
 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 1 de 23

# PO01 POLÍTICA DE CERTIFICADOS DE FIRMA ELECTRÓNICA AVANZADA

## 1. INFORMACIÓN DEL DOCUMENTO


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

CONTROL DE VERSIONES				
Versión:	Fecha de Publicación:	Preparado/ Actualizado por:	Aprobado por:	Descripción:
1.0	04/03/2022	<b>Osvaldo Martínez</b>	Rafael Pérez	Creación
1.1	13/03/2023	<b>Nicolás Borbarán</b>	Rafael Pérez	Incorporación del procedimiento de enrolamiento de firma electrónica avanzada con token en domicilio del solicitante. Actualización URL de la página web.


 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 2 de 23

## CONTENIDO

<b>1.</b>	<b>INFORMACIÓN DEL DOCUMENTO</b>	<b>1</b>
<b>2.</b>	<b>CONTEXTO</b>	<b>4</b>
<b>3.</b>	<b>IDENTIFICACIÓN DE LA POLÍTICA DE CERTIFICACIÓN</b>	<b>4</b>
3.1.	PRESENTACIÓN	4
3.2.	IDENTIFICACION	4
3.3.	ACRÓNIMOS	4
<b>4.</b>	<b>TITULARES</b>	<b>5</b>
<b>5.</b>	<b>PROCEDIMIENTO DE REGISTRO</b>	<b>5</b>
5.1.	SOLICITUD DE CERTIFICADO	5
5.2.	AUTENTICACIÓN E IDENTIFICACIÓN	6
5.2.1.	<i>ACEPTACIÓN DEL CERTIFICADO POR PARTE DEL SOLICITANTE</i>	7
5.2.2.	<i>RECHAZO DE LA SOLICITUD</i>	7
5.3.	EMISIÓN DEL CERTIFICADO	8
5.3.1.	<i>PUBLICACIÓN DEL CERTIFICADO</i>	9
5.4.	CONSULTA Y VERIFICACIÓN DEL CERTIFICADO	10
5.4.1.	<i>VERIFICACIÓN DE ESTADO DEL CERTIFICADO</i>	10
5.4.2.	<i>CONSULTA CRL</i>	10
5.4.2.1.	<i>PERFIL DE CRL</i>	10
5.4.3.	<i>CONSULTA OCSP</i>	12
<b>6.</b>	<b>USO DE LOS CERTIFICADOS</b>	<b>12</b>
6.1.	COMUNIDAD DE USUARIOS	12
6.2.	APLICABILIDAD	12
6.2.1.	<i>FIRMA Y NO REPUDIO</i>	12
6.2.2.	<i>INTEGRIDAD</i>	12
6.3.	DETALLES DE CONTACTO	12
6.4.	USOS DEL CERTIFICADO	12
6.5.	USOS NO AUTORIZADOS	13
6.6.	LÍMITES DE USO	13
<b>7.</b>	<b>OBLIGACIONES CA, RA, TITULAR Y RECEPTOR</b>	<b>13</b>
7.1.	OBLIGACIONES DE LA CA	13
7.2.	OBLIGACIONES DE LA AR	14
7.3.	OBLIGACIONES DEL TITULAR	14
7.4.	OBLIGACIONES DEL RECEPTOR	15
<b>8.</b>	<b>DECLARACIÓN DE LAS GARANTÍAS, SEGUROS Y RESPONSABILIDADES DE LAS PARTES</b>	<b>15</b>
8.1.	GARANTÍAS DE LA PSC	15
8.2.	GARANTÍAS DEL TITULAR	15

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 3 de 23

8.3.	RESPONSABILIDADES DE LA PSC	15
8.4.	RESPONSABILIDADES DE LA AUTORIDAD CERTIFICADORA (AC)	16
8.5.	RESPONSABILIDADES DE LA AUTORIDAD DE REGISTRO (AR)	16
8.6.	RESPONSABILIDADES DEL TITULAR	16
<b>9.</b>	<b>PRIVACIDAD Y PROTECCIÓN DE LOS DATOS</b>	<b>17</b>
9.1.	TIPOS DE INFORMACIÓN A PROTEGER	17
9.2.	TIPOS DE INFORMACIÓN QUE PUEDE ENTREGARSE	17
9.3.	INFORMACIÓN DEL CERTIFICADO	17
9.4.	ENTREGA DE INFORMACIÓN SOBRE LA REVOCACIÓN DEL CERTIFICADO	18
9.5.	ENTREGA DE INFORMACIÓN EN VIRTUD DE UN PROCEDIMIENTO JUDICIAL	18
9.6.	ENTREGA DE INFORMACIÓN A PETICIÓN DEL TITULAR	18
<b>10.</b>	<b>SUSPENSIÓN Y REVOCACIÓN DEL CERTIFICADO</b>	<b>18</b>
10.1.	SUSPENSIÓN	18
10.1.1.	<i>CAUSAS DE SUSPENSIÓN DEL CERTIFICADO</i>	18
10.1.2.	<i>EFECTO DE LA SUSPENSIÓN</i>	18
10.1.3.	<i>PROCEDIMIENTO DE SUSPENSIÓN</i>	19
10.1.3.1.	RECEPCIÓN DE SOLICITUDES DE SUSPENSIÓN	19
10.1.3.2.	DECISIÓN DE SUSPENDER	19
10.1.3.3.	COMUNICACIÓN Y PUBLICACIÓN DE LA SUSPENSIÓN	19
10.2.	REVOCACIÓN	19
10.2.1.	<i>CAUSAS DE REVOCACIÓN DEL CERTIFICADO</i>	19
10.2.2.	<i>EFECTO DE LA REVOCACIÓN</i>	20
10.2.3.	<i>PROCEDIMIENTO DE REVOCACIÓN</i>	20
10.2.3.1.	RECEPCIÓN DE SOLICITUDES DE REVOCACIÓN	20
10.2.3.2.	DECISIÓN DE REVOCAR	21
10.2.3.3.	COMUNICACIÓN Y PUBLICACIÓN DE LA REVOCACIÓN	21
<b>11.</b>	<b>ADMINISTRACIÓN DE LA ESPECIFICACIÓN DE LA CP</b>	<b>21</b>
11.1.	PROVEEDORES	21
11.2.	AUDITORIAS	21
11.3.	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	22
11.4.	CONTROLES	22
11.5.	RIESGOS	22
11.6.	CULTURA DE SEGURIDAD	22
11.7.	MANTENCIÓN DE LA INFRAESTRUCTURA	22
11.8.	PLAN DE SEGURIDAD	22
11.9.	PLAN DE ADMINISTRACIÓN DE LLAVES	22
11.10.	RESPONSABILIDAD SOBRE LOS ACTIVOS	23
11.11.	CONTROL DE ACCESO	23
<b>12.</b>	<b>JERARQUÍA DE NORMAS</b>	<b>23</b>

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 4 de 23

## 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 N° 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.

## 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. IDENTIFICACION

Esta CP puede localizarse en la siguiente url: [https://signapis.com/pdf/politica\\_certificados.pdf](https://signapis.com/pdf/politica_certificados.pdf).

### 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

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 5 de 23

#### 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


El solicitante interesado en obtener un Certificado de Firma Electrónica Avanzada de e-Digital PKI deberá completar y enviar el formulario de solicitud que estará a su disposición en la dirección url: <https://signapis.com/solicitud-de-certificado.html>.

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 ante la AR, 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.

En dicho formulario, existen 2 opciones para realizar la validación fehaciente de identidad del titular del certificado a generar:

- **En Oficinas de Signapis:** El usuario completa el registro seleccionando la opción de “Enrolamiento presencial” y coordina con la Autoridad de Registro, según disponibilidad, una visita a las oficinas de Signapis y realiza el registro y comprobación fehaciente de identidad de manera presencial, en horario hábil de lunes a viernes entre 9:00 y 17:00 hrs.
- **En Domicilio del Solicitante:** El solicitante completa el registro seleccionando la opción “Enrolamiento en domicilio del solicitante” para realizar el registro y comprobación fehaciente de identidad en las dependencias del usuario y coordina la visita al domicilio señalado por el solicitante, con el operador de la Autoridad de Registro, acorde a la disponibilidad de su agenda. En el numeral 5.2. del documento se establece el detalle sobre la visita del operador de la Autoridad de Registro.

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 6 de 23

## 5.2. AUTENTIFICACIÓN E IDENTIFICACIÓN

- **Visita del operador de la Autoridad de Registro al domicilio del solicitante**

El operador de la Autoridad de Registro coordina con el solicitante 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.


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

- **Registro en oficinas comerciales de Signapis o en Domicilio del solicitante (visita del operador de la Autoridad de Registro)**

Se requerirá de la comparecencia presencial del Solicitante, ya sea en dependencias de e-Digital PKI o mediante una visita del operador de la Autoridad de Registro a las dependencias del solicitante.

a) En presencia del operador de la Autoridad de Registro, el Solicitante deberá completar el formulario de solicitud de Firma Electrónica Avanzada adjunto al Contrato de Suscripción de Firma Electrónica Avanzada con los siguientes datos:

- Nombres del Solicitante
- Apellido Paterno del Solicitante
- Apellido materno del Solicitante
- Cédula de identidad
- Serie de Cédula de Identidad
- Dirección
- Región

	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 7 de 23

- Ciudad
- Comuna
- Correo Electrónico
- Repetir correo Electrónico
- Número celular de contacto

- b) 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 visualmente que la persona que comparece corresponde a la que se identifica.
- c) Con el número y serie de la Cédula de Identidad, se consultará vía web al Servicio de Registro Civil e Identificación la verificación de los datos entregados, obteniendo la verificación de estado de fallecido o de defunción del Solicitante, además del estado de vigencia y bloqueo de la Cédula de Identidad.
- d) El operador de la Autoridad de Registro tomará una fotografía a la Cédula de Identidad del Solicitante.
- e) El operador de la Autoridad de Registro tomará fotografía digital al Solicitante.
- f) 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 (este acto es manual y no se utilizan dispositivos tecnológicos), quedando una copia en poder del Solicitante y otra en poder del operador de la Autoridad de Registro. Este contrato será almacenado físicamente en dependencias de e-Digital PKI y su respaldo digital será guardado en un directorio de acceso restringido.


### 5.2.1. ACEPTACIÓN DEL CERTIFICADO POR PARTE DEL SOLICITANTE

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 N°24 de la Ley N° 19.799.

### 5.2.2. RECHAZO DE LA SOLICITUD

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

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 8 de 23

- El solicitante no comparece presencialmente el día y hora agendados para la autenticación 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 a través del formulario WEB, desencadenando nuevamente los procesos de Agendamiento, Autenticación e Identificación descritos en los puntos 5.1 y 5.2, respectivamente.


### 5.3. EMISIÓN DEL CERTIFICADO

Aprobada la solicitud, el operador de la Autoridad de Registro procederá a la emisión del certificado y entrega de este al Titular.

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.

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 con las extensiones correspondientes y, además, el operador de la Autoridad de Registro elimina de su notebook la copia del certificado del



 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 9 de 23

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 importado.

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.


### 5.3.1. 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
<b>Versión</b>	Versión del certificado X.509	3
<b>DN del Sujeto</b>	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
<b>DN del Emisor</b>	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

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 10 de 23

CERTIFICADO DIGITAL DE FIRMA ELECTRÓNICA AVANZADA DE PERSONA NATURAL (Entidad Final)		
	E-mail (E)	contacto@signapis.com
<b>Número de Serie</b>	Serial Number Es el Identificador del Certificado con Valor único dado por DN Emisor	0x0000000000000000000000000000000000000000000000000000000000000000 Generado aleatoriamente por la AC un número irreplicable
<b>Período de validez</b>	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
<b>Largo de llave</b>	Key Size	2048 bits
<b>Clave pública</b>	Public Key	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (...)
<b>Algoritmo de Firma</b>	Signature Algorithm	SHA256withRSA
<b>Fingerprint</b>	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](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

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 11 de 23

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

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 12 de 23

### 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 los 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.pdf](https://signapis.com/manuales/manual_ocsp.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

Oficina	Badajoz 100 Oficina 1519, Las Condes, Santiago, Chile
e-mail	<a href="mailto:contacto@signapis.com">contacto@signapis.com</a>
Teléfono	(+56) 2 2248 1264
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.

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 13 de 23

## 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).

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 14 de 23


- k) Conservar la información del certificado durante a lo menos 6 años desde la emisión inicial del mismo, de conformidad con el Artículo N° 12 de la Ley N° 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, debe garantizar el registro y comprobación fehaciente de identidad, la seguridad y protección de los medios de enrolamiento y la entrega 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.

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 15 de 23

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

	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 16 de 23

- e) La PSC se compromete a mantener vigente y disponer un seguro de responsabilidad civil que cubra el valor mínimo exigido en el Artículo N°14 de la Ley N°19.799.

#### **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 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 y en las dependencias de esta.
- 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 portable seguro (token, 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 ni la clave propietaria del mismo.
- f) Custodiar el Certificado, 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.



 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 17 de 23

- g) 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.
- h) Solicitar la revocación del Certificado cuando se cumpla alguno de los supuestos previstos en el numeral 10.2.1 de esta CP.
- i) 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.º19.799 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 N.º 19.799.

### 9.3. INFORMACIÓN DEL CERTIFICADO

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

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 18 de 23

- a) RUT
- b) Correo electrónico
- c) Nombre titular
- d) Tipo de certificado
- e) Empresa emisora de certificado PSC
- f) Datos de la acreditación de e-Digital PKI (Declaración del emisor)

#### **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.

##### **10.1.2. EFECTO DE LA SUSPENSIÓN**

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 19 de 23

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**

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.

#### **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:

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 20 de 23

- f) Solicitud voluntaria del titular.
- g) Pérdida o inutilización por daños del soporte del Certificado.
- h) Fallecimiento del signatario oficializado por el Servicio de Registro Civil.
- i) Cese en su actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.
- j) 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.
- k) Que se detecte que las claves privadas del titular o de la PSC han sido comprometidas, bien por que concurren 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.
- l) Por incumplimiento por parte de la AR, PSC o el titular de las obligaciones establecidas en esta CP.
- m) 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.
- n) Por resolución judicial o administrativa que lo ordene conforme a derecho.
- o) 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

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.

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 21 de 23

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.

### **10.2.3.2. DECISIÓN DE REVOCAR**

Una vez recibida y autenticada la solicitud de revocación, el operador 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.

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 22 de 23

### **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**

 <b>e-Digital PKI</b> <small>Una gestión simple y digital</small>	PO01 Política de Certificados de Firma Electrónica Avanzada	USO EXTERNO
Versión: 1.1	Propiedad de e-Digital PKI SpA	Pág. 23 de 23

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 “PS01 Política General de Seguridad de la Información”.

\*\*\*\* FIN DEL DOCUMENTO \*\*\*\*