

Table of Contents

Descripción de la Aplicación	2
------------------------------	---

Descripción de la Aplicación

La aplicación Tibisay Móvil ofrece funcionalidades de firma electrónica y verificación de firma en dispositivos móviles como teléfonos inteligentes y tabletas. La arquitectura inicial propuesta para la aplicación se muestra en la figura 1.

Figura 1. Arquitectura propuesta para la aplicación Tibisay Móvil

Se proponen tres (03) módulos en la arquitectura: Módulo de Gestión de Documentos, Módulo de Gestión Criptográfica y un Módulo de Gestión de Claves y Certificados.

- **Módulo de Gestión de Documentos:** se encarga de gestionar todas las operaciones relacionadas con un objeto documento, en distintos formatos, dentro de la aplicación. Se incluyen aquí operaciones para seleccionar, abrir y eliminar documentos. Estos documentos además pueden ser compartidos con otras aplicaciones para su difusión y distribución.
- **Módulo de Gestión Criptográfica:** se encarga de gestionar todas las operaciones criptográficas relacionadas con la firma electrónica y la verificación de documentos firmados electrónicamente en distintos formatos.
- **Módulo de Gestión de Claves y Certificados Electrónicos:** se encarga de gestionar los objetos claves privadas y certificados electrónicos en un entorno seguro dentro del dispositivo móvil. El módulo gestiona un repositorio protegido para almacenar las claves que los usuarios utilizan para firmar electrónicamente los documentos.

Tibisay Móvil permitirá que un usuario seleccione un documento de algún formato para firmarlo electrónicamente o para verificar su firma en caso de estar firmado. Los formatos de firma aceptados serán: PDF, PKCS#7 y BDOC. Los documentos PDF podrán incluir una imagen de la firma manuscrita del usuario capturada a través de la pantalla del dispositivo móvil, que se insertará al momento de firmarlo electrónicamente con un certificado electrónico.

Los certificados electrónicos y sus correspondientes claves privadas serán almacenados en un repositorio seguro para claves dentro del dispositivo. Las claves se importarán a través del formato PKCS#12 de transporte de claves y certificados electrónicos. Un usuario podrá tener asociado más de un certificado electrónico con el cual firmar electrónicamente un documento.

Los documentos gestionados por la aplicación se podrán compartir con otras aplicaciones para su distribución.

Para el desarrollo del proyecto se utilizan herramientas libres y estándares reconocidos y aplicables a las tecnologías con las que se trabaja. Asimismo se siguen los lineamientos establecidos en la [Gestión de Procesos de Software Libre](#) propuesta por la fundación CENDITEL.