

Universidad Internacional de La Rioja

Escuela Superior de Ingeniería y Tecnología

Máster Universitario en Ingeniería de Software y Sistemas Informáticos

Desarrollo de una Plataforma de IA con control de datos sensibles para el sector empresarial: Aplicación en Open Finance

|  |  |
| --- | --- |
| Trabajo fin de estudio presentado por: | Jonathan Francisco Lema Collaguazo |
| Tipo de trabajo: | Desarrollo |
| Director/a: | David Segurado Moreno |
| Fecha: |  |

Resumen

Se completará en las siguientes etapas

Abstract

Se completará en las siguientes etapas

Índice de contenidos

[1. Introducción 1](#_Toc147741191)

[1.1. Justificación 1](#_Toc147741192)

[1.2. Planteamiento del problema 3](#_Toc147741193)

[1.3. Estructura del trabajo 3](#_Toc147741194)

[2. Contexto y estado del arte 4](#_Toc147741195)

[3. Objetivos concretos y metodología de trabajo 5](#_Toc147741196)

[3.1. Objetivo general 5](#_Toc147741197)

[3.2. Objetivos específicos 5](#_Toc147741198)

[3.3. Metodología del trabajo 6](#_Toc147741199)

[4. Desarrollo específico de la contribución 7](#_Toc147741200)

[4.1. Tipo 1. Desarrollo práctico 7](#_Toc147741201)

[4.1.1. Identificación de requisitos 7](#_Toc147741202)

[4.1.2. Descripción del sistema software desarrollado 8](#_Toc147741203)

[4.1.3. Evaluación 8](#_Toc147741204)

[4.2. Tipo 2. Planificación de un proyecto de desarrollo de software 8](#_Toc147741205)

[4.2.1. Identificación de requisitos 8](#_Toc147741206)

[4.2.2. Descripción de la planificación del proyecto de desarrollo de software 9](#_Toc147741207)

[4.3. Tipo 3. Desarrollo de metodología 9](#_Toc147741208)

[4.3.1. Identificación de requisitos 10](#_Toc147741209)

[4.3.2. Descripción de la metodología 10](#_Toc147741210)

[4.3.3. Evaluación 10](#_Toc147741211)

[5. Conclusiones y trabajo futuro 11](#_Toc147741212)

[5.1. Conclusiones 11](#_Toc147741213)

[5.2. Trabajo futuro 11](#_Toc147741214)

[Referencias bibliográficas 12](#_Toc147741215)

[Anexo A. Artículo 13](#_Toc147741216)

[Anexo B. Título anexo 17](#_Toc147741217)

Índice de figuras

**No se encuentran elementos de tabla de ilustraciones.**

Índice de tablas

No se encuentran elementos de tabla de ilustraciones.

# Introducción

Se realizará este apartado en la etapa final del proyecto

## Justificación

El uso de la IA Generativa ha venido creciendo de forma exponencial en el sector empresarial, al ofrecer herramientas capaces de automatizar tareas especializadas y reducir drásticamente las curvas de aprendizaje (OpenIA, 2022). Diversos informes apuntan a que esta tecnología permite mejorar la productividad y agilizar la generación de conocimiento, ya que los usuarios, incluso sin formación técnica, pueden beneficiarse rápidamente de las capacidades de los modelos de lenguaje (McKinsey & Company, 2023) .Sin embargo, este avance conlleva nuevos desafíos de seguridad y confidencialidad cuando se manejan datos sensibles, dado que muchos sistemas de IA actuales no incorporan mecanismos intrínsecos de filtrado o anonimización de la información (Dwork, 2008).

En este sentido, algunas empresas han optado por bloquear por completo el uso de estas herramientas, temiendo posibles fugas de información crítica o incumplimientos de normativas de protección de datos (European Union Agency for Cybersecurity [ENISA], 2021). No obstante, el mero acto de prohibir la IA Generativa puede suponer una barrera a la innovación, limitando la competitividad de la organización frente a otras que sí aprovechan las ventajas de estas tecnologías. Es por ello que la solución pasa por habilitar un entorno corporativo controlado, en el cual los modelos puedan ser utilizados con la garantía de que cualquier tipo de dato sensible sea detectado y anonimizado antes de exponerse, salvaguardando así la privacidad y cumpliendo con marcos regulatorios como el RGPD (Kairouz et al., 2020).

A la vez, se hace cada vez más evidente la necesidad de “entrenar” modelos con conocimiento experto de forma amigable para usuarios no técnicos (Lewis et al., 2020). En la actualidad, la popularidad de herramientas como ChatGPT demuestra que la IA Generativa puede democratizar la obtención de respuestas complejas, pero también expone la carencia de filtros adecuados y la falta de verificación de las fuentes. Así, surgió la segunda problemática que se pretende abordar: la importancia de contar con expertos que verifiquen y optimicen la información suministrada al modelo, asegurando exactitud y confiabilidad. De esta manera, se reduce el riesgo de adoptar ciegamente lo que “dice” la IA y se promueve un uso responsable y crítico en el entorno empresarial (Ren et al., 2022).

Por tanto, la presente investigación propone el desarrollo de una plataforma centrada en dos grandes pilares: (1) control de datos sensibles, mediante la anonimización o descarte de información crítica antes de su procesamiento por la IA, y (2) entrenamiento de modelos accesible para personal experto en la materia, aun sin conocimientos técnicos. Con esta aproximación, se abre una vía para que el sector empresarial adopte la IA Generativa de manera confiable, potenciando su competitividad sin poner en riesgo la seguridad de la información y fomentando, a la vez, el desarrollo de criterios críticos y mecanismos de validación en la adopción de estas nuevas tecnologías.

## Planteamiento del problema

El uso de la IA Generativa en entornos empresariales ha evidenciado la necesidad de contar con mecanismos que garanticen el tratamiento seguro de la información, en especial cuando se manejan datos sensibles. Muchas organizaciones, ante el riesgo de exposición de información confidencial, optan por limitar o prohibir su uso, lo que repercute negativamente en la competitividad y en la adopción de soluciones tecnológicas innovadoras.

La forma de solventar esta situación se basa en establecer mecanismos de control de la IA que, por un lado, detecte y anonimize la información crítica o sensible antes de que sea procesada por un modelo y, por otro, facilite la formación y el uso de dichas herramientas sin la necesidad de la prohibición.

La presente trabajo de investigación y desarrollo propone el diseño e implementación de una plataforma que cumpla con dos objetivos generales:

* Control de datos sensibles: implementar un sistema de anonimización o descarte que sirva como “firewall” de la información. Este mecanismo deberá funcionar de forma transparente para el usuario y permitirá a las empresas aprovechar la IA sin riesgos de fuga de datos.
* Entrenamiento de modelos accesible: habilitar un entorno que facilite el entrenamiento y la configuración de la IA por parte de expertos en diversos dominios, aun sin conocimientos técnicos. Esta herramienta debe ser intuitiva, guiando paso a paso el proceso de carga, filtrado y verificación de la información.

Esta plataforma brindaría a las organizaciones una vía intermedia entre la prohibición total y el uso descontrolado de la IA Generativa, permitiendo un aprovechamiento responsable de sus capacidades. Adicionalmente, la plataforma deberá contar con buenas prácticas que permita un correcto control y gestión de accesos para contar con la posibilidad de monitoreo y mejora continua.

## Estructura del trabajo

Este apartado se desarrollará al final

# Contexto y estado del arte

## Impacto de la IA generativa en el trabajo cotidiano

La adopción de la IA Generativa ha crecido de manera exponencial en los últimos años, impulsada por la proliferación de modelos de lenguaje capaces de producir texto coherente y contextual sin necesidad de una configuración compleja por parte del usuario (OpenIA, 2022). Herramientas como ChatGPT o Google Bard han logrado democratizar la inteligencia artificial, facilitando su implementación en diversos entornos y acelerando la adopción por parte de personas sin perfiles técnicos (McKinsey & Company, 2023).

Esta tendencia, lejos de revertirse, se presenta como un cambio de paradigma que obliga a las empresas a adaptarse para no quedar rezagadas. Diversos estudios señalan que la productividad y la eficiencia en la creación de contenido, la atención al cliente y la automatización de tareas rutinarias han mejorado significativamente con el uso de sistemas de IA Generativa (Kairouz, 2020). Sin embargo, la facilidad de acceso y el rápido ritmo de implantación superan a menudo la capacidad de las organizaciones para controlar la información que los usuarios introducen en estos servicios (Sfetcu, 2024).

Como consecuencia, se hace imprescindible un enfoque que combine la explotación de las ventajas competitivas de la IA Generativa con la protección de datos sensibles, especialmente cuando las plataformas se nutren de información crítica de la organización. En este sentido, sistemas de filtrado, anonimización y auditoría representan soluciones clave para salvaguardar la confidencialidad y cumplir con las regulaciones vigentes, sin obstaculizar el potencial de innovación ni el crecimiento empresarial. Bajo esta premisa, se justifica la necesidad de plantear propuestas centradas en salvaguardar los datos, al tiempo que se preserva la usabilidad y la efectividad de la IA para todos los perfiles involucrados.

## Regulación y protección de datos

La rápida adopción de la IA Generativa en entornos empresariales ha desencadenado numerosas preocupaciones vinculadas a la protección de datos, especialmente cuando los usuarios introducen información sensible en modelos externos o servicios en la nube. En la Unión Europea, el Reglamento General de Protección de Datos (RGPD) obliga a las organizaciones a implementar medidas que garanticen la confidencialidad, integridad y disponibilidad de la información personal que procesan, con sanciones económicas que pueden llegar hasta el 4% de la facturación global (Comisión Europea, 2016). De manera análoga, en Estados Unidos, la Ley de Privacidad del Consumidor de California (CCPA) y normativas sectoriales como HIPAA, en el ámbito sanitario, exigen salvaguardas para proteger los datos de los usuarios, así como la obligación de notificar brechas de seguridad.

Este escenario se complica por la falta de estandarización en el uso de herramientas de IA Generativa. Algunas empresas operan con plataformas externas cuyas políticas de tratamiento de datos pueden ser ambiguas, incrementando el riesgo de filtración de información confidencial y de incumplir las normas de privacidad (Sfetcu, 2024). Además, el desconocimiento de los empleados sobre la ubicación y forma de almacenamiento de la información que introducen en dichas herramientas agrava el problema (Kairouz, 2020).

En respuesta, han surgido propuestas que contemplan la anonimización o seudonimización de datos antes de su envío a la IA. Estas prácticas, contempladas en el propio RGPD bajo el principio de “privacidad desde el diseño”, permiten a las organizaciones minimizar la exposición de información crítica sin renunciar a los beneficios de la IA Generativa (Dwork, 2008). Sin embargo, la implementación de tales soluciones no siempre es sencilla, pues requiere de herramientas especializadas y del diseño de políticas internas que coordinen los procesos de negocio con el cumplimiento normativo. De ahí surge la necesidad de desarrollar plataformas que unifiquen la protección de datos, el control de acceso y la facilidad de uso, promoviendo una adopción responsable de la IA Generativa en el ámbito empresarial.

## tecnologías y metodologías asociadas a la ia generativa

En la actualidad, muchas de las tecnologías de IA Generativa que han alcanzado un uso masivo se caracterizan por interfaces amigables y accesibles vía web, orientadas a usuarios sin un perfil necesariamente técnico. Ejemplos notorios son ChatGPT, Google Bard y otras plataformas de diálogo con lenguaje natural basadas en grandes modelos de lenguaje (OpenIA, 2022). Su popularidad se fundamenta en la posibilidad de que un empleado de cualquier área pueda redactar consultas en lenguaje natural y obtener respuestas de alta calidad de manera inmediata (McKinsey & Company, 2023). Sin embargo, esta misma accesibilidad expone un punto crítico: el intercambio de datos confidenciales o sensibles sin que medie un proceso previo de filtrado o anonimización (Edemacu & Wu, 2024).

### Vulnerabilidades en el manejo de datos sensibles

Debido a la falta de conocimientos técnicos de gran parte de los usuarios, es frecuente que se compartan con la IA documentos o fragmentos de información que contengan, por ejemplo, nombres de clientes, cifras de facturación o detalles contractuales, sin tomar en cuenta los riesgos de privacidad o los posibles incumplimientos legales (ENISA, 2021). Como resultado, los proveedores externos de IA podrían almacenar e indexar dichos datos, dejando a la organización sin control sobre su destino o forma de utilización (Kairouz et al., 2020).

Además de ello, diversas plataformas de IA Generativa mantienen políticas de uso y manejo de datos que, si bien estipulan ciertos niveles de protección, no siempre se alinean con la normativa local o las políticas internas de la empresa. Esta disparidad incrementa la probabilidad de filtraciones y dificulta la trazabilidad de lo que ocurre con la información sensible tras su ingreso en el sistema (Dwork, 2008).

### Procesos de filtrado y anonimización en el ámbito empresarial

Para mitigar los riesgos mencionados, han surgido soluciones enfocadas en la detección y tratamiento de datos sensibles antes de su envío a la IA. Entre los mecanismos más empleados destacan:

* Identificación y extracción de PII (Personally Identifiable Information): A través de librerías como Spacy o Presidio, capaces de reconocer nombres, direcciones o números de identificación personal (Arvanitakis & Moustakides, 2020).
* Seudonimización y cifrado selectivo: En lugar de eliminar la información, se la sustituye por equivalentes o se la cifra de modo que su recuperación requiera claves de desencriptación (Ren et al., 2022).
* Enmascaramiento semántico: Consiste en reemplazar términos sensibles por tokens genéricos (por ejemplo, <CLIENTE\_X>), salvaguardando la coherencia del texto y evitando divulgar datos críticos.

No obstante, la mayoría de estas herramientas o metodologías suelen requerir intervención de personal especializado en NLP (Procesamiento de Lenguaje Natural) y ciberseguridad, generando barreras para equipos de negocio que buscan adoptar la IA Generativa de forma ágil. En la práctica, esto se traduce en procesos manuales o semi-automatizados que ralentizan la adopción de soluciones de IA y desincentivan su uso continuo (Nunes & Abreu, 2022).

### Prácticas y propuestas similares

Existen iniciativas denominadas “privacy firewalls” o “data preprocessors” cuyo objetivo es actuar como una capa intermedia entre el usuario y la plataforma de IA Generativa, analizando el contenido enviado y bloqueando o anonimizando la información sensible. Sin embargo, la mayoría de estos enfoques están centrados únicamente en la protección de datos y no contemplan la necesidad de un entorno en el que usuarios no técnicos puedan también entrenar y validar modelos con información de dominio específico (Lewis et al., 2020).

Ante este panorama, se identifica una oportunidad clara para soluciones integrales que reúnan, en una misma plataforma, la filtración y anonimización de información sensible y la facilidad de entrenamiento de modelos por parte de expertos de negocio. La propuesta que se desarrolla en esta investigación busca cubrir justamente este vacío, combinando controles de seguridad con una interfaz intuitiva que permita a los especialistas de área, sector o industria entrenar sus propios modelos y dejarlos disponibles para el uso interno de una empresa—en el caso de este trabajo será el ámbito de Open Finance—extender el conocimiento del modelo sin comprometer la confidencialidad de los datos.

## Caso de estudio y entrenamiento del modelo

Se ha elegido al Open Finance como caso de estudio para el entrenamiento del modelo, ya que el autor tiene un grado de expertise alta en ese campo de conocimiento y estará en capacidad de identificar conocimiento especializado para la fase de entrenamiento y criterio suficiente para entender que las respuestas a preguntas serán adecuadas.

### Contexto inicial sobre el tema especializado

Open Finance se deriva de la evolución de Open Banking y se centra en la interconexión y apertura de datos financieros a través de interfaces estandarizadas y seguras (Yang et al., 2022). Bajo esta premisa, múltiples entidades—bancos, fintech, aseguradoras, entre otros—comparten información financiera de forma controlada para ofrecer servicios y productos más personalizados. Sin embargo, esta apertura de datos también expone a las organizaciones a mayores riesgos de mala manipulación o uso indebido de la información cuando se introducen soluciones tecnológicas sin una adecuada supervisión (Arner, Barberis & Buckley, 2020).

### Equipos no técnicos y mala interpretación de la información

En regiones en proceso de regulación hace que se creen grupos de trabajo mixtos en los que tienen que abordar temas técnicos con el objetivo de aterrizar una normativa legal en un estándar técnico que permita la interoperabilidad de los participantes del ecosistema Open Finance. Ante esta problemática, las herramientas de IA Generativa han permitido que temáticas muy complejas se puedan abordar sin dependencia de expertos en ese campo, lo que ha permitido que el desarrollo y aterrizaje de estos estándares tengan una mayor velocidad. Por otro lado está el problema de que la IA Generativa no necesariamente llega a dar una respuestas válida y las personas que hacen uso de estas herramientas no tienen el criterio para validar o no las respuestas.

### Motivación y enfoque del casos de estudio

Dada la criticidad de la información manejada y la elevada responsabilidad legal de las instituciones financieras, Open Finance se presenta como un terreno idóneo para evaluar soluciones que combinen el uso de la IA Generativa con mecanismos de control. Por un lado, el sector financiero demanda alta precisión en los modelos para ofrecer recomendaciones y servicios confiables; por otro, exige estrictas garantías de seguridad y cumplimiento normativo (Arner et al., 2020). Esta dualidad resalta la pertinencia de contar con una plataforma y un perfil externo que pueda validar este proceso garantizando el cumplimiento objetivo de la plataforma.

# Objetivos concretos y metodología de trabajo

## Objetivo general

Diseñar y desarrollar una plataforma tecnológica que facilite a usuarios el acceso a módulos de IA Generativa que han sido previamente entrenados por expertos y en la que la información entregada sea adecuada para el uso en un entorno empresarial.

La plataforma adicionalmente tendrá un módulo en el que se podrá entrenar el modelo de forma amigable y sin necesidad de conocimientos técnicos de IA, sino de un conocimiento experto en el área de conocimiento con el objetivo de validar las informaciones recibidas. Este módulo deberá contar con una capa de filtrado o anonimización de datos de acuerdo a las leyes de protección de datos vigentes.

## Objetivos específicos

* Definir los requerimientos funcionales y no funcionales de la plataforma, de manera que esta permita a los usuarios acceder a módulos especializados para la generación de modelos entrenados para uso empresarial.
* Diseñar una arquitectura de alto nivel que contemple, al menos, las siguientes capacidades:
* Habilitación de módulos organizados por temáticas y con capacidad de habilitación y restricción por tipos de usuarios.
* Inclusión, dentro de cada módulo, de una interfaz interactiva que permita la captura estructurada de texto.
* Diseño y validación del modelo de IA basados en RACs dentro de plataformas que garanticen que no habrá uso de los datos para entrenamientos del modelo general

## Metodología del trabajo

La metodología empleada para el desarrollo del Trabajo de Fin de Máster (TFM) se basará en el marco ágil Scrum, complementado con elementos de Kanban para el seguimiento continuo del avance.

**Enfoque Ágil**

El desarrollo se estructurará en tres sprints, con una duración estimada de un mes cada uno, alineados con las entregas parciales requeridas por la Universidad Internacional de La Rioja (UNIR). Durante estos sprints se utilizarán los siguientes artefactos de Scrum:

* Product Backlog: conjunto priorizado de funcionalidades y requisitos a desarrollar.
* Sprint Backlog: subconjunto de tareas seleccionadas para cada sprint.
* Sprint Burndown: herramienta de seguimiento del progreso diario respecto a los objetivos del sprint.

Para la gestión visual de tareas e historias de usuario se integrará un tablero Kanban, permitiendo el monitoreo detallado del avance dentro del backlog de cada sprint.

**Ceremonias**

Las ceremonias establecidas para asegurar el cumplimiento de los objetivos del TFM son:

* Daily Meeting interno: revisión diaria del backlog y actualización del estado de las historias de usuario dentro del tablero Kanban, promoviendo la visibilidad y la identificación temprana de bloqueos.
* Retrospectiva mensual con el director del TFM: evaluación del incremento de valor entregado, análisis de impedimentos y recepción de retroalimentación general sobre el desarrollo del trabajo.

Adicionalmente, se invitará a una profesional del sector externo con experiencia en Finanzas Abiertas, quien asumirá el rol de cliente potencial. Esta persona participará en las sesiones de retrospectiva con el objetivo de validar las entregas, proporcionar retroalimentación sobre el diseño de la plataforma y asegurar la alineación con las necesidades del mercado.

**Enfoque hacia un MVP**

Como parte de la estrategia de desarrollo ágil, se priorizará la creación de un Producto Mínimo Viable (MVP) en el menor tiempo posible. Este MVP será una versión inicial funcional de la plataforma, susceptible de ser testada por usuarios reales, lo cual permitirá validar tempranamente los supuestos de diseño y orientar la evolución del producto hacia una versión potencialmente utilizable.

# Desarrollo específico de la contribución

En este apartado debes desarrollar la descripción de tu contribución. Es muy dependiente del tipo de trabajo concreto, y puedes contar con la ayuda de tu director para estudiar cómo comunicar los detalles de tu contribución. A continuación, te presentamos la estructura habitual para cada uno de los tipos de trabajo, aunque **suele ser común desarrollar los apartados en función de las fases o actividades que se hayan establecido en la metodología de trabajo**.

## Tipo 1. Desarrollo práctico

En este tipo de trabajo es importante justificar los criterios de diseño empleados para desarrollar el software, seguido de la descripción detallada del producto resultante y finalizando con una evaluación de la calidad y aplicabilidad del producto. Esto suele verse reflejado en la siguiente estructura de subapartados:

### Identificación de requisitos

En este apartado se debe indicar el trabajo previo realizado para guiar el desarrollo del software. Esto debería incluir la identificación adecuada del problema a tratar, así como del contexto habitual de uso (empresa, institución, etc.). Idealmente, la identificación de requisitos se debería hacer contando con expertos en la materia a tratar. Además, deberás describir en detalle las características del sistema. Como mínimo querrás mencionar:

* Qué tecnologías se utilizaron (incluyendo justificación de por qué se emplearon y descripciones detalladas de las mismas).
* Cómo se organizó el desarrollo.
* Qué personas participaron (con datos demográficos, si procede) o qué técnicas de sistemas se emplearon.
* Cómo transcurrió el desarrollo.
* Qué instrumentos de seguimiento y evaluación se utilizaron durante el proceso de desarrollo.

### Descripción del sistema software desarrollado

En el caso de un desarrollo práctico, deberían aportarse detalles del proceso de desarrollo, incluyendo las fases e hitos del proceso. También deben presentarse diagramas explicativos de la arquitectura o funcionamiento, así como capturas de pantalla que permitan al lector entender el funcionamiento del programa.

### Evaluación

La evaluación debería cubrir por lo menos una mínima evaluación de la usabilidad de la herramienta, así como de su aplicabilidad para resolver el problema propuesto. Estas evaluaciones suelen realizarse con usuarios expertos.

## Tipo 2. Planificación de un proyecto de desarrollo de software

Este tipo de trabajo es similar al tipo anterior, partiendo de la identificación detallada de requisitos y describiendo a fondo el modelo de proceso de desarrollo de software empleado, con la descripción completa de todas las actividades del proceso, pero sin desarrollar su implementación.

### Identificación de requisitos

En este apartado se debe indicar el trabajo previo realizado para guiar el desarrollo del programa. Esto debería incluir la identificación adecuada del problema a tratar, así como del contexto habitual de uso (empresa, institución, etc.). Idealmente, la identificación de requisitos se debería hacer contando con expertos en la materia a tratar. Además, deberás describir las características del proyecto de desarrollo de software. Como mínimo querrás mencionar:

* Qué tecnologías se utilizaron en el proceso de desarrollo (incluyendo justificación de por qué se emplearon y descripciones detalladas de las mismas).
* Cómo se organizó el proceso de desarrollo.
* Qué personas participaron (con datos demográficos, si procede) o qué técnicas de sistemas se emplearon.
* Cómo se planificó el proceso de desarrollo.
* Qué instrumentos de seguimiento y evaluación se utilizaron durante el proceso de desarrollo.

### Descripción de la planificación del proyecto de desarrollo de software

En el caso de una planificación de proyecto de desarrollo de software, deberían aportarse detalles del modelo de proceso de desarrollo, incluyendo las fases e hitos del proceso. También deben incluirse un estudio del dominio, un análisis y modelado de los requisitos del software y un modelado del diseño del software. Se recomienda el uso de diagramas explicativos de la arquitectura o funcionamiento. Al fin y al cabo, en el proyecto tiene que quedar definido todo lo que se va a realizar durante el ciclo de desarrollo del software. Por lo que es importante también describir cómo se va a implementar el software, cómo se va a testear y cómo se va a validar.

## Tipo 3. Desarrollo de metodología

La estructura de este tipo de trabajos es similar a la del primer tipo, partiendo de la identificación formal de los requisitos, describiendo a fondo la metodología y realizando una evaluación de su validez y aplicabilidad.

### Identificación de requisitos

En este apartado se debe indicar el trabajo previo realizado para identificar los roles, las tecnologías y los contenidos implicados para diseñar la metodología. Esto debería incluir la identificación adecuada del problema a tratar, así como del contexto habitual de uso (empresa, institución, etc.). Idealmente, la identificación de requisitos se debería hacer contando con expertos en la materia.

### Descripción de la metodología

En el apartado de descripción de la metodología se debería describir con todo detalle la metodología propuesta. El objetivo de una metodología es que se pueda aplicar en distintitos entornos, por lo que este apartado suele estructurarse como un manual detallado de cómo aplicar la metodología. Debería incluir descripciones detalladas de los roles implicados, de las tecnologías empleadas y de los elementos observables en cada una de las etapas. Puede ser útil acompañar las descripciones de diagramas de flujo o actividades que ayuden a comprender el proceso de aplicación de la metodología.

### Evaluación

La evaluación debería centrarse en validar la metodología propuesta y en asegurar su efectividad para abordar el problema tratado. Cuando sea posible, la mejor evaluación sería la implantación de la metodología en un escenario concreto y la observación de si esto supone una mejora en los resultados. Cuando esto no sea posible, la metodología debería ser, al menos, validada por usuarios expertos que estudien la propuesta y aporten su opinión mediante entrevistas estructuradas y/o cuestionarios.

# Conclusiones y trabajo futuro

## Conclusiones

Este último apartado es habitual en todos los tipos de trabajos y presenta el resumen final de tu trabajo y debe servir para informar del alcance y relevancia de tu aportación.

Suele estructurarse empezando con un resumen del problema tratado, de cómo se ha abordado y de por qué la solución sería válida.

Es recomendable que incluya también un resumen de las contribuciones del trabajo, en el que relaciones las contribuciones y los resultados obtenidos con los objetivos que habías planteado para el trabajo, discutiendo hasta qué punto has conseguido resolver los objetivos planteados. Las conclusiones ofrecidas deberán ser consecuencia del trabajo realizado y, por lo tanto, deberán marcar el grado de consecución de los objetivos propuestos (cada objetivo del trabajo se enlazará con una conclusión).

## Trabajo futuro

Finalmente, se suele dedicar un último apartado a hablar de líneas de trabajo futuro que podrían aportar valor añadido al trabajo realizado. La sección debería señalar las perspectivas de futuro que abre el trabajo desarrollado para el campo de estudio definido. En el fondo, debes justificar de qué modo puede emplearse la aportación que has desarrollado y en qué campos.

Referencias bibliográficas

# Bibliografía

Comisión Europea. (Mayo de 2016). *Reglamento (UE) 2016/679 del Parlamento Europeo.* Obtenido de https://ec.europa.eu/info/law/law-topic/data-protection\_en

Dwork, C. (2008). Differential Privacy: A Survey of Results. *International Conference on Theory and Applications of Models of Computation* (págs. 1-17). Lecture Notes in Computer Science .

Edemacu, K., & Wu, X. (2024). *Privacy Preserving Prompt Engineering: A Survey.* Arkansas.

Kairouz, P. (2020). *Advances and open problems in federated learning.* Foundations and Trends in Machine Learning.

McKinsey & Company. (2023). *The economic potential of generative AI: The next productivity frontier.*

OpenIA. (30 de Noviembre de 2022). *OpenIA*. Obtenido de https://openai.com/es-ES/index/chatgpt/

Sfetcu, N. (2024). Threats of Artificial Intelligence for Cybersecurity. *IT & C*, Volumen 3 - numeral 3.

1. Artículo

Como requisito adicional y obligatorio en el anexo A se deberá incluir un artículo de investigación que resuma el trabajo realizado y los principales resultados obtenidos. Debe incluir lo más importante de cada capítulo y no debe ser una copia literal de lo expuesto en la memoria.

Este artículo, que puede ser en español o en inglés, deberá seguir la plantilla proporcionada a continuación y tendrá una extensión de entre 6 y 8 páginas.

Título

Nombre y Apellidos del Estudiante

Universidad Internacional de la Rioja, Logroño (España)

Fecha

Palabras Clave

Tres a cinco palabras clave ordenadas alfabéticamente y separadas por comas.

Resumen

Breve resumen del trabajo realizado (extensión máxima: 150 palabras). Este resumen debe incluir el objetivo o propósito de la investigación, la metodología, los resultados y las conclusiones.

I. Introducción

I

intoducción en la que debes resumir de forma esquemática pero suficientemente clara lo esencial de cada una de las partes del trabajo.

La lectura de esta introducción ha de dar una primera idea clara de lo que se pretendía, las conclusiones a las que se ha llegado y del procedimiento seguido.

II. Estado del Arte

Estudio a fondo del dominio de aplicación, citando numerosas referencias.

Debe aportar un buen resumen del conocimiento que ya existe en el campo de los problemas habituales identificados.

Numerar las citas de forma consecutiva entre corchetes [1].

III. Objetivos y Metodología

Objetivo general, objetivos específicos y metodología de trabajo aplicada.

IV. Contribución

Desarrollar la descripción de tu contribución.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

V. Resultados

Descripción de los resultados obtenidos.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

*Resultados 1*

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.



Fig. 1. Magnetization as a function of applied field. Note that “Fig.” is abbreviated. There is a period after the figure number, followed by two spaces. It is good practice to explain the significance of the figure in the caption.

En la Figura 1…

En la Tabla I …

Tabla I

Units for Magnetic Properties

|  |  |  |
| --- | --- | --- |
| Symbol | Quantity | Conversion from Gaussian and CGS EMU to SI a |
| Φ | magnetic flux | 1 Mx → 10−8 Wb = 10−8 V·s |
| B | magnetic flux density,  magnetic induction | 1 G → 10−4 T = 10−4 Wb/m2 |
| H | magnetic field strength | 1 Oe → 103/(4π) A/m |
| m | magnetic moment | 1 erg/G = 1 emu  → 10−3 A·m2 = 10−3 J/T |
| M | magnetization | 1 erg/(G·cm3) = 1 emu/cm3  → 103 A/m |
| 4πM | magnetization | 1 G → 103/(4π) A/m |
| σ | specific magnetization | 1 erg/(G·g) = 1 emu/g → 1 A·m2/kg |
| j | magnetic dipole  moment | 1 erg/G = 1 emu  → 4π × 10−10 Wb·m |
| J | magnetic polarization | 1 erg/(G·cm3) = 1 emu/cm3  → 4π × 10−4 T |
| χ*,* κ | susceptibility | 1 → 4π |
| χρ | mass susceptibility | 1 cm3/g → 4π × 10−3 m3/kg |
| μ | permeability | 1 → 4π × 10−7 H/m  = 4π × 10−7 Wb/(A·m) |
| μr | relative permeability | μ → μr |
| w, W | energy density | 1 erg/cm3 → 10−1 J/m3 |
| N, D | demagnetizing factor | 1 → 1/(4π) |

Vertical lines are optional in tables. Statements that serve as captions for the entire table do not need footnote letters.

aGaussian units are the same as cgs emu for magnetostatics; Mx = maxwell, G = gauss, Oe = oersted; Wb = weber, V = volt, s = second, T = tesla, m = meter, A = ampere, J = joule, kg = kilogram, H = henry.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

*Resultados 2*

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

VI. Discusión

Tras la presentación objetiva de los resultados, querrás aportar una discusión de los mismos.

VII. Conclusiones

Resumen de las contribuciones del trabajo, en el que relaciones las contribuciones y los resultados obtenidos con los objetivos que habías planteado para el trabajo, discutiendo hasta qué punto has conseguido resolver los objetivos planteados.

Finalmente, hablar de líneas de trabajo futuro que podrían aportar valor añadido al TFM realizado. La sección debería señalar las perspectivas de futuro que abre el trabajo desarrollado para el campo de estudio definido. En el fondo, debes justificar de qué modo puede emplearse la aportación que has desarrollado y en qué campos.

Apéndices

Apéndices, en caso de ser necesario.

Referencias

1. Bermejo, J., Abad, C., Bermejo, J. R., Sicilia, M. A. & Sicilia, J. A. (2020). A Systematic Approach to Malware Analysis (SAMA). *Applied Sciences*, 10(4), 1360.
2. De Vicente, J., Bermejo, J., Bermejo, J. R. & Sicilia, J. A. (2019). The Application of a New Secure Software Development Life Cycle (S-SDLC) with Agile Methodologies. *Electronics*, 8(11), 1218.
3. Sicilia, J. A., Quemada, C., Royo, B. & Escuín, D. (2016). An optimization algorithm for solving the rich vehicle routing problem based on Variable Neighborhood Search and Tabu Search metaheuristics. Jo*urnal of Computational and Applied Mathematics*, 291, pp. 468-477.

1. Título anexo

El resto de los anexos debe de recoger todo aquello que puede ser interesante para el trabajo pero que no es estrictamente esencial, y que distraería la lectura si se colocara en el cuerpo: encuestas, resultados de pilotos, documentos adicionales, capturas de pantalla, código, etc. Pueden incluirse los anexos que se consideren necesarios. Estos no computarán a efectos de extensión del trabajo. Cada parte adicional se numera como un anexo y se ofrece en una página diferente.