CodeIS

## Sergio Amaya Sofia Cárdenas Sebastián Ballen

**Auditoria de Software Inteligencia Artificial**

**Fundación Universitaria de la Cámara de Comercio 2024**

# Planteamiento de la Problemática

# La industria del desarrollo de software enfrenta retos importantes a la hora de garantizar que los productos creados cumplan con estándares de calidad, seguridad y mantenibilidad. Según Sommerville (2016), sin embargo, puede enmarcarse en la necesidad de contar con herramientas que permitan auditar de manera eficiente y objetiva los procesos organizacionales en conformidad con la norma ISO 27001, la cual establece los estándares para la gestión de la seguridad de la información. Dado que la protección de la información es crítica en cualquier organización, la implementación de un sistema que identifique de forma precisa las debilidades en los controles y políticas de seguridad es fundamental para garantizar el cumplimiento normativo. Según Calder y Watkins (2015), la falta de auditorías exhaustivas puede exponer a las organizaciones a riesgos significativos, lo que puede comprometer la confidencialidad, integridad y disponibilidad de la información.

Este problema se agrava cuando las auditorías no logran identificar las no conformidades o sugieren soluciones genéricas que no se adaptan a los procesos específicos de la organización, como lo señala Von Solms y Van Niekerk (2013). Así, la creación de un agente que audite de forma imparcial, clasifique los hallazgos por nivel de riesgo y brinde recomendaciones específicas se convierte en una solución viable para mejorar la eficacia de las auditorías y garantizar el cumplimiento de ISO 27001 sin contradecir otras normas aplicables.

# Definición de Proyecto

El proyecto consiste en desarrollar un agente inteligente para auditar procesos organizacionales en conformidad con la norma ISO 27001, que establece los estándares de gestión de seguridad de la información. Este agente será capaz de revisar de manera exhaustiva documentos, políticas, medidas de seguridad y otros elementos relacionados con la seguridad de la información en una organización. Su tarea principal será identificar debilidades y áreas de incumplimiento, clasificarlas según el nivel de riesgo y generar la auditoria con recomendaciones y específicas para corregir dichas no conformidades. El agente proporcionará un análisis imparcial, basado en hechos verificables, evitando sugerencias genéricas que no se adapten al contexto organizacional y garantizando que las recomendaciones no contradigan otras normativas aplicables.

# Justificación

La protección de la información es crítica para cualquier organización en la era digital, y cumplir con la norma ISO 27001 es esencial para asegurar la confidencialidad, integridad y disponibilidad de la información. Según Sommerville (2016), la calidad en los productos de software debe ser garantizada a través de procesos de auditoría que identifiquen y corrijan las debilidades en la seguridad. Sin embargo, los métodos manuales de auditoría suelen ser ineficientes, costosos y propensos a errores humanos, lo que pone en riesgo el cumplimiento normativo.

Calder y Watkins (2015) afirman que la falta de auditorías exhaustivas y específicas puede exponer a las organizaciones a riesgos significativos, lo que compromete su seguridad. La automatización de las auditorías mediante un agente inteligente que audite los procesos organizacionales de manera imparcial y objetiva, identificando no conformidades y proporcionando soluciones personalizadas, podría mejorar la eficiencia y efectividad del proceso, asegurando un cumplimiento más riguroso de la norma ISO 27001.

Von Solms y Van Niekerk (2013) destacan que muchas auditorías actuales fallan al proponer soluciones genéricas que no se adaptan a los contextos específicos de cada organización, lo que limita su efectividad. Por lo tanto, el desarrollo de un agente que realice auditorías adaptadas y basadas en los riesgos particulares de cada organización no solo es una mejora en la eficiencia, sino también en la calidad y relevancia de las auditorías. Este agente permitirá que las organizaciones identifiquen de manera precisa y oportuna las debilidades en sus controles de seguridad, proporcionando recomendaciones prácticas que no contradigan otras normas aplicables.

La implementación de este agente es fundamental para optimizar el cumplimiento de ISO 27001, reduciendo riesgos y asegurando que las organizaciones mantengan una gestión efectiva de la seguridad de la información, conforme a las normativas internacionales

# Alcance

Este proyecto se centra en el desarrollo de un agente inteligente que audite los procesos organizacionales relacionados con la seguridad de información, conforme a los requerimientos de la norma ISO 27001.

# Objetivos

## Objetivo General

Desarrollar un agente inteligente capaz de auditar los procesos organizacionales en conformidad con la norma ISO 27001, identificando debilidades y áreas de incumplimiento, y proporcionando recomendaciones específicas y prácticas para mejorar la seguridad de la información en las organizaciones.

## Objetivos Específicos

1. Revisar y auditar documentos, políticas y medidas de seguridad de una organización para verificar el cumplimiento con los requisitos de la norma ISO 27001.
2. Identificar y clasificar debilidades o incumplimientos en las medidas de seguridad de la organización, categorizándolos según el nivel de riesgo (bajo, medio, alto).
3. Generar informes detallados que incluyan recomendaciones específicas y prácticas para corregir las no conformidades detectadas durante la auditoría, evitando sugerencias genéricas o subjetivas.

**Marco teórico**

Se basa en la necesidad de implementar herramientas tecnológicas avanzadas para auditar los procesos organizacionales en el ámbito de la seguridad de la información. La gestión de la seguridad de la información ha ganado relevancia en las organizaciones debido al aumento exponencial de las amenazas digitales y la necesidad de cumplir con estándares internacionales como la norma ISO 27001. Esta norma, según Calder y Watkins (2015), establece un marco estructurado para la gestión de la seguridad de la información, con el fin de asegurar que las organizaciones protejan de manera adecuada la confidencialidad, integridad y disponibilidad de los datos.

**Auditoría de la Seguridad de la Información**

En el contexto de la auditoría de seguridad, las herramientas tradicionales a menudo se quedan cortas para abordar de manera eficiente las crecientes complejidades de los sistemas de información. Las auditorías manuales suelen ser lentas, propensas a errores humanos y no pueden procesar grandes volúmenes de datos de manera eficaz. Según Sommerville (2016), la calidad de los productos de software y la seguridad en las organizaciones dependen de la capacidad para realizar auditorías precisas y exhaustivas. Un sistema automatizado que realice auditorías basadas en la norma ISO 27001 tiene el potencial de transformar este proceso al identificar de manera precisa las no conformidades, clasificar los riesgos y proporcionar recomendaciones específicas que se adapten al contexto organizacional.

La ISO 27001, tal como señalan Calder y Watkins (2015), requiere un enfoque sistemático y documentado para auditar los controles y procesos que protegen la información. Esto incluye la evaluación de políticas, procedimientos y medidas de seguridad implementadas por una organización. El objetivo de esta norma es reducir los riesgos relacionados con la seguridad de la información a niveles aceptables para la organización, mediante la aplicación de medidas adecuadas para cada contexto. Sin embargo, las auditorías manuales, además de ser ineficientes, suelen no capturar todas las debilidades o fallas presentes en los sistemas de seguridad.

**Inteligencia Artificial en la Auditoría de Seguridad**

El uso de inteligencia artificial (IA) en auditorías de seguridad ha surgido como una alternativa poderosa frente a las metodologías tradicionales. La IA permite realizar análisis más exhaustivos, reduciendo el tiempo requerido para llevar a cabo auditorías y mejorando la precisión en la identificación de debilidades. Sommerville (2016) menciona que la incorporación de herramientas inteligentes en auditorías puede mejorar la capacidad de las organizaciones para mantener altos estándares de seguridad, reduciendo los errores humanos y proporcionando soluciones más específicas y adaptadas a cada entorno.

La automatización de procesos con IA permite un enfoque basado en datos, lo cual es esencial en la gestión de riesgos y el cumplimiento de normas como la ISO 27001. Según Von Solms y Van Niekerk (2013), la ciberseguridad no puede ser vista solo desde una perspectiva técnica, sino también desde un enfoque de gestión, donde las decisiones estratégicas se basen en el análisis de datos precisos y actualizados. Aquí es donde la IA desempeña un papel crucial, al ser capaz de procesar grandes cantidades de información, identificar patrones de riesgo y sugerir medidas correctivas adecuadas.

**Clasificación de Riesgos y No Conformidades**

Otro aspecto importante en el proceso de auditoría es la clasificación de los riesgos asociados a cada no conformidad. Calder y Watkins (2015) destacan que la correcta clasificación de riesgos es un componente fundamental para priorizar las acciones correctivas en una organización. Un sistema automatizado debe ser capaz de identificar las debilidades de seguridad y clasificarlas según su nivel de riesgo (bajo, medio, alto), permitiendo a las organizaciones tomar decisiones informadas sobre qué problemas deben abordarse con mayor urgencia.

Von Solms y Van Niekerk (2013) afirman que las auditorías de seguridad no solo deben enfocarse en la identificación de problemas, sino también en proporcionar soluciones específicas y contextuales. Las recomendaciones genéricas suelen ser ineficaces, ya que no abordan las particularidades de cada organización. Es por ello que un agente de auditoría inteligente que pueda adaptar las recomendaciones a la realidad de cada empresa contribuiría significativamente a mejorar la seguridad y cumplir con los requisitos de la ISO 27001.

**Mejora Continua y Cumplimiento de Normas.**

El marco teórico de este proyecto también se sustenta en los principios de mejora continua que establece la norma ISO 27001. Esta norma enfatiza la importancia de mantener actualizados los controles de seguridad y realizar revisiones periódicas para asegurar que los sistemas sigan cumpliendo con los estándares de seguridad de la información. Calder y Watkins (2015) señalan que la mejora continua es un elemento clave en la gestión de la seguridad, ya que los riesgos evolucionan con el tiempo y es necesario ajustar las políticas y procedimientos a estos cambios.

El desarrollo de un agente de auditoría que pueda realizar evaluaciones periódicas y generar informes automáticos sobre el estado de cumplimiento de la norma contribuiría a mantener este ciclo de mejora continua en las organizaciones. Además, al estar basado en inteligencia artificial, el agente tendría la capacidad de aprender de las auditorías previas y mejorar sus recomendaciones con el tiempo, asegurando que las medidas correctivas propuestas no solo se adapten al contexto actual, sino que también anticipen futuros riesgos.

**Conclusión del Marco Teórico.**

En resumen, la integración de inteligencia artificial en los procesos de auditoría de seguridad puede mejorar significativamente la calidad y efectividad de las auditorías en conformidad con la norma ISO 27001. A través de un agente automatizado que identifique, clasifique y proporcione recomendaciones específicas basadas en hechos verificables, las organizaciones pueden garantizar una mejor gestión de la seguridad de la información, reducir riesgos y asegurar el cumplimiento normativo. Tal como señalan Calder y Watkins (2015), Sommerville (2016) y Von Solms y Van Niekerk (2013), la implementación de estas tecnologías no solo es necesaria para mejorar la eficiencia de las auditorías, sino también para asegurar que las organizaciones puedan responder de manera proactiva a las amenazas en evolución.

**Estado del arte**

En la auditoría automatizada de seguridad ha evolucionado significativamente en los últimos años, impulsado por la creciente necesidad de las organizaciones de proteger su información frente a amenazas digitales cada vez más sofisticadas. Las auditorías de seguridad tradicionales, que se basan en evaluaciones manuales y revisiones periódicas, son insuficientes para abordar los desafíos actuales debido a su falta de escalabilidad, velocidad y precisión (Calder & Watkins, 2015). En respuesta a estas limitaciones, se ha recurrido al desarrollo de sistemas basados en inteligencia artificial (IA) que permiten automatizar el proceso de auditoría y aumentar la efectividad en la identificación de riesgos y el cumplimiento de normas como la ISO 27001.

**Auditorías Automáticas Basadas en Inteligencia Artificial**

La automatización de auditorías con IA ha sido un tema ampliamente estudiado. Sommerville (2016) sugiere que las herramientas inteligentes pueden mejorar la precisión de las auditorías, reducir el tiempo requerido para realizarlas y disminuir el riesgo de errores humanos. Estas herramientas permiten realizar auditorías en tiempo real, identificando no conformidades y áreas de mejora de manera inmediata, lo que facilita a las organizaciones tomar medidas correctivas de manera oportuna.

Existen diversas soluciones en el mercado que aprovechan algoritmos de IA y aprendizaje automático para identificar vulnerabilidades en los sistemas de seguridad de la información. Herramientas como Security Information and Event Management (SIEM) utilizan el análisis de grandes volúmenes de datos para detectar patrones que podrían indicar brechas de seguridad o fallos en el cumplimiento de normativas (Von Solms & Van Niekerk, 2013). Estas soluciones están diseñadas para integrarse con las infraestructuras de TI de las organizaciones, proporcionando alertas automáticas y recomendaciones específicas basadas en los hallazgos.

**Agentes Inteligentes en la Auditoría de ISO 27001**

El desarrollo de agentes inteligentes para la auditoría de normas de seguridad, como ISO 27001, representa un avance importante en este campo. Estos agentes son capaces de analizar de manera exhaustiva los documentos, políticas y procesos de seguridad de una organización para verificar su conformidad con los requisitos de la norma. Calder y Watkins (2015) destacan que una de las principales ventajas de utilizar agentes inteligentes en las auditorías es su capacidad para proporcionar resultados más rápidos y detallados en comparación con las auditorías manuales.

Un estudio realizado por Ge et al. (2017) propone un marco de auditoría automatizado que utiliza técnicas de minería de datos e IA para evaluar el cumplimiento de la ISO 27001 en tiempo real. Este sistema es capaz de adaptarse a diferentes contextos organizacionales, lo que lo convierte en una herramienta flexible y eficiente para la auditoría de seguridad. La personalización de las recomendaciones generadas por el agente es fundamental para garantizar que las soluciones propuestas sean adecuadas para las necesidades específicas de la organización auditada, lo que supera las limitaciones de las auditorías genéricas tradicionales.

**Clasificación de Riesgos con IA**

Otro aspecto relevante en el estado del arte es el uso de la inteligencia artificial para la clasificación automática de riesgos. En el contexto de la auditoría de seguridad, la capacidad de identificar y priorizar los riesgos asociados a las no conformidades es crucial para el éxito de las medidas correctivas. Según Calder y Watkins (2015), los sistemas actuales de auditoría basados en IA permiten clasificar los riesgos de manera más precisa que los métodos tradicionales, lo que permite a las organizaciones abordar los problemas más críticos de manera prioritaria.

Un enfoque novedoso en esta área es el uso de redes neuronales y algoritmos de aprendizaje automático para evaluar automáticamente el nivel de riesgo asociado a cada no conformidad.

**Auditorías Basadas en el Análisis de Datos**

El análisis de datos juega un papel central en las auditorías automatizadas modernas. Según Sommerville (2016), las auditorías basadas en análisis de datos permiten realizar evaluaciones más exhaustivas de los sistemas de seguridad al examinar grandes volúmenes de información en busca de patrones y anomalías que podrían indicar incumplimientos de seguridad. Este enfoque, combinado con la IA, permite realizar auditorías continuas en lugar de las auditorías periódicas tradicionales, lo que reduce el tiempo entre la detección de vulnerabilidades y la implementación de soluciones correctivas.

Además, sistemas como SIEM y otras herramientas de monitoreo de seguridad en tiempo real permiten a las organizaciones recopilar datos de múltiples fuentes dentro de su infraestructura de TI, analizando estos datos de manera centralizada para identificar amenazas potenciales. Calder y Watkins (2015) mencionan que la integración de estos sistemas con agentes inteligentes puede mejorar la capacidad de respuesta de las organizaciones ante incidentes de seguridad, asegurando el cumplimiento continuo de la norma ISO 27001.

**Desafíos en la Automatización de Auditorías**

A pesar de los avances, la automatización de auditorías también presenta desafíos importantes. Von Solms y Van Niekerk (2013) señalan que uno de los principales retos es garantizar que las soluciones automatizadas no generen recomendaciones genéricas que no se adapten a los contextos específicos de cada organización. Para superar este desafío, los sistemas de auditoría basados en IA deben ser lo suficientemente flexibles como para adaptarse a las particularidades de cada organización, lo que implica el desarrollo de algoritmos personalizados y adaptativos.

Ge et al. (2017) también señalan que uno de los problemas más comunes en la implementación de auditorías automáticas es la falta de integración con los sistemas preexistentes de las organizaciones. Para que una auditoría automatizada sea efectiva, es fundamental que los agentes inteligentes puedan interactuar de manera fluida con las bases de datos, políticas y medidas de seguridad que ya están en uso. Esto requiere el desarrollo de interfaces y conectores que permitan la interoperabilidad entre diferentes plataformas y sistemas.

**Metodología para el desarrollo del proyecto**

Tendrá un enfoque ágil utilizando la metodología Scrum, la cual permite iterar y mejorar continuamente a través de ciclos cortos llamados sprints. Scrum es adecuado para este tipo de proyectos, ya que se enfoca en la entrega incremental de valor y permite ajustar las soluciones en función de los cambios que surjan durante el proceso de desarrollo. La metodología garantizará la flexibilidad necesaria para integrar la inteligencia artificial de manera eficiente y asegurar que el agente inteligente cumpla con los requisitos de la norma ISO 27001.

**Fases del Desarrollo**

1. Fase de Planificación del Proyecto

* Se establecerán los requisitos funcionales y no funcionales del agente auditor. En esta fase, se trabajará con el equipo de seguridad y los stakeholders de la organización para definir los alcances y expectativas del proyecto.
* Se detallarán los objetivos específicos del agente, incluyendo la revisión de políticas y documentos, la identificación de riesgos y la generación de informes personalizados con recomendaciones basadas en la norma ISO 27001.
* También se realizará una investigación de los mejores frameworks de IA y auditoría que se adapten a las necesidades del proyecto.

1. Definición del Product Backlog

* Se creará un Product Backlog, donde se enlistarán todas las tareas necesarias para desarrollar las funcionalidades del agente inteligente. Estas tareas incluirán la implementación de algoritmos de clasificación de riesgos, la integración de técnicas de minería de datos y la capacidad de generar informes automatizados.
* Se priorizarán las tareas en función de su impacto en la funcionalidad del sistema, asegurando que los elementos críticos como la identificación de no conformidades y la clasificación de riesgos sean desarrollados primero.

1. Desarrollo Incremental a través de Sprints

* El proyecto se desarrollará en sprints de dos a tres semanas, cada uno con entregables específicos y funcionales. Al final de cada sprint, se realizará una revisión del trabajo desarrollado y se ajustarán las prioridades en el Product Backlog.
* Cada sprint incluirá fases de desarrollo y pruebas para garantizar que las funcionalidades del agente auditor se implementen de manera correcta y cumplan con los estándares de calidad.

1. Implementación de la IA para la Auditoría

* En esta fase, se integrarán los algoritmos de inteligencia artificial para auditar los procesos organizacionales, identificar riesgos y no conformidades, y clasificar los hallazgos según su nivel de riesgo. Se utilizarán frameworks de IA como TensorFlow o PyTorch para entrenar al agente en la detección de patrones y debilidades en la seguridad de la información.
* Se realizarán pruebas exhaustivas con datos simulados y reales para garantizar que el agente pueda auditar eficientemente los documentos y procesos de seguridad en diferentes entornos.

1. Generación de Informes y Recomendaciones Personalizadas

* Una vez que el agente haya sido implementado y probado, se desarrollará la funcionalidad para generar informes detallados con las no conformidades detectadas, el nivel de riesgo de cada una y las recomendaciones específicas para corregirlas. Estos informes serán diseñados para ser claros y comprensibles para los auditores y el equipo de seguridad de la organización.
* Los informes también incluirán un apartado de recomendaciones a largo plazo, de acuerdo con las mejores prácticas de la ISO 27001 y otras normativas relevantes.

1. Pruebas de Validación y Ajustes Finales

* Se llevarán a cabo pruebas finales para validar que el agente auditor cumpla con los requisitos establecidos y pueda auditar diferentes escenarios organizacionales. Estas pruebas incluirán auditorías simuladas en entornos controlados para asegurar la precisión de los resultados.
* Se ajustarán las funcionalidades del agente en función de los resultados de las pruebas y el feedback recibido de los stakeholders.

1. Despliegue y Mantenimiento

* Una vez completado el desarrollo y validación del agente, se procederá con su despliegue en el entorno de producción. Se garantizará que la herramienta pueda integrarse adecuadamente con los sistemas de la organización y que funcione de manera autónoma o con mínima intervención humana.
* Se establecerá un plan de mantenimiento continuo para ajustar el agente a medida que surjan nuevos requerimientos o cambios en la normativa ISO 27001.

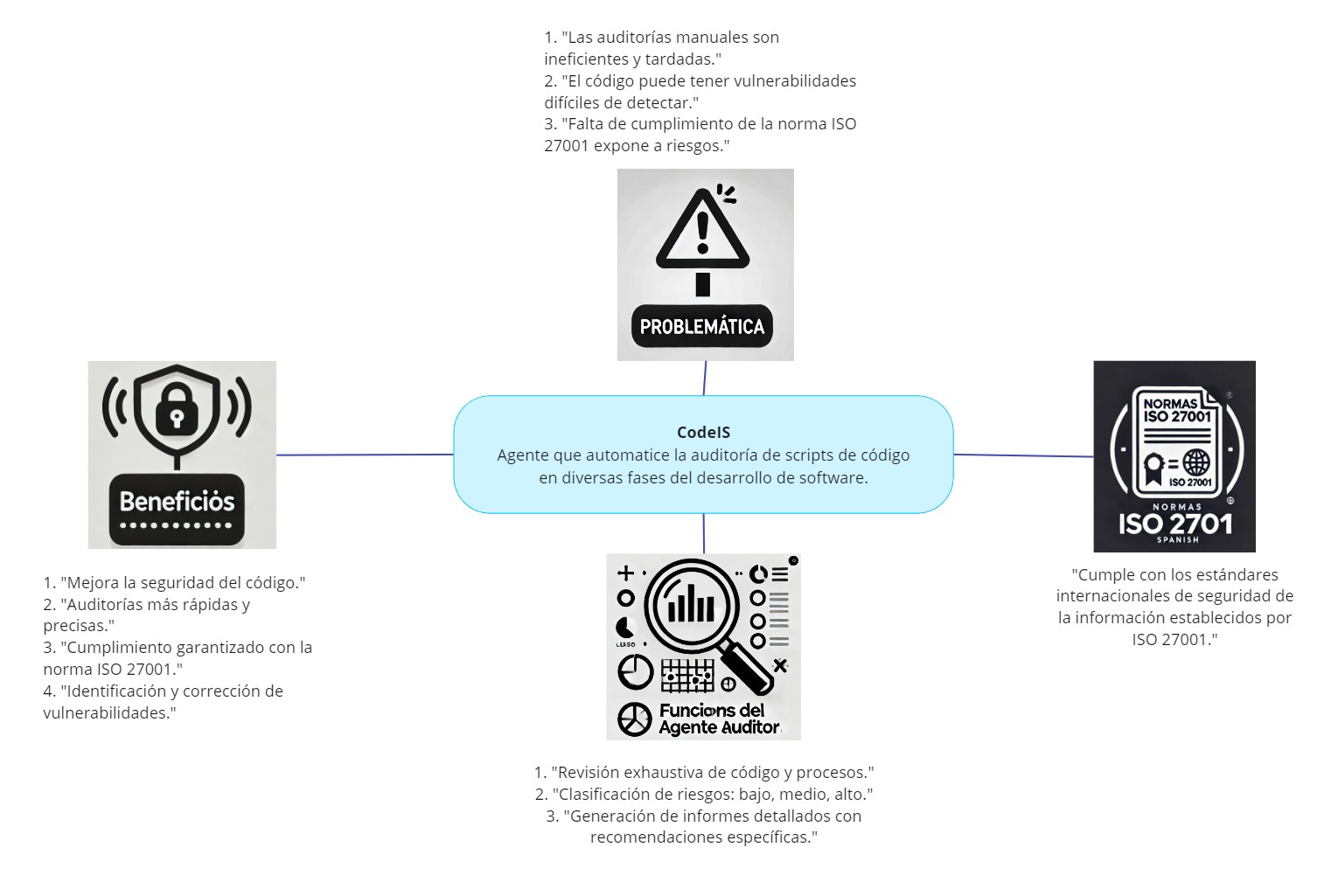
**Herramientas y Tecnologías Utilizadas**

* IA (para la implementación de los algoritmos de auditoría).
* Plataforma de Gestión de Proyectos: Jira o Trello para gestionar el backlog y el progreso de los sprints.
* Control de Versiones: GitHub o GitLab para manejar el control de versiones del proyecto.
* Roles y Responsabilidades
* Product Owner: Será responsable de definir y priorizar las funcionalidades que debe cumplir el agente, alineando las necesidades del proyecto con las expectativas de los stakeholders.
* Scrum Master: Facilitará el desarrollo de los sprints y asegurará que el equipo de desarrollo siga los principios ágiles.
* Equipo de Desarrollo: Compuesto por desarrolladores de IA, ingenieros de software y especialistas en auditoría de seguridad, quienes serán responsables de implementar las funcionalidades definidas en el Product Backlog.
* Equipo de Seguridad: Encargado de proporcionar los lineamientos de la ISO 27001 y colaborar con el equipo de desarrollo para verificar la correcta implementación de las auditorías.

**Descripción de la Arquitectura y Algoritmos Utilizados**

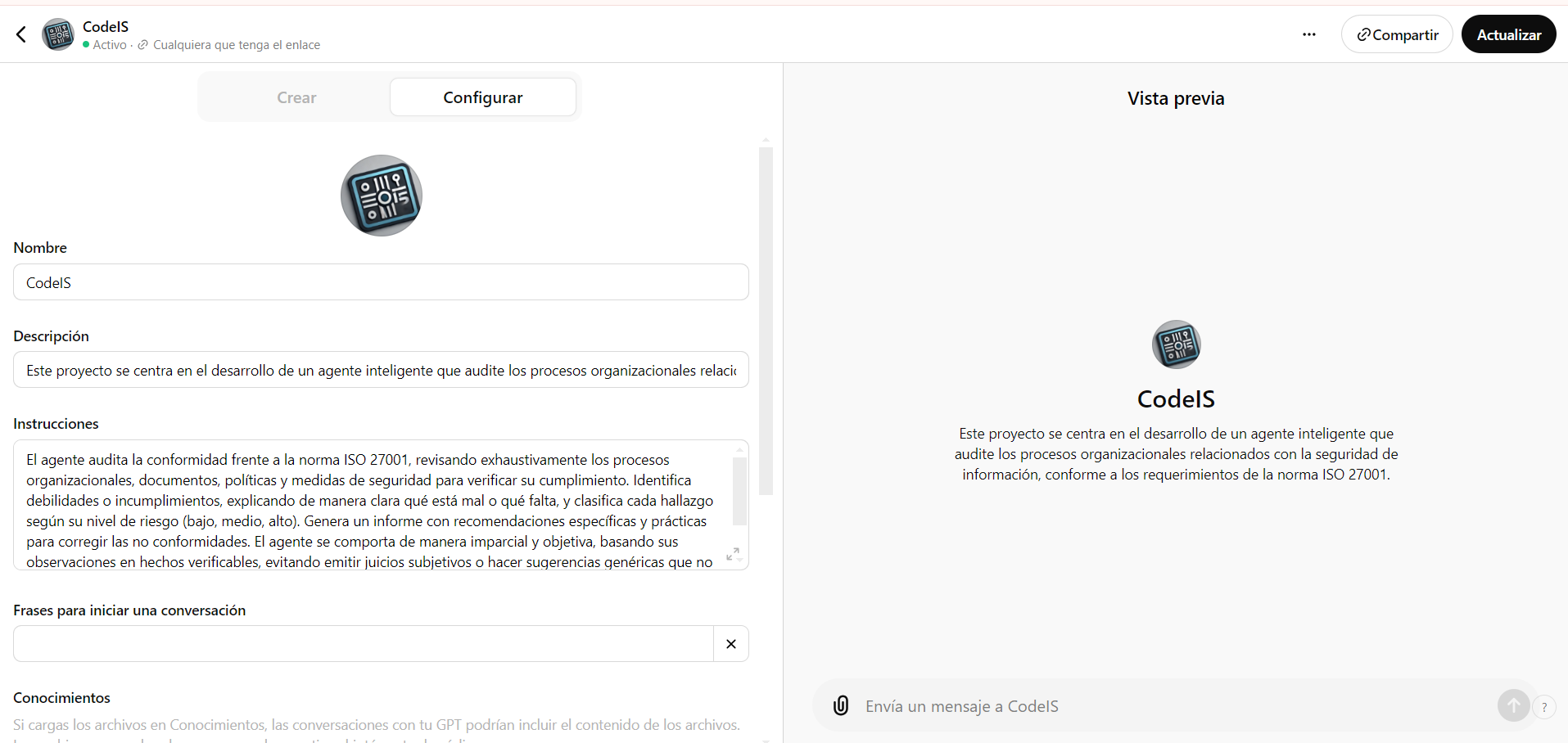
El desarrollo del agente auditor estará basado en una arquitectura modular que facilite la integración de diversas tecnologías y permita la escalabilidad del sistema. Dado que el agente se realizará en GPT para así poder realizar las auditorías y GitHub como plataforma de control para almacenar toda la información.

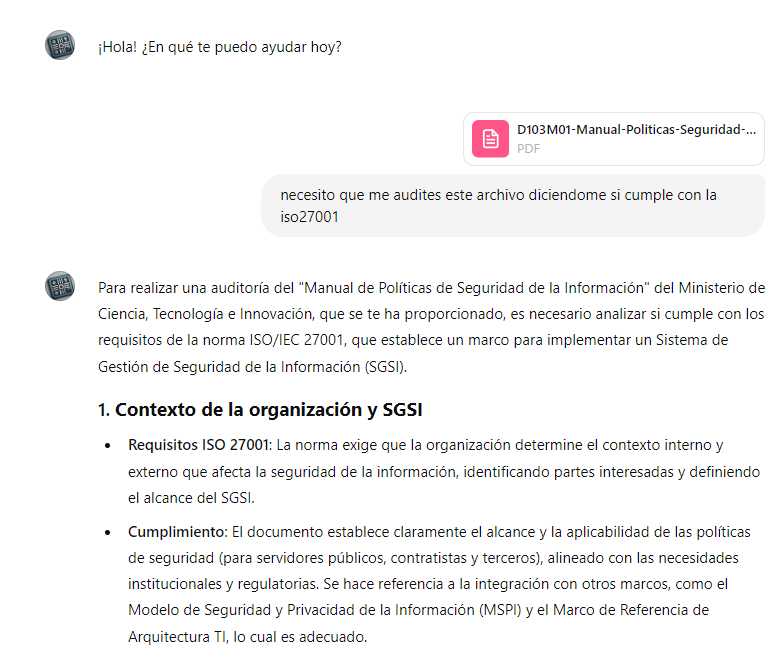
**Diagrama de caso de uso**

****

**Pruebas y resultados**

Se creo agente mediante la herramienta de ChatGPT.



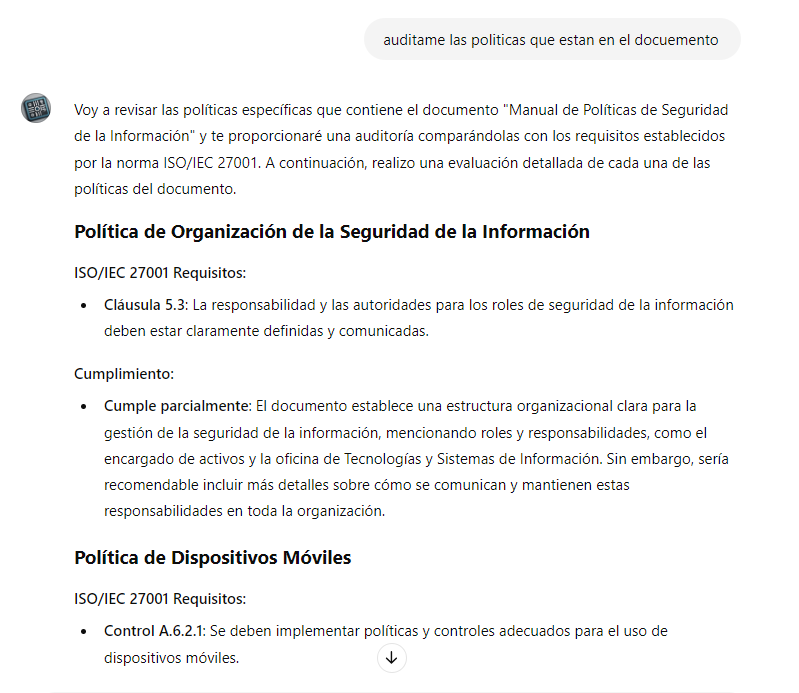


Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

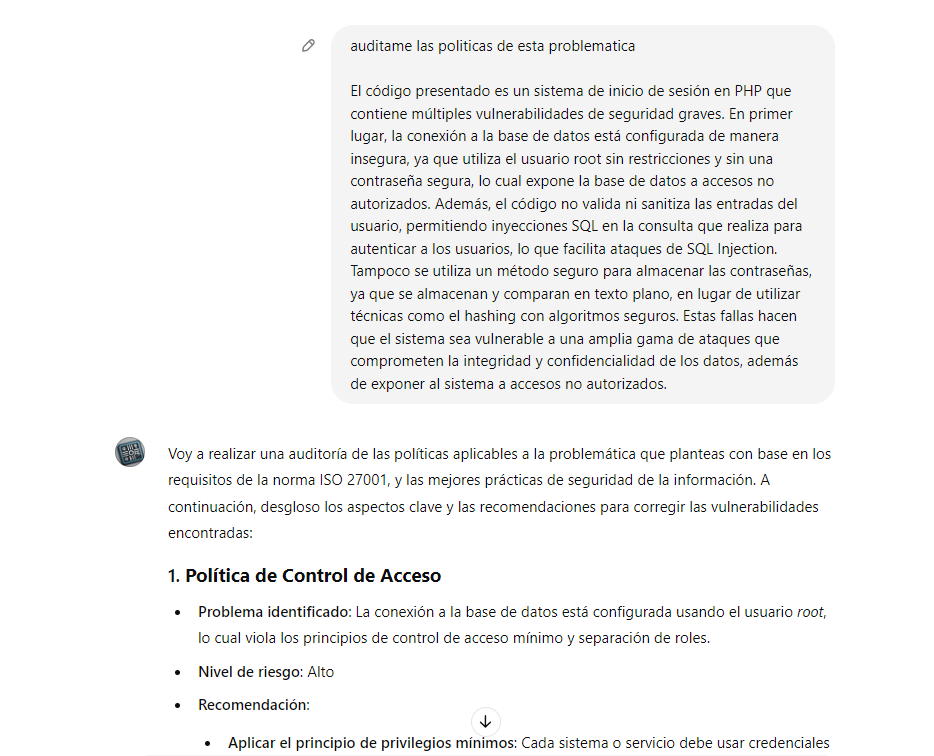
**Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente**



Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente



Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Referencias

 Calder, A., & Watkins, S. (2015). *ISO 27001/ISO 27002: A Pocket Guide*. IT Governance Ltd.

 Sommerville, I. (2016). *Software Engineering* (10th ed.). Pearson.

 Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.

 alder, A., & Watkins, S. (2015). *ISO 27001/ISO 27002: A Pocket Guide*. IT Governance Ltd.

 Ge, M., Zhang, X., & Zhao, C. (2017). Framework of automatic auditing system for ISO 27001 compliance using data mining and AI techniques. *Journal of Information Security, 8*(2), 125-139.

 Ma, X., Li, Y., & Wang, J. (2018). Risk assessment based on artificial intelligence in cybersecurity auditing. *International Journal of Computer Applications, 180*(14), 25-32.

 Sommerville, I. (2016). *Software Engineering* (10th ed.). Pearson.

 Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.