Sistema de firmado digital

Ernesto Borbón

Gerardo Villegas

Felipe Villaseñor

José de Jesús Gutiérrez

Andrea Velázquez

Rodrigo Morales

Isabel Moreno

Pablo Ochoa

¿Qué puede hacer el sistema?

Dota a sus usuarios de un certificado que los autentifica, y les deja renovarlo.

Favorece la rápida firma y verificación de documentos.

Permite que un documento sea firmado por varias personas, y soporta su verificación.

Además de los usuarios regulares, cuenta con usuarios tipo administrador para realizar acciones que requieren de más control.

¿Qué puede hacer un usuario?

- Iniciar sesión
- Crear su cuenta
- Cambiar su contraseña
- Firmar uno o más documentos
- Unificar firmas
- Verificar la(s) firma(s)

¿Qué puede hacer un admin?

El admin además de tener las mismas facultades de un usuario, tiene algunas funcionalidades adicionales:

Dar de alta administradores: crea un usuario de tipo administrador, con su propio certificado.

Cambiar contraseñas: El admin puede cambiar cambiar las contraseñas de usuarios, si al usuario se le llega a olvidar.

Borrar usuarios: El admin tiene la capacidad de eliminar usuarios, invalidado las firmas del usuario después de la eliminación.

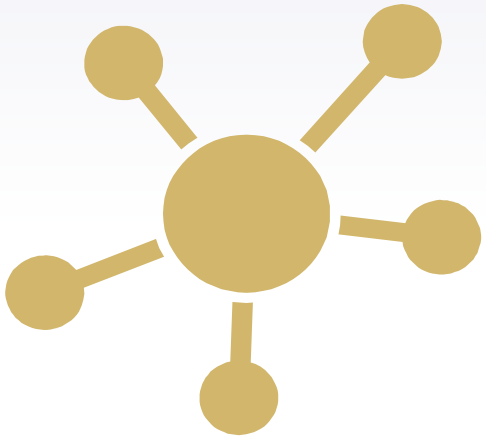
¿Dónde se almacena la información?

Claves públicas

Se encuentran en una base de datos instancia de **PostreSQL**, junto con más información relevante de los usuarios.

Los certificados

Al generar un certificado, la clave privada encriptada se sube a un contenedor de **Azure** storage.



¿Por qué el sistema es seguro?

La fortaleza del mecanismo:

El algoritmo de firmado utilizado es el ED25519. Este utiliza el algoritmo de firmado digital de la curva de Edward (EdDSA).

Romper una firma EdDSA bien construida podría llevar alrededor de 4 millones de años o requerir una computadora cuántica

¿Por qué el sistema es seguro?

Autenticidad

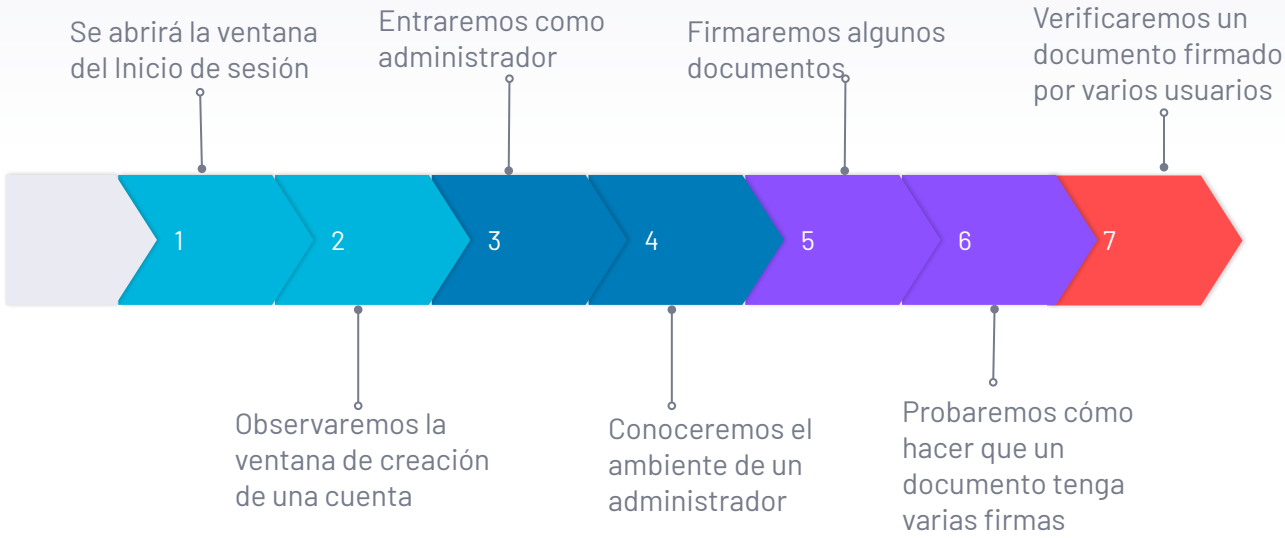
Hay **garantía** de saber quién realiza las acciones.

Integridad

Al basarse en hashes*, si existiera una modificación en el documento, la **verificación** fracasaría.

*Hash: un identificador en función de los datos que consiste en una serie de caracteres.

¿Qué veremos?


Se abrirá la ventana del Inicio de sesión
Entraremos como administrador
Firmaremos algunos documentos
Verificaremos un documento firmado por varios usuarios
1
2
3
4
5
6
7
Observaremos la ventana de creación de una cuenta
Conoceremos el ambiente de un administrador
Probaremos cómo hacer que un documento tenga varias firmas

DEMO

A continuación se presentará la versión demo de la aplicación

¡Gracias!