# Autenticación de Usuarios

## Creación de Usuario

El sistema de Clientes solicita la creación del usuario en el sistema de seguridad(Single Sign On) con el correo que proporciono el Cliente durante el proceso de compra del producto.

El sistema de seguridad le envía un correo al Usuario con una liga donde podrá definir su contraseña.

## Creación de Token

El sistema de Clientes solicita la creación del token en el sistema de seguridad(Single Sign On).

El sistema de seguridad le envía un correo al Usuario con el token.

## Definición de Contraseña

El usuario utilizando la liga que se le envio por correo define su contraseña.

## Registro de la Clave Publica de la FIEL

El usuario se autentica y selecciona la opción Registro de la Clave Publica de la FIEL el sistema le muestra la opción para que pueda capturar la ruta del archivo .cer y la opción de aceptar.

## Registro del Certificado de Sello Digital

El usuario se autentica y selecciona la opción Registro del Certificado de Sello Digital el sistema le muestra la opcion para que pueda capturar la ruta de los archivos .cer, .key y la clave de acceso y la opción de aceptar.

El sistema encripta la contraseña de la clave privada del CSD con una nueva masterkey y almacena los archivos .cer y .key.

1. El sistema genera una masterkey nueva
2. El sistema desencripta la contraseña de la clave privada del CSD con la masterkey actual, la encripta con la masterkey nueva y la almacena encriptada.
3. El sistema encripta la masterkey nueva con la clave publica de la FIEL y la almacena

## Autenticación

Para autenticar a los usuarios dentro del sistema se utilizara un mecanismo de usuario y contraseña, una vez autenticado se utilizara la FIEL para implementar el mecanismo de **no repudio de transacciones.**

El Flujo es el siguiente:

1. El usuario se autentica utilizando su usuario y contraseña en el sistema(Producto PSRDD).
2. El usuario solicita realizar una transacción en el sistema que debe ser confirmada utilizando la FIEL.
3. El sistema solicita desencriptar la masterkey
   1. El sistema obtiene la masterkey encriptada y la envía del lado del cliente(navegador)
   2. Dentro del navegador utilizando la clave privada y contraseña de la clave privada de la FIEL se desencripta y se envía de regreso al server
4. El sistema realiza la transacción
5. El sistema mantiene la masterkey desencriptada mientras dure la sesión

## Autenticación via token

Para autenticar a un sistema cliente se utilizara el token proporcionado, una vez autenticado se utilizara la FIEL para implementar el mecanismo de **no repudio de transacciones.**

El Flujo es el siguiente:

1. El sistema cliente se autentica utilizando el token en el sistema(Producto PSRDD).

## Fin de Sesión

Cuando la sesión de un Usuario termina ocurre lo siguiente:

1. El usuario solicita al sistema terminar su sesión.
2. El sistema encripta la contraseña de la clave privada del CSD con una nueva masterkey
   1. El sistema genera una masterkey nueva
   2. El sistema desencripta la contraseña de la clave privada del CSD con la masterkey actual, la encripta con la masterkey nueva y la almacena encriptada.
   3. El sistema encripta la masterkey nueva con la clave publica de la FIEL y la almacena
3. La sesión finaliza exitosamente y se le avisa al usuario.

## Glosario

FIEL: Firma Electronica

CFE: Certificado de Firma Electronica

CSD: Certificado de Sello Digital

.CER: Clave publica

.KEY: Clave privada

masterkey: Clave de acceso al CSD

Sistema Cliente: Sistema que se conecta via WebServices

# Expiración de sesión por inactividad

El aplicativo debe contar con sesiones que expiren después de máximo 10 minutos de inactividad. El reingreso deberá de solicitar de nuevo las credenciales.

Pantalla

# Línea base de seguridad

"El aplicativo debe tener aplicada una línea base de seguridad que debe incluir como mínimo:

- Implementación de autenticación de los usuarios (internos o clientes).

- Implementación de mecanismo de no repudio de transacciones.

- Protección contra inyección de código

- Inicio de sesión seguro

- Validación de datos de entrada / salida para evitar errores en el procesamiento de la información.

- Manejo de errores.

- Endurecer el sistema. (Hardening)

Los activos (aplicativos, servidores, bases de datos, dispositivos de red, etc.) del centro de datos que dan soporte al proceso de CFDI deben tener contar con líneas base de seguridad documentadas e implementadas, que consideren como mínimo:

- Protección del BIOS en arranque de los sistemas.

- Deshabilitación de unidades de almacenamiento removibles.

- Instalación del S.O. en partición exclusiva.

- Inhabilitación de puertos, protocolos usuarios y servicios innecesarios.

- Recomendaciones de seguridad del fabricante del equipo y sistema operativo."

Documento con configuración y línea base de seguridad del aplicativo, listado de activos, versión del sistema.

# Implementar controles de validación de integridad de datos

"Deberán de existir procesos y procedimientos para la gestión de la integridad de la información almacenada y gestionada en servicio.

Implementar un proceso de monitoreo que detalle el mecanismo de control de cambios realizados sobre la información sensible de los contribuyentes y los documentos digitales.

Se debe de validar que la información es consistente e integra, que los registros no se pueden cambiar sin que se generen alertas.

Se deberán de implementar medios para validar y mantener la integridad de la información."

# Implementar controles de validación de seguridad de la aplicación.

"Debe existir una política y procedimientos para llevar a cabo la validación de la seguridad del aplicativo. Considerando las pruebas de seguridad para al menos los siguientes rubros:

A1: SQL Injection

A2: Cross-site Scripting

A3: Broken Authentication and Session Management

A4: Insecure Direct Object Reference

A5: Cross-site Request Forgery

A6: Security Misconfiguration

A7: Failure to Restrict URL Access

A8: Insufficient Transport Layer Protection

A9: Unvalidated Redirects and Forwards "

Implementar controles de validación de seguridad de datos para el flujo de la aplicación.

"Debe existir una política y procedimientos para llevar a cabo la validación de los datos ingresados a la aplicación, con el fin de identificar y realizar la gestión adecuada. Se deberá considerar:

Uso de catálogos

Validación de entradas

Codificación de salidas

Validación y administración de contraseñas.

Administración de sesión

Practicas de criptografía

Administración de errores y bitácora.

Protección de datos

Seguridad de la comunicación

Configuración del sistema

Seguridad en la base de datos

Administración de archivos

Mejores prácticas de codificación"

# Prevención de Pérdida de Datos

"Se debe de implementar un procedimiento que registre y monitorea la actividad de cada equipo que interviene o tiene contacto con la operación del servicio, a fin de evitar el uso indebido o perdida de la información.

Ej. Acceso a archivo, copias, impresiones, etc."