos.

f. Registro y monitorización de actividades.

g. Respuesta ante incidentes de seguridad tecnológica.

Otro concepto clave es la auditoría de cumplimiento, es poder recoger para cada uno de los controles de la norma las siguientes evidencias:

- **Evidencias documentales:** Registros que demuestran la implementación de controles.
- **Identificación de no conformidades:** Aspectos en los que los controles no cumplen con los requisitos establecidos.
- **Acciones correctivas:** Medidas tomadas para abordar las no conformidades.

2.2. Relación con proyectos con la misma funcionalidad

En el mercado actual existen varias herramientas que ayudan a gestionar el cumplimiento de la norma ISO 27001. A continuación, se presenta un análisis de algunas de las herramientas que actualmente están en el mercado.

Scytale

Plataforma Web que centraliza la documentación y flujos de trabajo para el cumplimiento normativo. Facilita auditorías internas y asignación de tareas, además de permitir el monitoreo en tiempo real del progreso de cumplimiento (**Scytale, 2024**).

- **Ventajas:** Interfaz intuitiva y automatización de tareas repetitivas y monitoreo en tiempo real del estado de cumplimiento.
- **Desventajas:** Enfocado principalmente en empresas grandes, limitando su accesibilidad para PYMES.

ISMS.online

Herramienta diseñada para gestionar todo el ciclo de vida de un SGSI, con integraciones avanzadas y guías para implementar ISO 27001 (**ISMS.online, 2025**).

- **Ventajas:** Repositorio centralizado de documentación y capacidades de integración para grandes entornos corporativos.
- **Desventajas:** Complejidad inicial y curva de aprendizaje elevada para usuarios sin experiencia y costos altos que dificultan su adopción en PYMES.

Advisera Conformio

Solución que también proporciona guías para la implementación de controles ISO 27001, incluyendo herramientas para evaluaciones de riesgos y gestión documental (**Advisera, 2025).**

- **Ventajas:** Ideal para pequeñas empresas y diseño simplificado que facilita el uso para nuevos usuarios.
- **Desventajas:** Funcionalidades limitadas para organizaciones con necesidades avanzadas y baja personalización.

Compleye

Plataforma web que centraliza la gestión de la conformidad y ofrece plantillas predefinidas para la implementación de SGSI (**Compleye, 2023**).

- **Ventajas**: Simplificación de auditorías de ciberseguridad y más de 30 plantillas listas para su uso.
- **Desventajas**: Enfocado en startups y pequeñas empresas, lo que puede limitar su funcionalidad para empresas más grandes.

Secureframe

Solución automatizada para el cumplimiento normativo, con capacidades de monitoreo continuo y gestión de seguridad de proveedores (**Secureframe, 2025**).

- **Ventajas:** Acelera el proceso de cumplimiento y reduce el esfuerzo manual. También ofrece monitoreo continuo para garantizar el cumplimiento.
- **Desventajas:** Costos elevados para PYMES y curva de aprendizaje inicial para usuarios sin experiencia.

ProActive QMS

Herramienta integral para gestionar auditorías y certificaciones, con funcionalidades avanzadas como paneles de control, alertas y evaluaciones de conformidad (**ProActive QMS, 2025**).

- **Ventajas**: Funcionalidad robusta con soporte experto y Acceso móvil para gestión sobre la marcha.
- **Desventajas**: Costos mensuales elevados, limitando su accesibilidad para PYMES, principalmente enfocada a empresas de mediano a gran tamaño.

OnSpring

Solución flexible y personalizable para gestionar auditorías y riesgos, adaptada a grandes organizaciones (**OnSpring, 2023**).

- **Ventajas**: Alta flexibilidad y adaptabilidad a flujos de trabajo específicos e integración con otras herramientas empresariales.
- **Desventajas**: Complejidad y costos elevados que dificultan su implementación en PYMES.

2.3. Estudio de viabilidad

2.3.1. Alcance del proyecto

El alcance de este proyecto se centra en la auditoría de los 93 controles establecidos en la norma ISO 27001. Excluyendo para una segunda fase todo lo relativo a la documentación obligatoria requerida para una certificación completa del Sistema de Gestión de Seguridad de la Información (SGSI).

Los elementos que quedarían incluidos en el Alcance son:

- **Evaluación de Controles:** Se incluirá un análisis detallado del grado de implementación y de la efectividad de cada uno de los 93 controles de la ISO 27001 apoyándose en IA generativa para dicha evaluación.
- **Registro de Evidencias:** Se permitirá adjuntar aquella documentación de las pruebas que respaldan tanto el cumplimiento como aquellas que pudieran identificar deficiencias en los controles evaluados.
- **Generación de Informes:** Elaboración de reportes que reflejen el estado actual de los controles, facilitando la toma de decisiones. Estos informes están enfocados a perfiles como el CIO de la empresa o los auditores.

Elementos que quedarían Excluidos del Alcance en esta primera versión:

- **Documentación Obligatoria del SGSI:** No se contempla la creación o gestión de documentos esenciales como la política de seguridad de la información, el alcance del SGSI, la metodología de evaluación de riesgos, la declaración de aplicabilidad, entre otros. Todos ellos, son imprescindibles para una certificación completa según la ISO 27001 (**Advisera, 2013).**
- **Procesos de Certificación:** El proyecto no incluye la preparación específica para auditorías externas ni garantiza la obtención de la certificación ISO 27001, ya que se enfoca únicamente en la auditoría interna de los controles.

Este enfoque permite a las organizaciones, especialmente a las pequeñas y medianas empresas, concentrarse en la implementación y mejora continua de los controles de seguridad, estableciendo una base sólida que facilite futuras iniciativas hacia una certificación completa del SGSI.

2.3.2. Estudio de la situación actual

Las PYMES se enfrentas a diversas barreras a la hora de afrontar la implantación de la norma ISO 27001. Las principales barreras son: falta de recursos económicos, dependencia de consultores externos y a complejidad de la aplicación de la ISO.

Limitaciones Actuales:

- **Altos costes:** El coste medio de una implementación de una ISO 27001 con ayuda de una empresa especializada es muy costoso y no suele estar al alcance de los presupuestos de una PYME.
- **Dependencia de consultores:** La falta de personal capacitado genera una alta dependencia de servicios externos, elevando los costos y no permitiendo que sea el propio personal de la empresa el encargado de llevarla delante de forma autónoma.
- **Complejidad**: Pese a existir algunas aplicaciones que ayudan al cumplimiento de la ISO, la mayoría de las soluciones comerciales actuales suelen tener una curva de aprendizaje alta y no eximen de necesitar de un experto para validar que lo que se aplica cumple con la norma.

Necesidades Identificadas:

- Herramientas accesibles económicamente.
- Soluciones que incluyan funcionalidades adaptadas al tamaño y capacidad de las PYMES.
- Automatización avanzada mediante tecnologías como la inteligencia artificial.

En este contexto, la decisión de desarrollar la herramienta propuesta, no solo se diferencia por satisfacer las necesidades de las PYMES, sino que también introduce un enfoque innovador al usar la Inteligencia Artificial para suplir a los auditores externos y eliminar todos los costes asociados a estos.

3. METODOLOGÍAS USADAS

3.1. Justificación de la Metodología a Utilizar

Para el desarrollo de esta aplicación, se ha seleccionado una metodología híbrida conocida como **Water-Scrum-Fall**. Esta combina elementos de dos metodologías muy diferentes: Waterfall y Agile (SCRUM) (Cloud Coach, 2021; IEBS Business School, 2025).

Este enfoque permite mantener la gestión tradicional de proyectos Waterfall que es más estructurada, para poder cumplir con tiempos, alcance y precios fijados. Pero a la vez nos permite explotar la flexibilidad y adaptabilidad de SCRUM durante el desarrollo (Takeuchi, 2024).

Por tanto, la idea es usar Waterfall al principio y final del proyecto y SCRUM durante la fase de desarrollo y pruebas.

Aunque no es parte del alcance de este TFG, para futuras fases de ampliación y mantenimientos tanto correctivo como evolutivo se conseja el uso de SCRUM ya que es un método flexible que permite hacer cambios y agregar nuevas funciones de manera organizada, priorizando lo más importante, aportando valor en cada sprint.

3.2. Fases del Proyecto

3.2.1. Fase de Planificación y Diseño: Waterfall

En esta fase inicial del proyecto, utilizaremos la metodología Waterfall para planificación y diseño de la aplicación. Se ha elegiodo Waterfall para esta fase respondiendo a la necesidad de una estructura clara y detallada, dado que el tiempo disponible para abordar este TFG viene marcado por un máximo de 450 horas (18 créditos). Por tanto, el desarrollo debe quedar fijado y el alcance definido desde el principio.

Esta fase incluirá:

1. **Definición de funcional, Tecnologías y Análisis del Mercado:**

a. Se estudiarán herramientas y soluciones similares en el mercado para identificar tendencias en software similares y oportunidades de diferenciación con el resto de los competidores.
b. Se evaluará el tipo de solución más adecuada (web, móvil o híbrida), considerando accesibilidad, experiencia del usuario y viabilidad dentro del tiempo y recursos disponibles.
c. Y al igual que el tipo de solución, se escogerán las tecnologías más adecuadas para la implementación del sistema de nuevo asegurando compatibilidad con los requisitos funcionales, pero teniendo en cuenta de nuevo el poco tiempo del que se dispone para programarla.

2. **Estructuración del Proyecto, Alcance y Planificación Futura:**
   a. Durante esta fase se delimitará el alcance del desarrollo inicial. Definiremos que funcionalidades serán implementadas en este proyecto y cuales se abordarán en futuras expansiones formando parte de un futuro proyecto evolutivo.

Por todo esto, resulta más conveniente optar por el método Waterfall en esta fase. Este enfoque permite definir claramente el proyecto, reduciendo así el riesgo de desviaciones. De esta manera, aseguramos a futuro que cada fase se completará dentro de los plazos establecidos desde el inicio y por tanto no se comprometerá la planificación inicial.

3.2.2. Fase de Desarrollo: Agile (SCRUM)

Una vez completada la fase de planificación y diseño, toda la fase de desarrollo se llevará a cabo mediante la metodología Agile. Más concretamente se adoptará el marco de trabajo SCRUM.

Esta fase se llevará a cabo en ciclos iterativos (sprints). Esto facilita la entrega continua y el ajuste de la aplicación a medida que se avanza en su desarrollo.

Los aspectos a destacar de esta fase y de la metodología Agile son:

1. **Preparación del Backlog y Planificación de Sprints:**

Antes de iniciar los sprints, se elaborará un backlog detallado con todas las user stories necesarias para el desarrollo del sistema, priorizando las tareas según su impacto y necesidad.

2. **Planificación de Sprints:**
   En cada sprint (que en este proyecto, tendrán una duración aproximada de dos semanas), se priorizarán las tareas de desarrollo para poder desde el primer momento aportar valor a la aplicación. Se comenzará montando un sistema de login, luego un CRUD para la ingesta y administración de los datos maestros, y posteriormente se irá avanzando en tareas más complejas ya relacionadas con las auditorías. Finalmente se abordarán las integraciones de IA de ChatGPT como apoyo a las respuestas de los usuarios y los informes o dashboards.
3. **Desarrollo Incremental:**
   SCRUM permite la entrega de funcionalidades de manera incremental, esto garantiza que al final de cada sprint se obtenga una versión funcional de la aplicación.
   Esta planificación permite asegurar que las funcionalidades que se van entregando vayan desde el principio generando valor y puedan validarse en una fase temprana sin tener que esperar a fases posteriores. Esto evita tener que rehacer partes del código más adelante y permite realizar ajustes en función de la retroalimentación recibida al final de cada Sprint.
4. **Revisión y Ajustes:**
   Al final de cada sprint, se llevará a cabo una revisión junto con los stakeholders, Es aquí cuándo podremos identificar áreas de mejora o ajustes a realizar en el siguiente ciclo de desarrollo (sprint).

Este enfoque como ya he indicado anteriormente facilita la adaptabilidad a los cambios y nos permite mantener la calidad de la aplicación a lo largo del proyecto.

El uso de Agile, y específicamente SCRUM, se caracteriza por proporcionar flexibilidad y adaptabilidad. Esto es esencial para garantizar que las funcionalidades se ajusten de acuerdo con los comentarios y las necesidades de los usuarios, que pueden ir cambiando a durante el desarrollo de la aplicación. Además, permite realizar ajustes rápidos sin afectar la planificación global.

3.2.3. Fase de Implementación y Lanzamiento: Waterfall

Una vez que se hayan completado los sprints de desarrollo, la fase de implementación y lanzamiento volverá a seguir un enfoque Waterfall. Esta fase incluirá:

1. **Documentación:**

En esta etapa, se generará la documentación técnica y de usuario necesaria para el uso adecuado de la aplicación.

2. **Lanzamiento:**

Una vez validadas todas las funcionalidades, la aplicación se desplegará en el entorno de producción.

3. **Post-mortem**

Se realizará un post-mortem del proyecto para analizar los resultados, identificar los aciertos y las áreas de mejora. Esta evaluación final permitirá optimizar futuros desarrollos y sentar una base sólida para la evolución de la aplicación.

El uso de Waterfall en esta fase final permite garantizar un cierre estructurado y ordenado del proyecto.

3.3. Futuras Fases de Ampliación y Mejora: SCRUM

Aunque quede fuera del alcance de este TFG, se sugiere que las futuras fases de mejora y mantenimientos evolutivos de la aplicación utilicen SCRUM de manera exclusiva. Esto permitirá:

- Introducir nuevas funcionalidades de forma iterativa y adaptativa.
- Incorporar mejoras basadas en retroalimentación real de los usuarios.
- Priorizar cambios según el valor aportado al negocio.

4. TECNOLOGÍAS Y HERRAMIENTAS UTILIZADAS EN EL PROYECTO

En este apartado se detallan las tecnologías y herramientas utilizadas en el desarrollo del proyecto. Se incluyen tanto los lenguajes de programación, bases de datos y frameworks empleados, como las herramientas utilizadas para la gestión del desarrollo y control de versiones.

El análisis realizado forma parte de la primera etapa del presente proyecto, correspondiente a la Fase de Planificación y Diseño, enmarcada dentro del enfoque Waterfall, la cual se desarrolla en detalle en el apartado 6.1.

4.1. Análisis de Tecnologías y Justificación de Elección

Antes de detallar cada tecnología usada, se procede a realizar un análisis de las opciones disponibles en el mercado y se justifica la selección de cada una.

4.1.1. Backend

Se analizaron las siguientes tecnologías para el desarrollo del backend:

- **PHP:** Lenguaje ampliamente utilizado en el desarrollo web, con buena compatibilidad con bases de datos y servidores web. Es fácil de aprender y cuenta con una gran comunidad de soporte (The PHP Group, 2023). Es de código abierto y gratuito.
- **Node.js:** Plataforma basada en JavaScript, ideal para aplicaciones en tiempo real y microservicios (Node.js Foundation, 2023). Es de código abierto y gratuito.
- **Python (Django/Flask):** Lenguaje versátil con frameworks robustos, ideal para aplicaciones con alto procesamiento de datos (Van Rossum, 2023). Es de código abierto y gratuito.
- **Java (Spring Boot):** Framework para aplicaciones empresariales, con enfoque en escalabilidad y seguridad (Pivotal Software, 2023).

Se eligió PHP por su compatibilidad con Apache y MySQL, su facilidad de desarrollo, por ser el lenguaje más conocido por el desarrollador y su integración con la API de OpenAI, crucial para la auditoría ISO 27001. Además,

PHP es una tecnología de código abierto y gratuita, lo que facilita su adopción sin costos adicionales.

4.1.2. Frontend

Se compararon las siguientes opciones para el diseño del frontend:

- **Bootstrap:** Framework CSS con componentes predefinidos para el desarrollo rápido de interfaces responsivas (Bootstrap, 2023). Es de código abierto y gratuito.
- **Tailwind CSS:** Sistema de utilidades CSS altamente personalizable, aunque con una curva de aprendizaje mayor (Tailwind Labs, 2023). Es de código abierto y gratuito.
- **Material UI:** Biblioteca de componentes basada en Material Design, ideal para aplicaciones React (Google, 2023).

Se eligió **Bootstrap** ya que permite un desarrollo ágil, garantizando una interfaz responsiva sin necesidad de personalizar estilos desde cero, lo que reduce el tiempo de desarrollo. Además, al ser de código abierto y gratuito, facilita su adopción sin costos adicionales.

4.1.3. Entorno de Desarrollo

Las herramientas evaluadas fueron:

- **XAMPP:** Paquete todo-en-uno con Apache, PHP y MySQL, de fácil instalación (Apache Friends, 2023). Es de código abierto y gratuito.
- **Laragon:** Alternativa a XAMPP, optimizada para Windows (Laragon, 2023). Es de código abierto y gratuito.
- **Docker:** Plataforma basada en contenedores, ideal para entornos escalables (Docker Inc., 2023). Es de código abierto y gratuito.

Se eligió XAMPP por su facilidad de instalación y compatibilidad con las tecnologías usadas. Además, al ser de código abierto y gratuito, facilita su uso en entornos de desarrollo sin costos adicionales.

4.1.4. Editor de Código

Se evaluaron:

Visual Studio Code (VS Code): Editor ligero con soporte para extensiones y Git (Microsoft, 2023). Es de código abierto y gratuito.

PHPStorm: IDE especializado en PHP, con herramientas avanzadas (JetBrains, 2023).

Sublime Text: Editor rápido, pero con menos integraciones modernas (Sublime HQ, 2023).

VS Code fue seleccionado por su facilidad de uso, integración con GitHub y extensibilidad. Al ser de código abierto y gratuito, permite su utilización sin costos de licencia.

4.1.5. Control de Versiones

Opciones consideradas:

- **GitHub:** Plataforma basada en Git con amplia adopción (GitHub, 2023). Dispone de una versión gratuita.
- **GitLab:** Alternativa con mejor integración CI/CD (GitLab Inc., 2023). Dispone de una versión gratuita.
- **Bitbucket:** Utilizado principalmente con Atlassian (Atlassian, 2023). Dispone de una versión gratuita.

Se eligió GitHub por su integración con VS Code y facilidad de gestión de ramas. Además, su versión gratuita permite almacenar repositorios y gestionar el control de versiones sin costos adicionales.

4.2. Tecnologías Usadas

4.2.1. Backend: PHP 8.2.12

PHP (Hypertext Preprocessor) es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML (The PHP Group, 2023).

PHP a diferencia de javascript se ejecuta del lado del servidor por tanto el cliente solo ve el código html resultante sin poder ver que es lo que php hace por detrás. También te permite consultar contenidos de bases de datos facilitando la interacción con sistemas como MySQL (Oracle Corporation, 2023).

Actualmente esta tecnología es la base de muchas páginas web dinámicas y sistemas de gestión de contenidos populares, como WordPress o Joomla (The PHP Group, 2023).

Algunas características destacadas de PHP incluyen:

- **Interactividad con servidores web:** PHP se ejecuta en el servidor y permite generar contenido dinámico en las páginas web (The PHP Group, 2023).
- **Compatibilidad con múltiples bases de datos:** Admite MySQL, PostgreSQL, SQLite y otros sistemas de gestión de bases de datos (Oracle Corporation, 2023).
- **Extensibilidad mediante bibliotecas:** PHP permite la integración de múltiples bibliotecas y frameworks para ampliar sus funcionalidades (The PHP Group, 2023).
- **Comunidad activa y documentación extensa:** PHP cuenta con una gran comunidad de desarrolladores y recursos en línea para soporte (The PHP Group, 2023)

En este proyecto, PHP es el lenguaje principal del backend, utilizado para manejar la lógica de negocio, la autenticación de usuarios, la gestión de auditorías y la comunicación con la base de datos MySQL. Además, PHP permite la integración con la inteligencia artificial de OpenAi , necesario para la ejecución de este proyecto.

La elección de PHP para este proyecto se debe principalmente a su facilidad de uso, pero también a su amplia compatibilidad y la disponibilidad de bibliotecas y herramientas que facilitan el desarrollo de aplicaciones robustas y escalables.

4.2.2. FrontEnd: Bootstrap

Bootstrap es un framework de código abierto diseñado para facilitar el desarrollo de sitios y aplicaciones web. Proporciona una colección de estilos predefinidos en CSS y componentes reutilizables en JavaScript, lo que permite crear interfaces de usuario modernas y adaptables (Bootstrap, 2023).

Bootstrap se caracteriza por su diseño responsivo, lo que le permite adaptarse automáticamente a distintos tamaños de pantalla y dispositivos, asegurando una correcta experiencia de usuario. Además, ofrece una amplia variedad de componentes reutilizables, como botones, formularios, alertas y modales, que facilitan el desarrollo de las interfaces sin necesidad de crear los elementos desde cero.

Otra ventaja de Bootstrap es su compatibilidad con múltiples navegadores, garantizando un funcionamiento estable en los principales navegadores como Chrome, Firefox, Edge y Safari. Asimismo, permite modificar estilos fácilmente mediante CSS o variables en SCSS, permitiendo adaptar la apariencia del diseño a las necesidades específicas de cada proyecto.

La elección de Bootstrap en este proyecto se debe a su facilidad de integración con HTML, CSS y JavaScript, además de su amplia documentación, que agiliza el desarrollo de interfaces. Se ha utilizado para la construcción del frontend, garantizando una interfaz de usuario moderna, intuitiva y adaptable a distintos dispositivos gracias a sus componentes predefinidos, lo que ha permitido reducir mucho el tiempo de desarrollo.

4.3. Herramientas de Desarrollo y Gestión Usadas

4.3.1. Servidor Local - XAMPP 3.3.0

XAMPP es un entorno de desarrollo que permite configurar un servidor local de manera sencilla. Se compone de Apache (servidor web), MySQL/MariaDB (gestor de bases de datos), PHP (lenguaje de programación) y Perl (Apache Friends, 2023.). Su instalación simplificada y compatibilidad con

múltiples sistemas operativos lo convierten en una herramienta ideal para el desarrollo y pruebas de aplicaciones web.

En este proyecto, XAMPP 3.3.0 se ha utilizado como entorno de desarrollo local para probar y validar la funcionalidad de la aplicación antes de su implementación en un entorno de producción.

Algunas características clave de XAMPP incluyen:

- Facilidad de instalación: Proporciona un paquete preconfigurado con todos los servicios necesarios.
- Compatibilidad con múltiples plataformas: Funciona en Windows, macOS y Linux.
- Panel de control intuitivo: Permite desde este, gestionar el servidor Apache, la base de datos MySQL y la configuración de PHP.

La elección de XAMPP en este proyecto se debe a su facilidad de uso, su rápida configuración y su integración con las tecnologías usadas en este proyecto: PHP y MySQL.

4.3.2. Editor de Código:Visual Studio Code

Visual Studio Code (VS Code) es un editor de código fuente desarrollado por Microsoft. Se trata de una herramienta ligera, soporta múltiples lenguajes de programación. Permite personalizar el entorno de trabajo gracias a su compatibilidad con numerosas extensiones (Microsoft, 2023).

Algunas de las características clave de Visual Studio Code incluyen:

- Soporte para múltiples lenguajes: Compatible con PHP, JavaScript, HTML, CSS, entre otros.
- Extensibilidad: Posibilidad de instalar extensiones para añadir funcionalidades adicionales como depuración, resaltado de sintaxis y autocompletado de código.

- Integración con Git: Permite la gestión de repositorios directamente desde el editor.
- Depuración integrada: Facilita la identificación y solución de errores en el código.
- Live Server: Extensión útil para visualizar cambios en tiempo real en proyectos web.

En este proyecto, Visual Studio Code se ha utilizado como el editor de código principal para el desarrollo del backend en PHP y la gestión de archivos de frontend con HTML, CSS y JavaScript. Su integración con Git y GitHub ha facilitado el control de versiones del código fuente directamente desde el editor.

La elección de Visual Studio Code en este proyecto se debe principalmente a que es una herramienta gratuita y de código abierto y que cubre el 100% de las funcionalidades que se necesitaban para ejecutar este proyecto. También, se ha tenido en cuenta su facilidad de uso y de nuevo la amplia comunidad de soporte, garantizando soluciones a posibles problemas durante el desarrollo.

4.3.3. Control de Versiones: GitHub

GitHub es una plataforma de control de versiones basada en Git que permite la colaboración y gestión eficiente del código fuente en proyectos de software. Es ampliamente utilizada para almacenar, compartir y mantener el historial de cambios en los archivos de código mediante repositorios remotos. Destacar de GitHub:

- Control de versiones distribuido: Permite a los desarrolladores trabajar en paralelo sin conflictos.
- Gestión de ramas: Facilita la organización del trabajo mediante ramas dedicadas a desarrollo, pruebas y producción.
- Compatible con herramientas de automatización para pruebas y despliegue continuo como Azure Devops

- Historial de cambios y revisiones: Posibilita la recuperación de versiones anteriores y la auditoría del código fuente.

Se decidió usar GitHub en este proyecto por su integración con Visual Studio Code, su facilidad para administrar ramas y la posibilidad de recuperar versiones del histórico del código. Durante el proyecto, el código se ha estructurado a través del uso de dos ramas principales:

- Branch “desarrollo”: Destinada a la implementación y prueba de nuevas funcionalidades antes de su despliegue.
- Branch “main”: Contiene la versión estable del código, lista para producción.

*4.3.4. Integración con IA: **API de ChatGPT***

La Inteligencia Artificial Generativa (IA Generativa) es un tipo de inteligencia artificial diseñada para crear contenido original a partir de patrones y datos previamente analizados. A diferencia de los sistemas tradicionales de IA que se limitan a clasificar, analizar o predecir datos, la IA generativa tiene la capacidad de producir contenido de manera autónoma (OpenAI, 2023a).

Un ejemplo destacado de IA generativa es ChatGPT, un modelo de inteligencia artificial desarrollado por OpenAI, diseñado para generar respuestas en lenguaje natural a partir de texto ingresado por un usuario. Utiliza técnicas de aprendizaje profundo y procesamiento del lenguaje natural (NLP) para comprender preguntas y generar respuestas coherentes y útiles en diversos contextos (OpenAI, 2023b).

Se basa en la arquitectura GPT (Generative Pre-trained Transformer), entrenada con grandes volúmenes de texto para responder preguntas, ayudar en la redacción de contenido, programar, traducir y mucho más (OpenAI, 2023b).

La API de ChatGPT es una interfaz que permite integrar las capacidades del modelo en aplicaciones, sitios web o sistemas sin necesidad de usar directamente la plataforma de OpenAI (OpenAI, 2023a).

A través de la API, los desarrolladores pueden enviar consultas al modelo y recibir respuestas automatizadas, lo que permite crear asistentes virtuales, chatbots, herramientas de automatización, generación de contenido, entre otros.

En este proyecto, la API de OpenAI se ha utilizado para evaluar la información ingresada en las auditorías ISO 27001, proporcionando retroalimentación sobre el cumplimiento de los controles, posibles mejoras y una estimación del nivel de conformidad alcanzado.

La integración con PHP se realiza mediante solicitudes HTTP a la API de OpenAI. Esto permite enviar información estructurada sobre las auditorías y recibir respuestas en formato JSON con análisis automatizados.

Justamente el uso de la API de OpenAI en este proyecto es lo destaca a esta herramienta de auditoría frente al resto de herramientas del mercado.

5. ESTIMACIÓN DE RECURSOS Y PLANIFICACIÓN

5.1. Preparación para SCRUM

5.1.1. Roles dentro del equipo

Scrum define tres roles principales en el equipo de trabajo: el Product Owner, el Scrum Master y el Development Team. Estos roles facilitan la gestión ágil del proyecto y optimizan el desarrollo de software en ciclos iterativos. (Schwaber y Sutherland, 2020).

Para la correcta ejecución del modelo Scrum, se han identificado los siguientes roles necesarios:

- **Product Owner (PO):** Define las prioridades del proyecto, mantiene el backlog y asegura que el producto final cumple con los requisitos del usuario o stakeholder.
- **Scrum Master:** Facilita el proceso Scrum, eliminando impedimentos y asegurando que el equipo siga la metodología.
- **Development Team:** Equipo encargado del desarrollo, compuesto por programadores.

5.1.2. Creación de épicas, features y backlog items

El backlog de producto en Scrum se estructura jerárquicamente en épicas, features y user stories. Esta organización permite una planificación más eficiente y una mejor adaptabilidad a los cambios durante el desarrollo del proyecto (Rubin, 2012).

- **Épicas:** Son grandes bloques funcionales que agrupan características relacionadas dentro del producto. Representan objetivos clave y de alto nivel.
- **Features:** Cada épica se divide en features, que son funcionalidades específicas que permiten el cumplimiento del objetivo de la épica.

- **Backlog Items (User Stories):** Son tareas detalladas dentro de cada feature, diseñadas desde la perspectiva del usuario final para describir necesidades específicas.

5.1.3. Estimación basada en Rangos de Complejidad en el Proyecto

En metodologías ágiles como Scrum, la estimación del esfuerzo se suele realizar con la técnica de Planning Poker, donde un equipo de desarrollo asigna puntos de esfuerzo a cada backlog item de manera colaborativa (Schwaber & Sutherland, 2020). Sin embargo, dado que este proyecto ha sido desarrollado de manera individual sin contar con un grupo de desarrollo y coincidiendo en la misma persona los diferentes roles de Scrum, se ha optado por una estimación personal basada en Rangos de Complejidad en lugar de Planning Poker.

Este método permite evaluar la complejidad de cada tarea de forma relativa, considerando factores como el tiempo requerido, la incertidumbre y la dificultad de implementación, utilizando una escala de valores predefinidos que reflejan distintos niveles de esfuerzo y complejidad (Fairley, 2009).

Proceso de Estimación:

1. Se analizaron todas las user stories y se definió claramente su alcance.
2. Se compararon tareas para determinar su complejidad relativa.
3. Se asignó un puntaje basado en rangos de complejidad, considerando la dificultad técnica y el esfuerzo estimado.
4. En caso de encontrar tareas con un puntaje demasiado alto, se evaluó la posibilidad de dividirlas en varias tareas para facilitar su gestión.
5. Los valores estimados fueron registrados en el backlog del proyecto en Azure DevOps.

El uso de puntos de historia para cada user story permitió medir **el esfuerzo** de manera efectiva, optimizando la planificación del desarrollo y

ajustando los tiempos de trabajo de acuerdo con la dificultad de cada backlog item.

En paralelo, también se estableció un sistema de **priorización** para épicas y features basado en la urgencia y el impacto en el sistema, categorizando las tareas en niveles alta (1), media (2) o baja (3) (Scrum.org, 2023).

Order	Work Item Type	Title	State	Priority
1	Epic	Login, Gestión de Usuarios y Roles	New	1
	Feature	CRUD Usuarios	New	2
	Feature	CRUD Roles y Permisos	New	2
	Feature	Módulo de Autenticación (Login)	New	2
	Feature	Control de Sesión y Acceso	New	2
2	Epic	Gestión de Auditorías	New	1
	Feature	CRUD Periodos de Auditoría Backoffice	New	2
	Feature	CRUD Auditorías Backoffice	New	2
	Feature	Módulo de Auditorías Frontend	New	2
3	Epic	Gestión de Controles ISO	New	1
	Feature	CRUD Controles ISO Backoffice	New	2
	Feature	Gestión de Evidencias de Controles Frontend	New	2
4	Epic	Integración AI para Análisis de Controles	New	1
	Feature	Configurar API para ChatGPT en OpenAI	New	2
	Feature	Añadir Funcionalidad de Revisión Automática de Evidencias con IA	New	2
5	Epic	Reportes y Estadísticas	New	1
	Feature	Generar reportes de cumplimiento	New	2
6	Epic	Realizar pruebas unitarias y de integración	New	1

Ilustración 1 Priorización de tarea en el proyecto (extraído de Azure DevOps)

5.1.4. Planificación de los Sprints: Priorización y estimación de esfuerzo

Los sprints son iteraciones de trabajo dentro del marco de Scrum, en los que se desarrolla y entrega un incremento del producto con funcionalidades potencialmente utilizables (Schwaber & Sutherland, 2020). En este proyecto, se

planificaron y ejecutaron los siguientes sprints con una duración de dos semanas cada uno:

- **Sprint 1:** Se enfocó en la configuración inicial del sistema, la gestión de usuarios y autenticación para establecer la seguridad del sistema.
    - Duración: **Del 11 de noviembre de 2024 al 24 de noviembre de 2024.**
    - Priorización: **Alta**
    - Esfuerzo estimado: **72 puntos**

- **Sprint 2:** Del 25 de noviembre de 2024 al 08 de diciembre de 2024. Se desarrollaron los módulos de auditorías y controles ISO 27001. Permitiendo la gestión eficiente de las auditorías y la validación de cumplimiento mediante evidencias.
    - Duración: **Del 25 de noviembre de 2024 al 08 de diciembre de 2024.**
    - Priorización: **Alta**
    - Esfuerzo estimado: **95 puntos**

- **Sprint 3:** Acabar el Frontend del módulo de auditorías, implementar la funcionalidad de IA para revisión automática de evidencias y desarrollar el sistema de generación de reportes gráficos sobre cumplimiento de controles ISO 27001.
    - Duración: **Del 09 de diciembre de 2024 al 22 de diciembre de 2024.**
    - Priorización: **Media**
    - Esfuerzo estimado: **70 puntos**

Durante cada sprint, se trabajó en los elementos asignados del backlog, realizando un seguimiento y evaluaciones finales (Rodríguez, 2020).

Este enfoque iterativo permitió entregar valor de manera continua, optimizando el desarrollo del software y asegurando la calidad del producto final (Gutiérrez & Soto, 2021).

En el apartado 6 se desglosan por Sprint todas las User Story o backlog items abarcados en el proyecto y el esfuerzo de cada uno de ellos. Cada User Story es priorizada utilizando una estimación basada en "puntos de historia" para medir el esfuerzo relativo de cada tarea.

5.2. Métricas de Desempeño en Scrum

En un proyecto Scrum, es crucial medir diferentes métricas para evaluar el rendimiento del equipo y la eficiencia del desarrollo. A continuación, un estudio del proyecto en función a sus métricas:

5.2.1. Velocidad del Equipo

La velocidad es el número de puntos de historia completados en un sprint. La velocidad de un equipo en Scrum es una de las métricas fundamentales para evaluar su rendimiento (Schwaber & Sutherland, 2020).

Durante los tres sprints analizados, la velocidad promedio fue de **79 puntos de esfuerzo por sprint**, con una **desviación de 13.89**, indicando un rendimiento relativamente estable para sprint 1 y 3 pero con variaciones en el segundo sprint.

5.2.2. Análisis del Esfuerzo Total y Distribución

- **Sprint 1**: 72 puntos de esfuerzo, 14 user stories
- **Sprint 2:** 95 puntos de esfuerzo, 18 user stories
- **Sprint 3:** 70 puntos de esfuerzo, 10 user stories

El Sprint 2 representó la mayor carga de trabajo (40.08% del esfuerzo total), seguido del Sprint 1 (30.38%) y el Sprint 3 (29.54%). Este patrón muestra que se abordo un mayor volumen de trabajo en el segundo Sprint.

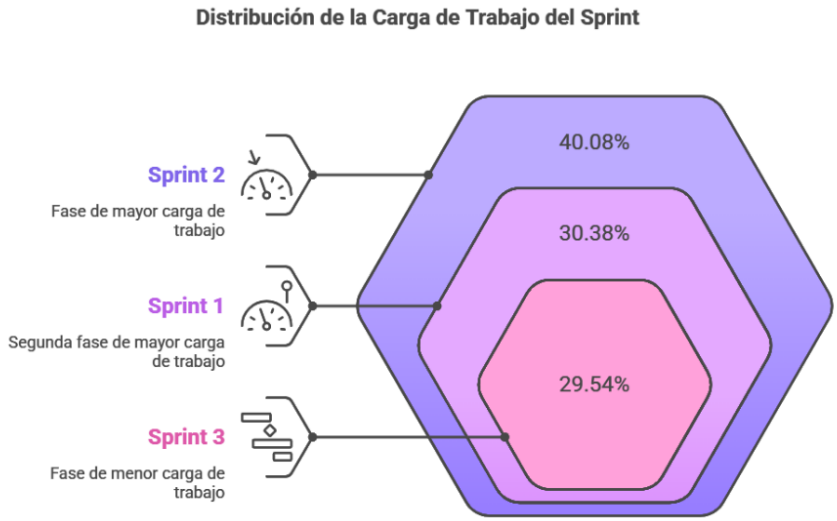


Ilustración 2 Napkin.ai. (2025). Diagrama conceptual sobre Esfuerzo total y Distribución [Imagen generada por inteligencia artificial].

5.2.3. Distribución del Esfuerzo por Categoría

El esfuerzo total se distribuyó en diversas funcionalidades:

- **CRUD Usuarios:** 19 puntos
- **CRUD Roles y Permisos:** 18 puntos
- **Módulo de Autenticación:** 15 puntos
- **Control de Sesiones y Acceso:** 20 puntos
- **Módulo de Auditorías:** 34 puntos
- **Configuración de API OpenAI:** 19 puntos
- **Revisión Automática con IA:** 8 puntos
- **Generación de Reportes:** 9 puntos

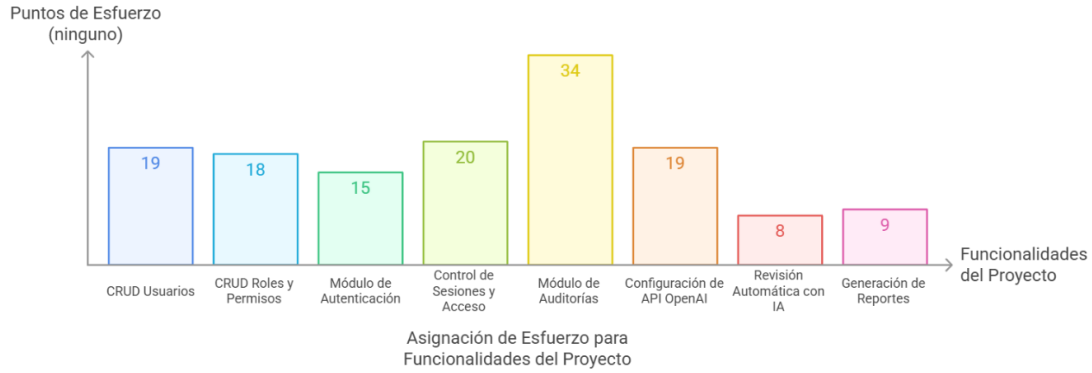


Ilustración 3 Napkin.ai. (2025). Diagrama conceptual Esfuerzo por Funcionalidad del Proyecto [Imagen generada por inteligencia artificial]. Napkin.ai.

El Módulo de Auditorías demandó el mayor esfuerzo, reflejando la importancia de esta funcionalidad dentro del sistema.

5.2.4. Análisis del Esfuerzo Promedio por User Story

La complejidad de las historias de usuario varió entre sprints. Se calculó el esfuerzo promedio por user story en cada iteración:

- **Sprint 1:** 5.14 puntos por historia
- **Sprint 2:** 5.28 puntos por historia
- **Sprint 3:** 7.00 puntos por historia

Ilustración 4 Napkin.ai. (2025). Diagrama conceptual sobre Esfuerzo por Historia de Usuario por sprint [Imagen generada por inteligencia artificial]. Napkin.ai.

El Sprint 3 presentó un incremento significativo en la complejidad de las historias, Esto fue debido a la incertidumbre de la integración con la API de ChatGPT que era la tarea más novedosa y la que nunca antes se había abordado.

5.2.5. Esfuerzo Promedio por Hora de Trabajo

Este cálculo nos dice cuántos puntos de esfuerzo se completan por cada hora trabajada en cada sprint.

$$\frac{Total\ de\ esfuerzo}{Total\ de\ horas\ trabajadas}$$

$$\frac{237\ puntos}{3\ \times\ 80\ horas}\ =\ 237\ /\ 240\ =\ 0.99\ puntos/hora$$

Tabla 1 Esfuerzo Promedio por Hora de Trabajo

Sprint	Esfuerzo Total (puntos)	Horas Totales	Esfuerzo por Hora (puntos/hora)
Sprint 1	72	80	0.90
Sprint 2	95	80	1.19
Sprint 3	70	80	0.88

El Sprint 2 fue el más eficiente en términos de esfuerzo por hora (1.19 puntos/hora), lo que indica que se logró más trabajo en menos tiempo.

El Sprint 3 tuvo el mayor tiempo promedio por user story (8.00 horas por historia), lo que indica que las historias eran más complejas o requerían más esfuerzo.

En promedio, el equipo completó 0.99 puntos de esfuerzo por cada hora trabajada

5.2.6. Horas Promedio por User Story: Productividad

Este cálculo nos dice cuántas horas, en promedio, se han dedicado a cada user story.

$$Horas\ por\ historia\ = \frac{80\ horas\ por\ sprint}{Número\ de\ historias\ del\ sprint}$$

Tabla 2 Horas Promedio por User Story: Productividad

Sprint	User Stories	Horas Totales	Horas por Historia (horas/historia)
Sprint 1	14	80	5.71
Sprint 2	18	80	4.44
Sprint 3	10	80	8.00

En promedio por cada historia de usuario salen 5.8 horas. El Sprint 2 fue el más eficiente (4.44 horas/historia) y Sprint 3 el más demandante (8 horas/historia).

5.3. Planificación temporal del proyecto

A continuación, se pasa a detallar la planificación del proyecto incluyendo la primera fase waterfall, la segunda fase Agile(dividida en 3 Sprints) y la tercera fase y final nuevamente waterfall.

Tabla 3 Planificación temporal del proyecto

Fase	Fecha de Inicio	Fecha de Finalización	Descripción	Horas Totales
Planificación y Análisis	01/10/2024	10/11/2024	Definición de requisitos, análisis de viabilidad y diseño del backlog en Azure DevOps.	80
Desarrollo Iterativo (Scrum - Sprints)	11/11/2024	22/12/2024	Implementación del sistema en tres sprints de dos semanas cada uno.	120
Sprint 1: Autenticación y Gestión de Usuarios	11/11/2024	24/11/2024	Desarrollo del sistema de autenticación, gestión de roles y permisos.	45

Sprint 2: Módulo de Auditorías y Gestión de Evidencias	25/11/2024	08/12/2024	Implementación de auditorías y controles ISO 27001, con subida de evidencias.	40
Sprint 3: Integración de IA y Generación de Reportes	09/12/2024	22/12/2024	Integración de la API de OpenAI y desarrollo de reportes gráficos sobre cumplimiento.	35
Pruebas y Validación	23/12/2024	12/01/2025	Pruebas funcionales, de integración y seguridad del sistema. Ajustes finales.	24
Documentación y Presentación Final	13/01/2025	31/01/2025	Elaboración de informes, manual de usuario y preparación para la defensa del proyecto.	16
TOTAL				**360 Horas**

5.4. valoración de la dedicación y el coste económico

5.4.1. Coste de Desarrollo

Dado que el único desarrollador/Consultor ha desempeñado múltiples funciones en el proyecto con un salario bruto anual de 35.000 €. La dedicación total del desarrollo ha sido de 240 horas, distribuidas de la siguiente manera:

- **Planificación y Análisis:** 80 horas
- **Desarrollo (Sprints):** 120 horas
- **Pruebas y Validación:** 24 horas
- **Documentación y Presentación:** 16 horas

El salario por hora del desarrollador se calcula de la siguiente manera:

- **Salario por hora:** 35.000 € / 1.760 horas ≈ 19,89 € por hora
- **Coste total de desarrollo:** 240 horas × 19,89 € ≈ 4.773,60 €

5.4.2. Infraestructura en AWS

Amazon Web Services (AWS) es una de las plataformas de computación en la nube más utilizadas en el mundo, ofrece servicios escalables para alojamiento web, bases de datos y almacenamiento. Se ha elegido AWS para este proyecto debido a su fiabilidad, seguridad, y la capacidad de escalar los recursos en función del número de usuarios concurrentes. Además, AWS permite optimizar costos al pagar solo por los recursos utilizados, garantizando un equilibrio entre rendimiento y presupuesto (Amazon Web Services, 2024).

Para alojar la aplicación en AWS, se han considerado los siguientes servicios clave:

Tabla 4 Listado de Servicios a contratar en AWS

Servicio AWS	Descripción	Costo Aproximado Mensual
EC2 (Elastic Compute Cloud)	Servidor virtual para alojar la aplicación.	Desde 8,50 € (t2.micro) hasta 250 € (m5.large con Auto Scaling).
RDS (Relational Database Service)	Base de datos MySQL gestionada.	Desde 10 € (db.t3.micro) hasta 120 € (db.m5.large).
S3 (Simple Storage Service)	Almacenamiento de documentos y evidencias de auditoría.	5 € por cada 100GB.
Transferencia de Datos	Coste variable según el tráfico de usuarios.	Desde 10 € por 100GB.

5.4.3. Escalabilidad en AWS según Usuarios Concurrentes

A continuación, se detallan los costos estimados en función del número de usuarios concurrentes.

Escenario 1: 50 Usuarios Concurrentes (Pequeño)

- **EC2:** t2.micro (1 vCPU, 1GB RAM) → 8,50 €/mes
- **RDS:** db.t3.micro (1 vCPU, 1GB RAM) → 10 €/mes
- **S3:** 50GB → 2,50 €/mes
- **Costo Total Mensual: 21 €/mes**
- **Costo Total Anual: 252 €**

Escenario 2: 200 Usuarios Concurrentes (Mediano)

- **EC2:** t3.medium (2 vCPU, 4GB RAM) → 40 €/mes
- **RDS:** db.t3.medium (2 vCPU, 4GB RAM) → 40 €/mes
- **S3:** 100GB → 5 €/mes
- **Costo Total Mensual: 85 €/mes**
- **Costo Total Anual: 1.020 €**

Escenario 3: 500 Usuarios Concurrentes (Grande)

- **EC2:** t3.large (2 vCPU, 8GB RAM) → 80 €/mes

- **RDS:** db.t3.large (2 vCPU, 8GB RAM) → 80 €/mes
- **S3:** 200GB → 10 €/mes
- **Costo Total Mensual: 170 €/mes**
- **Costo Total Anual: 2.040 €**

Escenario 4: 2000+ Usuarios Concurrentes (Muy Grande)

- **EC2:** m5.large (4 vCPU, 16GB RAM) + Auto Scaling → 150 €/mes
- **RDS:** db.m5.large (4 vCPU, 16GB RAM) → 120 €/mes
- **S3:** 500GB → 20 €/mes
- **Costo Total Mensual: 290 €/mes**
- **Costo Total Anual: 3.480 €**

5.4.4. Costes Indirectos

Electricidad: Durante el desarrollo del proyecto, se ha utilizado un portátil modelo Dell Latitude 5420 con un consumo promedio de 100W (0,1 kWh) durante 240 horas. Basándonos en el precio medio de la electricidad entre noviembre del 2024 y marzo de 2025 fue de 0,10998 €/kWh: 24 kWh × 0,10998 €/kWh = **2,64€ mensuales.**

Internet: Sabiendo que la duración del proyecto han sido 240 horas, eso supone 30 días completos de uso de internet por lo que se puede decir que se ha usado una mensualidad completa. El **coste de la internet domestica es de 40€/mes.**

Amortizacion de Hardware: Se ha utilizado un portátil modelo Dell Latitude 5420 valorado en 2.100. A efectos de amortización, se estima una vida útil de 4 años con un uso promedio de 2.000 horas al año (40 horas/semana por 50 semanas al año), lo que da un total de 8.000 horas de vida útil.

Por tanto, cada hora cuesta 0,2625 € que multiplicado por las 240 horas que ha durado el proyecto nos sale un **coste total por amortización del hardware imputable al proyecto de 63€**

Licencias de Software de Desarrollo: Se han usado todo herramientas gratuitas.

- Visual Studio Code: Gratuito
- Windows 11 Home: Preinstalado en el equipo, sin coste adicional imputable
- Otros (GitHub, XAMPP): Gratuitos

5.4.5. Costes estimados de mantenimiento.

Se estima que para su futura comercialización se necesite dar un soporte que incluya:

- Soporte técnico.
- Monitorización de rendimiento y seguridad.
- Actualizaciones Evolutivas y correctivas.
- Posibles tareas de escalado de infraestructura.

Para ello, se estiman unos gastos de:

Tabla 5 Costes estimados de mantenimiento

Escenario	Horas estimadas/año	Coste hora (€)	Coste mantenimiento anual (€)
50 Usuarios	30 h	19,89 €	596,70 €
200 Usuarios	60 h	19,89 €	1.193,40 €
500 Usuarios	100 h	19,89 €	1.989,00 €
2000+ Usuarios	200 h	19,89 €	3.978,00 €

5.4.6. Coste Total del Proyecto y coste de comercialización en el Primer Año

Sumando el coste de desarrollo, el coste de la API de ChatGPT y los costes indirectos quedarían de la siguiente manera coste de desarrollo de la aplicación:

Tabla 6 Costes de desarrollo del producto

Coste del proyecto	Coste de Desarrollo	Costes Indirectos	Coste API ChatGPT	Coste Total Año
App ISO 27001	4.773,60 €	105,64 €	10,00 €	**4.889,24 €**

Basándonos en los costes por franjas de usuarios tanto de AWS como de la API de ChatGPT, los costes de comercialización anuales son los siguientes:

Tabla 7 Costes de comercialización

Usuarios Concurrentes	Coste Anual de AWS	Coste API ChatGPT	Coste mantenimiento anual (€)	Coste Total Año
50 Usuarios	252,00 €	60,00 €	596,70 €	**908€**
200 Usuarios	1.020,00 €	360,00 €	1.193,40 €	**2573€**
500 Usuarios	2.040,00 €	1.200,00 €	1.989,00 €	**5.229 €**
2000+ Usuarios	3.480,00 €	6.000,00 €	3.978,00 €	**13.458€**

6. DESARROLLO DEL CONTENIDO DEL PROYECTO.

6.1. Fase de Planificación y Diseño (Waterfall)

6.1.1. Objetivo de la fase

Esta fase inicial corresponde con la etapa de planificación y diseño del proyecto, desarrollada como ya se ha indicado bajo un enfoque Waterfall. El objetivo fue:

1. **Definir los requerimientos funcionales** *(Ver apartado 1.3. Objetivos propuestos (generales y específicos).*
2. **Delimitar el alcance del proyecto** *(Ver apartado 2.3.1. Alcance del proyecto),*
3. **Seleccionar las tecnologías adecuadas** para su posterior implementación y desarrollo bajo la metodología SCRUM. *(Ver apartado 4. Tecnologías y herramientas utilizadas en el proyecto)*

6.1.2. Planificación general del proyecto

Se diseñó una planificación temporal para dividir la fase de desarrollo en tres sprints:

Tabla 8 Planificación temporal del proyecto

Sprint	**Fechas**	**Módulos principales**
Sprint 1	11–24 nov 2024	Autenticación y gestión de usuarios
Sprint 2	25 nov–8 dic 2024	Auditorías, controles, subida de evidencias
Sprint 3	9–22 dic 2024	Integración con IA y generación de reportes

6.2. Sprint 1 - Fase de Desarrollo: Agile (SCRUM)

6.2.1. Objetivo del Sprint

El primer sprint se centró en dos puntos principales:

1. Elaborar el modelo de datos completo que sirva de base para ir construyendo toda la aplicación
2. Establecer la base del sistema en cuanto a la gestión de usuarios, control de sesiones y seguridad del acceso.

Para este sprint, quería dejarse hecho toda la gestión de accesos y permisos, era fundamental garantizar que cada usuario accediera con sus credenciales, y que su rol y permisos limitaran correctamente las funcionalidades disponibles en la aplicación.

6.2.2. Historias de Usuario Abordadas

A continuación, se desglosan las principales user stories que se completaron en este sprint agrupadas por features y Épicas:

Épica 1: Gestión de Usuarios

Feature 1.1: Módulo de Usuarios Backend

Tabla 9 User stories de la Feature Moódulo de Uauarios backend

ID	User Story	Esfuerzo (h)
323	Como Administrador, crear usuarios con nombre, email, rol y empresa	8
324	Como Administrador, editar información de los usuarios	5

325	Como Administrador, eliminar usuarios	3
326	Como Usuario, ver la lista de usuarios de mi empresa	3

Feature 1.2 : Módulo de Autenticación

Tabla 10 User stories de la Feature Moódulo de Autenticacioón

ID	User Story	Esfuerzo (h)
332	Como Usuario registrado, iniciar sesión con correo y contraseña	6
333	Como Usuario, ver error en login si las credenciales son incorrectas	4
334	Como Usuario registrado, restablecer contraseña en caso de olvido	5

Feature 1.3 : Módulo de Sesiones

Tabla 11 User stories de la Feature Moódulo de Sesiones

ID	User Story	Esfuerzo (h)
336	Como Usuario autenticado, mantener la sesión activa	3
337	Como Usuario autenticado, cerrar sesión desde cualquier dispositivo	3

Épica 2: Gestión de Roles y Permisos

Feature 2.1: Módulo de Roles

Tabla 12 User stories de la Feature Moódulo de Roles

ID	User Story	Esfuerzo (h)
328	Como Administrador, crear, editar y eliminar roles	7
329	Como Administrador, asignar un rol a los usuarios	5
330	Como Administrador, restringir la eliminación de un rol si está asignado	6

Feature 2.2: Control de Accesos por Rol

Tabla 13 User stories de la Feature Control de Accesos por ROl

ID	User Story	Esfuerzo (h)
338	Como Usuario, restricción de acceso según su rol	7
339	Como Administrador, restricción de vistas según los permisos del usuario	7

6.2.3. Diseño y Arquitectura

Se diseñaron las siguientes entidades clave en la base de datos:

- Usuarios: id, nombre, email, contraseña (hash), empresa_id, rol_id, activo
- Roles: id, nombre, permisos
- Empresas: id, nombre, sector, dirección, etc.

Estas entidades permiten gestionar un sistema multiempresa con acceso controlado por perfil de usuario.

Además, como parte de este sprint, se elaboró el modelo entidad-relación (ER) completo de la aplicación utilizando MySQL Workbench. Este modelo incluye todas las entidades del sistema, no solo las relacionadas con el inicio de sesión y la gestión de usuarios, sino también las futuras tablas para auditorías, controles ISO, evidencias, periodos, etc. La elaboración de este modelo permitió definir claramente las relaciones, claves primarias y foráneas, y fue clave para poder continuar con el desarrollo del reto de la aplicación en los siguientes sprints.

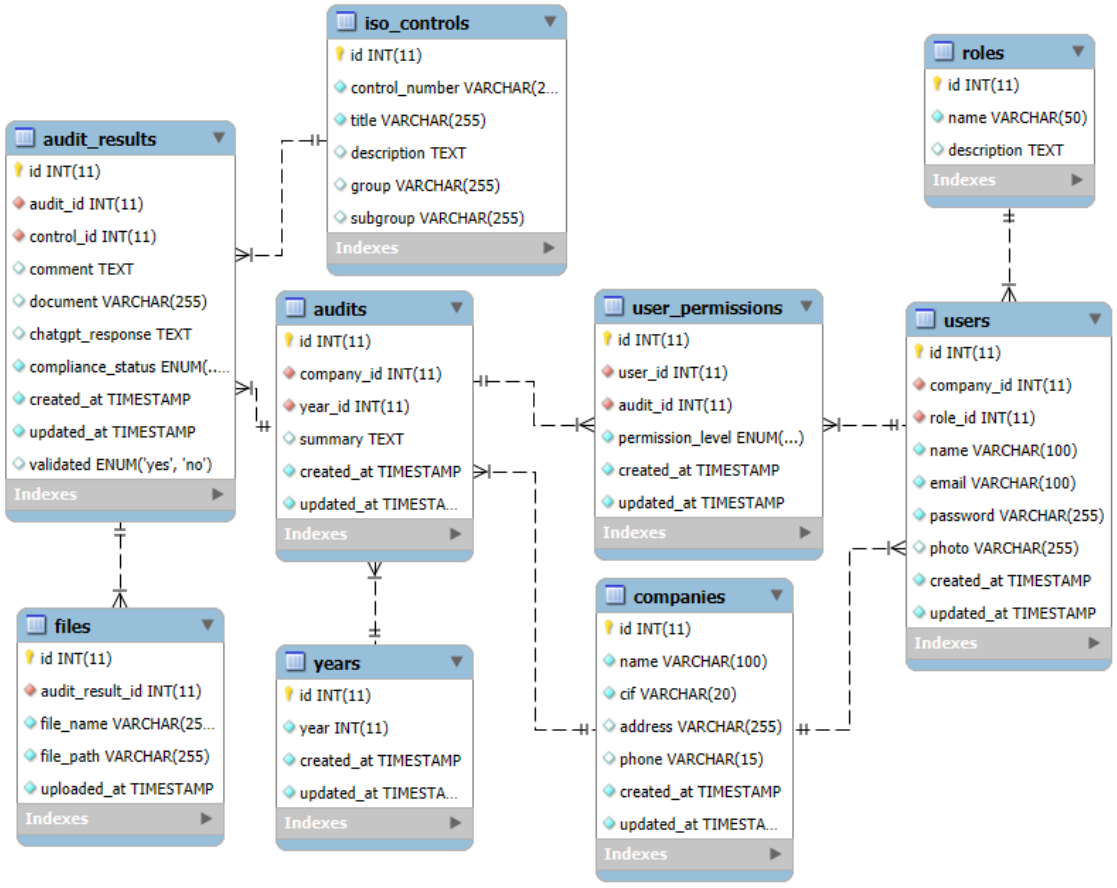


Ilustración 5 Modelo E/R de la aplicación

La interfaz de login se desarrolló como la página de entrada al sistema. En ella se valida el email y la contraseña introducidos por el usuario desde el backend. Si las credenciales son correctas, se inicia la sesión y se redirige al área privada del sistema.

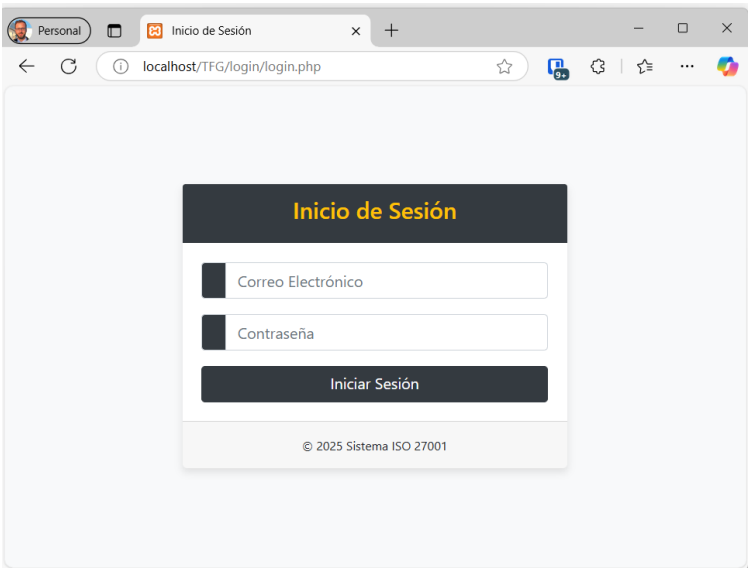


Ilustración 6 Página Inicial: Inicio de Sesión

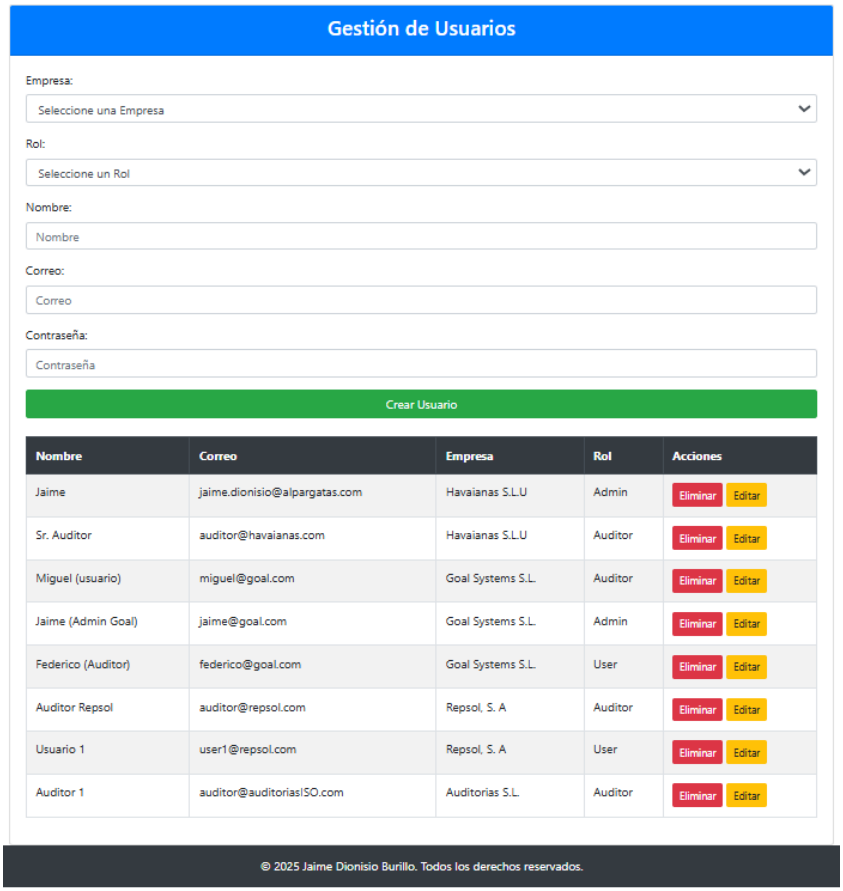
La validación se realiza completamente en el servidor, mediante consultas SQL seguras y verificación de contraseñas cifradas. Las páginas internas del sistema están protegidas con una verificación de sesión activa, para evitar accesos no autorizados.

6.2.4. Desarrollo Técnico

Autenticación de Usuarios: El sistema de login se implementó en PHP utilizando sesiones ($_SESSION) para mantener al usuario autenticado. Las contraseñas se almacenan de forma segura mediante password_hash() y se validan con password_verify() al momento del inicio de sesión.

Gestión de Roles y Permisos: El control de acceso se gestiona mediante condicionales en el backend que validan el valor del rol almacenado en la sesión ($_SESSION["usuario"]["rol"]). Esto permite restringir el acceso a determinadas secciones y mostrar contenido diferente según el tipo de usuario autenticado.

Gestión CRUD de Usuarios Roles y Permisos: Desde el backend se permite la creación, edición y eliminación de usuarios. Los formularios están implementados en PHP y permiten registrar información como el nombre, correo electrónico, rol y empresa asociada del usuario.



z

Persistencia y Seguridad:

- Las contraseñas se almacenan cifradas mediante funciones nativas de PHP.
- Se realiza la conexión a la base de datos mediante mysqli y las consultas se construyen directamente con variables PHP.
- Los datos recibidos a través de formularios se gestionan mediante métodos POST.

6.2.5. Pruebas y Validaciones

Durante este sprint se realizaron pruebas funcionales manuales en entorno local para verificar el correcto funcionamiento de las funcionalidades

implementadas. Las pruebas se centraron en asegurar el flujo de autenticación y la gestión de usuarios. Las validaciones realizadas fueron las siguientes:

1. **Inicio de sesión con credenciales correctas:** Se comprobó que, al introducir un correo y contraseña válidos, el sistema autenticaba correctamente al usuario y redirigía al dashboard.
2. **Inicio de sesión con credenciales incorrectas:** Se probó que, al introducir un correo inexistente o una contraseña incorrecta, el sistema mostraba un mensaje de error sin permitir el acceso.
3. **Creación de usuarios:** Se verificó que el sistema permitía registrar nuevos usuarios a través del formulario correspondiente, asignándoles un rol y una empresa.
4. **Edición de usuarios**: Se probó a modificar los datos existentes, como nombre, correo electrónico o rol, con éxito.
5. **Eliminación de usuarios:** Se validó la eliminación de registros desde el backend y su correcta desaparición de la tabla de usuarios.
6. **Acceso restringido por sesión:** Se comprobó que, si no existía una sesión activa, el acceso a páginas protegidas redirigía automáticamente a la pantalla de login.

6.2.6. Conclusión del Sprint 1

Este primer sprint permitió establecer los cimientos del sistema, tanto a nivel funcional como estructural. Más allá de desarrollar el login y la gestión de usuarios, fue clave definir la arquitectura de base de datos y consolidar el modelo E/R que guiará el desarrollo completo de la aplicación.

A nivel técnico, trabajar con sesiones y gestionar roles desde PHP resultó manejable y permitió un control sencillo pero efectivo del acceso a la plataforma. Este proceso ayudó también a detectar patrones de reutilización y a preparar el código para escalarlo en los siguientes sprints.

6.3. Sprint 2 - Fase de Desarrollo: Agile (SCRUM)

6.3.1. Objetivo del Sprint

El segundo sprint se centró en desarrollar la funcionalidad principal de la aplicación que consta de:

1. La gestión de auditorías ISO 27001 asignadas a cada empresa y divididas por año,
2. Dentro de cada auditoría, la evaluación detallada de los controles de la norma ISO 27001.

Esta fase permitió a los usuarios navegar por las diferentes auditorías a las que tenían acceso organizadas por empresa y por año. Una vez dentro de cada auditoría, se muestran los controles organizados por categorías, y es posible ver el estado de cada control y poder acceder a registrar comentarios por cada control, y establecer el estado de cumplimiento.

Es en este Sprint donde ya se consigue no solo aportar valor como tal sino aportar ya una funcionalidad práctica para poder trabajar con las auditorias de la ISO.

6.3.2. Historias de Usuario Abordadas

A continuación, se desglosan las principales user stories que se completaron en este sprint agrupadas por features y Épicas:

Épica 3: Gestión de Auditorías

Feature 3.1: Gestión de Periodos

Tabla 14 User stories de la Feature Gestión de Periodos

ID	User Story	Esfuerzo (h)
342	Como Administrador, crear nuevos periodos de auditoría (años)	5
343	Como Administrador, editar periodos de auditoría	4

344	Como Administrador, eliminar periodos si no tienen auditorías asociadas	4
345	Como Auditor, ver lista de periodos disponibles	3

Feature 3.2: Módulo de Auditorías Backend

Tabla 15 User stories de la Feature Módulo auditorias Backend

ID	User Story	Esfuerzo (h)
347	Como Administrador, crear auditorías asignadas a empresa y periodo	8
348	Como Administrador o Auditor, editar auditorías existentes	6
349	Como Administrador, eliminar auditorías sin controles asociados	4

Feature 3.3: Módulo de Auditorías Frontend

Tabla 16 User stories de la Feature Módulo de Auditorías Frontend

ID	User Story	Esfuerzo (h)
350	Como Auditor, ver todas las auditorías de todas las empresas	5
351	Como Empleado de una empresa, ver solo las auditorías de mi empresa	4
353	Como Auditor, ver listado de auditorías en panel de control	6
354	Como Auditor o Administrador, acceder al detalle de una auditoría	7

Feature 3.4: Módulo de Controles ISO

Tabla 17 User stories de la Feature Módulo de Controles ISO

ID	User Story	Esfuerzo (h)
355	Como Usuario con permisos, navegar por los controles de la auditoría	9
356	Como Usuario, subir documentos como evidencia de cumplimiento	7

357	Como Auditor, ver resumen general del cumplimiento de auditoría	5

6.3.3. Diseño y Arquitectura

Durante este sprint se incorporaron nuevas tablas a la BBDD con las entidades relativas a la gestión de auditorías que teníamos en el modelo ER.

- **audit:** En la que se almacena id, empresa_id, año_id
- **audit_results:** Se almacena su Id, udit_id, control_id, comentarios, respuesta de ChatGPT, estado de cumplimiento y si está o no validado por el auditor
- **controles_iso:** id, número del control, título del control, Descripción del control y los grupos y subgrupos a los que pertenece el control.
- **auditoria_control:** id, auditoria_id, control_id, estado, comentario
- **files:** almacena los datos como nombre del fichero ruta y el Id de los ficheros que se suben al sistema como evidencias de cumplimiento del control y la Audit_result Id asociada a cada archivo.

Estas entidades permiten evaluar individualmente cada control por cada auditoría, manteniendo los comentarios, evidencias y el estado por separado y mostrarlos agrupados por grupos.

La estructura permite múltiples auditorías independientes por empresa y año, con seguimiento individualizado.

El contenido de los 93 controles se cargó mediante el script insert_controles.sql, agrupados por categoría y subgrupo. Esta estructura lógica facilitó la implementación del menú lateral de navegación y la edición por control.

6.3.4. Desarrollo Técnico

- **Gestión de auditorías**:
  A través del backend se permite crear auditorías asignadas a una

empresa y un periodo concreto. Esto habilita el sistema para iniciar una evaluación del cumplimiento ISO 27001 personalizada por cada cliente.

Ilustración 7 CRUD Gestión de Auditorias

- **Navegación estructurada por controles**:
  En el archivo menus/menu_controles_iso.php se desarrolló un menú lateral dinámico que muestra los controles categorías de la norma. Esto mejora la experiencia del usuario y facilita el seguimiento del progreso.

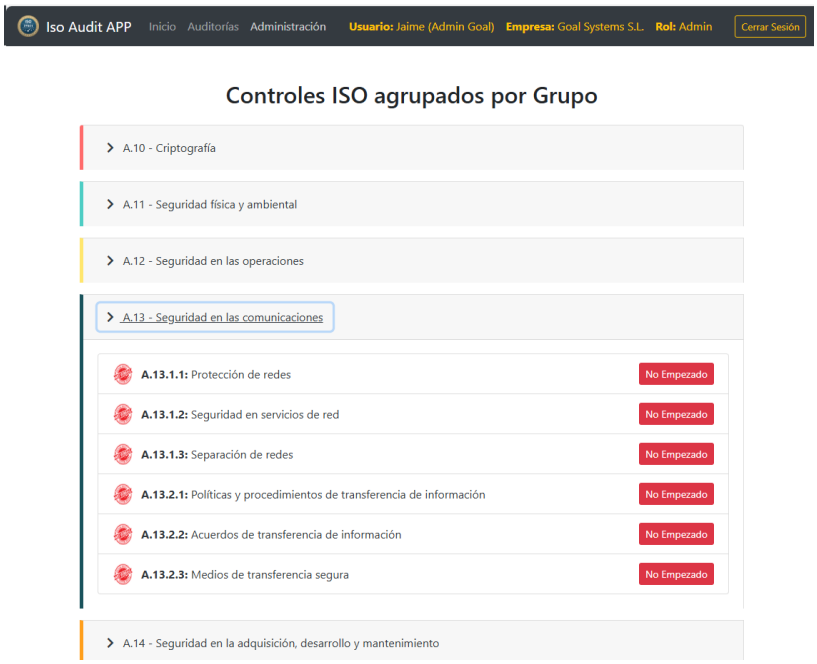


Ilustración 8 Menú para navegar por los controles de la ISO 27001

- **Evaluación de cada control**:
  Tanto el usuario como el auditor puede acceder a cada uno de los controles, donde se muestran:

  1. Un desplegable a modo consulta, con la descripción completa del control.
  2. El estado actual del mismo (cumplido, en_progreso, no_cumplido)
  3. Un campo para introducir comentarios justificativos de como se ha cumplido ese control.
  4. La sugerencia de la IA sobre el estado de cumplimiento del control (Se desarrollará en el siguiente sprint)
  5. Un módulo para poder subir archivos que complementen las evidencias de cumplimiento de dicho control.

6.3.5. Pruebas y Validaciones

Durante este sprint se realizaron pruebas funcionales manuales en entorno local para verificar el correcto funcionamiento del módulo de auditorías. Las validaciones realizadas fueron las siguientes:

- **Creación de auditorías asignadas a empresas y años**: Se verificó que se generaban correctamente los registros y se asociaban los controles a cada nueva auditoría.
- **Visualización estructurada de controles**: Se comprobó que el menú lateral cargaba correctamente las categorías y subgrupos, y permitía navegar por los controles sin errores.
- **Evaluación de controles individuales**: Se probó la funcionalidad de selección de estado y el guardado de comentarios. También se verificó que la información persistía correctamente en base de datos.
- **Almacenamiento y gestión de archivos**: Se probó a subir ficheros y a eliminar ficheros dentro de cada respuesta al cumplimiento de cada control.
- **Acceso restringido por sesión y rol**: Se comprobó que solo usuarios autenticados podían acceder a las vistas de auditorías y edición de controles. Y se comprobó que solo los usuarios auditores podían ver la opción de marcar el estado de cumplimiento de ese control.

6.3.6. Conclusión del Sprint 2

Este sprint representó un gran paso en la evolución del sistema, pasando de una arquitectura básica de autenticación de usuarios a una herramienta ya totalmente operativa para empezar a gestionar las auditorías. Quedaron funcionales la creación de nuevas auditorias, la visualización de una forma estructurada de todos los controles de la norma ISO 27001 así como la gestión de cada uno de los controles. Todo esto tanto del punto de vista del auditor como del usuario final.

Se deja preparado el terreno para la incorporación de nuevas funcionalidades, como la carga de evidencias documentales y la evaluación automatizada mediante inteligencia artificial.

6.4. Sprint 3 - Fase de Desarrollo: Agile (SCRUM)

6.4.1. Objetivo del Sprint

El objetivo de este tercer sprint fue añadir al sistema una funcionalidad diferencial: la capacidad de analizar los controles evaluados mediante inteligencia artificial generativa (IA), utilizando el modelo ChatGPT.

A través de esta integración, se buscó ofrecer una recomendación automatizada para cada control evaluado, identificar posibles debilidades y generar una visión más clara del estado del cumplimiento de la norma ISO 27001 como si un auditor externo lo hubiera revisado.

Además, se desarrollaron dos gráficas de resumen de cumplimiento para facilitar ver en un modo rápido y visual el estado de cada auditoría.

6.4.2. Historias de Usuario Abordadas

Las principales user stories completadas durante este sprint fueron:

Épica 4: Gestión de Controles ISO

Feature 4.1: Mantenimiento de Controles ISO

Tabla 18 User stories de la Feature Mantenimiento Controles ISO

ID	User Story	Esfuerzo (h)
360	Como Administrador, crear nuevos controles ISO 27001	7
361	Como Administrador, editar la información de los controles ISO	5
362	Como Administrador, eliminar controles si no están asociados	4

Feature 4.2: Navegación de Controles ISO

Tabla 19 User stories de la Feature Navegación Controles ISO

ID	User Story	Esfuerzo (h)
363	Como Auditor, ver los controles organizados por grupo y subgrupo	6

Épica 5: Evaluación de Auditoría por el Usuario

Feature 5.1: Cumplimentación de Controles

Tabla 20 User stories de la Feature Cumplimentación de Controles

ID	User Story	Esfuerzo (h)
365	Como Usuario, seleccionar un control para registrar información	7
366	Como Usuario, ingresar comentario sobre la implementación del control	6
367	Como Usuario, subir documentos como evidencia de cumplimiento	7
368	Como Auditor, ver resumen del cumplimiento de los controles	5
369	Como Auditor o Admin, descargar evidencias asociadas a cada control	5

Épica 6: Integración con Inteligencia Artificial

Feature 6.1: Configuración OpenAI

Tabla 21 User stories de la Feature Configuración OpenAI

ID	User Story	Esfuerzo (h)
372	Como Administrador, configurar la API de OpenAI	8
373	Como Administrador, gestionar credenciales de la API	6
374	Como Administrador, verificar que la conexión con OpenAI funcione	5

Épica 7: Visualización de Cumplimiento

Feature 7.1: Gráficas de Cumplimiento

Tabla 22 Gráficas de Cumplimiento

ID	User Story	Esfuerzo (h)
378	Como Usuario autorizado, ver gráficos visuales del estado de cumplimiento	9

6.4.3. Diseño y Arquitectura

Durante este sprint no se introdujeron nuevas tablas en la base de datos, pero sí se ampliaron las funcionalidades del módulo de auditorías y controles para incorporar análisis automatizado. La arquitectura se complementó con una función que construye un prompt dinámico que une lo que tiene que cumplirse en ese control, que es lo que dice el usuario que ha hecho ese año para cumplirlo y lo envía a la API de ChatGPT, obteniendo una respuesta que se muestra junto al estado del control de una forma estructurada diciendo al usuario el grado de cumplimiento, que ha hecho bien que no ha hecho bien y las futuras mejoras de cara al siguiente año.

El flujo de trabajo es el siguiente:

1. Usuario accede al control y escribe un comentario.

2. El sistema permite enviar ese comentario a ChatGPT.
3. Se recibe una recomendación IA (fortalezas, debilidades, sugerencias).
4. El contenido se muestra bajo el control correspondiente se almacena en la base de datos para posteriores consultas.

6.4.4. Desarrollo Técnico

1. **Integración con la API de OpenAI (ChatGPT):**
   Se desarrolló una función en PHP que construye un prompt estructurado incluyendo:

   a) Descripción del control
   b) Comentario introducido por el usuario que está cumplimentando los controles de la norma ISO 27001.
   c) Como quiero que sea la estructura de la respuesta que me devuelva

   El prompt se envía mediante cURL a la API de OpenAI, y se recibe una respuesta textual con una recomendación generada automáticamente.

- **Visualización de la respuesta de la IA:** En la misma vista de edición del control (edit_audit_control.php), se añadió un botón para generar la recomendación con IA y un campo donde se muestra el resultado devuelto por el modelo.

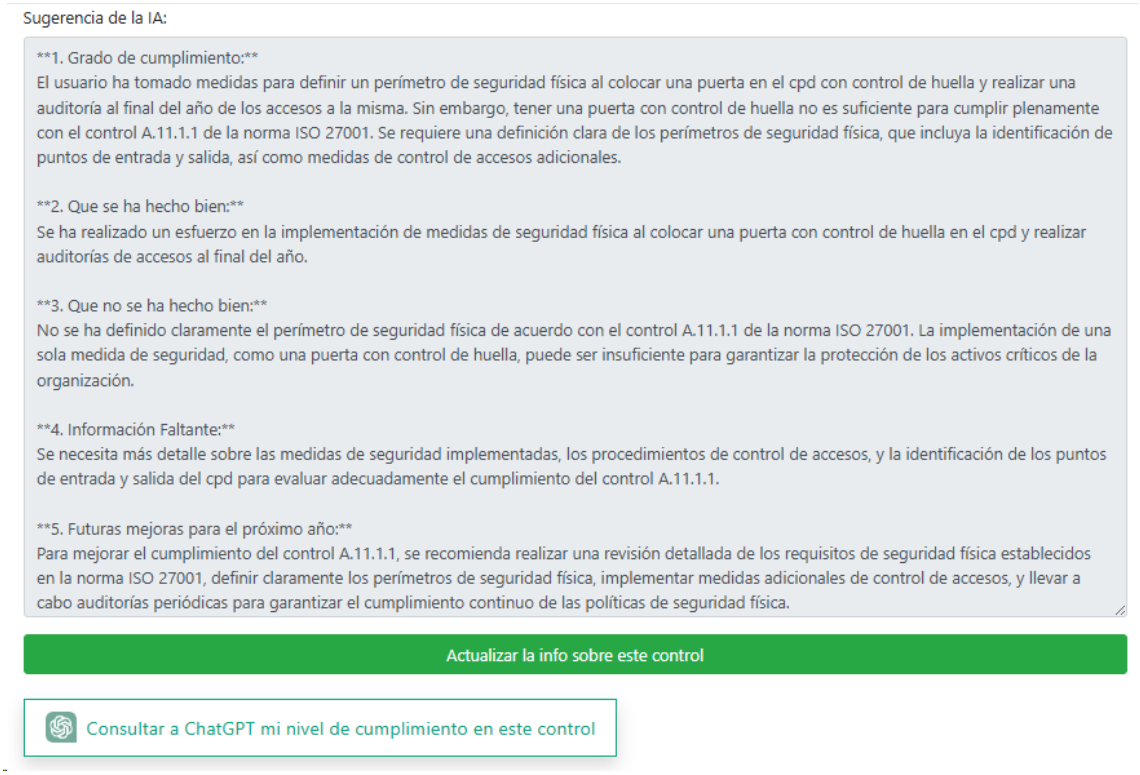


Ilustración 9 Respuesta de la IA según las acciones declaradas por el usuario

2. **Resumen gráfico del cumplimiento:** Se implementaron dos gráficas para cada auditoría que muestran:

   a) Porcentaje global de cumplimiento de la auditoría

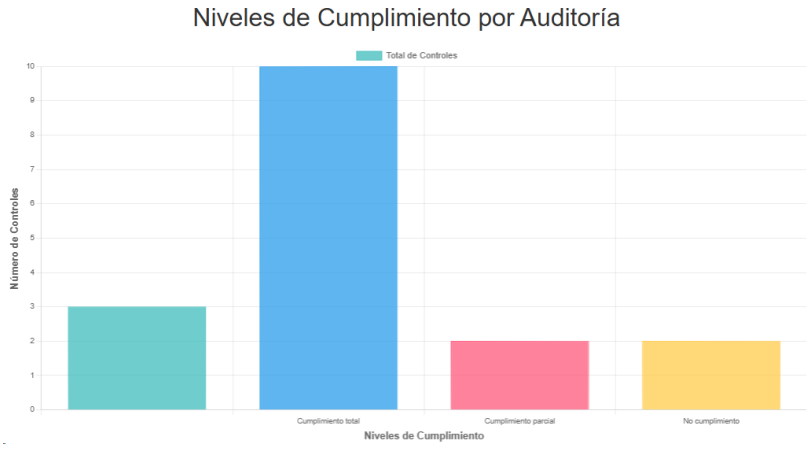


Ilustración 10 Grafica de niveles de cumplimiento dentro de cada auditoría

b) Porcentaje de controles implementados por cada categoría de la norma ISO 27001.

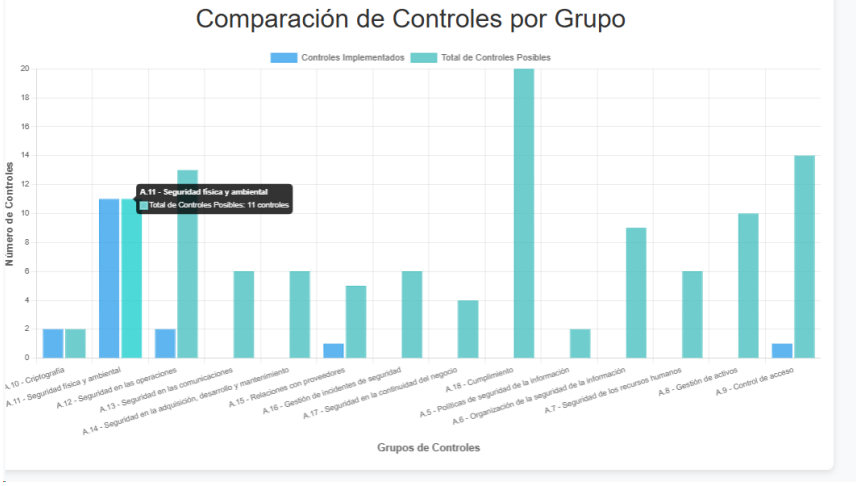


Ilustración 11 Total de controles implementados por grupo

Estas vistas se desarrollaron usando JavaScript más concretamente Chart.js y se alimentan de los datos almacenados en la base de datos.

6.4.5. Pruebas y Validaciones

Se realizaron pruebas funcionales en entorno local, incluyendo:

- Validación de la conexión con la API de OpenAI utilizando la clave de acceso.
- Envío de comentarios reales a la IA y análisis de la coherencia de las recomendaciones generadas.
- Prueba de casos límite (comentarios vacíos, muy extensos o contradictorios).
- Verificación de la actualización en tiempo real del resumen gráfico tras editar controles con los últimos cambios.

6.4.6. Conclusión del Sprint 3

Este sprint permitió implementar una funcionalidad diferencial dentro del sistema: la integración con inteligencia artificial generativa para complementar la evaluación de controles ISO. Esta característica no solo aporta valor añadido a la herramienta, sino que posiciona el proyecto como una solución innovadora frente a otras alternativas tradicionales del mercado como se ha explicado anteriormente.

La generación de recomendaciones automáticas facilita al usuario el análisis técnico que hubiera hecho un auditor real pudiendo así avanzar con la norma sin depender tanto del auditor externo.

Las dos gráficas de resumen de cumplimiento permiten tanto al auditor como al usuario poder visualizar de forma rápida el estado general de las auditorías realizadas y aquellas que se encuentran en curso.

Esta fase marca el final del desarrollo funcional previsto en el alcance del proyecto, dejando la aplicación lista para validaciones finales y despliegue.

7. Pruebas De La Solución

7.1. Objetivo del Plan de Pruebas

El objetivo de este plan es verificar el correcto funcionamiento de la herramienta, desarrollada.

Estas pruebas permiten identificar errores, comprobar el cumplimiento de requisitos funcionales y validar que el sistema actúa según lo esperado para cada tipo de usuario.

7.2. Pruebas Funcionales

Tabla 23 Pruebas Funcionales

Nº	Módulo	Prueba	Resultado Esperado
1	Login	Inicio de sesión con datos correctos	Acceso al panel correspondiente
2	Login	Acceso con datos inválidos	Mensaje de error
3	Control de acceso	Acceso a vista sin login	Redirección al login
4	Usuarios	Crear un nuevo usuario	Usuario registrado y visible
5	Usuarios	Editar datos de un usuario existente	Cambios guardados correctamente
6	Usuarios	Eliminar un usuario existente	Usuario eliminado de la base de datos
7	Empresas	Crear una nueva empresa	Empresa añadida correctamente
8	Empresas	Editar una empresa existente	Información actualizada
9	Empresas	Eliminar una empresa	Empresa eliminada o desactivada
10	Años/Periodos	Crear un nuevo año de auditoría	Periodo registrado correctamente
11	Años/Periodos	Editar año existente	Año modificado
12	Años/Periodos	Eliminar un año existente	Periodo eliminado o inactivo
13	Roles	Crear un nuevo rol	Rol añadido correctamente

14	Roles	Editar un rol	Cambios guardados
15	Roles	Eliminar un rol no asignado	Rol eliminado del sistema
16	Auditorías	Crear auditoría asignada a empresa y año	Controles vinculados automáticamente
17	Auditorías	Editar auditoría	Cambios visibles en listados
18	Auditorías	Eliminar auditoría	Auditoría eliminada correctamente
19	Controles ISO	Acceder a un control y dejarlo como “empezado”	Estado actualizado a “en progreso”
20	Controles ISO	Cambiar estado de control	Estado guardado
21	Controles ISO	Añadir o editar comentario	Comentario almacenado correctamente
22	Evidencias	Subir archivo válido como evidencia	Archivo vinculado y accesible
23	Evidencias	Subir archivo no válido	Mensaje de error
24	IA Generativa	Generar recomendación desde comentario	Respuesta visible
25	IA Generativa	Verificar coherencia entre comentario y recomendación	Coherencia contextual
26	Gráficas	Ver resumen gráfico global y por categoría	Gráficas cargadas por pantalla
27	Gráficas	Verificar actualización de gráficas al cambiar estados	Gráficas actualizadas en tiempo real
28	Filtros	Aplicar filtros por año/empresa	Auditorías correctamente filtradas
29	Permisos	Solo auditores pueden marcar cumplimiento de controles	Restricción aplicada correctamente
30	Permisos	Solo administradores acceden a zona de administración	Acceso denegado a otros roles
31	Permisos	Usuarios ven solo auditorías de su empresa	Auditorías filtradas por empresa
32	Permisos	Auditores ven todas las auditorías	Acceso sin restricciones
33	Zona Admin	Editar respuestas de usuarios desde administración	Cambios reflejados correctamente

7.3. Pruebas de integración

Tabla 24 Pruebas de Integración

Nº	Módulo	Prueba	Resultado Esperado
I1	Auditorías / Controles	Crear auditoría y vincular controles	Controles relacionados automáticamente
I2	Controles / Gráficas	Cambiar estado de control y actualizar gráficas	Gráficas actualizadas dinámicamente
I3	Evidencias / Controles	Subir evidencia y verificar asociación al control	Asociación registrada correctamente
I4	IA	Enviar comentario y mostrar respuesta en control	Recomendación visible junto al control

7.4. Pruebas de interfaz (UI/UX)

Tabla 25 Pruebas de Interfaz UI/UX

Nº	Módulo	Prueba	Resultado Esperado
UI1	Menú lateral	Verificar agrupación visual por categoría	Jerarquía clara por tipo de control
UI2	Formularios	Validación de campos obligatorios	Mensajes de error de validación
UI3	Responsive	Visualizar bien en distintas resoluciones	Layout adaptable al dispositivo desde el que se accede.
UI4	Gráficas	Verificar que no se solapen en navegadores	Renderizado correcto en Chrome/Firefox/Edge

7.5. Pruebas de seguridad

Tabla 26 Pruebas de seguridad

Nº	Módulo	Prueba	Resultado Esperado
S1	Acceso	Acceso a URL interna sin sesión	Redirección al login
S2	Roles	Acceder como usuario a vista de administración	Acceso bloqueado

S3	Empresa	Usuario ve auditorías solo de su empresa	Filtro aplicado automáticamente
S4	Roles	Eliminar rol asignado	Acción bloqueada o aviso

7.6. Pruebas con IA (OpenAI api)

Tabla 27 Pruebas con IA

Nº	Módulo	Prueba	Resultado Esperado
IA1	Generación	Generar respuesta desde comentario coherente	Recomendación útil y relacionada
IA3	Contextual	Modificar entrada y recibir nueva recomendación	Respuesta ajustada al nuevo contenido
IA4	Errores	Simular fallo en conexión o clave inválida	Error manejado con mensaje sin romper interfaz

8. PLAN DE FORMACIÓN DE USUARIOS

Este plan tiene como finalidad capacitar a los diferentes tipos de usuarios dependiendo de su rol en el uso eficiente de la aplicación: Usuarios, Auditores o Administradores.

8.1. Alcance de la Formación

Usuarios (Empleados de una empresa auditada)

- Acceso restringido a su empresa y auditorías relacionadas.
- Carga de evidencias y documentación.
- Seguimiento del estado de cumplimiento.

Auditores

- Acceso a auditorías de diferentes empresas.
- Evaluación de controles y cumplimiento ISO 27001.
- Validación y comentarios sobre evidencias.

Administradores

- Gestión completa de la aplicación.
- Creación y administración de usuarios, auditorías y configuraciones generales.
- Configuración de roles y permisos.

8.2. Metodología de Enseñanza

Sesiones Teórico-Prácticas: Explicación de conceptos y posterior práctica guiada en la plataforma.

Material de Apoyo: Manuales en PDF y videos tutoriales.

Casos Prácticos: Simulación de escenarios reales de auditoría.

Pruebas de Evaluación: Validación de conocimientos adquiridos mediante ejercicios prácticos.

8.3. Plan de Formación por Perfil

8.3.1. Usuarios (Duración: 2 Horas)

1. **Introducción a la Plataforma (30 min)**

- Acceso a la plataforma con credenciales personales y navegación por la interfaz.
- Revisión del menú lateral, controles asignados y funcionalidades disponibles.
- Explicación del rol del usuario en el proceso de auditoría: aportar información y evidencias para los controles asignados.

2. **Carga de Evidencias (45 min)**

- Aprendizaje sobre cómo redactar correctamente qué se ha hecho para cumplir un control.
- Subida de documentos justificativos: políticas, actas, capturas, registros, etc.
- Uso de la IA para recibir retroalimentación sobre el cumplimiento, mejoras sugeridas y grado estimado de conformidad.

3. **Seguimiento del Cumplimiento (45 min)**

- Consulta del estado de auditoría y de los controles completados o pendientes.
- Acceso y visualización de gráficas globales y por categoría, con explicación sobre cómo interpretarlas para entender el nivel de cumplimiento general y por áreas.

8.3.2. Auditores (Duración: 3 Horas)

1. **Introducción a la Plataforma y Gestión de Auditorías (30 min)**

- Acceso al sistema con perfil de auditor y exploración del entorno de trabajo.
- Revisión del listado de auditorías disponibles y navegación por sus controles.
- Creación de nuevas auditorías: asignación a empresa y selección de periodo.
- Exploración de la estructura de controles ISO agrupados por categoría

2. **Evaluación de Controles ISO (1h 30 min)**

- Revisión de respuestas redactadas por los usuarios y análisis de evidencias asociadas.
- Evaluación de cumplimiento para cada control: asignación de estado (cumplido, en progreso, no cumplido).
- Inclusión de comentarios u observaciones técnicas directamente en el sistema.
- Verificación de la recomendación generada por la IA: el auditor evaluará si la retroalimentación automática proporcionada al usuario es correcta, coherente y útil.
- Complementar o corregir, si es necesario, la orientación ofrecida por la inteligencia artificial.

3. **Informes y Reportes (1h)**

- Acceso a los gráficos de cumplimiento general y por categoría ISO.
- Interpretación de los resultados para detectar áreas con bajo cumplimiento.
- Exportación de informes para uso interno o entrega a las empresas auditadas.
- Revisión de estadísticas de progreso a lo largo del periodo de evaluación.

8.3.3. Administradores (Duración: 2,5 Horas)

1. **Introducción a la Plataforma y Gestión General (30 min)**

- Acceso a la plataforma con perfil de administrador.
- Visión general de las funcionalidades disponibles para la gestión completa del sistema.
- Navegación por las secciones clave: usuarios, empresas, auditorías y controles.

2. **Gestión de Usuarios, Roles y Empresas (1h)**

- **Usuarios:** Alta, edición y eliminación de usuarios del sistema. Asignación de roles y vinculación a empresas.
- **Roles:** Creación y configuración de roles personalizados. Ajuste de permisos según el tipo de usuario.
- **Empresas:** Registro de nuevas empresas auditadas. Edición de sus datos y asociación a usuarios y auditorías.

3. **Configuración de Auditorías y Controles ISO (30 min)**

- Creación manual de auditorías y periodos de evaluación.
- Gestión de controles ISO 27001.
- Supervisión de auditorías activas.

4. **Mantenimiento del Sistema y Servidor (30 min)**

- Instrucciones para detener e iniciar los servicios de Apache y MySQL.
- Gestión de la base de datos: consultas, copias de seguridad e importación de scripts.
- Buenas prácticas de mantenimiento:
    - Comprobación periódica del estado de los servicios.
    - Backup regulares de la base de datos y del código fuente.

9. CONCLUSIONES

El desarrollo de esta herramienta web permite abordar de manera práctica y fácil el proceso de cumplimiento de los controles de la ISO 27001, adaptándolo a las necesidades de pequeñas y medianas empresas. Este software facilita considerablemente este proceso a las PYMES gracias al uso de inteligencia artificial la sustituyendo la dependencia de un auditor durante el proceso.

A través de un enfoque iterativo en sprints y una fase inicial de análisis detallado, se ha logrado construir un sistema funcional y escalable en un periodo corto de tiempo que puede servir como base para un futuro programa comercializable.

9.1. Objetivos alcanzados

Durante este trabajo se han conseguido cumplir los objetivos propuestos al inicio del proyecto:

- Se ha diseñado e implementado una plataforma web funcional para la gestión y evaluación de auditorías ISO 27001.
- Se ha implementado un sistema de gestión de usuarios, roles y permisos que permite separar claramente las funcionalidades entre usuarios, auditores y administradores.
- Se ha facilitado la carga de evidencias por parte de los empleados auditados y la posterior revisión por parte de los auditores.

- Se ha integrado una API de inteligencia artificial (OpenAI) que asiste en la evaluación de controles mediante la generación de recomendaciones automáticas.
- Se ha proporcionado una visualización clara del estado de cumplimiento mediante gráficos, lo que permite tanto al auditor como a la empresa tener una visión global del proceso.

9.2. Conclusiones del trabajo y personales

A nivel técnico, el proyecto ha supuesto un reto multidisciplinar que ha implicado trabajar con tecnologías de backend, frontend, bases de datos, e integración con APIs externas. Para mí, este desafío ha sido especialmente significativo, ya que mi perfil está más orientado a los sistemas, la administración de infraestructuras y la gestión de proyectos, no tanto al desarrollo puro.

Esto ha exigido un esfuerzo adicional en el aprendizaje y aplicación de conceptos técnicos avanzados, pero también ha sido una oportunidad para ampliar mis competencias y salir de mi zona de confort. La integración de la inteligencia artificial ha sido, además, una de las partes más enriquecedoras, al permitir automatizar parte del análisis de cumplimiento normativo y sentar las bases para futuras mejoras inteligentes dentro del sistema.

A nivel personal, este trabajo ha reforzado mi capacidad de análisis funcional y adaptación tecnológica. También ha mejorado mis habilidades de documentación y programación.

Además, el hecho de haber participado previamente en un proceso real de implantación de la norma ISO 27001 en una PYME me ha aportado una visión práctica sobre cómo debe ser una herramienta de este tipo para ser realmente útil. Esta experiencia me ha permitido entender qué necesita un usuario de una pequeña empresa: simplicidad, orientación guiada e información clara de lo que pide la norma en cada control. Gracias a ello, he podido diseñar una solución centrada en facilitar el trabajo del usuario no experto, sin renunciar a la rigurosidad exigida por la norma.

9.3. Vías futuras

Este proyecto podría evolucionar en distintas direcciones interesantes:

Ampliación de normas: Adaptar la plataforma para gestionar auditorías de otras normativas ISO..

Sistema de notificaciones: Incorporar alertas automáticas entre auditores y usuarios para recordar a usuarios que deben aportar evidencias o para avisar de vencimientos de auditorías o avisar al auditor una vez que el usuario rellena algún control de la norma.

Añadir un módulo donde poder añadir y editar toda la otra documentación que se debe aportar en una auditoria ISO 27001 como:

- Política de Seguridad de la Información
- Declaración de Aplicabilidad (SoA - Statement of Applicability)
- Análisis de Riesgos y Plan de tratamiento de riesgos
- Procedimientos internos
- Formación y concienciación
- Evidencias de mejora continua

10. BIBLIOGRAFÍA

International Organization for Standardization. (2022). ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO. https://www.iso.org/standard/27001

Secureframe. (19 de febrero de 2025). *¿Cuánto cuesta la certificación ISO 27001?* Secureframe. https://secureframe.com/es-es/hub/iso-27001/certification-cost

Advisera. (8 de febrero de 2011). *¿Cuánto cuesta la implementación de la norma ISO 27001?* 27001Academy https://advisera.com/27001academy/es/blog/2011/02/08/cuanto-cuesta-la-implementacion-de-la-norma-iso-27001

Advisera. (2013). *Lista de documentos obligatorios exigidos por la norma ISO 27001 (Revisión 2013)*. https://advisera.com/27001academy/es/knowledgebase/lista-de-documentos-obligatorios-exigidos-por-la-norma-iso-27001-revision-2013/

ISOTools. (17 de diciembre de 2018). *Aplicabilidad de la norma ISO 27001: problemas comunes en las empresas*. https://www.isotools.us/2018/12/17/aplicabilidad-norma-iso-27001-problemas-comunes-empresas/

GlobalSuite Solutions . (2023). *¿Qué es la norma ISO 27001 y para qué sirve?.* https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve

Advisera. (2025). Conformio: ISO 27001 compliance software. https://advisera.com/conformio

Compleye. (2023). Compliance management made easy. https://www.compleye.io

ISMS.online. (2025). The all-in-one place for your ISO 27001 compliance. https://www.isms.online

OnSpring. (2023). Audit, risk & compliance solutions. https://www.onspring.com

Cloud Coach. (7 de octubre de 2021). *A guide to Water-Scrum-Fall project management*. Cloud Coach. https://cloudcoach.com/blog/a-guide-to-water-scrum-fall-project-management/

IEBS Business School. (23 de abril de 2025). *Modelos híbridos en dirección de proyectos: cómo se combinan Agile y la gestión tradicional*. IEBSchool. https://www.iebschool.com/hub/modelos-hibridos-en-direccion-de-proyectos-como-se-combinan-agile-y-la-gestion-tradicional-management/

Mamá… ¿Qué es Scrum? (1 de junio de 2020). *Cómo unir Agile y Waterfall: modelo híbrido*. Mamá ¿Qué es Scrum?. https://mamaqueesscrum.com/2020/06/01/como-unir-agile-y-waterfall-modelo-hibrido/

Takeuchi, E. (12 de junio de 2024). *Water-Scrum-Fall: How to hybrid Scrum and Waterfall to keep adaptability in long-term development*. Medium. https://medium.com/beyond-agile-leadership/water-scrum-fall-how-to-hybrid-scrum-and-waterfall-to-keep-adaptability-in-long-term-development-a69277a9007b

ProActive QMS. (2025). ISO management software for compliance & quality control. https://www.proactiveqms.com

Scytale. (2024). ISO 27001 compliance automation. https://scytale.ai

Secureframe. (2025). ISO 27001 compliance made easy. https://secureframe.com

The PHP Group. (2023). PHP: Hypertext Preprocessor. https://www.php.net/

Oracle Corporation. (2023). MySQL 8.0 Reference Manual. https://dev.mysql.com/doc/

The PHP Group. (2023). ¿Qué es PHP?. https://www.php.net/manual/es/intro-whatis.php

GitHub. (2023). *GitHub Documentation*. https://docs.github.com/

Bootstrap. (2023). Introduction to Bootstrap. https://getbootstrap.com/docs/5.3/getting-started/introduction/

Apache Friends. (2023). XAMPP Apache + MariaDB + PHP + Perl. https://www.apachefriends.org/index.html

Microsoft. (2023). Visual Studio Code Documentation. https://code.visualstudio.com/docs

Han, J. (2018). Mastering Visual Studio Code: A Complete Guide to Working in VS Code. Packt Publishing.

Edge, R. (2021). Visual Studio Code for Web Developers.

Microsoft. (2013). Using Git source control in VS Code. https://code.visualstudio.com/docs/sourcecontrol/overview

OpenAI. (2023). OpenAI API Documentation. https://platform.openai.com/docs

OpenAI. (2023). GPT-4 Technical Report. https://openai.com/research/gpt-4

ChatGPT. (2025, febrero 19). Explicación sobre ChatGPT y su API [Respuesta generada por un modelo de IA]. OpenAI.

Cohn, M. (2006). Agile estimating and planning. Pearson.

Fairley, R. (2009). Managing and leading software projects. Wiley.

Rubin, K. S. (2012). Essential Scrum: A practical guide to the most popular agile process. Addison-Wesley.

Schwaber, K., & Sutherland, J. (2020). The Scrum Guide: The definitive guide to Scrum: The rules of the game. Scrum.org. https://scrumguides.org

Scrum.org. (2023). Understanding story points and agile estimation. https://www.scrum.org

Gutiérrez, P., & Soto, M. (2021). *Scrum y la gestión ágil de proyectos*. Alfaomega.

Rodríguez, J. (2020). *Metodologías Ágiles en Desarrollo de Software: Scrum, Kanban y XP*. Ediciones Díaz de Santos.

Scrum.org. (2023). *Guía oficial de Scrum*. https://www.scrum.org/resources/scrum-guide-español

Amazon Web Services. (2024). *What is AWS?* https://aws.amazon.com/what-is-aws/

AWS. (2024a). *Amazon EC2 Pricing*. https://aws.amazon.com/ec2/pricing/

AWS. (2024b). *Amazon RDS Pricing*. https://aws.amazon.com/rds/pricing/

AWS. (2024c). *Amazon S3 Pricing*. https://aws.amazon.com/s3/pricing/

AWS. (2024d). *AWS Data Transfer Pricing*. https://aws.amazon.com/pricing/data-transfer/

11. ANEXOS

11.1. Manual de instalación.

A continuación, se describe el procedimiento necesario para desplegar y probar la aplicación de forma local, utilizando **XAMPP** como entorno de servidor web y base de datos.

11.1.1. Requisitos previos

- **Sistema operativo:** Windows 10 o superior (también compatible con macOS o Linux, con ajustes menores).
- **Navegador web:** (Chrome, Firefox, Edge).

11.1.2. Instalación de XAMPP

1. Acceder a la página oficial de descarga: https://www.apachefriends.org/es/index.html
2. Descargar el instalador correspondiente al sistema operativo (Windows).
3. Ejecutar el instalador como administrador.
4. Durante la instalación, seleccionar los siguientes componentes:
    - Apache
    - MySQL
    - PHP
    - phpMyAdmin
5. Finalizar la instalación y ejecutar el Panel de control de XAMPP.

11.1.3. Iniciar los servicios necesarios

1. Abrir el Panel de control de XAMPP (XAMPP Control Panel).
2. Pulsar en Start para los módulos:
    - Apache
    - MySQL

Estos servicios deben quedar en color verde y marcados como activos.

11.1.4. Crear la base de datos MySQL

1. Acceder a phpMyAdmin desde el navegador:
   http://localhost/phpmyadmin
2. Hacer clic en la pestaña Bases de datos.
3. Crear una nueva base de datos con el nombre: ***tfg***
4. Seleccionar ***utf8mb4_spanish_ci*** como cotejamiento (collation) y confirmar.

11.1.5. Importar la estructura de la base de datos

1. Dentro de phpMyAdmin, seleccionar la base de datos **tfg**.
2. Ir a la pestaña Importar.
3. Seleccionar el archivo **basededatos.sql** proporcionado
4. Hacer clic en **Continuar** para ejecutar la importación.
   Este archivo genera todas las tablas necesarias y también insertarn los 93 controles de ISO 27001.

11.1.6. Copiar el proyecto a la carpeta del servidor

1. Crear la carpeta:

   C:\xampp\htdocs\tfg

2. Copiar la carpeta proyecto.zip proporcionada a la siguiente ruta:

   C:\xampp\htdocs\tfg

3. Descomprimir el archivo proyecto.zip.

11.1.7. Configurar la conexión a la base de datos

1. Abrir el archivo C:\xampp\htdocs\tfg\database\db.php y confirmar los siguientes datos:

   ```
   php
   CopiarEditar
   $servername = "localhost";
   $username = "root";
   $password = "";
   $database = "tfg";
   ```

No es necesario establecer contraseña si se utiliza la configuración por defecto de MySQL en XAMPP, en el caso que se haya puesto otro usuario y password para acceder, debe cambiarse en este archivo.

11.1.8. Acceder a la aplicación

1. Abrir el navegador y escribir la siguiente URL:

   http://localhost/tfg

2. Se cargará la interfaz de login del sistema.

11.1.9. Usuarios de prueba

Por defecto ya hay creados tres usuarios de prueba que representan los 3 roles posibles en la aplicación.

- **Admin: jaime@goal.com**
- **Auditor: miguel@goal.com**
- **Usuario: federico@goal.com**

Todos ellos con **Contraseña:** 1 (cifrada en base de datos con password_hash)

Se recomienda borrarlos una vez se creen los usuarios definitivos de la aplicación.

11.2. Manual de Usuario de la Aplicación

11.2.1. Acceso a la Plataforma

Para acceder a la plataforma, el usuario debe abrir el navegador web y dirigirse a la URL del sistema, por ejemplo:

http://localhost/tfg/

1.1.1.1 Pantalla de login

Ilustración 12 Pantalla de Login

- Introducir correo electrónico registrado.
- Introducir la contraseña asociada.
- Pulsar en el botón "Iniciar sesión".

NOTA:

- En caso de error en las credenciales, se mostrará un mensaje de advertencia.

Ilustración 13 Login incorrecto aviso

- En caso de olvido de contraseña, el usuario debe contactar con el administrador para su recuperación.

11.2.2. Navegación General

Una vez iniciada sesión, el usuario verá una página de bienvenida donde puede iniciar el trabajo pulsando **"Empieza Ahora"**.

Ilustración 14 Págian de bienvenida

1.1.1.2 Barra de navegación superior

Ilustración 15 Barra de navegación

- **Nombre de Usuario:** Visualiza el nombre del usuario y su rol.
- **Empresa:** Muestra la empresa a la que pertenece el usuario.

- **Rol de Usuario:** Indica si es Administrador, Auditor o Usuario.
- **Botón "Cerrar Sesión":** Finaliza la sesión de manera segura.
- **Menú Principal:** Acceso rápido a Inicio, Auditorías y Administración (sólo Administradores).

11.2.3. Listado de Auditorías

Accediendo a **Auditorías** en el menú, se despliega el listado de auditorías disponibles.

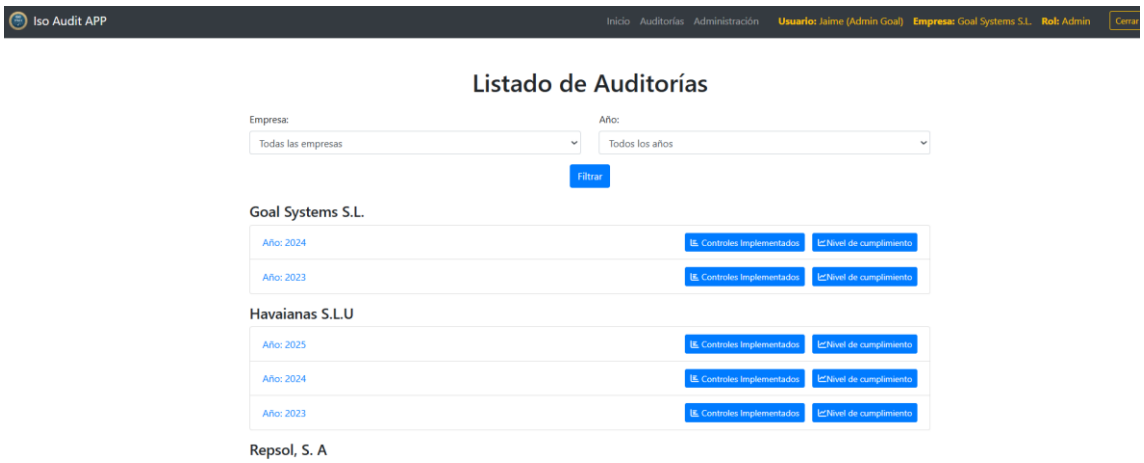


Ilustración 16 Listado de Auditorías

1.1.1.3 Filtrado de Auditorías

- **Empresa:** Filtrar por empresa.
- **Año:** Filtrar por año de auditoría.

11.2.4. Acceso a Gráficas.

- **Controles Implementados:** Gráfica por categorías ISO (Organizacional, Personas, Tecnológica, Física).
- **Nivel de Cumplimiento:** Gráfica general de cumplimiento.

11.2.5. Diferencias de Vista por Rol

- **Usuarios normales:** Solo ven auditorías de su empresa.
- **Auditores y Administradores:** Ven todas las auditorías existentes.

11.3. Visualización de los Controles ISO de una Auditoría

Una vez que se selecciona en el panel anterior una auditoríia se abre el panel completo con sus controles

Ilustración 17 Listatdo de controles

11.3.1. Agrupación de Controles

Todos los controles se muestran agrupados por familias, al pinchar sobre una de ellas se despliega mostrando todos aquellos que pertenecen a esta:

Ilustración 18 Listado de controles desplegado

11.3.2. Estado de los Controles

- **Rojo:** No revisado ni validado por el auditor.
- **Verde:** Revisado y validado por el auditor.

11.3.3. Acceso al control:

Junto con cada control, encontrará un botón para acceder a rellenar los datos del control y dependiendo de su contenido nos indicará si es un control aun no trabajado o si el control ya se ha estado trabajando previamente por el usuario:

- **Actualizar Control** si ya se ha estado trabajando previamente en el control.
  Actualizar Control
- **No Empezado** si aún no se ha trabajado.
  No Empezado

11.4. Rellenar un Control de Auditoría

Una vez que se accede a un control encontramos un panel como el que se muestra en la imagen:

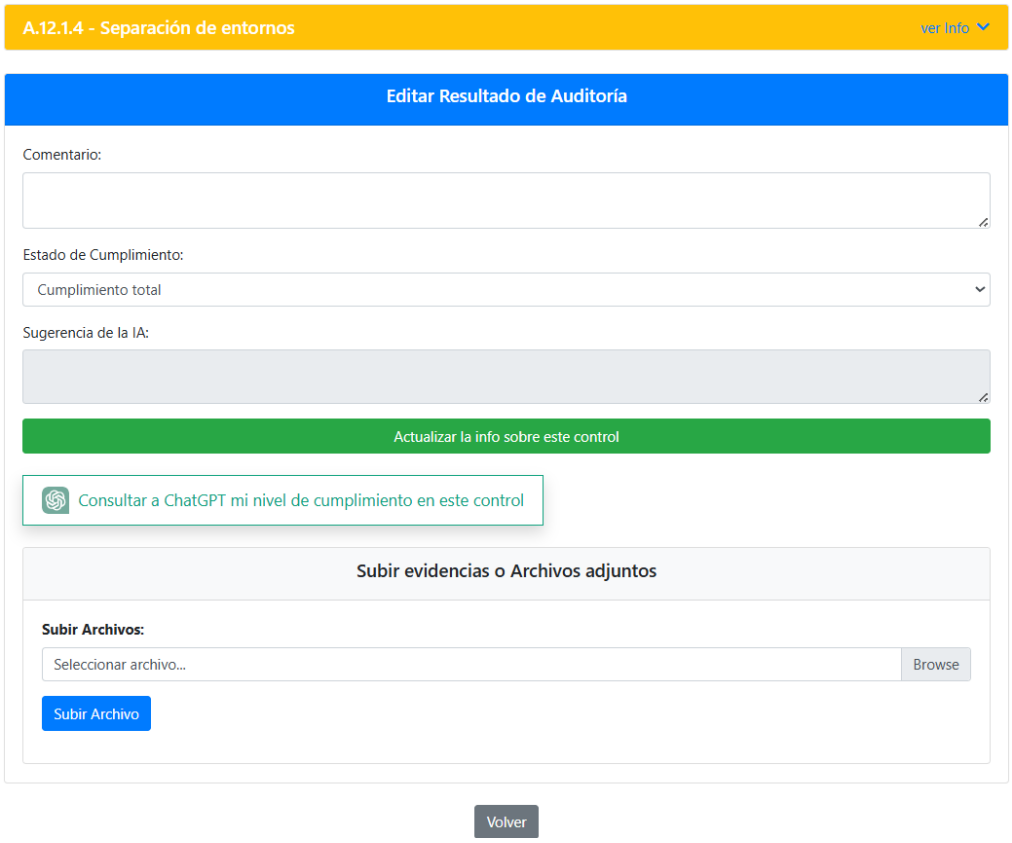


Ilustración 19 Edición de control

11.4.1. Información del Control

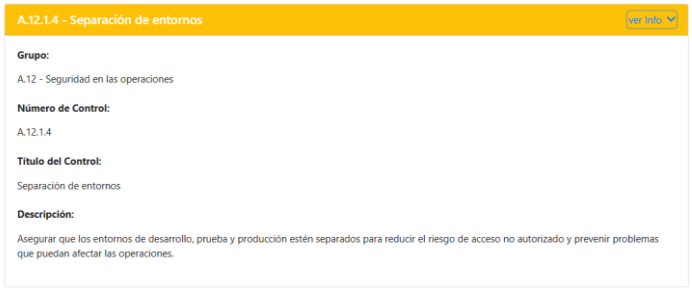


Ilustración 20 Desplegable de información del control

Se trata de un desplegable que muestra pulsando sobre "Ver Info" toda la información relativa a ese control a modo consulta (Grupo, Número, Título, Descripción de este).

11.4.2. Edición del Resultado de Auditoría

1. **Comentario:** Descripción de cumplimiento, es aquí donde el usuario debe explicar claramente lo que ha hecho ese año para cumplir con el control sobre el que estamos trabajando, también es recomendable

explicar que documentación se va a aportar junto con esta explicación como evidencias de cumplimiento.

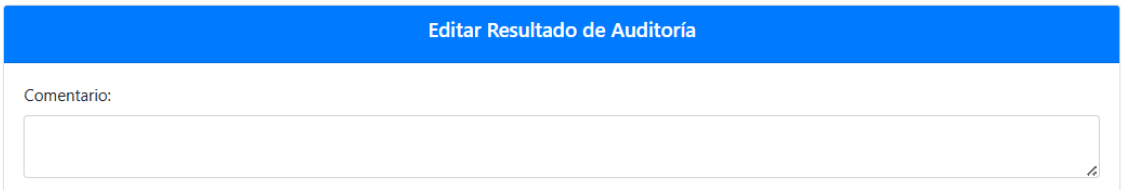


Ilustración 21 Detalle apartado de comentarios sobre el control

2. **Estado de Cumplimiento:**

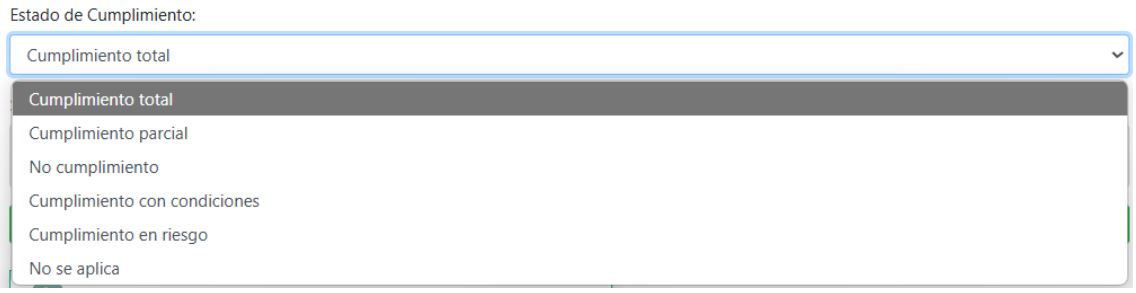


Ilustración 22 Detalle apartado: Estado de cumplimiento

a) **Cumplimiento total:**
   El control está completamente implementado y funciona eficazmente sin deficiencias.
b) **Cumplimiento parcial:**
   El control está parcialmente implantado, pero presenta carencias que deben corregirse.
c) **No cumplimiento:**
   El control no está implementado ni existen medidas que cumplan su propósito.
d) **Cumplimiento con condiciones:**
   El control está implantado pero su eficacia depende de factores externos o condicionantes.
e) **Cumplimiento en riesgo:**
   El control está implantado, pero existen riesgos conocidos que pueden afectar su efectividad.
f) **No se aplica:**
   El control no es relevante para la organización por su naturaleza, contexto o alcance.

3. **Consulta a la IA (Evaluación automática opcional.):**

Este botón permite al usuario solicitar una evaluación automática de su respuesta escrita para un control específico.

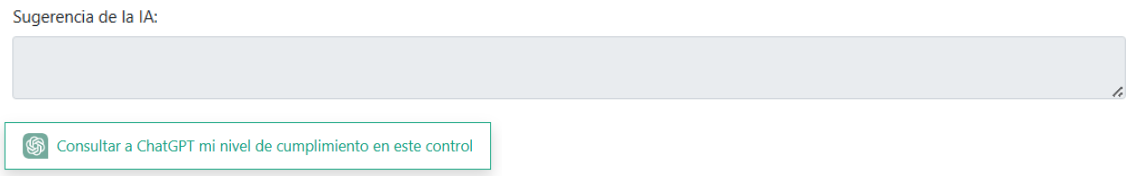


Ilustración 23 Detalle de la Consulta a la IA

Al pulsarlo, la plataforma envía el comentario redactado por el usuario a un modelo de inteligencia artificial (ChatGPT) que analiza el contenido y genera una sugerencia sobre el nivel de cumplimiento del control.
El resultado se muestra automáticamente en el campo "Sugerencia de la IA", proporcionando retroalimentación sobre si el cumplimiento parece adecuado, si faltan evidencias o si existen riesgos.

Esta funcionalidad sirve como apoyo adicional para que el usuario pueda validar o mejorar su respuesta antes de ser revisada por un auditor humano.

4. **Validado:** (Solo auditores).

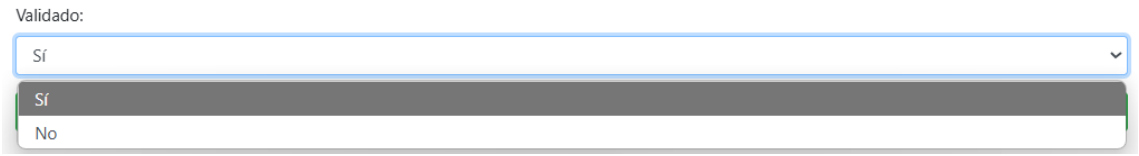


Ilustración 24 Pestaña de validación de controles de un Auditor

Esta opción es específica de auditores y sirve para validar la revisión de este control.

11.4.3. Subida de Evidencias

La plataforma permite adjuntar documentos de evidencia para respaldar el cumplimiento de cada control auditado.

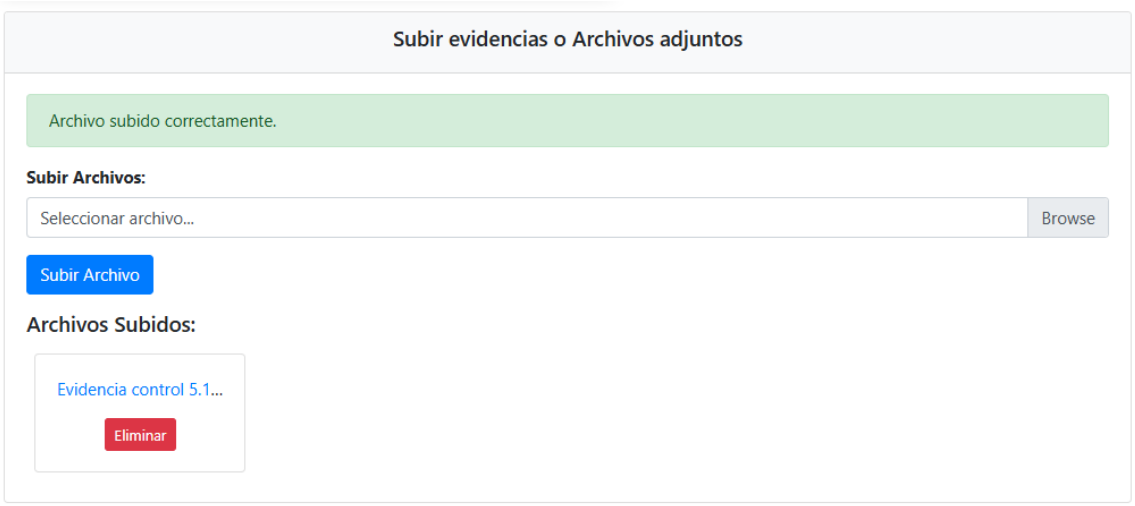


Ilustración 25 Detalle apartado de subida de archivos

1. **Seleccionar Archivo:**
   El usuario debe pulsar el botón "Browse" para abrir el explorador de archivos local y seleccionar el documento que desea adjuntar.
   Se admiten formatos habituales como PDF, Word, imágenes, etc.

2. **Subir Archivo:**
   Una vez seleccionado el archivo, se debe pulsar el botón azul **"Subir Archivo"**.
   Al completarse la carga correctamente, el sistema mostrará un mensaje de confirmación en color verde:
   "Archivo subido correctamente."

3. **Gestión de Archivos Subidos:**
   Los archivos subidos aparecen listados en la misma sección, mostrando su nombre y ofreciendo un botón rojo **"Eliminar"** por si se desea borrar alguna evidencia asociada.

Cada documento se guarda vinculado al control ISO correspondiente, permitiendo su consulta y validación posterior por parte del auditor.

11.4.4. Guardar Cambios

Cada vez que se quiera actualizar el control debe usarse el botón: "Actualizar la info sobre este control".

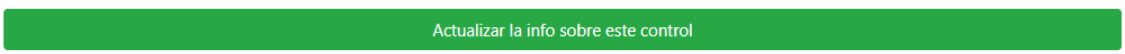


Ilustración 26 Botón para guardar cambios en la edición de controles

11.5. Visualización de Gráficas

Tanto auditores como usuarios tienen a su disposición dos gráficas:

1.1.1.4 Gráfico general de cumplimiento

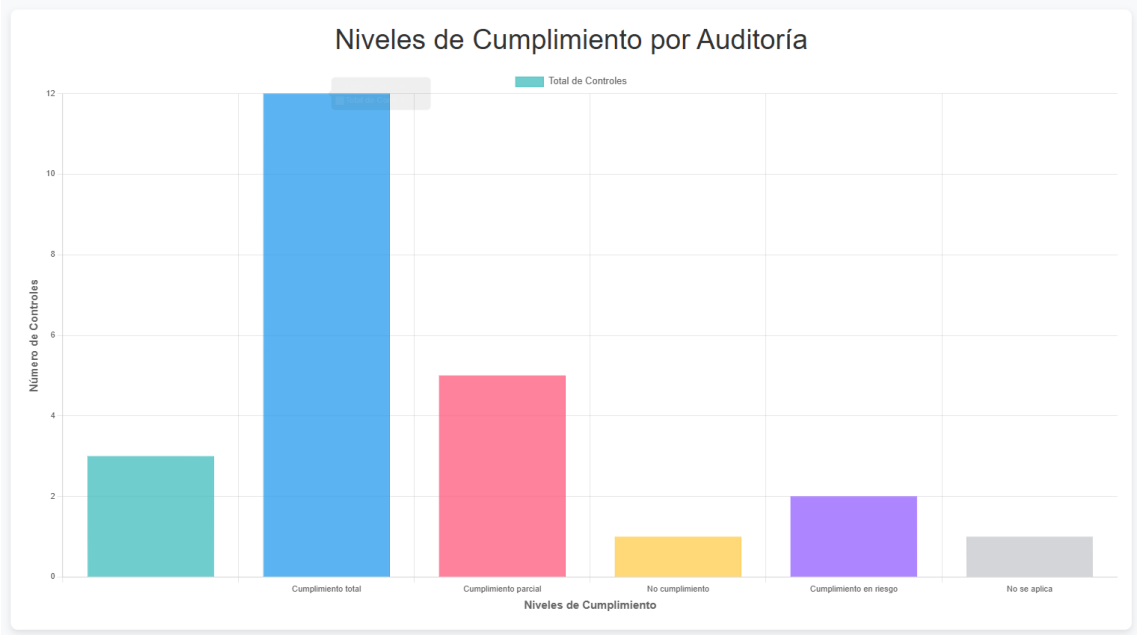


Ilustración 27 Gráfico general de cumplimiento

Esta gráfica representa el estado de cumplimiento de todos los controles evaluados en una auditoría concreta. Cada barra muestra el número de controles clasificados según su nivel de cumplimiento

Esta visualización permite detectar rápidamente el grado de madurez de la empresa respecto a la norma ISO 27001 y ayuda a priorizar acciones de mejora.

1.1.1.5 Gráfico de cumplimiento por categorías ISO.

Ilustración 28 Gráfico de cumplimiento por categorías ISO.

Esta gráfica muestra la comparación entre el número de controles implementados y el número total de controles posibles en cada grupo de la norma ISO 27001. Cada grupo temático (por ejemplo, Criptografía, Seguridad física y ambiental, etc.) se representa en el eje horizontal, mientras que el número de controles se muestra en el eje vertical. Las barras de color azul indican los controles implementados, y las barras de color verde representan el total de controles que deberían implementarse.

11.6. Funcionalidades para Administradores

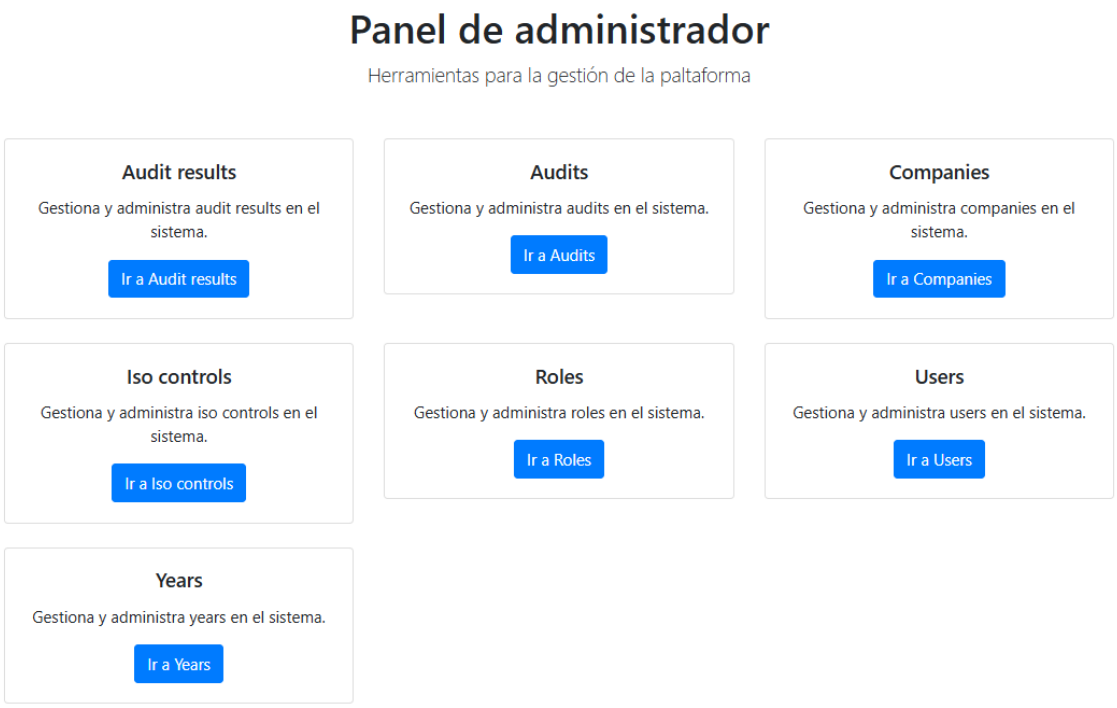


Ilustración 29 Panel de Administrador

Todos los módulos de Administración mantienen la misma estructura de gestión a continuación se detalla cada uno de ellos.

11.6.1. Gestión de Resultados: Audit Results

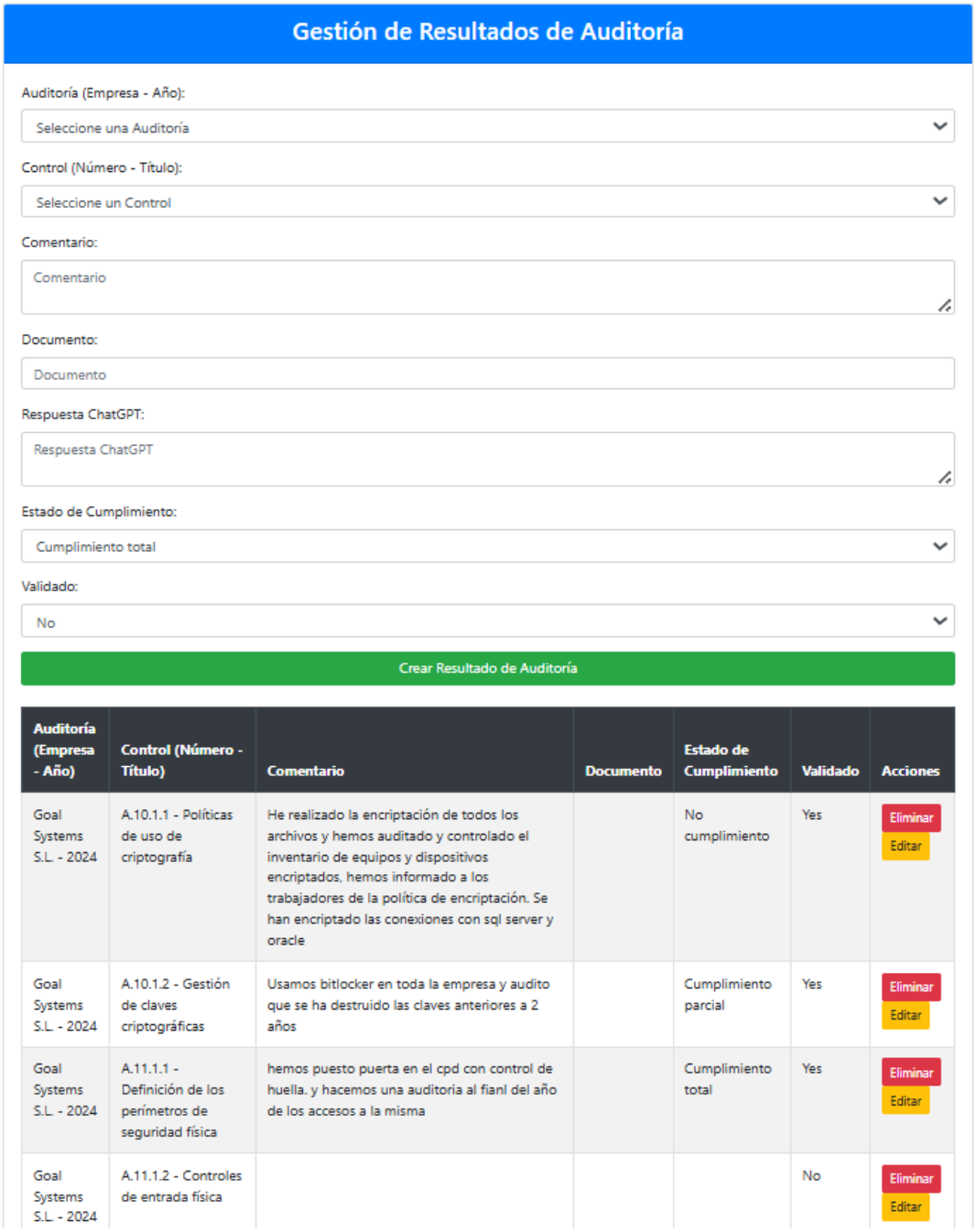


Ilustración 30 Administración - Gestión de resultados

Esta sección permite al administrador corregir directamente cualquier error en las respuestas aportadas por los usuarios, que no pueda ser subsanado desde el panel habitual de trabajo.

11.6.2. Gestión de Auditorías: Audits

Ilustración 31Administración - Gestión Auditorías

Desde este panel el administrador puede crear, editar o eliminar auditorías, asociándolas a una empresa y un año concreto, y gestionar su información básica antes de iniciar el proceso de auditoría.

11.6.3. Gestión de compañías: Companies

Ilustración 32Administración - Gestión Empresas

Desde este panel el administrador puede crear, editar o eliminar empresas registradas en el sistema, asociándoles información básica como nombre, CIF, dirección y teléfono, para su uso en las auditorías.

11.6.4. Gestión de Controles ISO: Iso Controls

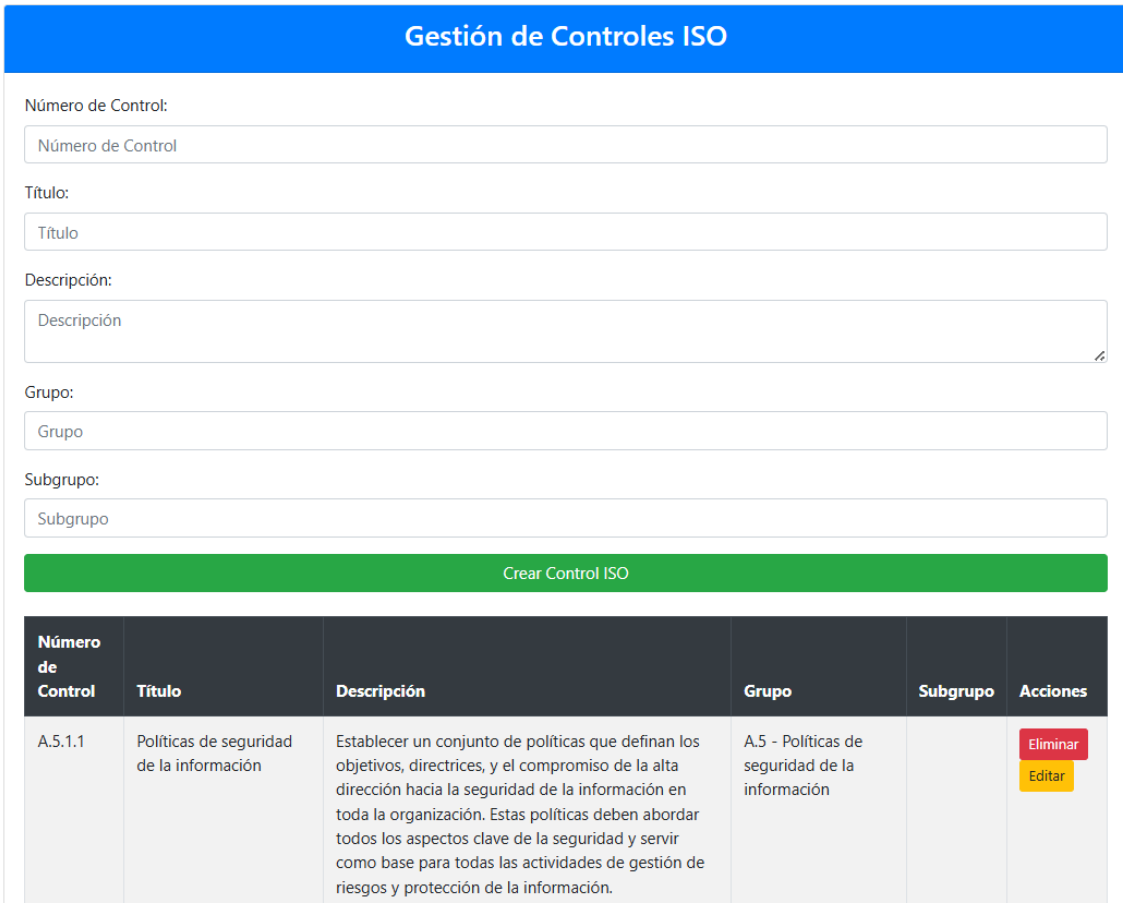


Ilustración 33 Adminsitración - Gestión de controles

Desde esta sección, el administrador puede crear nuevos controles que se añadirán a los controles a revisar en todas las auditorías. También es posible editar la información existente o eliminar controles si es necesario

11.6.5. Gestión de Roles

Ilustración 34 Administración - Gestión Roles

Desde esta sección, el administrador puede crear nuevos roles para crear nuevos permisos. También es posible editar la información existente o eliminar roles si es necesario

11.6.6. Gestión de Usuarios: Users

Ilustración 35 Administración - Gestión Usuarios

Desde esta sección, el administrador puede crear nuevos usuarios asociándolos a una empresa y asignándoles un rol (Admin, Auditor o Usuario). También es posible editar la información existente o eliminar usuarios si es necesario

11.6.7. Gestión de periodos de auditoría: Years

En esta sección el administrador puede crear, editar o eliminar los años disponibles para asociarlos a las auditorías.

Ilustración 36 Administración - Gestión Periodos auditoría