PO01 POLÍTICA DE CERTIFICADOS DE FIRMA ELECTRÓNICA AVANZADA

1. INFORMACIÓN DEL DOCUMENTO

HISTORIA DEL DOCUMENTO			
Nombre del documento:	PO01 Política de Certificados de Firma Electrónica Avanzada		
Generado por:	Osvaldo Martínez Burgos		
Revisado por	Rafael Pérez López	**Fecha de creación:**	04/03/2022
Aprobado por:	Rafael Pérez López	**Fecha de aprobación:**	20/04/2022
Oficializado por:	Comité de Riesgos y Seguridad	**Entrada en vigencia:**	22/04/2022

CONTROL DE VERSIONES				
Versión:	**Fecha de Publicación:**	**Preparado/ Actualizado por:**	**Aprobado por:**	**Descripción:**
1.0	04/03/2022	**Osvaldo Martínez**	Rafael Pérez	Creación
1.1	13/03/2023	**Nicolás Borbarán**	Rafael Pérez	Incorporación del procedimiento de enrolamiento de firma electrónica avanzada con token en domicilio del solicitante. Actualización URL de la página web.
1.2	07/09/2023	**Nicolás Borbarán**	Comité de Riesgos y Seguridad	Revisión anual. Correcciones de ortografía y redacción. No hay cambios en el texto del documento. En el punto *"5.4.3 CONSULTA OCSP"* se actualiza la URL del manual de consulta OCSP.
2.0	26/04/2024	**Nicolás Borbarán**	Comité de Riesgos y Seguridad	Incorporación del procedimiento de enrolamiento, revocación y suspensión/reactivación de certificado de Firma Electrónica Avanzada Online. Se agrega el proceso de reactivación de certificado suspendido de Firma Electrónica Avanzada con Token.

3.0	22/01/2025	**Nicolás Borbarán**	Comité de Riesgos y Seguridad	Actualización del documento acorde a las mejoras proporcionadas en el proceso de IAO 2024. Se incorpora *FIRMAKI* en el punto 2.1 "MARCAS COMERCIALES". En el numeral 5.1.1 "SOLICITUD DE CERTIFICADO FIRMA ELECTRÓNICA AVANZADA CON TOKEN" se actualiza la URL, se detalla formulario de solicitud y métodos de pago. Los numerales 5.2.1 "MODALIDAD 1: POR COMPARECENCIA PERSONAL ANTE OPERADOR AR DE E-DIGITAL PKI EN OFICINAS DE SIGNAPIS" y 5.2.2 "MODALIDAD 2: POR COMPARECENCIA PERSONAL ANTE OPERADOR AR EN DOMICILIO DEL USUARIO" se ajustan acorde a los procedimientos operacionales. En el numeral 5.2.3 "MODALIDAD 3: COMPROBACIÓN FEHACIENTE DE IDENTIDAD SEGÚN DECRETO 24 DE LA LEY 19.799" se ajustan referencias a la CPS. En el numeral 5.3.1 "EMISIÓN DEL CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA CON TOKEN" se agrega evidencia del ID token y clasificación FIPS 140-2 nivel 3, se modifica el proceso de importación de certificado al token del Titular, garantizando su control absoluto. En el numeral 5.3.2 "EMISIÓN DEL CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA ONLINE" se ajustan referencias a la CPS. En el numeral 10.1.3.1 "RECEPCIÓN DE SOLICITUDES DE SUSPENSIÓN" se actualizan las URLs y referencias a la CPS. En el numeral 10.2.3.1 "RECEPCIÓN DE SOLICITUDES DE REVOCACIÓN" se actualiza URL. En el numeral 12 "JERARQUÍA DE NORMAS" se incorpora matriz de concordancia entre CP y CPS.

CONTENIDO

2. CONTEXTO

La Política de Certificación (CP por sus siglas en inglés), es un documento que detalla procedimientos y prácticas para la entrega de la prestación de Servicios de Certificación cumpliendo plenamente los requisitos establecidos, de acuerdo con los criterios de evaluación de acreditación establecido por el Ministerio de Economía, Fomento y Turismo de Chile en conformidad a la ley Nº 19.799 y su Reglamento.

Este documento describe las condiciones con que e-Digital PKI, como Prestador de Servicios de Certificación, entrega sus servicios de certificación iniciando con la comprobación fehaciente de identidad de quien solicita un certificado, y cuenta con mecanismos seguros para la gestión del ciclo de vida de los certificados, tanto de los titulares como de la Autoridad de Certificación raíz e intermedia.

Este documento ha sido elaborado de acuerdo con el estándar RFC 3647 Marco de prácticas de certificación y políticas de certificación de infraestructura de llave pública de Internet X.509, y especifica las condiciones que aplican para el ciclo de vida de los certificados electrónicos.

La Políticas de Certificación (CP) y la Declaración de Prácticas de Certificación (CPS), son documentos complementarios que entregan una descripción del funcionamiento general y en detalle de la Infraestructura de Clave Pública (PKI) declarando los requerimientos de seguridad y asegurando el cumplimiento de estos y no incorporan cláusulas discriminatorias en contra de los titulares o partes que confían.

2.1. MARCAS COMERCIALES

Los nombres y logotipos de SIGNAPIS y FIRMAKI son marcas comerciales de e-Digital PKI.

3. IDENTIFICACIÓN DE LA POLÍTICA DE CERTIFICACIÓN

3.1. PRESENTACIÓN

El presente documento constituye la Política de Certificación de e-Digital PKI correspondiente a los Certificados de Firma Electrónica Avanzada, a la cual se hará referencia mediante el acrónimo de su denominación en inglés CP.

Este documento enmarca los preceptos aplicados al procedimiento de la emisión de los Certificados de Firma Electrónica Avanzada por e-Digital PKI.

3.2. IDENTIFICACIÓN

Esta CP puede localizarse en la siguiente url: https://signapis.com/pdf/politica_certificados.pdf.

e-Digital PKI fue acreditada según la resolución RAEX202202626, con fecha 03 de octubre de 2022, emitida por la Subsecretaría de Economía y Empresas de Menor Tamaño. Esta acreditación puede ser revisada en el siguiente enlace:https://www.entidadacreditadora.gob.cl/entidades/.

3.3. ACRÓNIMOS

Sigla	Descripción
AC	Autoridad Certificadora
AR	Autoridad de Registro
CP	Política de Certificación (Sigla en inglés)
CPS	Prácticas de Certificación (Sigla en inglés)
PSC	Prestador de Servicios de Certificación

4. TITULARES

Será sujeto a ser Titular del Certificado de Firma Electrónica Avanzada, quienes certifiquen ser persona natural, que tengan Cédula de Identidad vigente, emitida por el Servicio de Registro Civil e Identificación de Chile, permitiendo a esta PSC comprobar fehacientemente la identidad del Titular.

El certificado es personal e intransferible, por tanto, todo acto ejecutado con el propio certificado será considerado como un acto propio del titular.

5. PROCEDIMIENTO DE REGISTRO

5.1. SOLICITUD DE CERTIFICADO

5.1.1. SOLICITUD DE CERTIFICADO FIRMA ELECTRÓNICA AVANZADA CON TOKEN

El solicitante interesado en obtener un Certificado de Firma Electrónica Avanzada con Token de e-Digital PKI tendrá dos opciones de solicitud:

- **Formulario sitio web:** El solicitante deberá completar y enviar el formulario de solicitud disponible en el sitio web de Signapis (https://www.signapis.com/solicitud-de-certificado.html), proporcionando su nombre completo, correo electrónico, vigencia del certificado (1, 2 o 3 años), e indicando que incluye un token (obligatorio, ya que no se aceptan tokens que no hayan sido vendidos por e-Digital PKI). Asimismo, deberá seleccionar la modalidad de enrolamiento, que podrá ser en las oficinas comerciales de Signapis o en el domicilio del solicitante. Los detalles de ambas modalidades se describen en los numerales 5.2.1 y 5.2.2 del presente documento.

  Una vez completado el formulario, el solicitante será redirigido a la pasarela de pago para generar el pago y completar la solicitud. Posteriormente, el operador de la Autoridad de Registro se pondrá en contacto con el solicitante, vía correo electrónico, para coordinar la comprobación fehaciente de la identidad del solicitante (este proceso es de carácter presencial), según disponibilidad, en horario hábil de lunes a viernes entre 9:00 y 17:00 hrs.

- **Contacto correo electrónico:** El solicitante se comunicará via correo electrónico enviando su solicitud a la casilla de correo soporte@signapis.com indicando su nombre completo, correo electrónico, vigencia del certificado (1, 2 o 3 años), modalidad de enrolamiento (Oficinas comerciales de Signapis o domicilio del solicitante, el detalle de ambas modalidades se describe en los numerales 5.2.1 y 5.2.2 del presente documento).

  Una vez recibida la solicitud, el operador de la Autoridad de Registro se pondrá en contacto con el solicitante para proporcionar detalles sobre los ítems que incluyen el servicio de enrolamiento (y solicitar información adicional en caso de ser necesario) y sus valores comerciales (según vigencia del certificado, modalidad de enrolamiento y costo del dispositivo token FIPS 140-2 nivel 3). Asimismo, enviará las instrucciones para que el solicitante realice el pago a través de una transferencia bancaria (con la opción de emitir boleta o factura) y coordinará la comprobación fehaciente de la identidad del solicitante (este proceso es de carácter presencial), según disponibilidad, en horario hábil de lunes a viernes entre 9:00 y 17:00 hrs.

  Importante: En el caso de que el solicitante ya posea un token de un enrolamiento previo realizado a través de e-Digital PKI (dispositivo FIPS 140-2 nivel 3), deberá informar al operador de la Autoridad de Registro cuando se comunique con él, durante el proceso de solicitud, proporcionando el número de serie del token, el cual será validado con el inventario histórico de tokens de la PSC. En caso de ser validado el token, no se incorporará el valor del token en el monto final a pagar por el solicitante y podrá obtener su certificado en dicho dispositivo.

El envío de los datos solicitados a través del formulario o correo electrónico supondrá su consentimiento para ser registrado como solicitante de un Certificado de e-Digital PKI de Firma Electrónica Avanzada. La solicitud de este certificado no implicará en ningún caso su obtención si no se llegan a cumplir por parte del solicitante las cláusulas y condiciones establecidos en la CPS y en la Política de Certificación para los Certificados de Firma Electrónica Avanzada.

Asimismo, con el envío de los datos enviados a través del formulario o correo electrónico, el solicitante se compromete ante el operador de la Autoridad de Registro, a proporcionar toda la información necesaria, bien para registrar al solicitante como Titular, o con la finalidad de incluirla en el Certificado, de acuerdo con los requisitos establecidos en esta CP.

5.1.2. SOLICITUD DE CERTIFICADO FIRMA ELECTRÓNICA AVANZADA ONLINE

El solicitante interesado en obtener un Certificado de Firma Electrónica Avanzada Online de e-Digital PKI deberá completar y enviar el formulario de solicitud que estará a su disposición en el sitio web https://firmaki.com/auth/fearRegisterClaveUnica.

En el proceso de solicitud, el solicitante deberá validar su segundo factor de seguridad. Para ello, se requerirá de manera obligatoria validar su correo electrónico y, de forma opcional, su teléfono móvil. Ambos podrán ser utilizados al momento de realizar firmas con su certificado de Firma Electrónica

Avanzada. Deberá ingresar el código OTP enviado a su correo electrónico o teléfono móvil (SMS), el cuál consta de un código de 6 dígitos, para continuar con el proceso. En caso de que el solicitante opte por el teléfono móvil como segundo factor de seguridad , es de carácter obligatorio el uso de Método de Desbloqueo para asegurar el control del teléfono móvil.

El detalle del procedimiento se encuentra en la CPS en el numeral 4.1.2 "*SOLICITUD DE CERTIFICADO FIRMA ELECTRÓNICA AVANZADA ONLINE.*

El envío de los datos solicitados en este formulario supondrá su consentimiento para ser registrado como solicitante de un Certificado e-Digital PKI de Firma Electrónica Avanzada. La solicitud de este certificado no implicará en ningún caso su obtención si no se llegan a cumplir por parte del solicitante las cláusulas y condiciones establecidos en la CPS y en la Política de Certificación para los Certificados de Firma Electrónica Avanzada.

Asimismo, con el envío del formulario, el solicitante se compromete a proporcionar toda la información necesaria, bien para registrar al solicitante como Titular, o con la finalidad de incluirla en el Certificado, de acuerdo con los requisitos establecidos en esta CP.

5.2. AUTENTIFICACIÓN E IDENTIFICACIÓN

Para realizar la autentificación e identificación, se realizará el siguiente procedimiento acorde a la opción seleccionada para la validación de identidad:

5.2.1. MODALIDAD 1: POR COMPARECENCIA PERSONAL ANTE OPERADOR AR DE E-DIGITAL PKI EN OFICINAS DE SIGNAPIS

El operador de la Autoridad de Registro coordina con el solicitante, vía correo electrónico, la visita a las oficinas comerciales de Signapis.

Además, el operador de la Autoridad de Registro debe portar:

- Notebook de e-digital.
- Smartphone de e-digital.
- Dispositivo criptográfico token FIPS 140-2 nivel 3, donde está almacenada la llave privada y certificado del operador de la Autoridad de Registro (Certificado para acceder al software generador de certificados utilizado por Signapis, desde el Notebook de la Autoridad de Registro).
- Dispositivo criptográfico token FIPS 140-2 nivel 3, donde se almacenará la llave privada del titular y su certificado.
- Cámara fotográfica (no inteligente).
- Contrato impreso.
- Huellero (no captura datos biométricos).
- Lápiz.

Se requerirá de la comparecencia presencial del Solicitante en las oficinas de Signapis. A continuación, se detalla el procedimiento:

1. El operador de la Autoridad de Registro pedirá al Solicitante presentar su Cédula de Identidad Chilena original y en buen estado, con la cual validará que la fecha de vencimiento esté vigente.

2. El operador de la Autoridad de Registro realizará una consulta en línea al Servicio de Registro Civil e Identificación, utilizando el RUT y el número de documento de la Cédula de Identidad del Solicitante, para verificar su vigencia. Se guardará evidencia de la vigencia de la cédula.

3. El operador de la Autoridad de registro deja evidencia fotográfica de la cédula de identidad (ambos lados) y del rostro del solicitante (utilizando una cámara digital no inteligente) y almacena la evidencia.

4. El operador de la Autoridad de Registro entregará al Solicitante el Contrato de Suscripción de Firma Electrónica Avanzada en dos copias, debiendo estampar su huella dactilar y su firma en ambos ejemplares. Posteriormente, se procederá a tomar fotografías del contrato para obtener la evidencia en formato digital, utilizando el smartphone de e-Digital. Una copia permanecerá en poder del Solicitante, mientras que la otra será almacenada físicamente en las dependencias de e-Digital PKI.

5. El operador de la Autoridad de Registro procederá a resguardar las evidencias en un repositorio digital de acceso restringido y eliminará las evidencias de su Notebook.

5.2.2. MODALIDAD 2: POR COMPARECENCIA PERSONAL ANTE OPERADOR AR EN DOMICILIO DEL USUARIO

El operador de la Autoridad de Registro coordina con el solicitante, vía correo electrónico, la visita al domicilio acordado. Para asistir a las dependencias del solicitante, el operador de la Autoridad de Registro utilizará un medio de transporte (público o privado) que dependerá de la distancia del trayecto.

Además, el operador de la Autoridad de Registro debe portar:

- Notebook de e-digital.
- Smartphone de e-digital.
- Módem propio (Conexión propia del operador de la Autoridad de Registro a internet).
- Dispositivo criptográfico token FIPS 140-2 nivel 3, donde está almacenada la llave privada y certificado del operador de la Autoridad de Registro (Certificado para acceder al software generador de certificados utilizado por Signapis, desde el Notebook de la Autoridad de Registro).
- Dispositivo criptográfico token FIPS 140-2 nivel 3, donde se almacenará la llave privada del titular y su certificado.
- Cámara fotográfica (no inteligente).
- Contrato impreso.
- Huellero (no captura datos biométricos).
- Lápiz.

Se requerirá de la comparecencia presencial del Solicitante mediante una visita del operador de la Autoridad de Registro a las dependencias del solicitante. A continuación, se detalla el procedimiento:

1. El operador de la Autoridad de Registro pedirá al Solicitante presentar su Cédula de Identidad Chilena original y en buen estado, con la cual validará que la fecha de vencimiento esté vigente.

2. El operador de la Autoridad de Registro realizará una consulta en línea al Servicio de Registro Civil e Identificación, utilizando el RUT y el número de documento de la Cédula de Identidad del Solicitante, para verificar su vigencia. Se guardará evidencia de la vigencia de la cédula.

3. El operador de la Autoridad de registro deja evidencia fotográfica de la cédula de identidad (ambos lados) y del rostro del solicitante (utilizando una cámara digital no inteligente) y almacena la evidencia.

4. El operador de la Autoridad de Registro entregará al Solicitante el Contrato de Suscripción de Firma Electrónica Avanzada en dos copias, debiendo estampar su huella dactilar y su firma en ambos ejemplares. Posteriormente, se procederá a tomar fotografías del contrato para obtener la evidencia en formato digital, utilizando el smartphone de e-Digital. Una copia permanecerá en poder del Solicitante, mientras que la otra será almacenada físicamente en las dependencias de e-Digital PKI.

5. El operador de la Autoridad de Registro procederá a resguardar las evidencias en un repositorio digital de acceso restringido y eliminará las evidencias de su Notebook.

5.2.3. MODALIDAD 3: COMPROBACIÓN FEHACIENTE DE IDENTIDAD SEGÚN DECRETO 24 DE LA LEY 19.799

El solicitante que requiera un certificado de Firma Electrónica Avanzada Online, deberá demostrar su identidad a través de "ClaveÚnica" (Comprobación fehaciente de la identidad), según el artículo 1° del Decreto 24 de la Ley 19.799, el cual establece lo siguiente: *"La presente norma establece las condiciones bajo las cuales el Certificador o Prestador de Servicios de Certificación de Firma Electrónica Acreditado reconocerá el sistema denominado* ***"ClaveÚnica", como medio de comprobación fehaciente de la identidad del solicitante*** *de un certificado de firma electrónica avanzada, en los términos exigidos por el artículo 12 letra e) de la ley Nº19.799.".*

Además, el solicitante deberá completar exitosamente un mecanismo complementario, según el artículo 3° del Decreto 24 de la Ley 19.799, el cual establece lo siguiente: *"El Certificador o Prestador de Servicios de Certificación de firma electrónica avanzada una vez integrado al sistema denominado "ClaveÚnica" deberá, además,* ***implementar un mecanismo complementario digital de comprobación de identidad del solicitante*** *para la emisión de un certificado de firma electrónica avanzada.". Para ello, e-Digital PKI establece los siguientes mecanismos complementarios:*

- ***Transferencia de Fondos****: El solicitante deberá realizar un pago online desde una cuenta bancaria asociada a su RUT, validando de esta forma su identidad y el pago del certificado.*

- ***Desafío de preguntas****: El solicitante deberá responder correctamente el desafío de preguntas personales asociadas a la base de datos de nuestro proveedor acreditado.*

El paso a paso de estos procedimientos se encuentra detallado en la CPS en el numeral 4.2.3 "*MODALIDAD 3: COMPROBACIÓN FEHACIENTE DE IDENTIDAD SEGÚN DECRETO 24 DE LA LEY 19.799*" en los puntos "*Comprobación fehaciente de identidad del solicitante (ClaveÚnica)*" y "*Validación de identidad a través de Mecanismo Complementario Digital*".

Los certificados de titulares generados bajo el Decreto 24, con ClaveÚnica, serán almacenados en un dispositivo HSM centralizado que cumple con FIPS 140-2 nivel 3, según lo establecido en el artículo 5° del Decreto 24 de la Ley 19.799: "*Los certificados de firma electrónica avanzada, que se emitan utilizando el medio de comprobación de identidad referido en esta norma técnica, podrán ser almacenados en dispositivos, individuales o masivos, que cumplan con el estándar FIPS PUB 140-2: Security Requirements for Cryptographic Modules (mayo 2001)"*.

Por otra parte, el Titular que emita un proceso de firma con el Certificado de Firma Electrónica Avanzada Online deberá validar previamente un segundo factor de seguridad, según lo establece el artículo 5° del Decreto 24 de la Ley 19.799: "*Los datos de creación de firma, almacenados en dispositivos masivos, deberán encontrarse protegidos mediante un* ***segundo factor de seguridad*** *que permita al titular controlar que el acceso y utilización de éstos únicamente pueda ser realizado por él. Estos factores de seguridad deberán encontrarse declarados de manera clara en las Políticas y Prácticas de Certificación, con expresa mención de la fiabilidad que éstos tienen.*". El segundo factor de seguridad que dispondrá el Titular será un código de seguridad (OTP) que recibirá a su correo electrónico o SMS a su teléfono móvil. El correo electrónico o teléfono móvil que recibirá el código de seguridad, será validado en la etapa de enrolamiento, como se indica en la CPS en el numeral 4.1.2 "*SOLICITUD DE CERTIFICADO FIRMA ELECTRÓNICA AVANZADA ONLINE*".

Con respecto a las devoluciones y los plazos de reembolso, se detallan en la CPS en el numeral 4.2.3 "*MODALIDAD 3: COMPROBACIÓN FEHACIENTE DE IDENTIDAD SEGÚN DECRETO 24 DE LA LEY 19.799*" en el punto "*Validación de identidad a través de Mecanismo Complementario Digital*".

5.2.4. ACEPTACIÓN DEL CERTIFICADO POR PARTE DEL SOLICITANTE

- **Certificado de Firma Electrónica Avanzada con Token**

La firma e impresión de huella dactilar en el Contrato de Suscripción de Firma Electrónica Avanzada durante el enrolamiento, de forma manual y sin el uso de dispositivos tecnológicos, implica la aceptación del Certificado por parte del Solicitante.

La aceptación del Certificado deberá realizarse de forma expresa, ante un representante de la AR. El Solicitante confirma y asume que la información proporcionada para la generación del certificado es exacta y completa, con las consiguientes obligaciones que de ello se derive frente a la AR, la PSC o cualquier tercero que de buena fe confíe en el contenido del Certificado de acuerdo con lo descrito en el Artículo Nº24 de la Ley Nº 19.799.

- **Certificado de Firma Electrónica Avanzada Online**

Para la emisión del certificado FEA Online, la evidencia de la comprobación fehaciente de la identidad a través de ClaveÚnica, la evidencia exitosa del mecanismo complementario (transferencia de fondos o desafío de preguntas), aceptación de términos y condiciones, implicará la aceptación del certificado por parte del solicitante.

Aceptando el Certificado, el solicitante confirma y asume la exactitud del contenido de este, con las consiguientes obligaciones que de ello se derive frente a la AR, la PSC o cualquier tercero que de buena fe confíe en el contenido del Certificado.

5.2.5. RECHAZO DE LA SOLICITUD

El operador de la Autoridad de Registro podrá declarar la solicitud como 'Rechazada' bajo cualquiera de las siguientes causales:

- El solicitante no comparece presencialmente el día y hora agendados para la autentificación e identificación.
- El solicitante no presenta su cédula de identidad.
- La cédula de identidad del solicitante se encuentra vencida o en mal estado.
- Los datos de la persona que comparece presencialmente no coinciden con los datos del solicitante enviados a través del formulario web.
- Los datos de la persona que comparece presencialmente no coinciden con los datos de la cédula de identidad presentada.
- El solicitante es menor de 18 años.
- El solicitante se encuentra en condición de interdicto.
- El solicitante rehúsa a aceptar el Contrato de Suscripción de FEA.
- Cualquier otro incumplimiento al procedimiento establecido en el punto 5.2.

Si la AR decidiera rechazar la solicitud del Certificado, dicha decisión será comunicada de forma inmediata al Solicitante y a su vez, formalizada a través de correo electrónico.

En tal caso, el Solicitante podrá generar una nueva solicitud de Certificado, desencadenando nuevamente los procesos de Solicitud de Certificado, Autentificación e Identificación descritos en los puntos 5.1 y 5.2, respectivamente.

En caso de que la solicitud sea para la obtención de un certificado de Firma Electrónica Avanzada Online, la Autoridad de Registro de nuestro sistema rechazará las solicitudes bajo cualquiera de las siguientes causales:

- Los datos ingresados por el solicitante en el formulario de registro son inválidos.
- El solicitante no se valida correctamente con ClaveÚnica (comprobación fehaciente de identidad).
- El solicitante no responde exitosamente la cantidad mínima de respuestas exigidas en el desafío de preguntas (mecanismo complementario).

- El solicitante no realiza un pago online desde una cuenta bancaria asociada a su RUT en el mecanismo complementario de transferencia de fondos.
- El RUT del solicitante ingresado en el formulario de registro es diferente al validado con ClaveÚnica.
- El solicitante no efectúa el pago correspondiente al servicio contratado.
- El solicitante no acepta términos y condiciones.

5.3. EMISIÓN DEL CERTIFICADO

Aprobada la solicitud, el operador de la Autoridad de Registro o la Autoridad de Registro de nuestro sistema, procede a la emisión del certificado.

5.3.1. EMISIÓN DEL CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA CON TOKEN

Para la emisión de un certificado de Firma Electrónica Avanzada con token, el operador de la Autoridad de Registro proporcionará un dispositivo criptográfico token FIPS 140-2 nivel 3 y solicitará al Titular la creación de un PIN secreto para el token y una clave propietaria del certificado, quedando a total control y administración de su Firma Electrónica. En caso de dudas se entregará el soporte y asistencia por el operador de la Autoridad de Registro. Además, el operador de la Autoridad de Registro dejará evidencia del ID del dispositivo criptográfico del Titular y la clasificación FIPS 140-2 nivel 3.

Para la emisión del certificado (sea en las oficinas comerciales de Signapis o en las dependencias del Titular con la visita del operador de la Autoridad de Registro), el operador de la Autoridad de Registro genera un CSR o Certificate Signing Request (petición de certificado) con la información personal del Titular (nombre completo, RUT, número de documento, correo, comuna, país) y, a su vez, genera el par de llaves en el dispositivo criptográfico token FIPS 140-2 nivel 3 (token) del Titular. En este dispositivo, el titular del certificado genera sus credenciales privadas para acceder al token, con la finalidad de mantener el control absoluto, que posteriormente será utilizado en el software de Signapis para la emisión del certificado. Para acceder a dicho software, el operador de la Autoridad de Registro ingresa con un certificado personal e intransferible, almacenado en un dispositivo criptográfico token FIPS 140-2 nivel 3 (token del operador de la Autoridad de Registro), con sus credenciales correspondientes. Una vez que ingresa al sistema, procede a emitir el certificado del Titular con el CSR generado en el paso anterior. Luego, importa el certificado del Titular al dispositivo criptográfico token FIPS 140-2 nivel 3 del Titular, solicitando que ingrese su contraseña para acceder al token. Además, el operador de la Autoridad de Registro elimina de su notebook la copia del certificado del Titular y el CSR generado previamente. Finalmente, el operador de la Autoridad de Registro entrega el dispositivo criptográfico token FIPS 140-2 nivel 3 correspondiente al Titular, con el certificado y la llave privada almacenada.

Por último, se debe registrar en el sistema de inventario interno, la salida del dispositivo criptográfico, registrando el número de serie de cada elemento y la información del registro del Titular que dio origen al certificado que fue entregado Ej: Fecha, Rut, Nombre.

5.3.2. EMISIÓN DEL CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA ONLINE

Para la emisión del certificado de Firma Electrónica Avanzada Online, el Titular previamente deberá comprobar fehacientemente su identidad a través de ClaveÚnica y un mecanismo complementario (transferencia de fondos o desafío de preguntas).

Con respecto a la validación del segundo factor de seguridad, se detalló previamente en el numeral 5.1.2 "*SOLICITUD DE CERTIFICADO FIRMA ELECTRÓNICA AVANZADA ONLINE*".

Luego de que el Titular se identifique correctamente con los mecanismos dispuestos por e-Digital PKI, el sistema de la Autoridad de Registro solicitará al Titular la creación de su contraseña bajo su exclusivo control y que da acceso al dispositivo HSM centralizado y al certificado de firma electrónica avanzada.

El detalle del procedimiento se explica en detalle en la CPS en el numeral 5.1.2 "*EMISIÓN DEL CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA ONLINE*".

5.3.3. PUBLICACIÓN DEL CERTIFICADO

Una vez que el certificado ha sido aceptado por el titular y emitido por la CA, la PSC procederá a la publicación en el Registro de Acceso Público.

La publicación de los datos del Certificado en el Registro de Acceso Público significa que ha sido aceptado para que los terceros usuarios, de buena fe, confíen en el contenido del Certificado versión x509 v3.

Perfil de Certificado de la Política de Firma Electrónica Avanzada:

CERTIFICADO DIGITAL DE FIRMA ELECTRÓNICA AVANZADA DE PERSONA NATURAL (Entidad Final)		
Nombre del Campo	**Descripción**	**Valor**
Versión	Versión del certificado X.509	3
DN del Sujeto	Country (C)	Código del País del domicilio del Titular, p.e. CL
	Locality Name (L)	Ciudad del domicilio del Titular, p.e. Santiago
	Organization Name (O)	Persona Natural
	Organization Unit (OU)	RUN del Titular, p.e. 12345678-9
	Common Name (CN)	Nombre del Titular, p.e. PNombre SNombre PApellido SApellido
	E-mail (E)	Dirección de correo del Titular, p.e. PNombre123@dominio.com
DN del Emisor	Country (C)	CL
	Locality Name (L)	Santiago
	Organization Name (O)	e-Digital PKI

CERTIFICADO DIGITAL DE FIRMA ELECTRÓNICA AVANZADA DE PERSONA NATURAL (Entidad Final)		
	Organization Unit (OU)	77423125-0
	Common Name (CN)	Autoridad Certificadora Firma Electrónica Avanzada Signapis
	E-mail (E)	contacto@signapis.com
Número de Serie	Serial Number Es el Identificador del Certificado con Valor único dado por DN Emisor	0x00000000000000000000000000000000000000000 Generado aleatoriamente por la AC un número irrepetible
Período de validez	Valid From (Validez a partir de la Fecha)	dd-mm-aaaa hh:mm:ss CLST donde: dd= día; mm=mes; aaaa=año; hh=hora;mm=min; ss=seg.
	Valid Until (Validez hasta la Fecha)	dd-dd-aaaa hh:mm:ss CLST
Largo de llave	Key Size	2048 bits
Clave pública	Public Key	00 00 00 00 00 00 00 00 00 00 00 00 00 00 (...)
Algoritmo de Firma	Signature Algorithm	SHA256withRSA
Fingerprint	Huella del Certificado: SHA1: p.e. CC A1 F1 F4 E6 BB F6 C4 E6 7A E7 73 92 F5 A9 7F 31 5C 13 74	

Todas las especificaciones y condiciones de uso del certificado estarán publicadas en: https://signapis.com/pdf/declaracion_practicas.pdf.

5.4. CONSULTA Y VERIFICACIÓN DEL CERTIFICADO

5.4.1. VERIFICACIÓN DE ESTADO DEL CERTIFICADO

La información sobre el estado de vigencia o revocación de un certificado emitido por e-Digital PKI puede ser consultada a través del formulario web disponible en la siguiente URL: https://signapis.com/estado-de-certificado.html.

Para realizar una consulta, se debe conocer únicamente el RUT del titular.

Como respuesta, el formulario mostrará todos los certificados asociados al RUT indicado. Si el titular posee más de un certificado, se podrá distinguir entre estos mediante el número de serie del certificado.

5.4.2. CONSULTA CRL

La lista de revocación se encuentra disponible en el sitio web de acceso público, al que se puede acceder desde la dirección URL: https://signapis.com/lista-de-revocaciones.html.

5.4.2.1. PERFIL DE CRL

Perfil de CRL según estándar X.509V2 – CRL AC Intermedia Signapis		
Nombre	**Descripción**	**Valor**
Versión	Versión de la CRL	V2
Emisor	Country (C)	CL
	Locality Name (L)	Santiago
	Organization Name (O)	E-Digital PKI
	Organization Unit (OU)	77423125-0
	Common Name (CN)	Autoridad Certificadora Firma Electrónica Avanzada Signapis
	E-mail (E)	contacto@signapis.com
Fecha efectiva de emisión	Periodo de validez de la CRL	Fecha de emisión de la CRL en tiempo UTC
Siguiente actualización	Fecha emisión próxima CRL	Fecha emisión próxima CRL en tiempo UTC
Algoritmo de Firma	Algoritmo de firma de la CRL	SHA256withRSA
URL distribución	URL donde se publica la CRL: https://ca.signapis.com/ejbca/publicweb/webdist/certdist?cmd=crl&format=PEM&issuer=E%3Dcontacto%40signapis.com%2CCN%3DAutoridad+Certificadora+Firma+Electronica+Avanzada+Signapis%2COU%3D77423125-0%2CO%3DE-Digital+PKI%2CL%3DSantiago%2CC%3DCL	
Certificados revocados	Lista de certificados revocados especificando el número de serie, fecha de revocación y motivo de la revocación	
Authority Key Identifier	SHA-1 hash (60 bits) del emisor de llave pública	
Número CRL	Número único de la CRL	Identificador de la CRL

5.4.3. CONSULTA OCSP

Si se desea comprobar la vigencia de un certificado electrónico a través de una consulta en línea mediante el protocolo OCSP deben seguirse lo pasos señalados en el manual de consulta OCSP disponible en la siguiente URL del sitio web de acceso público de la PSC: https://signapis.com/manuales/manual_ocsp_v2.pdf.

6. USO DE LOS CERTIFICADOS

6.1. COMUNIDAD DE USUARIOS

El Titular de un Certificado de Firma Electrónica Avanzada de e-Digital PKI podrá ser cualquier persona natural siempre que esté conforme a los criterios establecidos en esta CP y en las Prácticas de Certificación (CPS). Este certificado permitirá sólo firmar de acuerdo con lo establecido en la ley 19.799 y su reglamento.

6.2. APLICABILIDAD

6.2.1. FIRMA Y NO REPUDIO

El receptor de un mensaje o documento firmado con el Certificado puede usar la clave pública del emisor para verificar que este último ha usado su clave privada para firmar el documento o mensaje. Esto permite verificar la identidad del emisor del mensaje o documento y que este mensaje o documento no ha sido alterado, lo que en el futuro da lugar al NO repudio del acto, es decir, se entiende como la capacidad de probar que una acción o evento que ha tenido lugar, de modo tal, que este evento o acción no pueda ser repudiado más tarde. El mensaje o documento firmado puede corresponder a una transacción y documento electrónico con validez legal según las normativas vigentes que dicen relación con la firma digital, de acuerdo con la ley 19.799.

6.2.2. INTEGRIDAD

El uso de este sistema de claves asimétricas permite comprobar al receptor de un mensaje que el mismo no ha sido alterado entre el envío y la recepción.

6.3. DETALLES DE CONTACTO

Dirección	Badajoz 100, Las Condes, Santiago, Chile
e-mail	contacto@signapis.com
Teléfono	+569 6492 6904
Horario atención	Días hábiles de lunes a viernes entre 09:00 y 17:00 horas

6.4. USOS DEL CERTIFICADO

Los Certificados emitidos por e-Digital PKI pueden ser utilizados de acuerdo con lo establecido en este documento y en la CPS para los siguientes propósitos: firmando documentos digitales en cualquier acto público o privado, con fines personales, profesionales, empresariales, comerciales o tributarios.

6.5. USOS NO AUTORIZADOS

Estos certificados son válidos para asumir responsabilidades económicas y compromisos en nombre propio permitidos por ley 19.799 Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, y en general serán válidos para los usos descritos en este documento. No se permite un uso del Certificado contrario a:

a) La normativa chilena y a los convenios internacionales ratificados por el Estado de Chile.
b) Lo establecido en la CPS y en la Política de Certificación.

Los certificados e-Digital PKI no pueden ser alterados, se deben utilizar tal y como son suministrados por la PSC.

En caso de haber alguna alteración, el certificado perderá su integridad quedando invalidado automáticamente. La verificación de integridad de cada certificado se realiza mediante funciones criptográficas “hash”, por ejemplo, sha1 o md5.

6.6. LÍMITES DE USO

En particular, este perfil de certificado se usa exclusivamente por personas naturales para certificados de firma electrónica avanzada.

7. OBLIGACIONES CA, RA, TITULAR Y RECEPTOR

7.1. OBLIGACIONES DE LA CA

a) Respetar lo estipulado en las Políticas y Prácticas de Certificación de Firma Electrónica Avanzada, así como lo dispuesto en el Contrato de Suscripción con el Titular.
b) Publicar las Políticas y Prácticas de certificación de Firma Electrónica Avanzada en el sitio web de acceso público de la PSC.
c) Informar a los titulares y a la Entidad Acreditadora sobre modificaciones a los documentos, publicando estas y sus modificaciones en el sitio web de acceso público de la PSC.
d) Contar con un seguro de responsabilidad civil con cobertura por el valor mínimo exigido por el artículo 14 de la Ley 19.799.
e) Utilizar sistemas fiables para el almacenamiento de los certificados reconocidos y permitir comprobar su autenticidad e integridad.
f) Emitir certificados conforme a esta CP, la CPS y a los estándares de aplicación.

g) Emitir certificados, que según la información disponible, se encuentre libre de errores de entrada de datos.
h) Emitir certificados cuyo contenido mínimo sea el definido en el Artículo Nº15 de la Ley Nº19.799.
i) Publicar los certificados emitidos en un Registro de Certificados de acuerdo con el Artículo Nº12 de la Ley Nº19.799, respetando las disposiciones de la Ley Nº19.628 sobre Protección de la Vida Privada.
j) Suspender y revocar los certificados según lo dispuesto en la CPS y publicar las mencionadas revocaciones en la CRL (Lista de Certificados Revocados).
k) Conservar la información del certificado durante a lo menos 6 años desde la emisión inicial del mismo, de conformidad con el Artículo Nº 12 de la Ley Nº 19.799.
l) No almacenar ni copiar los datos de creación de firma del Titular.
m) Proteger sus claves privadas de forma segura.
n) Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas.

7.2. OBLIGACIONES DE LA AR

a) Respetar lo dispuesto en los contratos firmados con el Titular.
b) Comprobar fehacientemente la identidad de los solicitantes de certificados de FEA.
c) En caso de realizar una visita a las dependencias del solicitante, se debe garantizar el registro y la comprobación fehaciente de identidad. Además, se deben proteger los medios de enrolamiento y asegurar la entrega segura del dispositivo criptográfico token FIPS 140-2 nivel 3 al Titular
d) Luego de importar el certificado en el dispositivo criptográfico token FIPS 140-2 Nivel 3, asignado al Titular, debe eliminar el certificado en el notebook del operador de la Autoridad de Registro.
e) Verificar la exactitud y autenticidad de la información suministrada por el solicitante de un Certificado de Firma Electrónica Avanzada.
f) Informar las obligaciones del PSC al solicitante y las de este último, antes de la emisión de un certificado.
g) Tramitar y entregar los certificados según lo estipulado en esta CP y en la CPS correspondiente.
h) Formalizar el contrato de suscripción con los Solicitantes.
i) Archivar los documentos suministrados por los Solicitantes.
j) Atender y tramitar las solicitudes de revocación y suspensión de certificados.
k) Comunicarse con los titulares para correcta gestión del ciclo de vida de los certificados.

7.3. OBLIGACIONES DEL TITULAR

a) La Veracidad en las declaraciones efectuadas al solicitar un Certificado de Firma Electrónica Avanzada, así como de la información que contiene el certificado una vez recibido.
b) El uso personal e intransferible de la llave privada custodiando diligentemente.
c) Mantener la confidencialidad de la información que le proporcione e-Digital para el uso del Certificado y del Servicio de certificación.
d) El uso apropiado del Certificado establecido en las Declaración de Prácticas de Certificación y las Políticas de Certificado respectivas.

e) Acogerse a lo dispuesto por los términos y condiciones, así como a las limitaciones de uso del certificado.
f) Utilizar la llave privada sólo en el dispositivo criptográfico proporcionado por e-Digital PKI, acorde a los niveles de seguridad señalados en este documento.
g) Notificar oportunamente una posible causa de revocación.
h) Notificar cualquier cambio en los datos originalmente suministrados para la creación del certificado y durante su periodo de validez.
i) Dejar de usar el certificado y la llave privada una vez solicitada la revocación, y cuando cualquiera certificado de la cadena de confianza deje de ser válido.

7.4. OBLIGACIONES DEL RECEPTOR

a) Realizar la verificación antes de confiar en la validez de un certificado y que se utiliza de las maneras previstas.
b) Aceptar que los mensajes o documentos firmados con la llave privada del Titular tienen el mismo efecto y validez legal que si se hubiera realizado la firma autógrafa.
c) Conocer y adherirse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados digitales en los que confía.
d) Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerada como causa de revocación.

8. DECLARACIÓN DE LAS GARANTÍAS, SEGUROS Y RESPONSABILIDADES DE LAS PARTES

8.1. GARANTÍAS DE LA PSC

De conformidad con el artículo 14 de la Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, e-Digital PKI ha contratado y mantiene un seguro, que cubre su eventual responsabilidad civil, por un monto equivalente a cinco mil unidades de fomento, como mínimo, tanto por los certificados propios como por aquellos homologados.

8.2. GARANTÍAS DEL TITULAR

Según lo declarado en el punto 7.1 Garantías de la PSC, el titular de certificados de e-Digital PKI u homologados por esta, está cubierto por la póliza de responsabilidad civil ante eventuales daños y perjuicios ocasionados por los servicios de certificación u homologación de certificados de firma electrónica de e-Digital PKI.

8.3. RESPONSABILIDADES DE LA PSC

a) La PSC no será responsable de los daños derivados de errores u omisiones de las obligaciones por parte del titular.

b) La PSC no será responsable de la utilización incorrecta de los certificados, ni de cualquier daño indirecto que pueda resultar de su uso.

c) Previa acción al pago o emisión de certificado, el PSC no será responsable por el retraso o la no ejecución de cualquiera de las obligaciones de esta CP a consecuencia de un acto de fuerza mayor, caso fortuito o en general, cualquier circunstancia que la PSC no pueda poseer control razonable, como por ejemplo: Desastres naturales, guerra, estado de sitio, alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico, de comunicación o básico, virus informáticos, estado de emergencia sanitaria, pandemias, endemia, estados de excepción y/o catástrofes en general.

d) El PSC no será responsable por interrupciones en los servicios que tengan como origen una falla en proveedores de éste o plataformas integradas de terceros (como, por ejemplo, el sistema de identificación de Registro Civil de Chile, sistema de ClaveÚnica, plataforma de sistema de pago, servicio de desafío de preguntas u otra integración que e-Digital PKI considere necesaria para el correcto cumplimiento de los protocolos acorde a lo exigido en la Ley 19.799 y/o Decreto 24 de dicha Ley)

e) La PSC no será responsable del contenido de los documentos suscritos electrónicamente mediante un Certificado de Firma Electrónica Avanzada.

f) La PSC se compromete a mantener vigente y disponer un seguro de responsabilidad civil que cubra el valor mínimo exigido en el Artículo Nº14 de la Ley Nº19.799.

8.4. RESPONSABILIDADES DE LA AUTORIDAD CERTIFICADORA (AC)

La AC responderá de las funciones que le correspondan conforme a esta CP y, en especial, asumirá toda la responsabilidad por la correcta emisión de certificados conforme a los estándares de aplicación, garantizando que cada certificado es único. La AC será responsable también de proteger sus claves privadas de forma segura, para asegurar la integridad de la cadena de confianza.

8.5. RESPONSABILIDADES DE LA AUTORIDAD DE REGISTRO (AR)

La AR responderá de las funciones que le correspondan conforme a esta CP y, en especial, asumirá toda la responsabilidad por la correcta comprobación fehaciente de la identidad del solicitante.

8.6. RESPONSABILIDADES DEL TITULAR

a) Descargar y almacenar el certificado en los dispositivos autorizados (token, FIPS 140-2 Nivel 3) por la PSC y que han sido validados por esta, de acuerdo con lo establecido en la Ley 19.799 "Sobre Documentos Electrónicos, Firma Electrónica Y Servicios De Certificación De Dicha Firma". La descarga y almacenamiento del certificado será realizada por el operador de la Autoridad de Registro en un dispositivo portable seguro (token, Fips 140-2 Nivel 3) proporcionado por e-Digital PKI.

b) El dispositivo portable seguro cuenta con un mecanismo que lo inhabilita en caso de reiterados intentos fallidos de acceso (hasta 15 intentos).

c) El Titular debe entregar una dirección válida para el enrolamiento en su domicilio, cuando solicite la visita del operador de la Autoridad de Registro en sus dependencias.

d) El Titular declarará en el "Contrato de Suscripción de FEA" que el uso de la clave privada correspondiente a su certificado y el conocimiento del PIN de acceso al dispositivo de almacenamiento del certificado (token o HSM, Fips 140-2 Nivel 3) así como a la clave propietaria del certificado, serán de su total responsabilidad.

e) No revelar la clave privada de seguridad del dispositivo en donde se encuentra almacenado el Certificado (Token o HSM) ni la clave propietaria del mismo.

f) Custodiar el Certificado (almacenado en Token), de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado y garantizar su seguridad, así como la del procedimiento para el cual se emiten, especialmente cuidando de no divulgar las claves privadas en cualquier otro documento que el titular conserve o transporte, especialmente si existe la posibilidad de extravío, hurto o sustracción indebida.

g) En el caso de elegir almacenar su certificado de firma electrónica avanzada un dispositivo masivo (FEA Online), según lo establecido en el párrafo segundo del artículo 5 del Decreto 24 de la Ley 19.799, deberá este encontrarse protegido mediante un segundo factor de seguridad, obligándose a mantener el exclusivo control de este segundo factor de seguridad, a fin de controlar el acceso y utilización del dispositivo.

h) Notificar de inmediato la pérdida, robo o falsificación del Certificado que contiene, así como el conocimiento por otras personas, contra su voluntad, del código de activación o de las claves privadas, solicitando la revocación del Certificado en conformidad con el procedimiento que se establece en la CPS.

i) Solicitar la revocación del Certificado cuando se cumpla alguno de los supuestos previstos en el numeral 10.2.1 de esta CP.

j) Destruir o borrar el Certificado que quede en desuso o que haya sido sustituido por otro a utilizar con los mismos fines.

9. PRIVACIDAD Y PROTECCIÓN DE LOS DATOS

9.1. TIPOS DE INFORMACIÓN A PROTEGER

La información personal de los titulares de certificados es de carácter confidencial (Art. 23 párrafo 2° de la ley 19.799), por lo tanto, estos datos e información serán tratados por e-Digital PKI de acuerdo con las obligaciones según lo dispuesto por Art. 12 b) de la ley N.°19.799 Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma, donde se estipula que la PSC debe mantener un

registro de acceso público de certificados, en el que quedará constancia de los emitidos y los que queden sin efecto, en los términos señalados en el reglamento. A dicho registro podrá accederse por medios electrónicos de manera continua y regular. Para mantener este registro, el certificador podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para ese efecto, y no podrá utilizarlos para otros fines. Dichos datos deberán ser conservados a lo menos durante seis años desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la ley N.º 19.628, sobre Protección de la Vida Privada y lo relativo al Titular en su rol de consumidor, las disposiciones de la ley N.º 19.496 que establece Normas Sobre Protección a los Derechos de los Consumidores.

e-Digital PKI no utilizará la información para otros fines que los exclusivos y relacionados con sus actividades de certificación, ni compartirá esta información con terceros salvo lo señalado en los puntos 8.2 al 8.6 de esta Política.

9.2. TIPOS DE INFORMACIÓN QUE PUEDE ENTREGARSE

Relacionado a lo anterior, como política general, e-Digital PKI no entregará información personal de sus clientes.

Sin perjuicio de lo anterior, los certificados emitidos por e-Digital PKI contienen información de identificación del titular, y el contenido del certificado está definido en la Ley Nº 19.799.

9.3. INFORMACIÓN DEL CERTIFICADO

El certificado de firma electrónica avanzada contiene los siguientes campos obligatorios de información de los titulares:

a) RUT
b) Correo electrónico
c) Nombre titular
d) Tipo de certificado
e) Empresa emisora de certificado PSC
f) Comuna del titular

9.4. ENTREGA DE INFORMACIÓN SOBRE LA REVOCACIÓN DEL CERTIFICADO

La información sobre el estado de vigencia o revocación de un certificado emitido por e-Digital PKI se encuentra publicada en: https://signapis.com/estado-de-certificado.html.

9.5. ENTREGA DE INFORMACIÓN EN VIRTUD DE UN PROCEDIMIENTO JUDICIAL

e-Digital PKI sólo entregará la información requerida en virtud de un procedimiento judicial o solicitud formal por orden de un tribunal del Poder del Estado Judicial Chileno.

9.6. ENTREGA DE INFORMACIÓN A PETICIÓN DEL TITULAR

e-Digital PKI administra información proporcionada por el propio solicitante y/o titular.

10. SUSPENSIÓN Y REVOCACIÓN DEL CERTIFICADO

La suspensión y revocación de Certificados son mecanismos para utilizar en el supuesto de que por alguna causa establecida en la presente CP se deje de confiar en el Certificado antes de la finalización de su período de validez originalmente previsto.

10.1. SUSPENSIÓN

10.1.1. CAUSAS DE SUSPENSIÓN DEL CERTIFICADO

Los Certificados podrán ser suspendidos cuando concurra alguna de las circunstancias siguientes:

a) Solicitud voluntaria del titular.
b) Pérdida o inutilización por daños del soporte del Certificado.
c) Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto de que se ponga en duda la fiabilidad del Certificado.
d) Por resolución judicial o administrativa que lo ordene conforme a derecho.
e) Por la concurrencia de cualquier otra causa especificada en la presente CP o CPS.

10.1.2. EFECTO DE LA SUSPENSIÓN

El efecto de la suspensión del Certificado es la pérdida de fiabilidad de este, originando el cese temporal de la operatividad del Certificado conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación, durante el periodo de suspensión.

La suspensión de un Certificado impide el uso legítimo del mismo por parte del titular durante el periodo de suspensión de este.

La suspensión del Certificado tendrá como consecuencia la notificación a terceros de que un Certificado ha sido suspendido cuando se solicite la verificación de este.

10.1.3. PROCEDIMIENTO DE SUSPENSIÓN

10.1.3.1. RECEPCIÓN DE SOLICITUDES DE SUSPENSIÓN

- **Solicitud de suspensión de Certificado de Firma Electrónica Avanzada con Token**

El Titular podrá solicitar la suspensión de su Certificado completando el formulario dispuesto en la url: https://signapis.com/revocar-o-suspender-certificado.html indicando 'Solicitud de Suspensión' en el campo 'tipo de solicitud'.

e-Digital PKI procederá a comprobar fehacientemente la identidad del Titular para la verificación de la identidad del propietario del certificado a través de los mismos mecanismos utilizados durante el enrolamiento del Titular.

Este procedimiento requiere de presencialidad del Titular en dependencias de e-Digital PKI o mediante visita en terreno del operador de la Autoridad de Registro.

Posterior a la suspensión de su certificado, el Titular podrá solicitar la reactivación del certificado. El Titular deberá realizar el mismo procedimiento que hizo para obtener la suspensión de su certificado FEA (verificar su identidad ante la comparecencia del operador de la Autoridad de Registro). El Titular deberá presentar su Cédula de Identidad vigente y en buen estado para identificarse. El operador de AR le hará entrega del formulario de reactivación de certificado suspendido, en donde se debe señalar claramente el nombre completo del Titular, RUT y fecha. El titular deberá firmar y estampar huella dactilar (este acto es manual y no se utilizan dispositivos tecnológicos).

- **Solicitud de suspensión de Certificado de Firma Electrónica Avanzada Online**

El Titular podrá solicitar la suspensión de su Certificado completando el formulario de revocación/suspensión dispuesta en el sitio web (https://firmaki.com/auth/fearRevokeCertificate), ingresando su correo electrónico, código de revocación/suspensión (enviado en el proceso de emisión del certificado detallado en el numeral 5.1.2, paso 4 del punto "Generación del Certificado de Firma Electrónica Avanzada Online" en la CPS) y el motivo de la suspensión.

Si el Titular desea reactivar su certificado suspendido, deberá completar el formulario de Solicitud de Reactivación disponible en el sitio web (https://firmaki.com/auth/fearRevokeCertificate) e ingresar correo electrónico y código de revocación/suspensión (enviado en el proceso de emisión del certificado detallado en el numeral 5.1.2, paso 4 del punto "Generación del Certificado de Firma Electrónica Avanzada Online" en la CPS). Una vez enviada la solicitud, el sistema de la Autoridad de Registro de Signapis verificará que el código de revocación/suspensión esté correcto y el certificado se encuentre suspendido al momento de realizar la solicitud. En caso de cumplir con lo señalado, el certificado será reactivado y se enviará al correo electrónico del usuario el número de serie del certificado indicando que fue reactivado correctamente.

10.1.3.2. DECISIÓN DE SUSPENDER

Una vez recibida y autenticada la solicitud de suspensión, el operador de la Autoridad de Registro de e-Digital PKI efectuará la suspensión efectiva del Certificado. La decisión de suspender un Certificado corresponde a la PSC.

10.1.3.3. COMUNICACIÓN Y PUBLICACIÓN DE LA SUSPENSIÓN

La decisión de suspender el Certificado será comunicada por la PSC al titular mediante correo electrónico, además la PSC publicará la suspensión del Certificado en la CRL. La suspensión comenzará a producir efectos a partir de su publicación por parte de la PSC.

10.2. REVOCACIÓN

10.2.1. CAUSAS DE REVOCACIÓN DEL CERTIFICADO

Los Certificados deberán ser revocados cuando concurra alguna de las circunstancias siguientes:

a) Solicitud voluntaria del titular.
b) Pérdida o inutilización por daños del soporte del Certificado.
c) Fallecimiento del signatario oficializado por el Servicio de Registro Civil.
d) Cese en su actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.
e) Inexactitudes graves en los datos aportados por el signatario para la obtención del Certificado, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el Certificado, no se adecuen a la realidad.
f) Que se detecte que las claves privadas del titular o de la PSC han sido comprometidas, bien por que concurran las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, o bien por cualesquier otras circunstancias, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al titular.
g) Por incumplimiento por parte de la AR, PSC o el titular de las obligaciones establecidas en esta CP.
h) Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto de que se ponga en duda la fiabilidad del Certificado.
i) Por resolución judicial o administrativa que lo ordene conforme a derecho.
j) Por la concurrencia de cualquier otra causa especificada en la presente CP.

10.2.2. EFECTO DE LA REVOCACIÓN

El efecto de la revocación del Certificado es la pérdida de fiabilidad de este, originando el cese permanente de la operatividad del Certificado conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

La revocación de un Certificado impide el uso legítimo del mismo por parte del titular.

La revocación del Certificado por causa no imputable al titular originará la emisión de un nuevo Certificado a favor del titular por el plazo restante para concluir el periodo original de validez.

La revocación del Certificado tendrá como consecuencia la notificación a terceros de que un Certificado ha sido revocado, cuando se solicite la verificación de este.

10.2.3. PROCEDIMIENTO DE REVOCACIÓN

10.2.3.1. RECEPCIÓN DE SOLICITUDES DE REVOCACIÓN

- **Solicitud de Revocación para Certificado de Firma Electrónica Avanzada con Token**

El Titular podrá solicitar la revocación de su Certificado completando el formulario dispuesto en la url: https://signapis.com/revocar-o-suspender-certificado.html indicando 'Solicitud de Revocación' en el campo 'tipo de solicitud'.

e-Digital PKI procederá a comprobar fehacientemente la identidad del Titular para la verificación de la identidad del propietario del certificado a través de los mismos mecanismos utilizados durante el enrolamiento del Titular.

Este procedimiento requiere de presencialidad del Titular en dependencias de e-Digital PKI o mediante visita en terreno del operador de la Autoridad de Registro.

- **Solicitud de Revocación para Certificado de Firma Electrónica Avanzada Online**

El Titular podrá solicitar la revocación de su Certificado completando el formulario de revocación dispuesto en la página web (https://firmaki.com/auth/fearRevokeCertificate). Debe completar los datos del formulario de revocación indicando su correo electrónico, código de revocación/suspensión y motivo.

10.2.3.2. DECISIÓN DE REVOCAR

Una vez recibida y autenticada la solicitud de revocación, el operador o sistema de la Autoridad de Registro de e-Digital PKI efectuará la revocación efectiva del Certificado. La decisión de revocar un Certificado corresponde a la PSC.

10.2.3.3. COMUNICACIÓN Y PUBLICACIÓN DE LA REVOCACIÓN

La decisión de revocar el Certificado será comunicada por la PSC al titular mediante correo electrónico, además la PSC publicará la revocación del Certificado en la CRL.

La revocación comenzará a producir efectos a partir de su publicación por parte de la PSC, salvo que la causa de revocación sea el cese de la actividad de la PSC, en cuyo caso, la pérdida de eficacia tendrá lugar desde que esa circunstancia se produzca.

11. ADMINISTRACIÓN DE LA ESPECIFICACIÓN DE LA CP

La PSC podrá modificar las estipulaciones de la presente CP, sin perjuicio de que se mantenga el nivel de calidad esencial de sus servicios de certificación, y serán publicadas en régimen de vigencia, siempre y cuando sean aprobadas por la Entidad Acreditadora del Ministerio de Economía.

11.1. PROVEEDORES

Las empresas y consultores que presten servicios deberán cumplir con las políticas, estándares y procedimientos detallados en el contrato de servicio específico, ítems que pueden ser evaluados en cualquier momento por e-Digital PKI y que se ajusten a la "Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación", en su versión vigente.

11.2. AUDITORIAS

Con el fin de velar por el correcto uso de los recursos de su propiedad, e-Digital PKI se reserva el derecho de auditar a la AR en todo momento y sin previo aviso, como también solicitar auditorías de seguridad externas sobre los procesos de la PSC o como es dictaminado por norma, entregar la información para el proceso de revisión anual ordinario de la Entidad Acreditadora, resguardando el cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los recursos de información, tanto lógicos como físicos y que se ajusten a la "Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación", en su versión vigente.

11.3. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

La misión del Comité de Seguridad de la Información es resolver las Políticas de Seguridad de la Información, sus ajustes y modificaciones, y estará formado por personal de la alta administración de la empresa. La Política de Seguridad de la información deberá ser revisada anualmente por el Comité de Seguridad y sus cambios validados por el Gerente General.

Las principales funciones del Comité están detalladas en el punto 5 del documento "PS01 Política General de Seguridad de la Información".

11.4. CONTROLES

El PSC dispone de controles internos de funcionamiento que regulan los aspectos que refuerzan la seguridad técnica, física, de procedimientos y de capacitación del personal los que están especificados en el punto 9 del documento "PO02 Declaración de las Prácticas de Certificación".

11.5. RIESGOS

e-Digital PKI realiza la gestión de riesgos a través de su Política de Gestión de Riesgos.

11.6. CULTURA DE SEGURIDAD

La forma en la que se lleva a cabo a través de lo especificado en el punto 10 del documento "PS01 Política General de Seguridad de la Información".

11.7. MANTENCIÓN DE LA INFRAESTRUCTURA

e-Digital PKI cuenta con mantención de los servicios de infraestructura contratados a un proveedor que cumple con las obligaciones y requisitos de la "Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación", en su versión vigente, esto permite que puedan ser aplicadas las mejoras de los procesos de Capacity planning que se lleven a cabo por el área de tecnología y que apruebe el SGSI.

11.8. PLAN DE SEGURIDAD

Mediante el Plan de Seguridad se trabaja en los ámbitos de acción durante el año con el objetivo de proveer protección a los recursos de información, según lo definido en el punto 2 del documento "PS04 Plan de un Sistema de Gestión de Seguridad de la Información".

11.9. PLAN DE ADMINISTRACIÓN DE LLAVES

En el documento "PS06 Plan de Administración de llaves", se define el plan de administración de las llaves criptográficas para e-Digital PKI, con el fin de resguardarlas y administrarlas durante su ciclo de vida.

11.10. RESPONSABILIDAD SOBRE LOS ACTIVOS

e-Digital PKI mantiene un inventario de activos el cual es revisado periódicamente y que se encuentra en el archivo "Inventario de Activos".

La Gerencia de e-Digital PKI es el propietario de sus activos y debe entregar los recursos necesarios para gestionarlos y así proveer productos y soluciones de Firma Electrónica (Certificados Digitales) de forma segura y eficiente.

11.11. CONTROL DE ACCESO

En e-Digital PKI el control de acceso a la información es de alta importancia, por lo que se regula en base a lo establecido en la "Política de Control de Accesos".

12. JERARQUÍA DE NORMAS

En todo lo no expresamente previsto por la presente Política de Certificación (CP) será de aplicación lo señalado en la CPS de e-Digital PKI. Los requisitos legales que la PSC debe cumplir están especificados en el punto 6.2 del documento "PS02 Política General de Seguridad de la Información".

- *Matriz de concordancia entre CP y CPS*

A continuación, se mencionan los numerales de los procesos principales de enrolamiento (solicitud de certificado, comprobación fehaciente de identidad y emisión del certificado) y la relación entre la CP y CPS.

Proceso	**Certificado FEA**	**CP**	**CPS**
Solicitud de certificado	Token	5.1.1	4.1.1
	Online	5.1.2	4.1.2
Comprobación fehaciente de identidad	Token	5.2.1 (oficinas de signapis) 5.2.2 (domicilio solicitante)	4.2.2 (Oficinas de signapis) 4.2.2 (Domicilio solicitante)
	Online	5.2.3	4.2.3
Emisión certificado	Token	5.3.1	5.1.1
	Online	5.3.2	5.1.2

**** FIN DEL DOCUMENTO ****