

# Sistema de Autorizaciones de Tareas con Firma Electrónica – Open Sign Trabajo fin

Edwin Mauricio Gonzalez Sierra

# ÍNDICE

- 01 – Contexto
- 02 – Objetivos
- 03 – Desarrollo
- 04 - Resultado

## Firma Digital y Electrónica

**1. Firma Electrónica:** La firma electrónica es una de las formas más accesibles para autenticar un documento, ya que emplea tecnología para obtener el consentimiento. Se reconocen dos tipos principales de firmas electrónicas:

- a. La firma electrónica simple: Este tipo de firma se valida mediante el uso de una cuenta y contraseña, sin necesidad de certificados que autentiquen la identidad del firmante. Su validez legal puede variar según el país.
- b. La firma electrónica avanzada: Compuesta por un conjunto de datos adjuntos a un mensaje electrónico, permite identificar al firmante y verificar su autenticidad. A diferencia de la firma electrónica simple, utiliza certificados digitales adquiridos por cada firmante, cumpliendo con los estándares internacionales de infraestructura de claves públicas (PKI).

**2. Firma Digital:** Es una modalidad de firma electrónica avanzada que se caracteriza por utilizar un certificado digital como método de autenticación, protegido mediante técnicas criptográficas.

# Objetivos

## Objetivo General:

Desarrollar 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:

1. Realizar una investigación de los productos y herramientas vigentes que ofrecen el servicio de una firma electrónica.
2. Analizar y realizar un levantamiento de requerimientos para desarrollar la herramienta que permita firmar tareas.
3. Desarrollar la herramienta que permita utilizar una firma electrónica para autorizar tareas.

# Investigación

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

# Desarrollo de la Herramienta

## Tecnologías

### Herramientas de desarrollo:

1. **Visual Studio Code:** editor de código fuente ligero pero potente desarrollado por Microsoft. Editor utilizado para desarrollo del proyecto.
2. **Github:** Plataforma de desarrollo colaborativo para resguardo de versiones de proyectos de desarrollo de software utilizando el sistema de control de versiones Git. Herramienta utilizada para alojar y llevar un control de versiones del proyecto.

### Librerías:

1. **PyCryptodome:** es una biblioteca de criptografía de bajo nivel para Python. Librería utilizada para generar llaves públicas y privadas.
2. **Bootstrap:** es un popular framework de desarrollo front-end de código abierto. Marco de referencia utilizada para crear una interfaz amigable para el usuario.
3. **Django:** framework web escrito en Python que permite a los desarrolladores crear aplicaciones web robustas y seguras con facilidad. Marco de referencia utilizado para desarrollo del proyecto.

### Lenguajes de Programación:

1. **Python:** lenguaje de programación interpretado y ampliamente utilizado para desarrollo de scripts por su gran cantidad de librerías. Lenguaje utilizado para desarrollo de la herramienta.
2. **Javascript:** es un lenguaje de programación de alto nivel que se utiliza ampliamente para el desarrollo web. Lenguaje utilizado para desarrollo de frontend.

# Resultado Final

The screenshot shows the OpenSign application's main interface. At the top, there is a header bar with the title "Open Sign" and links for "Roles y Perfil", "Inicio", and "Cerrar sesión". Below the header is a navigation bar with links for "Firmar Documento", "Documentos Firmados", "Comprobar Documento", "Crear Tareas", and "Tareas". The main content area features a large heading "Bienvenido a OpenSign" and a greeting message "¡Hola, edwing9300@gmail.com!".

This screenshot displays the "Verificar Documento Firmado" (Verify Signed Document) page. It includes a "Volver" (Back) button, a "Seleccionar Documento" (Select Document) section with a "Elegir archivo" (Select file) button and a message stating "No se eligió ningún archivo" (No file was selected), and a prominent blue "Verificar" (Verify) button. Below these, a "Detalles del Documento" (Document Details) section provides information about the signed document, including its name ("Nombre del Archivo: Recibo TGR-13571677.pdf"), signer ("Firmante: edwing9300@gmail.com"), and signing date and time ("Fecha de Firma: 12 de diciembre de 2024 a las 21:03").

This screenshot shows the "Documentos Firmados" (Signed Documents) page. It lists two signed documents: "Open-Sign.docx" (signed on 27 de noviembre de 2024 a las 14:13) and "Recibo TGR-13571677.pdf" (signed on 12 de diciembre de 2024 a las 21:03). Each document entry includes a "Descargar" (Download) button.

Nombre del Documento	Fecha de Firma	Descargar
Open-Sign.docx	27 de noviembre de 2024 a las 14:13	Descargar
Recibo TGR-13571677.pdf	12 de diciembre de 2024 a las 21:03	Descargar

# Conclusiones

**1. Objetivo:** Realizar una investigación de los productos y herramientas vigentes que ofrecen el servicio de una firma electrónica.

**Conclusión:** se investigó los productos y herramientas vigentes a la fecha de la presente investigación que ofrecen el servicio de firma electrónica, concluyendo que existe todo tipo de ámbito de aplicación para utilizar firmas electrónicas y así mismo existen herramientas que brindan distintas soluciones dependiendo de las necesidades de los usuarios, sin embargo, estos servicios no se encuentran al alcance de todos los usuarios.

**1. Objetivo:** Analizar y realizar un levantamiento de requerimientos para desarrollar la herramienta que permita firmar tareas.

**Conclusión:** Se realizo un levantamiento de requerimientos para desarrollar la herramienta Open Sign, permitiendo la escalabilidad de la herramienta en un futuro, aplicando mejores prácticas de desarrollo e implementando un S-SDLC para su desarrollo.

**1. Objetivo:** Desarrollar la herramienta que permita utilizar una firma electrónica para autorizar tareas.

**Conclusión:** Se desarrollo la herramienta Open Sign, permitiendo crear un módulo de autenticación integrando llaves privadas y públicas para los usuarios, registro de usuarios, asignación de roles y perfiles, firmar documentos con diferentes formatos de ofimática, por ejemplo. word, .xlsx, .ppt, .pdf, entre otros, crear tareas y asignarlas a los usuarios registrados, permitir autorizar o denegar las tareas por los usuarios administradores y descargar las tareas firmadas.

**Conclusión Final:** La herramienta desarrollada en Python utilizando librerías de código abierto como Django y Crypto. Open Sign, permite agilizar procesos mediante el uso de la firma electrónica permitiendo firmar documentos para confirmar la identidad de un usuario o creando y aprobando tareas utilizando firma electrónica. A continuación, se detallarán una serie de ventajas y desventajas de la herramienta:

**muchas gracias**