

4 de enero

2024

**CAPACITACIÓN
TÉCNICA DEL "SISTEMA
DE GESTIÓN DE FIRMAS
ELECTRÓNICAS
AVANZADAS"**

ELABORADO POR ING. GRACIELA EUNICE
ILLESCAS ACOSTA



CONTENIDO

| | |
|--|-----------|
| RESUMEN | 3 |
| ARQUITECTURA | 4 |
| COMPONENTES DESARROLLADOS | 6 |
| ARQUITECTURA DE LA BASE DE DATOS | 7 |
| ESPECIFICACIONES DE LA BASE DE DATOS | 7 |
| LÓGICA DEL SISTEMA | 9 |
| MÓDULOS..... | 13 |
| CÓDIGO FUENTE | 21 |
| ESTRUCTURA DE PROYECTOS JAVA SPRING BOOT | 21 |
| ESTRUCTURA DE PROYECTO LARAVEL | 24 |
| REPOSITORIOS | 25 |
| BASE DE DATOS..... | 26 |
| INSTALACIÓN Y DESPLIEGUE | 27 |
| DOCUMENTOS COMPLEMENTARIOS | 30 |

TABLA DE FIGURAS

| | |
|--|-----------|
| <i>Figura 1. Arquitectura del sistema</i> | <i>5</i> |
| <i>Figura 2. Funcionamiento seguridad</i> | <i>10</i> |
| <i>Figura 3. Funcionamiento firma electrónica</i> | <i>12</i> |
| <i>Figura 4. Login</i> | <i>14</i> |
| <i>Figura 8. Nuevo documento p.1</i> | <i>17</i> |
| <i>Figura 9. Nuevo documento p.2</i> | <i>18</i> |
| <i>Figura 10. Catálogos</i> | <i>19</i> |
| <i>Figura 13. API-Seguridad</i> | <i>22</i> |
| <i>Figura 14. API Firma-PKI</i> | <i>23</i> |
| <i>Figura 15. API Gestión</i> | <i>25</i> |
| <i>Figura 16. Configuración de producción para Seguridad</i> | <i>28</i> |
| <i>Figura 17. Configuración de producción para Firma PKI</i> | <i>29</i> |
| <i>Figura 18. Configuración de producción Frontend</i> | <i>29</i> |
| <i>Figura 19. Configuración producción Gestión</i> | <i>30</i> |

Resumen

Este documento sirve como material de referencia para la capacitación técnica dirigida al personal de la Unidad de Servicios Informáticos del TECDMX, enfocándose en explicar la arquitectura, lógica y organización del código fuente que constituye el Sistema de Gestión de Firmas Electrónicas.

La sección de Arquitectura proporciona una visión del diseño estructural del sistema, delineando cómo los componentes se ensamblan para formar la infraestructura. En la Lógica del Sistema, se mencionan procesos y flujos de trabajo que definen el funcionamiento del sistema, así como la importancia de cada elemento en sus operaciones.

En los Módulos, se examina la contribución de cada uno, poniendo énfasis en su función. La sección de Código Fuente se centra en las prácticas de desarrollo adoptadas y la estructura de los repositorios que facilitan la colaboración y el mantenimiento continuo. En cuanto a los Repositorios, se describe su gestión y cómo se emplean para controlar las versiones y el historial de cambios del código.

La parte de la Base de Datos muestra el diseño, las relaciones entre tablas y cómo se garantiza la coherencia y seguridad de los datos.

La Instalación y Despliegue contiene información guía para la puesta en marcha del sistema, asegurando que el personal pueda replicar y manejar el entorno operativo con confianza.

Por último, los Documentos Complementarios suministran recursos adicionales que profundizan en la comprensión del material cubierto, brindando manuales y guías de referencia esenciales.

En resumen, se presenta este documento como material de capacitación el cual contiene un listado de los elementos contenidos en el sistema y se proporcionan los

entregables acordados en el mismo con base en el contrato del servicio TECDMX/SA/JDA/051/2023.

Arquitectura

La arquitectura de un sistema es el marco que define la estructura y el comportamiento de los programas y plataformas que utilizamos. En esta sección, se describe la disposición y la interconexión de los componentes que forman la base del sistema.

El desarrollo del diseño de arquitectura del Sistema de Firma Electrónica se realizó buscando cumplir con los siguientes objetivos:

- **Escalabilidad:** El sistema puede volverse más robusto y expandirse sin perder calidad ni comprometer el funcionamiento.
- **Portabilidad:** Le permite a la aplicación ejecutarse en diferentes plataformas operativas.
- **Reutilización:** Se parte del criterio de reutilizar funcionalidades, módulos y operadores de software ya existente.
- **Desarrollo ágil:** Permite que el ciclo de desarrollo sea uniforme con la utilización de metodologías ágiles.

Por lo que se optó por una arquitectura Orientada a Servicios (SOA) de tres capas: capa de aplicación, capa de negocio y capa de acceso a datos. En este diseño las funcionalidades son proporcionadas como un conjunto de servicios. Estos servicios son unidades independientes de funcionalidad que se comunican a través de una red, bajo el protocolo HTTP.

A continuación la siguiente *figura 1.0* muestra como se encuentra diseñada la arquitectura del sistema.

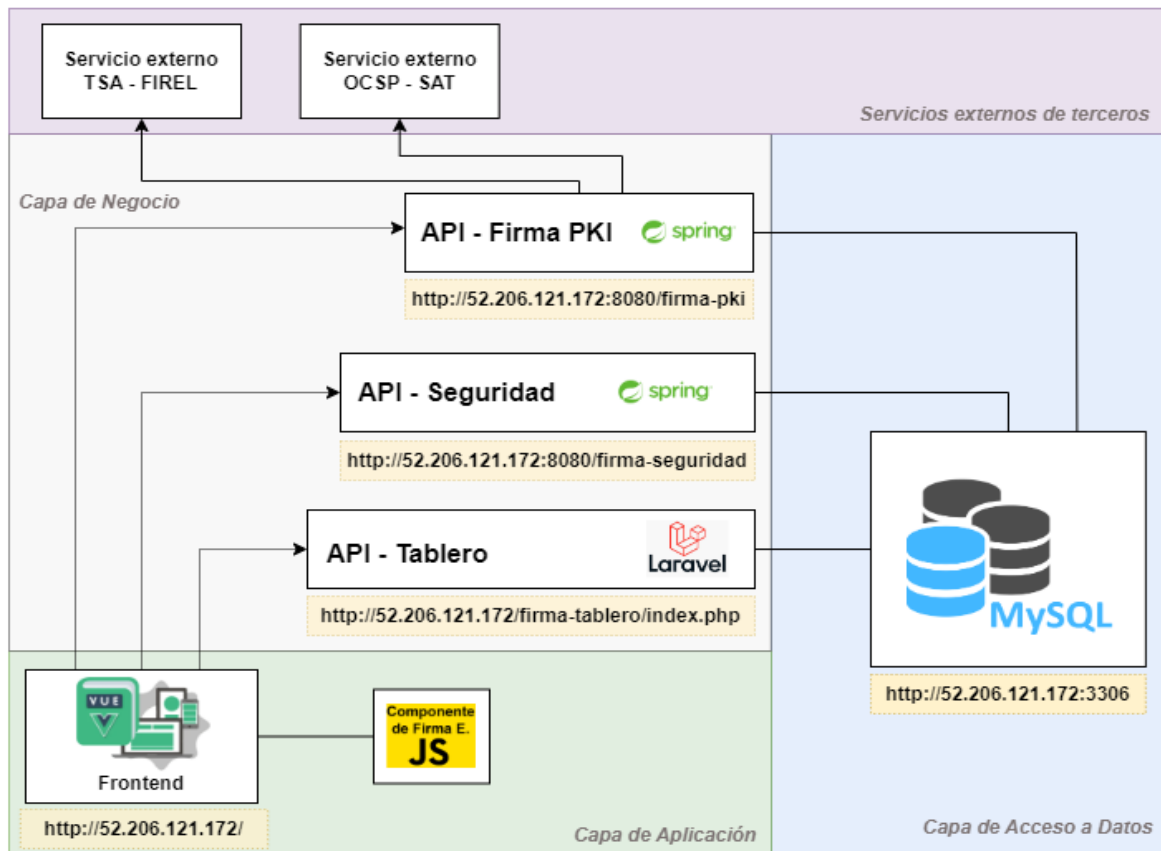


Figura 1. Arquitectura del sistema

La imagen muestra un diagrama de la arquitectura del sistema de gestión de firmas electrónicas, seguridad y funcionalidades del tablero de control, como aplicación web. El sistema se estructura en tres capas principales: Capa de Negocio, Capa de Aplicación y Capa de Acceso a Datos.

En la **Capa de Negocio**, hay tres API diferentes:

1. **API - Firma PKI:** Desarrollada con Spring, esta API se encarga de la gestión de firmas digitales, interactuando con servicios externos como TSA - FIREL para marcas de tiempo y OCSP - SAT para el estado de los certificados.
2. **API - Seguridad:** También construida con Spring, esta API esta dedicada a funciones de seguridad, que pueden incluir autenticación, autorización y otras medidas de protección de datos.

3. **API - Tablero:** Construida con Laravel, esta API gestiona el tablero de control, el cual es un panel de administración de documentos para el usuario del sistema.

En la **Capa de Aplicación**, se indica un componente de Frontend que utiliza Vue.js, usando una interfaz de usuario interactiva y moderna, para interactuar con las API mencionadas.

Finalmente, en la **Capa de Acceso a Datos**, se muestra una base de datos MySQL, que es donde se almacenan y se recuperan los datos para la aplicación.

Los servicios externos de terceros indican que el sistema se integra con otras plataformas o servicios para ciertas funcionalidades especializadas. Cada componente en el diagrama indica su ubicación en la red o cómo acceder a ellos para consumir sus servicios o gestionar su configuración.

Componentes Desarrollados

1. **Frontend.** Es la parte de una aplicación o sitio web que interactúa directamente con el usuario. Incluye la interfaz de usuario (UI) y la experiencia de usuario (UX). El frontend es responsable de recoger las entradas del usuario, procesarlas y presentar la información en un formato legible y accesible.
2. **API Rest.** Una API (Interfaz de Programación de Aplicaciones) Rest (Representational State Transfer) es un conjunto de normas y protocolos que permiten a diferentes sistemas de software comunicarse entre sí a través de HTTP. En una arquitectura RESTful, los datos y la funcionalidad se consideran recursos y se accede a ellos mediante URLs.
3. **Módulo de Firma.** Es el componente de software desarrollado del lado del cliente que contiene todas las funcionalidades necesarias para firmar digitalmente documentos. Este módulo garantiza la autenticidad e integridad

de los datos manteniendo el proceso de firma dentro del equipo del usuario y evitando que información sensible viaje a través de la red.

4. **Base de datos.** Se utiliza para almacenar, recuperar, actualizar y administrar los datos de manera estructurada y eficiente.
5. **Servicios externos.** Servicios que no pertenecen al sistema y que tampoco fueron desarrollados por el TECDMX, que permiten la incrustación de elementos encriptados para lograr la firma avanzada.

Arquitectura de la Base de Datos

En el diseño de la arquitectura de la Base de Datos se determinó dividirla en cuatro secciones principales:

1. **Sección de Tablero.** Contiene todas las tablas que realizan las operaciones de la gestión de documental y otras funcionalidades del sistema y de operación.
2. **Sección Institucional.** Involucra todas las tablas que contienen la información institucional de los empleados, puesto, área y unidad de adscripción.
3. **Sección de Seguridad.** Contiene todas las tablas que permiten la administración de usuarios, roles, permisos, autenticación y están relacionadas con la seguridad del sistema.
4. **Sección de Firma.** Contiene todas las tablas que permiten realizar las operaciones de firma electrónica avanzada, así como las operaciones de administración de las evidencias criptográficas.

Especificaciones de la Base De Datos

Nomenclatura: Se optó por definir una nomenclatura que facilitara la identificación de cada elemento y permitiera la escalabilidad y el mantenimiento de esta.

- **Mayúsculas y minúsculas.** Todas las palabras reservadas se deben escribir en mayúscula, mientras que para los nombres de tablas y las columnas se deben escribir en letras minúsculas. Ejemplos:

CREATE TABLE `pki_x509_registrados`

- **Nombres de tablas.** Todas las tablas deben nombrarse conforme a la siguiente estructura:
 - Identificador de la sección utilizando 3 caracteres: pki, tab, seg
 - Separador de las palabras con guion bajo.
 - Nombre de tabla.
 - Tablas catálogo agregar los caracteres cat después del identificador de la sección.

Ejemplos:

pki_transaccion

- **Nombres de columnas.** Todos los nombres deberán seguir los siguientes atributos:
 - **id:** Es el indicador de cada tabla, se define de tipo INT(Incrementable), el registro debe tener un número único. Siempre debe ser Indicado como llave primaria o llave foránea según la definición del campo.
 - **n:** Indica que el campo es de tipo numérico.
 - **s:** Indica que el campo es una cadena de texto.
 - **d:** Indica que el campo es de tipo fecha.
 - **c:** Indica que el campo contiene un valor predeterminado previamente definido.
 - **desc:** Indica que el campo contiene los detalles, descripción o valor amplio del registro.

Para profundizar en la comprensión de la arquitectura del sistema y obtener una visión más detallada de sus componentes y estructura, se recomienda consultar el documento de *"Documentación técnica completa que describe la arquitectura, el diseño, los microservicios y la base de datos"*, en el apartado de 'Arquitectura del

Sistema' de los documentos adjuntos como entregables correspondientes al mes de diciembre. Este documento complementario ofrece una descripción exhaustiva de la infraestructura técnica, proporcionando una explicación en profundidad de cada capa y módulo, las interconexiones entre los servicios y la lógica operativa del sistema.

Lógica del Sistema

En esta sección se aborda la lógica operativa del sistema, delineando los procesos y procedimientos que rigen el flujo de información y las decisiones automatizadas. Aquí, se traducen los requisitos de negocio en funciones técnicas y cómo estas interactúan para soportar y mejorar las operaciones.

SEGURIDAD: El desarrollo del API de seguridad utiliza el estándar abierto (RFC 7519) con JWT para transmitir información de manera compacta, autónoma y segura entre partes a través de objetos JSON bajo el protocolo HTTP. La implementación desarrollada firma digitalmente cada uno de los datos de comunicación por lo que la información puede ser verificada a partir de una clave (secreto) que implementa *BCrypt* para la codificación y decodificación de las cadenas de datos .

A continuación se muestra la siguiente *figura 2.0* que muestra la lógica con la que se encuentra desarrollado el componente de seguridad.

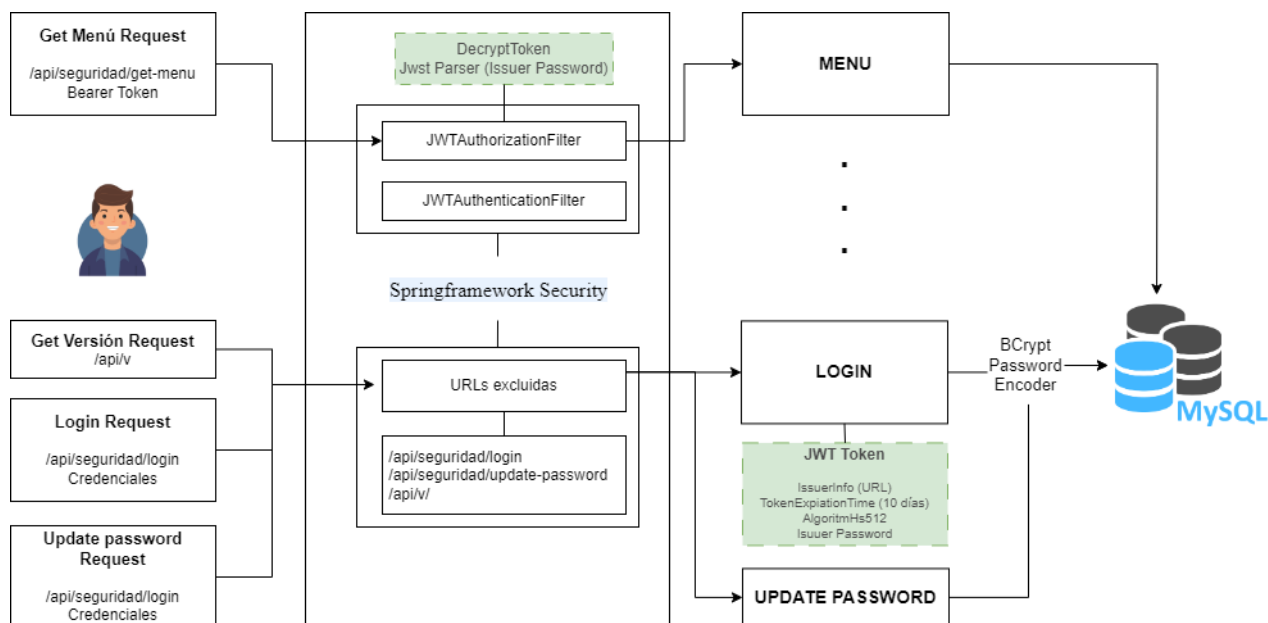


Figura 2. Funcionamiento seguridad

El diagrama de flujo que representa la seguridad y la autenticación en el sistema utilizando Spring Framework Security. Hay cuatro tipos principales de solicitudes que se manejan:

1. **Get Menú Request:** Se hace una petición para obtener un menú, utilizando un 'Bearer Token' como método de autenticación. Esta solicitud es procesada por filtros de seguridad JWT que incluyen 'JWTAuthorizationFilter' y 'JWTAuthenticationFilter'.
2. **Get Versión Request:** Se solicita la versión de la aplicación a través de una ruta específica "/apiv/".
3. **Login Request:** Para iniciar sesión, se envían credenciales a "/api/seguridad/login". Aquí, Spring Framework Security maneja la autenticación, y si es exitosa, se genera un JWT Token con especificaciones como tiempo de expiración, algoritmo y la contraseña del emisor.
4. **Update Password Request:** Similar al proceso de inicio de sesión, esta solicitud permite actualizar la contraseña a través de "/api/seguridad/update-password".

El diagrama también destaca las 'URLs excluidas' que no requieren autenticación, como los endpoints para iniciar sesión y actualizar la contraseña.

En la parte derecha del diagrama, se visualiza cómo se manejan los procesos de 'LOGIN' y 'UPDATE PASSWORD'. El proceso de 'LOGIN' se conecta con una base de datos MySQL, donde las contraseñas son codificadas usando BCrypt Password Encoder. El proceso de 'UPDATE PASSWORD' muestra la generación de un JWT Token que incluye detalles como el tiempo de vida del token y la información del emisor.

MÓDULO DE FIRMA ELECTRÓNICA : El componente de Firma Electrónica se realizó como un módulo independiente que lograra el objetivo de integrarse en cualquier tipo de aplicativo que soporte la incrustación de JavaScript. Este componente se conecta con el API de Firma-PKI para completar las funcionalidades de firma avanzada y registrar los procesos en la base de datos.

A continuación se muestra la siguiente *figura 3.0* que representa el flujo de la lógica de operación del componente de firma electrónica.

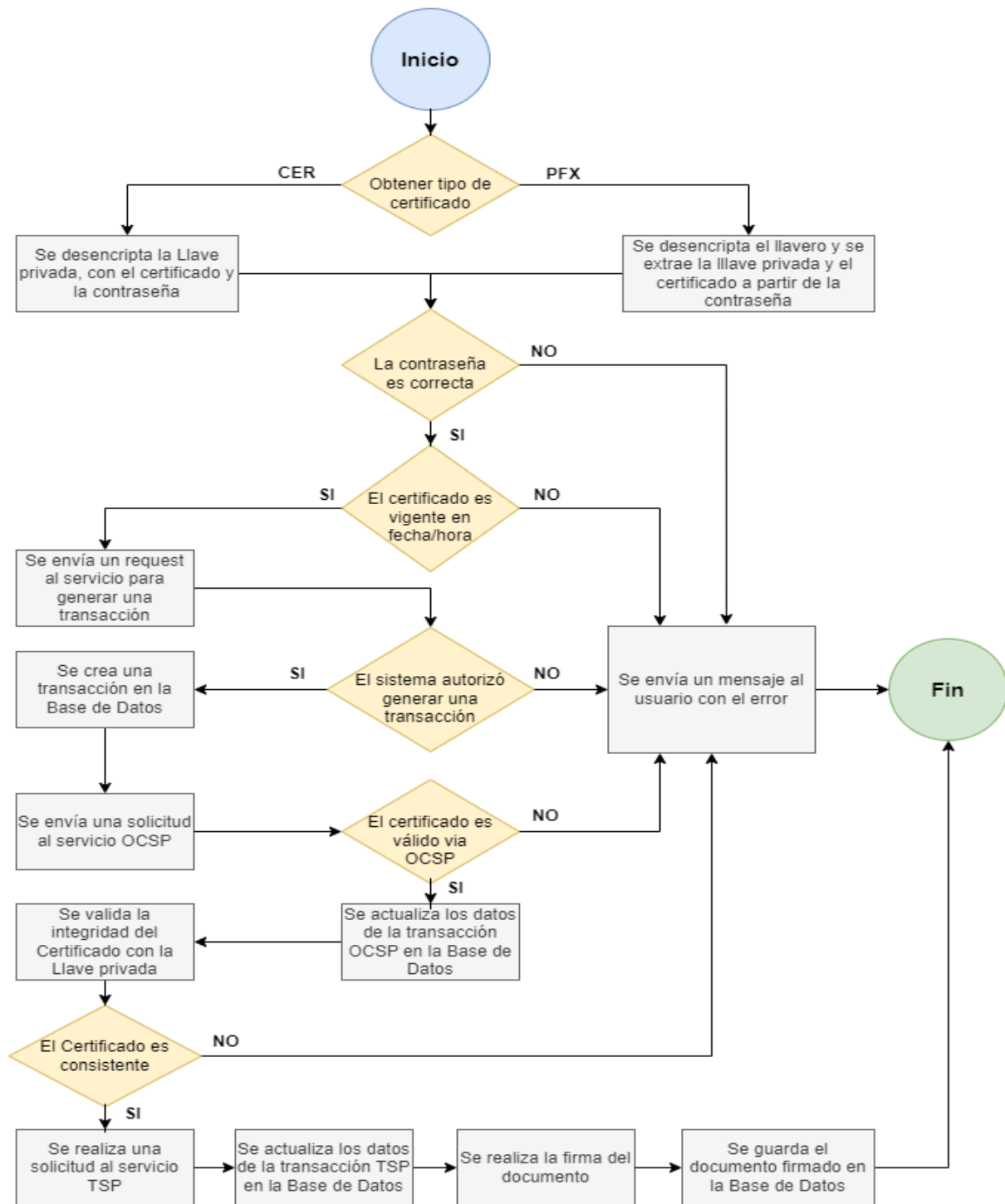


Figura 3. Funcionamiento firma electrónica

El diagrama anterior representa el flujo de trabajo de autenticación y firma electrónica que comienza con la obtención del tipo de certificado (CER o PFX).

Sigue un proceso de validación del certificado que incluye la descriptación y verificación de la contraseña, la comprobación de la vigencia del certificado y su validez a través del servicio OCSP.

Si el certificado es válido, se procede a la creación de una transacción en la base de datos y a la validación de la integridad del certificado. Finalmente, si el certificado es consistente, se realiza una solicitud al servicio TSP y se firma el documento, que luego se guarda en la base de datos. Si en algún punto el certificado no es válido o no se autoriza la transacción, el proceso se detiene y se informa al usuario del error.

Para obtener una comprensión detallada y profunda de la lógica que conforma al sistema, se aconseja la revisión del documento "*Documentación técnica completa que describe la arquitectura, el diseño, los microservicios y la base de datos*". Encontrará este material en la sección 'Lógica del Sistema' de los documentos adjuntos como entregables correspondientes al mes de diciembre, donde se desglosan los procesos, las reglas de negocio y los flujos de datos que coordinan las operaciones y funciones del sistema.

Módulos

En esta sección se abordan los módulos del sistema, haciendo mención de la funcionalidad de cada uno de ellos y como se encuentran conformados. También es posible consultarlos en <https://jel.tecdmx.org.mx>


Autenticación: Este módulo consta de lo siguiente:

- Login
- Registro de usuario
- Recuperación de contraseña

Para acceder de manera segura al "Sistema de Gestión de Firmas Electrónicas", los usuarios deben navegar a la dirección URL proporcionada: <https://jel.tecdmx.org.mx/account/login>.

Al ingresar a este enlace, se presentará la pantalla de inicio de sesión que es el portal para la autenticación del usuario. Esta interfaz está diseñada para garantizar la seguridad en el acceso al sistema, solicitando las credenciales necesarias para verificar la identidad del usuario antes de permitir el acceso a las funcionalidades avanzadas del sistema.

A continuación se muestran las siguientes figuras 4.0, 5.0, 6.0 las cuales corresponden al módulo de autenticación del sistema.



Iniciar sesión
Ingresar usuario y contraseña para continuar.

CORREO

CONTRASEÑA [¿Olvidaste tu contraseña?](#)

Judicial **Administrativo**

[¿No estas registrado? Crea una cuenta](#)

Figura 4. Login



Registro

¿Tienes cuenta? [Iniciar sesión](#)

USUARIO

CORREO ELECTRÓNICO

CONTRASEÑA

La contraseña debe tener al entre 8 y 16 caracteres, al menos un dígito, al menos una minúscula, al menos una mayúscula y al menos un caracter no alfanumérico.

Registrarse

Figura 5. Registro de usuario



Restablecer contraseña

Ingresa tu correo electrónico y se enviarán las instrucciones.

CORREO ELECTRÓNICO

Restablecer

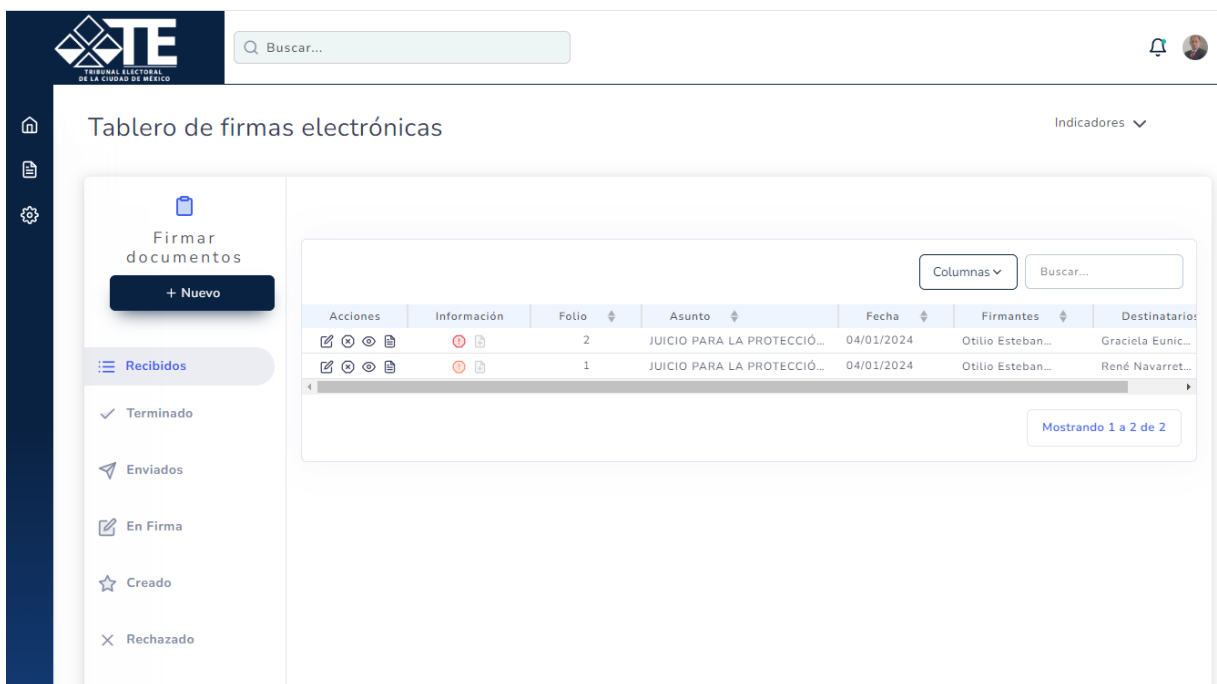
Figura 6. Restablecer contraseña

Tablero Principal: Este módulo contiene lo siguiente :

- Tablero Principal
- Nuevo Documento

Donde la pantalla del tablero principal presenta un conjunto de documentos asociados al usuario que ha iniciado sesión y nuevo documento permite la creación de un nuevo registro tras llenar una serie de campos solicitados.

A continuación de muestran las figuras 7.0 y 8.0 correspondientes a este módulo de Tablero principal.



Tablero de firmas electrónicas

Indicadores ▾

Firmar documentos
+ Nuevo

Recibidos

- ✓ Terminado
- 📧 Enviados
- ✍ En Firma
- ★ Creado
- ✗ Rechazado

| Acciones | Información | Folio | Asunto | Fecha | Firmantes | Destinatarios |
|----------|-------------|-------|------------------------------|------------|-------------------|-------------------|
| | | 2 | JUICIO PARA LA PROTECCIÓN... | 04/01/2024 | Otilio Esteban... | Graciela Eunic... |
| | | 1 | JUICIO PARA LA PROTECCIÓN... | 04/01/2024 | Otilio Esteban... | René Navarret... |

Mostrando 1 a 2 de 2

Figura 7. Tablero Principal

Nuevo documento para firma

Fecha de documento:
2024-01-07 ✓

Elaboró:
paola.montg@gmail.com

Destino de documento: -- Seleccionar -- ▼ Tipo de documento: -- Seleccionar -- ▼

Folio del documento: --- Folio especial: folio Número de Expediente: Expediente +

Asunto:
Asunto

Contenido:
Agregue el contenido

Agregar Firmantes

| NOMBRE | INSTRUCCIÓN | ESTADO | EDITAR |
|--------|-------------|--------|--------|
|--------|-------------|--------|--------|

Agregar Destinatarios

| NOMBRE | INSTRUCCIÓN | ESTADO | EDITAR |
|--------|-------------|--------|--------|
|--------|-------------|--------|--------|

Figura 5. Nuevo documento p.1

Notas:

Agregue sus observaciones

Configuración

☐ Firmar en este orden

☐ Mantener en modo captura

☐ Generar número de oficio

Prioridad

☐ Alta ☐ Media ☐ Baja

Fecha límite de firma:

Seleccionar

Documento(s) para firmar

Elegir archivos Sin archivos seleccionados

Cancelar Guardar captura Firmar ahora

Figura 6. Nuevo documento p.2

Catálogos: En este módulo se encuentran los accesos a los catálogos que conforman el sistema, desde aquí es posible realizar distintas acciones como: consultar, crear, editar, eliminar y registros.

Los catálogos son los siguientes:

- Personal
- Empleado-Puesto
- Puesto
- Tipo Documento
- Destino Documento
- Prioridad
- Etapa Documento
- Estado Usuario
- Sexo
- Expediente

- Área de Adscripción
- Roles

A continuación en la siguiente figura 10.0 se muestra la pantalla correspondientes a los catálogos.

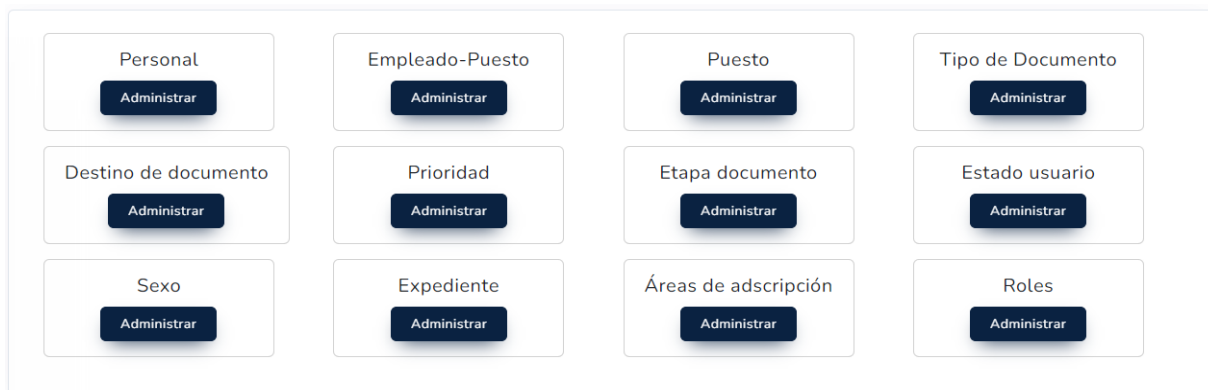


Figura 7. Catálogos

Administración: En este módulo el usuario podrá relizar distintas acciones desde su cuenta dependiendo de los permiso que hayan sido otorgados, este módulo se encuentra conformado por :

- Cambiar Contraseña
- Perfil

A continuación se muestran las figuras 11.0 y 12.0 que representan las pantallas que conforman este módulo.

Cambiar contraseña

NUEVA CONTRASEÑA

 Ingresa una nueva contraseña 

La contraseña debe tener al entre 8 y 16 caracteres, al menos un dígito, al menos una minúscula, al menos una mayúscula y al menos un caracter no alfanumérico.


CONFIRMAR NUEVA CONTRASEÑA

 Ingresa una nueva contraseña 





Cambiar contraseña

Figura 11. Cambiar contraseña

Perfil



Otilio Esteban Hernández Pérez

-  Director
-  otilio.hernandez@tecdmx.org.mx
-  Unidad de Sistemas Informáticos
-  Certificado
Válido de 17-12-20 a 17-12-24

Vincular certificado

Figura 12. Perfil de usuario

Para una comprensión más profunda y una exploración en detalle del funcionamiento de cada módulo del sistema, se invita a revisar el documento titulado "Documentación y capacitación Sistema de Gestión de Firmas Electrónicas " de los documentos adjuntos como entregables correspondientes al mes de diciembre.

Este proporciona una explicación pormenorizada de cada módulo, detallando su rol, funcionalidad, y cómo cada uno se integra y contribuye al conjunto del sistema.

Código Fuente

Este apartado muestra la manera en la que se encuentra organizado el código fuente del "Sistema de Gestión de Firmas Electrónicas". Proporciona una visión de la estructura del programa.

Estructura de proyectos Java Spring Boot

Las clases que conforman el proyecto se encuentran organizadas en cinco tipos de paquetes:

- 1) **Paquetes de configuración.** Es el paquete padre que contiene las clases de configuración y seguridad de la aplicación.
- 2) **Paquetes de servicios (api).** Contienen las clases correspondientes a la capa de aplicación y la capa de negocio. Aquí, se encuentran declaradas las clases Rest Controller y Service, así como las clases para la transferencia de datos. Se identifican fácilmente, ya que incluyen en su nomenclatura la palabra api seguida del nombre del servicio.
- 3) **Paquetes de acceso a datos.** Contienen las clases para el mapeo de las tablas de la base de datos llamadas Entidades, y que pueden identificarse por su nomenclatura que incluye la palabra **entity** en el nombre del paquete. así como, las que permiten realizar operaciones sobre en la base de datos llamadas Repositorios, y que pueden identificarse por su nomenclatura que incluye la palabra **repository**.
- 4) **Paquetes de propósito general.** Contienen las clases que se utilizan de manera compartida entre las diferentes funcionalidades de la aplicación. Pueden identificarse por su nomenclatura que incluye la palabra **utils**.

- 5) **Paquete de configuración de entornos.** Contiene clases donde es posible realizar configuraciones en los distintos entornos sobre los cuales podemos ejecutar el proyecto.

En las siguientes figuras 13.0 y 14.0 se muestra la organización del código fuente para las APIs realizadas en Spring Boot.

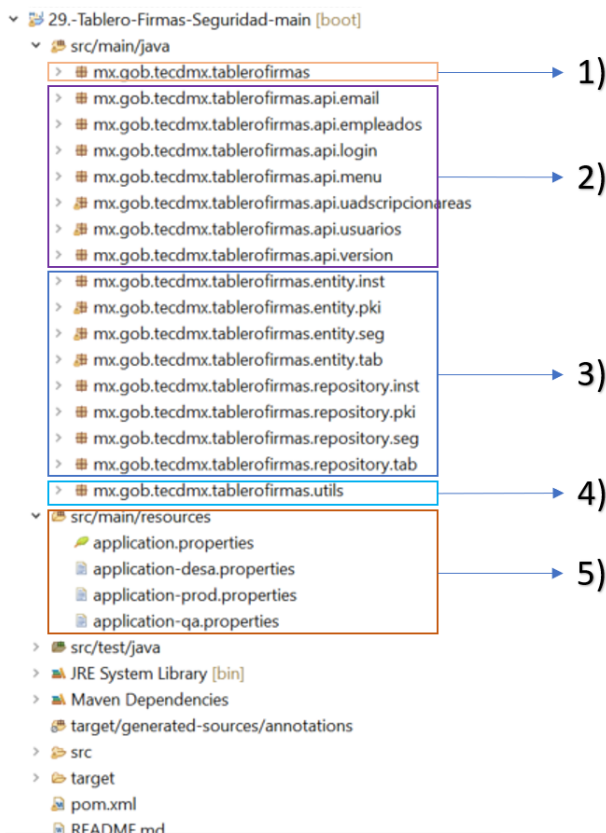


Figura 8. API-Seguridad

Para el caso del API de Firma PKI se agrega un paquete de código más.

Paquetes de seguridad. Contiene la clase que incluye los métodos que coadyuvan a la autenticación y administración de sesiones de usuario.

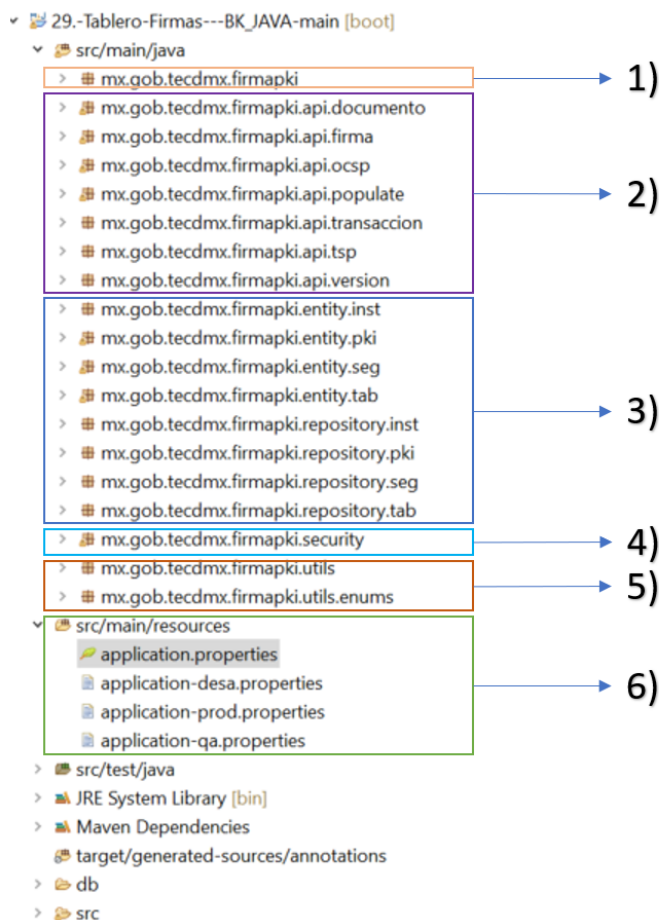


Figura 9. API Firma-PKI

La documentación correspondiente a estas APIs se encuentran en la siguiente URL:
<https://documenter.getpostman.com/view/12283459/2s9YRGwTo6#294c1bdf-b17d-43ba-ae2f-d51c41876b59>

Además, se puede acceder a una descripción detallada en la “*Documentación del API expuesta por los microservicios donde se describen los endpoints, los métodos, los parámetros y las respuestas esperadas*”, la cual se encuentra en los documentos correspondientes a los entregables de octubre. Esta documentación expone de manera pormenorizada los endpoints, métodos, parámetros y respuestas esperadas. Aquí, los usuarios pueden encontrar instrucciones específicas sobre cómo utilizar los servicios proporcionados por cada API desarrollada.

Estructura de proyecto Laravel

Controllers: Contiene las clases controladores .

Models: Contiene los Modelos Eloquent ORM (Object-Relational Mapper) incluido con Laravel, de las tablas de la base de datos que se ocupan para la gestión de documentos.

Public: Aquí se encuentra el archivo `index.php` del proyecto así como el `.htaccess` que contiene configuración.

Routes: El archivo `api.php` contiene todos los endpoints de los servicios desarrollados en este Proyecto backend. Y por último el archivo `.env` contiene los entornos y configuraciones de ejecución del Proyecto.

La siguiente figura 15.0 muestra la manera en la que se encuentra organizado el código fuente.

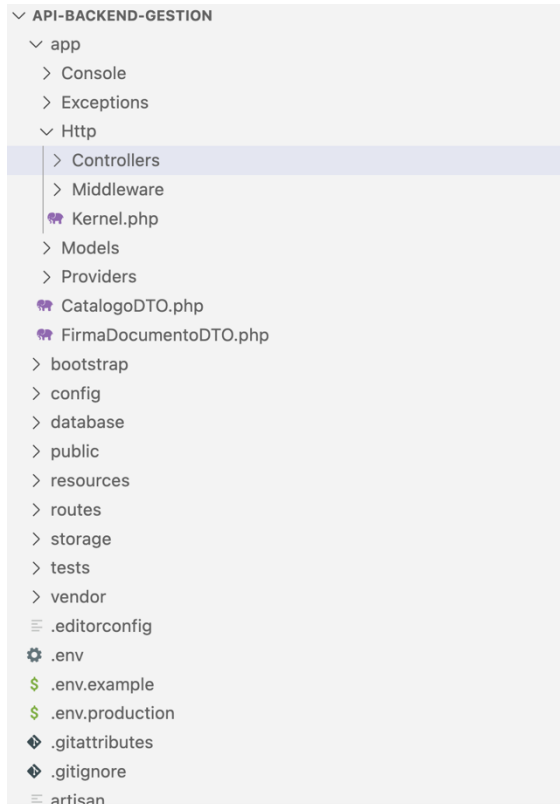


Figura 10. API Gestión

Repositorios

El código fuente del sistema, que incluye tanto el BackEnd como el FrontEnd, está alojado en un repositorio de GIT en la plataforma GitHub. El usuario 'sc-tecdmx' cuenta con los accesos necesarios para que pueda clonar o descargar el proyecto en su totalidad y tener acceso a todas las partes constituyentes del sistema para su revisión o desarrollo continuo.

En la siguiente tabla se encuentran los links de acceso a cada uno de los repositorios que conforman el backend y frontend del sistema.

| Proyecto API | Repositorio |
|---------------------|---|
| Frontend | https://github.com/sc-tecdmx/29.-Temporal-Front |
| Componente de Firma | https://github.com/sc-tecdmx/29.-Tablero-Firmas---BK_JS |

| | |
|-----------------------|---|
| API – Firma Tablero | https://github.com/sc-tecdmx/29.-Tablero-Firmas-Laravel |
| API – Firma Seguridad | https://github.com/sc-tecdmx/29.-Tablero-Firmas-Seguridad |
| API – Firma PKI | https://github.com/sc-tecdmx/29.-Tablero-Firmas---BK_JAVA |

Base de Datos

La configuración de la Base de Datos ha sido establecida siguiendo los parámetros específicos detallados más adelante. Es crucial preservar esta configuración al realizar migraciones o al establecer nuevos entornos de trabajo para asegurar la consistencia y el rendimiento óptimo del sistema.

| Atributo | Valor |
|-----------|--------------------|
| Nombre | db_mappings |
| Charset | utf8mb4 |
| Collation | utf8mb4_0900_ai_ci |

El modelo Entidad-Relación puede generarse directamente desde cualquier gestor de Base de Datos o también puede consultarse en el siguiente vínculo:

<https://dbdiagram.io/d/6587a1c189dea6279978553b>

El archivo script **.sql** se encuentran dentro del repositorio del proyecto de **Firma-PKI**, en una carpeta nombrada **bd**. También, esta carpeta contiene otros archivos que son necesarios para la puesta en marcha del sistema.

Para adquirir un entendimiento más detallado de la estructura del código fuente y los mecanismos operativos de la base de datos, se aconseja la revisión del documento *"Documentación técnica completa que describe la arquitectura, el diseño, los microservicios y la base de datos"* de los documentos adjuntos como entregables correspondientes al mes de diciembre. Este recurso esencial ofrece

una mayor explicación que facilita la navegación y el manejo eficaz de estos componentes del sistema.

Instalación y Despliegue

El servidor destinado a alojar el sistema debe estar adecuadamente preparado con las instalaciones y configuraciones pertinentes de las aplicaciones esenciales que se describen a continuación.

- **Apache 2** : Es un servidor web HTTP de código abierto y uno de los más populares en el mundo. Es mantenido por la Apache Software Foundation y es conocido por su sistema de configuración basado en archivos .htaccess, extensibilidad a través de módulos y compatibilidad con múltiples sistemas operativos. La instalación de Apache es generalmente sencilla y puede ser completada en unos pocos pasos utilizando los gestores de paquetes de los sistemas operativos más comunes.
- **Java**: Se compone de varias partes, incluyendo el tiempo de ejecución (Java Runtime Environment, JRE), que es necesario para ejecutar aplicaciones Java precompiladas, y el Kit de Desarrollo de Java (Java Development Kit, JDK), que es necesario para desarrollar y compilar programas Java. Dependiendo de las necesidades, se puede instalar el JRE o el JDK completo.
- **MySQL**: Es conocido por su rendimiento, confiabilidad y facilidad de uso. Se utiliza en una amplia variedad de aplicaciones, desde pequeños proyectos hasta grandes aplicaciones empresariales. Instalar MySQL implica configurar el servidor de base de datos y asegurarse de que esté optimizado para las necesidades específicas del entorno de producción.
- **WildFly**: Es un servidor de aplicaciones de código abierto y gratuito, implementado en Java y diseñado para ejecutar aplicaciones empresariales. Es conocido por su modularidad, ligereza y por ofrecer un arranque rápido y un alto nivel de rendimiento.

Estos requisitos previos son cruciales para asegurar un entorno operativo óptimo y la funcionalidad plena del sistema publicado.

Una vez que el servidor se encuentra preparado para alojar el sistema, es necesario realizar la configuración de los entornos activos en cada uno de los proyectos.

SpringBoot cuenta con una sección que permite y facilita la configuración de uno o más entornos de desarrollo. Para este proyecto se crearon los archivos necesarios para configurar tres entornos: ***application-des.properties***, ***application-qa.properties*** y ***application-prod.properties***. El entorno activo se debe especificar dentro del archivo nombrado ***application.properties***, modificando la propiedad nombrada ***spring.profiles.active***.

Las siguientes figuras 16.0 y 17.0 muestran la manera en la que se realiza la configuración para los proyectos de spring boot.

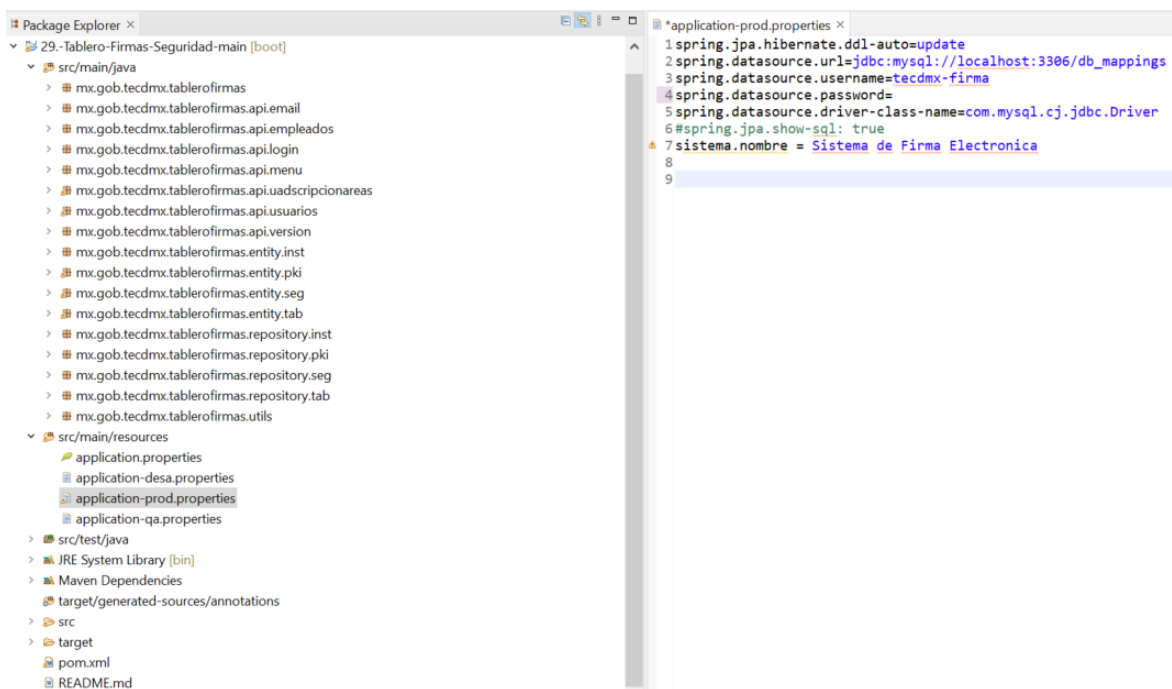


Figura 11. Configuración de producción para Seguridad

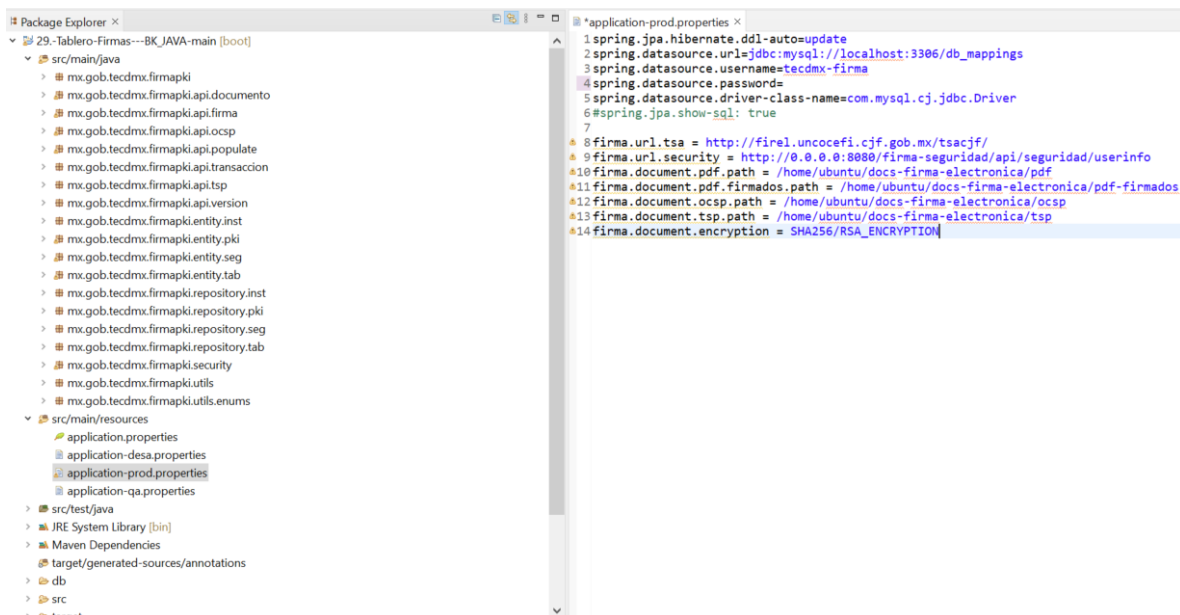


Figura 12. Configuración de producción para Firma PKI

Para el caso del proyecto realizado en laravel y en frontend trabajado en Vue. También es necesario realizar la configuración para los distintos entornos de trabajo. En la siguientes figuras 18.0 y 19.0 se muestra la manera en la que se debe configurar el entorno activo para publicación.



Figura 13. Configuración de producción Frontend

| | |
|---|--|
| <div> <div>API-BACKEND-GESTION</div> <div> <div>Models</div> <div>Providers</div> <div>CatalogoDTO.php</div> <div>FirmaDocumentoDTO.php</div> <div>bootstrap</div> <div>config</div> <div>database</div> <div>public</div> <div>resources</div> <div>routes</div> <div>storage</div> <div>tests</div> <div>vendor</div> <div>.editorconfig</div> <div>.env</div> <div>.env.example</div> <div>.env.production</div> <div>.gitattributes</div> <div>.gitignore</div> <div>artisan</div> <div>composer.json</div> </div> </div> | <pre> 1 APP_NAME=Laravel 2 APP_ENV=prod 3 APP_KEY=base64:6qo0ongJh5sz3laWR4Ec7MlwUInik/Id0JLEjGyvyuM= 4 APP_DEBUG=true 5 APP_URL=http://localhost 6 7 APP_URL_SEGURIDAD=http://localhost:8080/firma-seguridad 8 APP_URL_PKI=http://localhost:8080/firma-pki 9 10 LOG_CHANNEL=stack 11 LOG_DEPRECATIONS_CHANNEL=null 12 LOG_LEVEL=debug 13 14 DB_CONNECTION=mysql 15 DB_HOST=127.0.0.1 16 DB_PORT=3306 17 DB_DATABASE=db_mappings 18 DB_USERNAME="tecdmx-firma" 19 DB_PASSWORD="S!UBW2xK7#5MDYdB" 20 21 BROADCAST_DRIVER=log 22 CACHE_DRIVER=file 23 FILESYSTEM_DISK=local 24 QUEUE_CONNECTION=sync 25 SESSION_DRIVER=file 26 SESSION_LIFETIME=120 </pre> |
|---|--|

Figura 14. Configuración producción Gestión

Para obtener información detallada sobre la configuración y el despliegue del sistema en un entorno de producción, se aconseja revisar de manera completa la guía especializada titulada “Guía para el Despliegue del Sistema en un Entorno de Producción: Consideraciones y Pasos a Seguir” de los documentos adjuntos como entregables correspondientes al mes de noviembre. Este documento contiene instrucciones detalladas y recomendaciones clave para asegurar una correcta y eficiente publicación del sistema.

Documentos Complementarios

Junto con la entrega del sistema, se proporcionará un conjunto de documentos complementarios, que incluyen:

- Un documento detallado que proporciona instrucciones paso a paso sobre cómo utilizar el sistema
- Documentación técnica completa que describe la arquitectura, el diseño, los microservicios y la base de datos.
- Un registro de los cambios realizados en el sistema durante el proceso de desarrollo y pruebas.