

Universidad Internacional de La Rioja

Escuela Superior de Ingeniería y Tecnología

Máster Universitario en Ciberseguridad

Sistema de Autorizaciones de Tareas con Firma Electrónica – Open Sign

|  |  |
| --- | --- |
| Trabajo fin de estudio presentado por: | Edwin Mauricio Gonzalez Sierra |
| Tipo de trabajo: | TFM |
| Director/a: | Francisco Javier Álvarez Solís |
| Fecha: | 11/08/2024 |

Resumen

A la fecha de esta investigación, se han observado distintos casos de uso donde un sistema autorizador de tareas puede agilizar los procesos cotidianos en una empresa, algunas áreas donde se pueden implementar estos casos de uso pueden ser el área de ventas, recursos humanos, compras, legal, operaciones de TI, entre otros. El presente trabajo demostrara una solución a un problema común de los países latinoamericanos, el cual es garantizar la autenticidad, integridad y veracidad de los documentos digitales, por lo que la presente investigación demostrara por medio de un desarrollo de software una herramienta cuyo objetivo es firmar digitalmente estos documentos para garantizar que su integridad y agilizar procesos.

Las herramientas utilizadas son, el framework de Python, Django y Javascript. Mediante el desarrollo de esta herramienta se busca dar solución a la problemática anteriormente mencionada.

**Palabras clave:** Firmar Digitalmente, Django, veracidad, documentos digitales.

Abstract

To date of this research, different use cases have been observed where a task authorizing system can streamline daily processes in a company. Some areas where these use cases can be implemented may be the area of ​​sales, human resources, purchasing. , legal, IT operations, among others. The present work will demonstrate a solution to a common problem of Latin American countries, which is to guarantee the authenticity, integrity and veracity of digital documents, so this research will demonstrate, through software development, a tool whose objective is to sign digitally these documents to ensure their integrity and streamline processes.

The tools used are the Python framework, Django and Javascript. Through the development of this tool we seek to provide a solution to the aforementioned problem.

**Keywords:** Digital Signing, Django, veracity, digital documents.

Índice de contenidos

[1. Introducción 1](#_Toc150356204)

[1.1. Motivación 1](#_Toc150356205)

[1.2. Planteamiento del problema 2](#_Toc150356206)

[1.3. Estructura del trabajo 3](#_Toc150356207)

[2. Estado del arte 4](#_Toc150356208)

[3. Objetivos concretos y metodología de trabajo 5](#_Toc150356209)

[3.1. Objetivo general 5](#_Toc150356210)

[3.2. Objetivos específicos 5](#_Toc150356211)

[3.3. Metodología del trabajo 6](#_Toc150356212)

[4. Desarrollo específico de la contribución 7](#_Toc150356213)

[4.1. Tipo 1. Piloto experimental 7](#_Toc150356214)

[4.1.1. Descripción detallada del experimento 7](#_Toc150356215)

[4.1.2. Descripción de los resultados 8](#_Toc150356216)

[4.1.3. Discusión 8](#_Toc150356217)

[4.2. Tipo 2. Desarrollo de software 8](#_Toc150356218)

[4.2.1. Identificación de requisitos 8](#_Toc150356219)

[4.2.2. Descripción de la herramienta software desarrollada 8](#_Toc150356220)

[4.2.3. Evaluación 9](#_Toc150356221)

[4.3. Tipo 3. Desarrollo de metodología 9](#_Toc150356222)

[4.3.1. Identificación de requisitos 9](#_Toc150356223)

[4.3.2. Descripción de la metodología 9](#_Toc150356224)

[4.3.3. Evaluación 10](#_Toc150356225)

[5. Conclusiones y trabajo futuro 11](#_Toc150356226)

[Referencias bibliográficas 12](#_Toc150356227)

[Anexo A. 13](#_Toc150356228)

Índice de figuras

[Figura 1. *Ejemplo de figura realizada para nuestro trabajo.* 2](#_Toc150356229)

Índice de tablas

[Tabla 1. *Ejemplo de tabla con sus principales elementos.* 2](#_Toc150356230)

# Introducción

La presente investigación mostrara el proceso a un problema identificado, con relación a la comprobación de la autenticidad o veracidad de una aprobación de una tarea o documento mediante una firma electrónica. En las siguientes secciones se detallará lo siguiente:

* Sección 1.1: Detallara el problema de esta investigación, mostrando las principales debilidades de las herramientas actuales.
* Sección 1.2: Se plantearán los objetivos que se buscan alcanzar.
* Sección 1.3: Se describirá la estructura de los siguientes capítulos de la investigación.

## Motivación

Alguna vez, durante cursaba el presente Master de Ciberseguridad comprendí la importancia de poder firmar un documento digitalmente para certificar la veracidad del mismo, puesto que en mi país, Honduras, no existe representación de la Universidad Internacional de la Rioja – UNIR, al comienzo de mi master se me solicito el envió de mi título autenticado por un notario público, al enviarlo, de algún modo perdieron el documento firmado y sellado por el notario que certificaba la veracidad de mi título universitario, por lo que tuve que incurrir en los gastos nuevamente y volver a realizar el envió, además de los gastos, este proceso tomo alrededor de 2 meses.

Ante lo ocurrido, obtuve una idea, crear un sistema que genere confianza y me permita firmar documentos, entonces, comprendí que existen muchas aplicaciones en empresas y diferentes rubros, por ejemplo, cuando los bancos solicitan referencias bancarias, referencias laborales, se puede obtener un documento firmado digitalmente por la persona que dará fiabilidad a la referencia que se esta realizando. Actualmente existen varios servicios para firmar documentos como Adobe Acrobat, DocuSign, entre otros, sin embargo, no ofrecen una solución sin coste, por lo que la presente investigación buscara llenar ese vacío para generar confianza y seguridad a los usuarios.

## Planteamiento del problema

Durante la presente investigación, no se ha evidenciado la existencia de una herramienta que permita demostrar la veracidad de un documento o autorizar una tarea que esté al alcance de todas las personas puesto que todas las herramientas existentes son de paga. La finalidad de esta investigación es crear una herramienta que permita demostrar la autenticidad de un documento que se encuentre al alcance de todas las personas, cada persona puede crear un usuario y una firma en la herramienta y de este modo garantizar que la persona ha firmado el documento.

Tabla 1. *Comparativa de características de las herramientas y librerías.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Herramienta/ Librería** | **Algoritmos de Firma** | **Soporte de Certificados** | **Tipos de Archivos Soportados** | **Lenguajes / Plataforma** | **Licencia** |
| PyCryptodome | RSA, DSA, ECDSA, SHA256 | No tiene soporte nativo | Cualquier archivo binario | Python | BSD |
| OpenSSL | RSA, DSA, ECDSA | Sí | Cualquier archivo | Multiplataforma (C, CLI) | Apache 2.0 |
| Adobe Acrobat | RSA, SHA256 | Sí (PKI) | PDF | Windows, macOS | Propietaria |
| GnuPG (GPG) | RSA, DSA, ElGamal | Sí (PGP, OpenPGP) | Cualquier archivo | Multiplataforma | GPLv3 |
| DigiSigner | |  | | --- | | RSA, SHA256 |  |  | | --- | |  | | Sí | PDF | Multiplataforma (web) | Freemium |
| DocuSign | SHA256 | |  | | --- | | Sí (PKI) |  |  | | --- | |  | | PDF, DOCX, otros documentos | SaaS (web, API) | |  | | --- | |  |  |  | | --- | | Propietaria (SaaS) | |
| SignRequest | SHA256 | Sí | |  | | --- | | PDF, DOCX |  |  | | --- | |  | | |  | | --- | | SaaS (web, API) |  |  | | --- | |  | | Propietaria (SaaS) |
| HelloSign | RSA, SHA256 | Sí | PDF, DOC, otros documentos | SaaS (web, API) | Propietaria (SaaS) |
| SignTool (Microsoft) | RSA, SHA256 | Sí (PKI) | EXE, DLL, CAB | Windows (CLI) | Propietaria (Microsoft SDK) |
| BouncyCastle | RSA, DSA, ECDSA | Sí | Cualquier archivo binario | Java, C#, Android | MIT |

Fuente: Elaboración propia.

## Estructura del trabajo

En esta sección se explica de forma resumida cada uno de los capítulos que se presentaran en esta investigación. Se nombran las partes más relevantes de cada uno para obtener la idea central de que cada uno de ellos.

* Capitulo 2: Estado del arte o contexto de la investigación, se presentarán soluciones actuales al tema de investigación.
* Capitulo 3: Se describe el objetivo general y los objetivos específicos que se buscan cumplir.
* Capitulo 4: Desarrollo especifico de la herramienta que se ha investigado.

# Estado del arte

**Capítulo 1: Firma Electrónica y Firma Digital**

Comenzaremos esta investigación definiendo la diferencia entre firma digital y firma electrónica, para comenzar a establecer una diferencia entre ambas firmas, comenzaremos utilizando la definición ha establecido [1] Docusign para cada tipo de firma:

1. La firma electrónica se considera la manera más sencilla para autenticar un documento, puesto que usa la tecnología para completar una solicitud de consentimiento. Existen 2 tipos de firmas electrónicas:
   1. La firma electrónica simple: Se trata de una firma que pasa por una cuenta y clave para validarse, no cuenta con certificados para autenticar la identidad del firmante, es importante mencionar que la validez jurídica dependerá del país.
   2. La firma electrónica avanzada: Consiste en un conjunto de datos, adjuntos a un mensaje electrónico, que brinda la posibilidad de identificar al firmante y validar su legitimidad. A diferencia de la firma electrónica simple, utiliza certificados digitales auto adquiridos asignados a cada firmante. El diseño de esta firma cumple con estándares internacionales de infraestructura de claves públicas (PKI).
2. Firma Digital: Este tipo de firma viene siendo un tipo de firma electrónica avanzada que se distingue por utilizar un certificado digital como factor de autenticación. Este certificado es protegido por técnicas de criptografía.

En resumen, la firma electrónica simple es de naturaleza legal y contiene un marco normativo que le brinda validez jurídica. La firma digital también es legal, pero no tiene naturaleza jurídica en si misma. Su objetivo es encriptar la información para otorgarle mayor seguridad.

Hablando de seguridad, [2] Acronis nos dice en un artículo publicado el 2024 sobre mejores prácticas para firmas electrónicas, que las firmas electrónicas pueden estar expuestas a riesgos como la falsificación y suplantación de identidad, manipulación o robo de datos, si no se cuentan con medidas robustas de encriptación, doble factor de autenticación o uso de certificados digitales, además, de posibles riesgos legales si la firma no cumple con los requisitos mínimos definidos por la legislación.

**Capítulo 2: Regulaciones existentes para firmas electrónicas**

Existen regulaciones que varían según la región, estas regulaciones son:

1. **ESIGN Act (EEUU, Estados Unidos de América):** Las Firmas Electrónicas en el Mundo y La Ley Nacional de Comercio (ESIGN) se promulgó en los Estados Unidos en el año 2000. Eso reconoce las firmas electrónicas como legalmente válidas y exigibles para la mayoría de las transacciones, con algunas excepciones, como ciertas órdenes judiciales, testamentos vitales y documentos de poder notarial.
2. **UETA (EEUU, Estados Unidos de América):** Ley Uniforme de Transacciones Electrónicas (UETA) es una ley a nivel estatal en los Estados Unidos que ha sido adoptada por todos los EE. UU. estado, excluyendo Nueva York. Complementa la Ley ESIGN y proporciona un marco para las transacciones electrónicas.
3. **eIDAS (UE, Unión Europea):** La identificación electrónica y los servicios de confianza (eIDAS) es una regulación de toda la UE que entró en vigor en 2016. Como un marco legal para las firmas electrónicas, eIDAS garantiza el reconocimiento y la seguridad de la identificación y las firmas electrónicas.
4. **PEMRA (Canada):** En Canadá, la información personal La Ley de Protección y Documentos Electrónicos (PIPEDA) describe la legalidad de Firmas electrónicas. Es posible que se apliquen leyes provinciales además de lo que se señalados en la normativa nacional.
5. **PAA (Australia):** Ley de Transacciones Electrónicas de 1999 regula las firmas electrónicas en Australia, reconociendo su legalidad en la mayoría de los casos Transacciones.
6. **Indio Ley de Tecnología de la Información (India):** Ley de Tecnología de la Información de 2000, junto con sus modificaciones, proporcionan la base legal para las firmas y transacciones electrónicas en la India.
7. **ZertES (Suiza):** Ley Federal Suiza sobre la Las firmas (ZertES) son la ley primaria que rige las firmas electrónicas en Suiza, garantizando su validez jurídica.

**Capitulo 3: Normativas existentes para uso de firmas electrónicas**

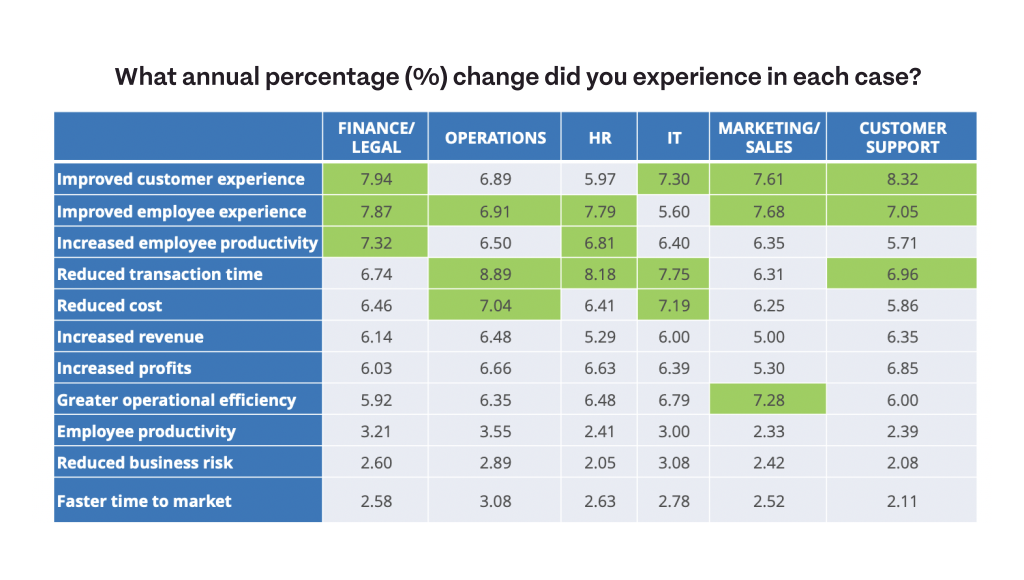
Cada una de estas normativas establece estándares de seguridad y buenas prácticas que las empresas que hacen uso de estas firmas deben cumplir, sin embargo, que sucede en los países donde su legislación no es tan avanzada y no contempla regulaciones para firmas electrónicas. Para estos casos, existen estándares de seguridad que se pueden seguir, a continuación, se presentan:

1. **Public-key infraestructura (PKI):** PKI proporciona un marco para Firmas electrónicas seguras. Emplea certificados digitales, criptográficos claves y autoridades de certificación para autenticar al firmante y proteger integridad de los documentos.
2. **Advanced encryption standars (AES):** AES se utiliza ampliamente para cifrar los datos de firma electrónica, asegurándose de que permanezcan confidenciales tanto cuando estén en tránsito y cuando está en reposo.
3. **Transport layer secuirty:** TLS establece conexiones para evitar escuchas y manipulaciones. Este protocolo puede ayudar Evite que los documentos firmados electrónicamente sean interceptados o manipulados.
4. **X.509 Standard:** X.509 es un estándar ampliamente aceptado para certificados digitales, que desempeñan un papel clave en las firmas electrónicas basadas en PKI.
5. **ISO 27001:** ISO 27001 es una norma internacional para sistemas de gestión de la seguridad de la información (SGSI) que se aplica ampliamente a todos los aspectos de ciberseguridad y protección de datos. Organizaciones que implementan firmas electrónicas a menudo se adhieren a la norma ISO 27001 para garantizar prácticas de seguridad sólidas.
6. **eIDAS Regulation:** En la Unión Europea, el eIDAS (Identificación Electrónica y Servicios de Confianza) establece normas para firmas electrónicas, definiendo varios niveles de seguridad de firma electrónica.
7. **NIST Guidelines:** El Instituto Nacional de Normalización y (NIST) proporciona pautas y estándares para firmas electrónicas seguras en los Estados Unidos.
8. **HIPAA and GDPR Compliance:** Para las firmas electrónicas utilizadas en asistencia sanitaria o que implique datos personales, el cumplimiento del Seguro de Salud Ley de Portabilidad y Responsabilidad (HIPAA) en los EE. UU. y los datos generales, El Reglamento de Protección (RGPD) en la UE es obligatorio.

**Capitulo 4: tendencias sobre el uso de firma electrónica por sector económico.**

Durante la presente investigación, se identificaron los sectores que incrementaron el uso de la firma electrónica durante el 2021, esto marca una clara tendencia en aumento sobre su uso sobre todo en áreas de atención al cliente, bancos, ventas, entre otros, la firma electrónica marca un avance en la agilización de los procesos.

Tabla 2. *Tendencias de uso de firma electrónica en mercados económicos.*



Fuente: IDC'sNorth America eSignature Market Survey, November 2021

Además, en la Tabla 3, se detallan en un proceso macro las medidas de seguridad y autenticación para firmas electrónicas donde se especifican normativas, medidas de autenticación y medidas tecnológicas, que se han venido detallando durante la investigación.

Tabla 3. *Medidas de seguridad y autenticación para firmas electrónicas.*



Fuente: elaboración Signeasy, 2023.

**Capitulo 5: Conclusiones**

En conclusión, existen muchas herramientas que permiten hacer uso de una firma electrónica en sus diferentes aplicaciones, también existen muchos estándares o regulaciones que permiten aplicar buenas prácticas para regular su uso y garantizar la seguridad de la misma, durante la presente investigación utilizaremos el marco de referencia ISO 27000, un marco de referencia y aceptado, además de ser muy utilizado en Latinoamérica, para el desarrollo de la herramienta Open-Sign, que buscara dar solución a los problemas de autorización de tareas con firmas electrónicas y comprobar la veracidad de un documento firmado por la herramienta.

# Objetivos concretos y metodología de trabajo

Este bloque es el puente entre el estudio del dominio y la contribución a realizar. Según el tipo concreto de trabajo, el bloque se puede organizar de distintas formas, pero los siguientes elementos deberían estar presentes con mayor o menor detalle.

## Objetivo general

Implementar una herramienta que permita certificar la veracidad de una autorización de una tarea o documento, mediante la implementación de una firma electrónica que esté al alcance de los usuarios.

## Objetivos específicos

### Realizar una investigación de los productos y servicios que ofrecen las herramientas vigentes que ofrecen el servicio de una firma electrónica.

### Analizar y realizar un levantamiento de requerimientos para desarrollar la herramienta que permita firmar tareas.

### Implementar y desarrollar la herramienta que permita utilizar una firma digital para autorizar tareas.

## Metodología del trabajo

Para alcanzar los objetivos definidos para la presente investigación se utilizará una metodología de trabajo en las siguientes fases:

1. Fase 1: Levantamiento de requerimientos para desarrollar la aplicación, definiendo los mokcups para definir módulos a desarrollar en herramienta web.
2. Fase 2: Implementar herramientas y desarrollo de requerimientos definidos en la fase 1.
3. Fase 3: Testeo de herramienta para comprobar que funcione según requerimientos de la fase 1.
4. Fase 4: Implementación de la herramienta.

# Desarrollo específico de la contribución

En este bloque (1-3 capítulos) 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.

## Tipo 1. Piloto experimental

Este tipo de trabajos suelen seguir la estructura típica al describir experimentos científicos, dividida en descripción del experimento, presentación de los resultados y discusión de los resultados. En general se espera una separación clara entre los tres elementos: descripción de los métodos de investigación, presentación de los resultados y discusión de los resultados.

### Descripción detallada del experimento

En el capítulo de Objetivos y Metodología del Trabajo ya habrás descrito a grandes rasgos la metodología experimental que vas a seguir. Pero si tu trabajo se centra en describir un piloto, deberás dedicar un capítulo a describir con todo detalle las características del piloto. 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 piloto.
* Qué personas participaron (con datos demográficos, si procede) o qué técnicas de sistemas se emplearon.
* Cómo transcurrió el experimento.
* Qué instrumentos de seguimiento y evaluación se utilizaron durante el desarrollo del experimento.
* Qué tipo de análisis estadísticos se empleó (si procede).

### Descripción de los resultados

En el siguiente capítulo deberás detallar los resultados obtenidos, con tablas de resumen, gráficas de resultados, identificación de datos relevantes, etc. Es una exposición objetiva, sin valorar los resultados ni justificarlos. Deberías describir los resultados y aportar tablas que resuman las principales observaciones.

### Discusión

Tras la presentación objetiva de los resultados, querrás aportar una discusión de los mismos. En este capítulo puedes discutir la relevancia de los resultados, presentar posibles explicaciones para los datos anómalos y resaltar aquellos datos que sean particularmente relevantes para el análisis del experimento.

## Tipo 2. Desarrollo de software

En un trabajo de desarrollo de software es importante justificar los criterios de diseño seguidos para desarrollar el programa, seguido de la descripción detallada del producto resultante y finalmente una evaluación de la calidad y aplicabilidad del producto. Esto suele verse reflejado en la siguiente estructura de capítulos:

### Identificación de requisitos

En este capítulo 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.

### Descripción de la herramienta software desarrollada

En el caso de desarrollos de software, 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 3. Desarrollo de metodología

La estructura de este tipo de trabajos es similar a la del tipo anterior, 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 capítulo 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 capítulo 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 capítulo 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 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

Este último bloque (habitualmente un capítulo; en ocasiones, dos capítulos complementarios) 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.

Finalmente, se suele dedicar una última sección a hablar de **líneas de trabajo futuro** que podrían aportar valor añadido al TFE 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

Una vez que el trabajo está terminado, hay que revisar el apartado “Referencias bibliográficas”. Si has usado un sistema automático (un gestor bibliográfico tipo Endnote, Refworks o Mendeley), inserta la bibliografía en la opción adecuada (APA).

Si lo has ido haciendo manualmente, repasa que todo es correcto: aparecen todas las referencias citadas en el texto, los autores están ordenados alfabéticamente por apellidos, las cursivas son correctas, los artículos tienen números de páginas, no faltan años ni ciudades de edición, se cumple en todas las referencias la normativa APA, etc.

Se recomienda evitar citas que hagan referencia a Wikipedia y que no todas las referencias sean solo enlaces de internet, es decir, que se vea alguna variabilidad entre libros, congresos, artículos y enlaces puntuales de internet.

Ejemplos:

1. Docusign, diferencia entre firma electronica y firma digital (2022).

https://www.docusign.com/es-mx/blog/diferencia-de-firma-electronica-y-firma-digital

1. Acronis, mejores practicas en firma electronica. (2024)

https://www.acronis.com/en-us/blog/posts/best-practices-for-e-signature/

1. Signeasy, Seguridad de la Firma Electrónica: ¿Que tan segura es su firma electrónica?

https://signeasy.com/blog/business/esignatures-security-and-authentication



En los anexos se recoge 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: el cuestionario utilizado, el desarrollo de las actividades de la propuesta, la legislación sobre el tema, 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.