PO01 – POLÍTICA DE CERTIFICACIÓN FIRMA ELECTRÓNICA AVANZADA

Versión	Realizado por	Revisado	Aprobado	Fecha
1.5	Encargado de Seguridad de la Información	Jefe operaciones CA	Gerente General	23-02-2026

CONTROL DE VERSIONES

Versión	Cambios de la versión	Fecha
1.0	Emisión del documento	01-06-2023
1.1	Revisión de documento	30-09-2024
1.2	Actualización de documento según observaciones EA	27-11-2025
1.3	Actualización de documento según observaciones EA	12-01-2026
1.4	Actualización de documento según observaciones EA	23-02-2026
1.5	Actualización de documento según observaciones EA	23-02-2026

Contenido

1. Introducción **5**
2. Alcance **5**
3. Glosario **5**
3.1. Titulares 7
4. Procedimiento de registro **7**
4.1. Características del procedimiento 7
4.2. Solicitud de certificado 7
4.3. Validación de identidad 7
5. Tipos y usos de certificados **8**
6. Obligaciones CA, RA, titular y receptor **9**
6.1. Obligaciones de la CA 9
6.2. La Autoridad de Registro (RA) 10
6.3. Obligaciones del Titular 11
6.4. Obligaciones de los Receptores 11
7. Declaración de las garantías, seguros y responsabilidades de las partes **12**
7.1. Garantías que entrega la PSC 12
7.2. Garantías para Titular 12
7.3. Eximentes de responsabilidad 12
7.4. Responsabilidades Financieras y Coberturas de Seguros 13
7.5. Responsabilidad del Titular 13
8. Protección de información **14**
8.1. Confidencialidad (Ley N° 19.799) 14
8.2. Excepción de Publicidad 14
8.3. Tratamiento y Conservación de Datos 14
8.5. Información Del Certificado 15
8.6. Entrega De Información Sobre La Revocación Del Certificado 15
8.7. Entrega De Información En Virtud De Un Procedimiento Judicial 15
8.8. Entrega De Información A Petición Del Titular 15
9. Suspensión y revocación de los certificados **15**
9.1. Revocación 15
9.1.1. Posibles causas de revocación 16
9.1.2. Formas de revocación 16
9.1.4. Publicación de la revocación 17
9.2. Caducidad 18
9.3. Renovación 18
9.3.1. Solicitud de renovación 18

9.3.2. Procedimiento de renovación 19
9.4. Suspensión 19
9.5. Concordancia de la Política de Certificación con los procedimientos operacionales 19
9.6. Término de actividades de la CA 20
9.7. Auditorías 20
9.8. Administración y modificaciones 21
9.9. Publicación de modificaciones 21
9.10. Información de contacto 21
10. Referencias 22

0

1. Introducción

Un Prestador de Servicios de Certificación (PSC), por definición legal, es una persona jurídica (ya sea pública o privada, nacional o extranjera) que presta servicios de certificación y tiene la facultad de otorgar certificados de firma electrónica. El PSC actúa expresamente como tercera parte de confianza entre las personas o instituciones que participan en un acto de identificación, autenticación, firma y gestión documental, mediante la utilización de certificados de firma electrónica.

TSP SpA, como Prestador de Servicios de Certificación (PSC), utiliza dos instrumentos fundamentales que establecen el marco de sus servicios y procedimientos de emisión: las “CP” o Políticas de Certificación, y las “CPS” o Declaraciones de Prácticas de Certificación. Estos documentos definen las reglas de emisión, gestión y uso de los certificados de firma electrónica, conforme a lo dispuesto en la Ley N° 19.799.

Política de Certificación (CP) es el conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad o clase de aplicación con requisitos de seguridad comunes. En el contexto de la presente acreditación, este documento define específicamente los alcances, normas y estándares de seguridad aplicables a la emisión y uso de los certificados de firma electrónica avanzada, asegurando el cumplimiento de los requisitos técnicos y legales exigidos para este tipo de certificación.

La Declaración de Prácticas de Certificación (CPS) es definida como un conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados. En general contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, además sobre la relación de confianza entre el Titular o Tercero que confía y la Autoridad de Certificación. Pueden ser documentos absolutamente comprensibles y robustos, que proporcionan una descripción exacta de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los certificados.

2. Alcance

Este documento establece las reglas de alto nivel que rigen el uso y la aplicación de los certificados de firma electrónica avanzada emitidos por el Prestador de Servicios de Certificación (PSC) en su rol de Autoridad de Certificación (CA).

Dichas reglas definen los requisitos comunes de seguridad y utilización y se identifican con el Identificador de Directiva (OID) = 1.3.6.1.4.1.54254.1.4, cumpliendo con el estándar ETSI TS 102 042.

3. Glosario

- **PSC**: TSP SpA, RUT 76.467.322-0
- **Representación Digital**: Es un documento representado en forma binaria, sin hacer referencia a su medio de almacenamiento o soporte, susceptible de ser firmado electrónicamente.
- **Documento Electrónico**: Es toda representación digital que dé testimonio de un hecho, una imagen o una idea.
- **Firma Electrónica Avanzada:** Aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier

modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.

- **Certificado de Firma Electrónica**: Es la certificación electrónica que da fe del vínculo entre el firmante o Titular del certificado y los datos de creación de firma electrónica. Este documento es emitido y firmado electrónicamente por un Prestador de Servicios de Certificación y asocia una clave pública con su Titular durante el período de vigencia del certificado. Debidamente almacenado y publicado, se utiliza para acreditar la identidad del Titular, asegurando que actúa bajo su exclusivo control, mediante sistemas que garantizan la seguridad técnica y criptográfica de los procesos de certificación.

- **Tercera parte interesada**: cualquier persona que reciba documentos firmados por el titular, utilizando un certificado digital emitido por la PSC, o que desee validar una firma electrónica emitida por la PSC.
- **Clave Privada**: Es aquella que se utiliza para firmar electrónicamente, utilizando un criptosistema asimétrico seguro.
- **Clave Pública**: Clave que es publicada y que al ser incorporada en un certificado digital válidamente emitido y almacenada en un repositorio, es utilizada para verificar las firmas electrónicas, basadas en su correspondiente o correlativa clave privada.
- **Criptosistema Asimétrico Seguro**: Es un método criptográfico que utiliza un par de claves compuesto por una clave privada utilizada para firmar electrónicamente y su correspondiente clave pública, utilizada para verificar esa firma electrónica, de forma tal que, con las longitudes de claves utilizadas, sea computacionalmente no factible tanto obtener o inferir la clave privada a partir de la correspondiente clave pública como desencriptar aquello que ha sido encriptado con una clave privada sin la utilización de la correspondiente clave pública.

3.1. Titulares

Conforme a lo establecido en el Artículo 2°, letra h) de la Ley N° 19.799 y el Artículo 2° del Decreto Supremo N° 181, se define como Titular a la persona natural a quien se otorga un certificado de firma electrónica avanzada.

La calidad de Titular se adquiere tras solicitar el certificado y validar su identidad mediante la presentación de su Cédula de Identidad vigente ante la Entidad de Certificación. El certificado emitido es aceptado por el Titular, quien lo utiliza bajo su exclusivo control y en nombre de quien se actúa.

4. Procedimiento de registro

4.1. Características del procedimiento

El registro es el procedimiento que entrega garantías fehacientes de la identidad del solicitante del certificado de firma electrónica avanzada. Este procedimiento se basa estrictamente en la validación presencial de identidad mediante Cédula de Identidad vigente. Adicionalmente, se exigirá que el solicitante haya generado o almacenado la llave privada en un dispositivo acreditado mediante estándar FIPS-140-2 nivel 3.

El procedimiento debe:

- Garantizar que la información suscrita en el certificado es exacta y fiel reflejo de la información entregada por el Titular en el acto de emisión del certificado, utilizando si es necesario todas las herramientas de verificación a su alcance.
- Hacer uso de la tecnología adecuada, tanto en Hardware como Software, para la emisión de los certificados.
- Informar preventivamente la proximidad de la caducidad de los certificados.
- Disponer la revocación de los certificados que no cumplan con las prácticas adecuadas de firma electrónica, o a petición del Titular.
- Disponibilizar lista de certificados revocados, la cual debe ser constantemente actualizada.
- Emplear los procedimientos de seguridad y gestión adecuados para garantizar que los datos de creación de firma (llave privada) se mantengan bajo el exclusivo control del Titular.

4.2. Solicitud de certificado

La solicitud de un certificado de firma electrónica avanzada debe ser realizada por el solicitante mediante la comparecencia a las oficinas de TSP SpA puntos de atención designados.

4.3. Validación de identidad

Deberá comprobarse fehaciente la identidad del solicitante de firma electrónica avanzada, conforme a lo establecido en el Art. N° 12, letra e) de la Ley N° 19.799 y su Reglamento. Esto podrá ser realizado mediante la comparecencia personal del solicitante a las oficinas de TSP SpA, a un notario u oficina del Servicio de Registro Civil e Identificación.

Para la verificación fehaciente de la identidad, el solicitante deberá presentar su Cédula de Identidad, la cual debe encontrarse vigente. El procedimiento de validación incluye obligatoriamente:

1. Cotejo del Nombre y Documento: El personal autorizado cotejará el nombre completo y el número de documento registrados en la solicitud con la información que figura en la Cédula de Identidad, exigiendo una coincidencia exacta de ambos datos. Esta verificación se realiza mediante consulta automatizada al servicio de validación de identidad de un Buró Nacional, el cual accede a las bases de datos oficiales del Registro Civil e Identificación a través de canal seguro HTTPS con autenticación de servicio.
2. Verificación de Imagen: Se realizará la confrontación visual del solicitante presente con la fotografía que figura en su Cédula de Identidad vigente para asegurar la identidad física del titular del documento. El operador de AR confirmará explícitamente en el sistema que la persona presente corresponde con el documento exhibido.
3. Registro de Evidencias: El sistema registrará automáticamente las siguientes evidencias de la validación realizada:
    a. Fecha y hora de la verificación (timestamp UTC)
    b. Identificación del operador de AR que realizó la validación
    c. RUT y número de serie del documento verificado
    d. Resultado de la consulta al servicio de validación (vigencia, correspondencia de datos)
    e. Confirmación explícita del operador sobre la verificación visual presencial
    f. Dirección IP y datos de sesión del operador

    Estas evidencias se almacenan de forma segura e inmutable en los registros de auditoría del sistema, permitiendo la trazabilidad completa del proceso de validación de identidad conforme a los requerimientos de la normativa vigente.

5. Tipos y usos de certificados

TSP SpA emite certificados de firma electrónica avanzada compatibles con el estándar ISO/IEC 9594-8. La estructura y contenido de los certificados cumplen rigurosamente con lo establecido en el Artículo 28 del Decreto Supremo N° 181 de 2002 (Reglamento de la Ley N° 19.799).

La estructura contiene, al menos, las siguientes menciones obligatorias:

1. Nombre completo, RUT y correo electrónico del titular (como identificación del firmante o titular).
2. Identificación del prestador de servicios de certificación (TSP SpA).
3. Número de serie del certificado.
4. Período de validez del certificado (indicando fecha de inicio y fecha de expiración).
5. Clave Pública del titular.
6. Firma electrónica avanzada del prestador de servicios de certificación.
7. Limitaciones de Uso o Usos de Clave (Key Usage), que codifica los usos específicos permitidos.

Los Certificados de Firma Electrónica Avanzada emitidos por TSP SpA, en su calidad de Prestador de Servicios de Certificación (PSC), podrán ser utilizados conforme a las regulaciones establecidas en este documento (CP) y en la Declaración de Prácticas de Certificación (CPS).

El propósito fundamental de estos certificados es permitir al Titular la suscripción de documentos electrónicos garantizando su autoría, integridad y no repudio. Su uso es válido para todo tipo de actos y contratos, sean de carácter público o privado, abarcando fines personales, profesionales, empresariales, comerciales o tributarios, siempre respetando las limitaciones técnicas definidas en el campo "Usos de Clave" (Key Usage) del certificado.

6. Obligaciones CA, RA, titular y receptor

6.1. Obligaciones de la CA

Los certificados digitales, se organizan en una jerarquía de confianza, denominada cadena de certificación, comenzando desde la CA raíz o Root CA, esto permite ser utilizado para firmar los certificados de las entidades certificadoras subordinadas o Sub CA necesarias, en estos términos TSP SpA se define como entidad raíz y una entidad intermedia, porque ha emitido un certificado par ser utilizado por el mismo para su cadena de certificación.

En el caso que otras entidades de certificación se quieran subordinar (Sub CA) a la jerarquía de certificación de TSP SpA, éste último firmará los certificados emitidos.

En el ejercicio de sus funciones y en conformidad con lo dispuesto en el Artículo 12° y el Título VI de la Ley N° 19.799, la Autoridad de Certificación (CA) asume las siguientes obligaciones:

- **Cumplimiento de Políticas**: Respetar estrictamente lo estipulado en esta Política de Certificación (CP) y en la Declaración de Prácticas de Certificación (CPS) de Firma Electrónica Avanzada, así como lo dispuesto en el Contrato de Suscripción con el Titular.
- **Publicación de Documentos:** Publicar y mantener disponibles las Políticas (CP) y Prácticas de Certificación (CPS) vigentes en el sitio web de acceso público dispuesto para tal efecto.
- **Información de Modificaciones:** Informar a los Titulares y a la Entidad Acreditadora sobre modificaciones a los documentos normativos, publicando las versiones actualizadas en el sitio web de acceso público.
- **Cobertura de Responsabilidad:** Operar contando con un seguro de responsabilidad civil o garantía equivalente vigente, con cobertura por el valor mínimo exigido por el Artículo 14 de la Ley N° 19.799.
- **Sistemas Fiables:** Utilizar sistemas fiables para la emisión y el almacenamiento de los certificados, que permitan comprobar su autenticidad e integridad y garantizar la seguridad de los procesos.
- **Emisión Conforme:** Emitir certificados conforme a esta CP, a la CPS y a los estándares de aplicación vigentes, asegurando que se encuentren libres de errores de entrada de datos según la información verificada.
- **Contenido del Certificado:** Emitir certificados cuyo contenido mínimo sea el definido en el Artículo 15 de la Ley N° 19.799 y la normativa técnica aplicable.
- **Registro Público:** Publicar los certificados emitidos en un Registro de Certificados de acuerdo con el Artículo 12 de la Ley N° 19.799, respetando las disposiciones de la Ley N° 19.628 sobre Protección de la Vida Privada.

- **Revocación y CRL:** Suspender y revocar los certificados según lo dispuesto en la CPS y publicar dichas revocaciones en la Lista de Certificados Revocados (CRL) de manera oportuna.
- **Conservación de Registros:** Conservar la información del certificado y los registros de auditoría durante al menos 6 años desde la emisión inicial del mismo, de conformidad con el Artículo 12 de la Ley N° 19.799.
- **No Custodia de Claves:** No almacenar, ni copiar y no mantener custodia de los datos de creación de firma (llave privada) del Titular, garantizando su exclusivo control.
- **Protección de Claves de la CA:** Proteger sus propias claves privadas de forma segura mediante dispositivos criptográficos de alta seguridad (HSM).
- **Información al Titular (Título VI):** Cumplir con el deber de información establecido en el Título VI de la Ley N° 19.799, comunicando al Titular las condiciones, límites de uso y costos del servicio antes de la emisión del certificado.
- **Pago de Aranceles:** Pagar oportunamente el arancel de supervisión fijado anualmente por la Entidad Acreditadora, que comprende el costo del peritaje y del sistema de acreditación.
- **Gestión del Cese de Actividades:** En caso de cesar voluntariamente su actividad o solicitar la cancelación de su inscripción, deberá:
    - Comunicarlo a la Entidad Acreditadora con una antelación no inferior a un mes.
    - Comunicarlo a los Titulares con una antelación mínima de dos meses.
- Traspasar los datos de los certificados a otro prestador acreditado (salvo oposición del Titular) o dejarlos sin efecto si no es posible el traspaso.
- **Comunicación de Insolvencia:** Informar inmediatamente a la Entidad Acreditadora sobre el inicio de cualquier procedimiento de quiebra, cesación de pagos o circunstancia que impida la continuación de su actividad.
- **Publicación de Resoluciones:** Publicar en sus sitios de dominio electrónico las resoluciones de la Entidad Acreditadora que le afecten directamente.

6.2. La Autoridad de Registro (RA)

La Autoridad de Registro (RA), como entidad delegada responsable de la validación presencial y la relación directa con el usuario, asume las siguientes obligaciones:

- **Verificación de Identidad e Información:** Comprobar fehacientemente la identidad de los solicitantes de certificados de Firma Electrónica Avanzada (FEA) y verificar la exactitud y autenticidad de toda la documentación suministrada, garantizando el cumplimiento de los requisitos de validación presencial.
- **Gestión de Solicitudes en Terreno (Visitas):** En caso de realizar la validación en las dependencias del solicitante, la RA debe garantizar los mismos estándares de comprobación fehaciente de identidad, asegurando en todo momento la custodia y protección de los medios de enrolamiento y del dispositivo criptográfico (token) durante el traslado y la entrega.
- **Gestión Segura del Dispositivo Criptográfico:** Realizar la entrega del dispositivo criptográfico (Token FIPS 140-2 Nivel 3) al Titular bajo estrictos protocolos de seguridad.
- **Control de Seguridad en la Estación de Trabajo:** En los casos donde el procedimiento técnico implique la importación temporal del certificado al dispositivo, la RA tiene la obligación estricta de **eliminar el**

certificado y cualquier dato de creación de firma de manera inmediata y permanente del computador o notebook del operador una vez cargado en el token, asegurando que no existan copias no autorizadas.

- **Deber de Información (Título VI):** Informar claramente al solicitante, antes de la emisión del certificado, sobre las obligaciones del Prestador de Servicios de Certificación (PSC) y las responsabilidades que asume el futuro Titular, conforme al Título VI de la Ley N° 19.799.
- **Formalización Contractual:** Formalizar el proceso mediante la firma del Contrato de Suscripción con los solicitantes y respetar lo dispuesto en dichos contratos una vez que adquieran la calidad de Titulares.
- **Gestión Documental y Archivo:** Archivar y custodiar de forma segura los documentos y antecedentes suministrados por los solicitantes, manteniendo la confidencialidad e integridad de los expedientes de registro.
- **Tramitación del Ciclo de Vida:** Tramitar y entregar los certificados según lo estipulado en esta CP y en la CPS correspondiente, así como atender y procesar diligentemente las solicitudes de revocación y suspensión.
- **Comunicación con el Titular:** Mantener canales de comunicación efectivos con los Titulares para la correcta gestión del ciclo de vida de los certificados (notificaciones de expiración, renovación, etc.).

6.3. Obligaciones del Titular

Se considerarán al menos las siguientes obligaciones por parte del titular:

- Conservar y dar uso adecuado al certificado digital, según lo descrito en el contrato de suscripción.
- Dar correcta custodia al certificado, resguardar su clave privada y no dar mal uso al mismo.
- Proteger el uso de su certificado mediante PIN.
- Informar a TSP SpA inmediatamente por cualquier situación que afecte directamente la validez del certificado, o si su clave privada se ve comprometida.
- Entregar toda la información de identificación personal o de su empresa que se le solicite, a través de cualquier medio, tecnología o evidencia que se necesite para su correcta identificación y validación.
- El solicitante deberá cancelar la tarifa establecida y publicada en la página web https://firma.digital por el certificado que solicite.

6.4. Obligaciones de los Receptores

Los **Receptores** de documentos electrónicos firmados digitalmente están obligados a:

- Verificar que el certificado de firma electrónica avanzada utilizado se encontrara **vigente** en el momento exacto de la firma del documento electrónico.
- Verificar que el certificado utilizado para firmar no se encontrara **revocado ni suspendido** al momento de la firma. Para cumplir con esta verificación, el Receptor deberá consultar la Lista de Certificados Revocados (CRL) vigente o utilizar el servicio de validación en línea (OCSP) dispuesto por la Autoridad de Certificación.

7. Declaración de las garantías, seguros y responsabilidades de las partes

7.1. Garantías que entrega 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, TSP SpA ha contratado y mantiene un seguro, que cubre su eventual responsabilidad civil, por un monto equivalente a cinco mil unidades de fomento. Así mismo la PSC declara que no realizará ni soportará la homologación de certificados de firma electrónica emitidos por otros prestadores.

7.2. Garantías para Titular

Según lo declarado en el punto 7.1 Garantías de la PSC, el titular de certificados de TSP SpA, está cubierto por la póliza de responsabilidad civil ante eventuales daños y perjuicios ocasionados por los servicios de certificación de certificados de firma electrónica de TSP SpA.

7.3. Eximentes de responsabilidad

En ningún caso la Autoridad Certificadora será responsable de los daños que tengan origen en el uso indebido o fraudulento de un certificado de Firma Electrónica.

Un certificado de Firma Electrónica provisto por la Autoridad Certificadora podrá establecer límites en cuanto a los posibles usos del certificado, en cuyo caso, la Autoridad Certificadora quedará eximida de cualquier responsabilidad por el uso que se dé a dichos certificados y que excedan tales límites.

La Autoridad Certificadora quedará exenta de responsabilidad por el incumplimiento o retraso en sus obligaciones cuando este se deba a situaciones de Caso Fortuito o Fuerza Mayor, conforme a la definición y los alcances establecidos en el Artículo 45 del Código Civil.

Se considerarán bajo esta eximente aquellos imprevistos imposibles de resistir, tales como guerra, pandemia, desastres naturales, actos de autoridad, terremotos, interrupción generalizada de servicios básicos o cualquier otro evento ajeno al control razonable de la Autoridad Certificadora.

La Autoridad Certificadora no será responsable de los daños derivados de la ejecución defectuosa u omisión de las obligaciones que corresponden al solicitante, titular y/o usuario.

La Autoridad Certificadora no será responsable de la incorrecta utilización de los certificados y las llaves, ni de cualquier daño indirecto que pueda resultar de la utilización del certificado, o de la información suministrada por la Entidad Acreditadora. En particular, el lucro cesante y la pérdida de ingresos o pérdida de datos serán considerados daños indirectos y no darán lugar a indemnización alguna.

La Autoridad Certificadora no será responsable de los daños que se deriven de aquellas operaciones en que se hayan superado las limitaciones de uso que se señalan en estas políticas y las correspondientes Prácticas de Certificación de cada tipo de certificado.

La Autoridad Certificadora no será responsable de las eventuales inexactitudes en el certificado que sean producto de errores en la información personal o en los datos de creación de firma que hayan sido presentados o generados por el Titular en su solicitud de certificado.

7.4. Responsabilidades Financieras y Coberturas de Seguros

TSP SpA mantendrá vigente un seguro de responsabilidad civil, dando estricto cumplimiento a lo exigido en el Artículo 14° de la Ley N° 19.799.

Este instrumento tiene por objeto garantizar la cobertura de los daños y perjuicios que se ocasionen a los Titulares o terceros con motivo de la actividad de certificación de firmas electrónicas

7.5. Responsabilidad del Titular

El Titular del certificado asume las siguientes obligaciones y responsabilidades:

- **Recepción y Aceptación:** Descargar y almacenar el certificado en los dispositivos criptográficos autorizados (Token FIPS 140-2 Nivel 3) proporcionados y validados por la PSC, aceptando las condiciones de seguridad del dispositivo.
- **Deber de No Revelar: No revelar a terceros** bajo ninguna circunstancia el PIN, la clave de activación o los Datos de Creación de Firma (Clave Privada) contenidos en el dispositivo.
- **Deber de Custodia Diligente:** Custodiar el dispositivo criptográfico (Token) de forma diligente, tomando todas las precauciones razonables para evitar su pérdida, hurto, sustracción, modificación o uso no autorizado. El Titular se obliga a no dejar el dispositivo conectado o desatendido en equipos de acceso público o compartido.
- **Notificación Inmediata:** Notificar de inmediato al PSC sobre la pérdida, robo, hurto o posible falsificación del Certificado o del dispositivo, así como el conocimiento o sospecha de que terceros han accedido a su PIN o claves privadas.
- **Solicitud de Revocación:** Solicitar la revocación inmediata del Certificado a través de los canales dispuestos en la CPS cuando ocurra cualquier evento que comprometa la seguridad de su firma o cuando cambien los datos contenidos en el certificado.
- **Destrucción Segura:** Destruir o borrar de forma segura cualquier copia del Certificado o claves que queden en desuso o que hayan sido sustituidas, para evitar su uso posterior.

8. Protección de información

8.1. Confidencialidad (Ley N° 19.799)

En estricto cumplimiento con el inciso segundo del Artículo 23° de la Ley N° 19.799, TSP SpA garantiza que toda la información personal entregada por los titulares es de carácter confidencial. La Autoridad de Certificación (CA) se obliga a no utilizar esta información para fines distintos a los exclusivamente relacionados con la actividad de certificación.

8.2. Excepción de Publicidad

No obstante lo anterior, y para dar cumplimiento a la obligación estipulada en el Artículo 12° letra b) de la Ley N° 19.799 y su Reglamento, TSP SpA mantendrá un Registro de Acceso Público de Certificados. En este registro quedará constancia de los certificados emitidos, revocados y expirados.

Para estos efectos, se considerarán datos públicos aquellos contenidos en el certificado (Nombre, RUT, Correo y Clave Pública), los cuales estarán disponibles para consulta continua y regular por parte de terceros, con el único fin de validar la vigencia de las firmas electrónicas.

8.3. Tratamiento y Conservación de Datos

Los datos mencionados serán conservados por el PSC durante, a lo menos, seis (6) años desde la emisión inicial del certificado, tal como lo exige la normativa sectorial.

En todo lo no previsto por la Ley de Firma Electrónica, el tratamiento de datos personales se regirá supletoriamente por las disposiciones de la Ley N° 19.628 sobre Protección de la Vida Privada.

8.4. Política de Privacidad Formal y Publicación

Complementando las disposiciones legales anteriores, TSP SpA dispone de una **Política de Privacidad** formal donde se detallan los procedimientos específicos de resguardo, tratamiento y derechos de los usuarios sobre sus datos.

Este documento se encuentra publicado y disponible para consulta permanente de los usuarios y Titulares en el Repositorio de Prácticas, accesible directamente en el siguiente enlace: **https://repo.firma.digital/politica-privacidad.pdf**

TSP SpA informa sobre la existencia y ubicación de esta política en su sitio web público, asegurando que cualquier interesado pueda acceder a ella de manera clara y transparente.

8.5. Información Del Certificado

En conformidad con el Artículo 28 del Decreto Supremo N° 181, el certificado de firma electrónica avanzada emitido por TSP SpA contiene, al menos, los siguientes campos obligatorios de información de los Titulares: a) RUT (Rol Único Tributario). b) Correo electrónico verificado. c) Nombre completo del Titular (CN). d) Tipo de certificado y Usos (Key Usage). e) Identificación del Emisor (TSP SpA). f) Número de Serie y Período de Validez (Fecha de emisión y expiración).

8.6. Entrega De Información Sobre La Revocación Del Certificado

La información actualizada sobre el estado de vigencia, suspensión o revocación de un certificado emitido por TSP SpA se encuentra publicada de manera permanente y gratuita en el Repositorio Público (CRL/OCSP), accesible en la siguiente dirección web: **https://psc.firma.digital/**

8.7. Entrega De Información En Virtud De Un Procedimiento Judicial

TSP SpA levantará la confidencialidad de los datos y entregará la información requerida únicamente cuando exista una orden judicial formal emanada de los Tribunales de Justicia de la República de Chile o del Ministerio Público, en el marco de una investigación legal y conforme a los procedimientos establecidos en la normativa vigente.

8.8. Entrega De Información A Petición Del Titular

TSP SpA administra la información proporcionada por el propio solicitante y/o Titular. En cumplimiento con la Ley N° 19.628, el Titular tiene el derecho permanente de solicitar a TSP SpA el acceso, rectificación o actualización de sus datos personales almacenados, solicitud que será atendida conforme a los procedimientos internos de atención al cliente.

9. Suspensión y revocación de los certificados

9.1. Revocación

El PSC procederá a revocar el certificado a solicitud del Titular cuando este considere que la seguridad de su clave privada ha sido comprometida o por voluntad propia.

Las solicitudes de revocación podrán ser iniciadas a través de tres canales habilitados: Presencial, Web y Correo Electrónico. Para cada uno de ellos, TSP SpA exige un mecanismo de autenticación robusto que garantice la identidad del solicitante:

1. Canal Presencial: Requiere autenticación física. El solicitante debe comparecer ante un Operador de la Autoridad de Registro (RA), quien validará su identidad mediante la exhibición de la Cédula de Identidad vigente y verificación visual.

2. Canal Correo Electrónico: Requiere autenticación electrónica o ratificación. En caso de no poder firmar (por pérdida de clave), se requerirá la ratificación presencial descrita en el punto 1.
3. Canal Web: Requiere ratificación presencial obligatoria. Al no permitir una verificación de identidad fehaciente por sí mismo, toda solicitud ingresada por este medio deberá ser ratificada físicamente ante un Operador de la RA para completar el proceso de autenticación.

El detalle operativo, plazos y direcciones de estos canales se encuentran descritos en el numeral 9.1.3 de este documento.

9.1.1. Posibles causas de revocación

- Solicitud del titular.
- Pérdida del certificado o alteración del elemento donde almacena el certificado.
- Fallecimiento del titular o de algún representado, término de la representación de la persona jurídica.
- Por alguna eventualidad que comprometa la llave privada del titular, ya sea por robo, alteración, divulgación o cualquier otro tipo de causal circunstancial.
- Por incumplimiento de suscripción, por parte de la CA o el titular.
- Por resolución judicial o administrativa.
- Por cualquier otro motivo, que exponga claramente o ponga en riesgo la llave privada del titular, o no se cumpla de alguna forma el contrato de suscripción.

9.1.2. Formas de revocación

La revocación se genera mediante solicitud previa, canalizada a través de los medios dispuestos en la CPS para estos efectos.

De conformidad con la definición de Titular establecida en el numeral 3.1, la solicitud de revocación podrá ser realizada por:

1. El Titular del certificado (persona natural).
2. El Representante Legal de la persona jurídica (institución o empresa) a la cual se encuentre vinculado el Titular en el certificado, quien deberá acreditar sus facultades para solicitar dicha revocación.

9.1.3. Canales de atención y procedimiento operativo

TSP SpA pone a disposición del Titular canales presenciales y remotos para gestionar la revocación o suspensión de sus certificados. Dependiendo del canal utilizado, se aplicarán distintos procedimientos de validación para garantizar la seguridad de la operación.

1. Canal Presencial (Validación Inmediata) Es el procedimiento estándar para Titulares que no tienen acceso a sus mecanismos de firma o para Representantes Legales.

- Procedimiento: El solicitante debe concurrir personalmente a las oficinas de TSP SpA o puntos de atención autorizados.
- Validación: El Operador de Registro verificará la identidad mediante la Cédula de Identidad vigente y, en caso de ser un tercero (Representante Legal), verificará además los poderes legales correspondientes. Una vez validado, la revocación se ejecuta de inmediato.

2. Canales Remotos (Sujetos a Ratificación) TSP SpA habilita canales digitales para iniciar la solicitud. Sin embargo, por seguridad y para evitar suplantaciones, estas solicitudes requieren una ratificación presencial posterior.

- A. Vía Correo Electrónico:
  - Acción: El Titular debe enviar un correo a soporte@firma.digital o revocacion@firma.digital indicando Nombre completo, RUT y motivo.
  - Requisito: Idealmente, el correo debe venir firmado digitalmente con el certificado a revocar (si el Titular aún posee control de este).
  - Ratificación: El Titular dispone de un plazo máximo de 48 horas hábiles para concurrir a las oficinas de TSP SpA con su cédula de identidad y ratificar la solicitud.
- B. Vía Formulario Web:
  - Acción: Completar el formulario disponible en https://psc.firma.digital/revocacion-suspension con los datos obligatorios (RUT, Nombre, Correo, Motivo).
  - Ratificación: Dado que este canal no permite verificar fehacientemente la identidad por sí solo, es obligatorio que el Titular concurra a las oficinas de TSP SpA con su cédula de identidad vigente para ratificar la solicitud en un plazo máximo de 48 horas hábiles.

Caducidad de la Solicitud Remota: Si el Titular no realiza la ratificación presencial dentro del plazo establecido (48 horas hábiles), la solicitud remota podrá ser desestimada por seguridad, debiendo iniciar el trámite nuevamente..

9.1.4. Publicación de la revocación

El acto de revocación será comunicado al Titular, indicando el origen y motivo de la decisión, a través del correo electrónico registrado.

Simultáneamente, la información sobre el estado de vigencia o revocación de los certificados se hará pública y estará disponible para terceros a través de los siguientes mecanismos, en concordancia con el documento técnico "TB02 - Estructura CRL y servicio OCSP":

1. Lista de Certificados Revocados (CRL): Disponible en: https://crl.firma.digital/firmadigitalFEA-G2.crl Conforme a los requisitos de acreditación (TB03), la CRL se actualizará y publicará diariamente (con una periodicidad mínima de 24 horas) o inmediatamente tras generarse una revocación crítica, asegurando la disponibilidad de la información actualizada.

2. Protocolo de Estado en Línea (OCSP): Disponible en: http://ocsp.firma.digital/status Este servicio permite la validación en tiempo real del estado del certificado, informando si este se encuentra "válido", "revocado" o "desconocido" de manera inmediata, sin la latencia de actualización de la CRL.

En caso de término de actividades de la Autoridad de Certificación (CA), se emitirá y publicará una última CRL con la totalidad de los certificados revocados, la cual se mantendrá disponible hasta la expiración del último certificado emitido.

9.2. Caducidad

Una vez finalizado el período de vigencia establecido, el certificado caducará de forma automática.

TSP SpA notificará anticipadamente al Titular vía correo electrónico antes de la fecha de vencimiento, con el fin de que este pueda gestionar su renovación de manera oportuna.

La expiración del plazo produce la invalidez inmediata del certificado, cesando desde ese momento su aptitud para generar nuevas firmas electrónicas válidas, sin perjuicio de las obligaciones de custodia y consulta de registros históricos que mantiene el Prestador de Servicios de Certificación.

9.3. Renovación

El procedimiento de renovación, se ejecuta cuando el certificado está próximo a caducar y el titular decide su renovación con la misma CA. Para dicho caso, TSP SpA emitirá un nuevo certificado y se generarán nuevas llaves, requiriendo verificar previamente la vigencia de la validación del titular, cuya vigencia es a lo más de 3 años, o bien generar una nueva verificación de identidad. Los certificados emitidos por TSP SpA tienen una vigencia que no podrá exceder de tres años contados desde la fecha de emisión; y para su renovación se debe cumplir:

- Que exista actividad de certificación previa en esta CA por parte del titular y emitido por TSP SpA.
- Que el titular solicite en los tiempos adecuados y preventivos para la renovación, y esta solicitud sea enviada a TSP SpA en los procedimientos declarados para esos efectos.
- Que la CA verifique que no exista una revocación previa del certificado original.
- Que el titular pueda hacer todas las actividades necesarias para solicitar la emisión de un certificado.

9.3.1. Solicitud de renovación

Para renovación de certificados digitales, se utilizará el mismo proceso de solicitud de certificado, desde la página web. Si se cumplen los requisitos para la emisión.

9.3.2. Procedimiento de renovación

Una vez recibida la solicitud y verificado que cumple con los requisitos. Se procesará la solicitud de la misma forma como se procesan los demás certificados.

- La CA emitirá el certificado solicitado
- La emisión del certificado generará un correo electrónico al solicitante. En el correo se informará que el certificado está disponible y que puede operar con su certificado en línea o ser descargado desde el sitio web.

Cabe destacar que para la verificación del titular se realizará lo siguiente:

- Se verificará la vigencia de la verificación de identidad almacenada, que confirma la identidad del suscriptor, requiriendo un nuevo procedimiento de enrolamiento si se considera vencida.
- Si está vencida se considera el mismo procedimiento descrito en el apartado de registro inicial.

9.4. Suspensión

La Suspensión procede cuando el Titular pierde temporalmente el acceso o control de sus datos de creación de firma (llave privada), sin que exista certeza de que su seguridad haya sido comprometida. Las solicitudes de suspensión deberán tramitarse utilizando los mismos canales y mecanismos de autenticación descritos en el numeral 9.1 de la presente Política (presencial , correo electrónico o formulario web), para garantizar la identidad del titular.

Aceptada la solicitud, el PSC procederá a la suspensión inmediata de la vigencia del certificado. Conforme al Artículo 33 del Decreto Supremo N° 181, esto conlleva el cese temporal de los efectos jurídicos del certificado. Durante este período, el certificado será incluido en la Lista de Certificados Revocados (CRL) con el código de razón correspondiente a "Suspensión" (Certificate Hold).

Levantamiento de la Suspensión: Si el Titular recupera el control de sus claves y confirma que no hubo compromiso de seguridad, podrá solicitar el levantamiento de la suspensión. Una vez verificada la identidad del Titular (bajo los mismos estándares del numeral 9.1), el PSC procederá a retirar el certificado de la CRL, restableciendo su plena vigencia y validez hasta su fecha de expiración original.

9.5. Concordancia de la Política de Certificación con los procedimientos operacionales

Los procedimientos operacionales de la PSC se hayan estructurados para dar cumplimiento a las declaraciones y garantías de la Declaración de Prácticas de Certificación (CPS). Ésta, a su vez, es la concreción de la Política de Certificación aplicada a las distintas CA de la PSC.

De esta manera, los procedimientos operacionales consideran, entre otros:

- **Política de Seguridad**: elaborada para alcanzar el nivel de seguridad declarado por la PSC en este documento.
- **Política de Gestión del Riesgo**: elaborada para alcanzar el nivel de seguridad declarado por la PSC en este documento.
- **Plan de Recuperación de Desastres**: elaborado para mantener la continuidad operacional declarada por la PSC en este documento.

- **Plan de Seguridad de la Información**: elaborado para alcanzar el nivel de seguridad de la información declarado por la PSC en este documento.
- **Implementación del Plan de Seguridad de la Información**: elaborado para alcanzar el nivel de seguridad de la información declarado por la PSC en este documento.
- **Plan de Administración de Llaves Criptográficas**: elaborado para que la gestión de las llaves criptográficas de la PSC pueda cumplir con los estándares de seguridad y continuidad declarados en este documento.
- **Plan de Seguridad Física**: elaborado para que las instalaciones de la PSC permitan alcanzar el nivel de seguridad declarado por la PSC en este documento.
- **Manual de Operaciones de la Autoridad Certificadora**: elaborado para alcanzar el nivel de seguridad y de continuidad operacional de la certificación digital, revocación y suspensión declarado por la PSC en este documento.
- **Manual de Operaciones de la Autoridad de Registro**: elaborado para alcanzar el nivel de seguridad y de continuidad operacional de la certificación digital, revocación y suspensión declarado por la PSC en este documento.
- **Procedimiento de Contratación de Personal**: elaborado para que el personal de la PSC pueda asegurar el nivel de seguridad declarado por la PSC en este documento.

9.6. Término de actividades de la CA

En el caso del cese de actividades de la CA se declaran las siguientes medidas:

- Comunicación preventiva del cese de actividades:
    - Notificación vía Web.
    - Publicación de anuncio de cese en al menos dos diarios de divulgación nacional.
    - Toda información se realizará con al menos 60 días antes de la fecha indicada de cese definitivo.
- Se traspasarán todas las obligaciones y derechos de los certificados a otra PSC existente, bajo el pleno consentimiento del titular.
- Si no es posible traspasar los certificados, se revocarán.
- Se indemnizará a los titulares que lo soliciten por sus certificados revocados con fecha anterior a la fecha de vigencia del mismo, con tope el costo del servicio descontando los días de vigencia hasta la fecha de revocación.

9.7. Auditorías

TSP SpA podría contar con procesos de auditoría internos y de terceros cada vez que permitan asegurar, mantener y mejorar contínuamente los altos niveles de seguridad en sus procesos.

Los procedimientos y frecuencia de las Auditorías de la Entidad Acreditadora dependiente del Ministerio de Economía están regidos por las guías de acreditación y a lo informado en la página web www.entidadacreditadora.gob.cl.

9.8. Administración y modificaciones

TSP SpA podrá realizar actualizaciones a la presente Política de Certificación (CP) fundamentadas en razones técnicas, comerciales o jurídicas, con el fin de mantener la mejora continua del servicio.

Sin embargo, en estricto cumplimiento con lo señalado en el Artículo 18° de la Ley N° 19.799, cualquier modificación sustancial que altere las condiciones generales bajo las cuales se otorgó la acreditación, será informada oportunamente a la Entidad Acreditadora para su conocimiento y registro, antes de su entrada en vigencia.

Aprobación del Documento: La responsabilidad de revisar, validar y aprobar las modificaciones a este documento recae exclusivamente en la Gerencia General de TSP SpA. Ningún cambio será oficial ni publicado sin la firma o autorización formal de dicha instancia.

9.9. Publicación de modificaciones

Publicación en Repositorio (Art. 12 Ley 19.799) Para dar cumplimiento a las letras a), b) y d) del Artículo 12° de la Ley N° 19.799, toda modificación aprobada a la CP o CPS será publicada de manera inmediata en el sitio web de acceso público de TSP SpA, disponible en: https://psc.firma.digital/

Notificación a la Entidad Acreditadora (Art. 18 Ley 19.799) En concordancia con el Artículo 18° de la Ley N° 19.799, las modificaciones que alteren las condiciones de acreditación serán informadas a la Entidad Acreditadora para su conocimiento y registro.

Plazos y Aceptación Tácita (Concordancia CPS 10.3) Todo cambio que involucre la operación de los certificados será informado vía Web a los Titulares y solicitantes. Conforme a lo establecido en el punto 10.3 de la CPS:

1. Las modificaciones se comunicarán en un período no superior a 15 días desde la aplicación de los cambios.
2. Transcurrido dicho plazo tras el comunicado, si no se recibe ninguna declaración por escrito de oposición por parte de los Titulares, las modificaciones se declararán como aceptadas tácitamente por la comunidad de usuarios y entrarán en plena vigencia.

.

9.10. Información de contacto

Para consultas respecto del contenido del presente documento, pueden ser realizadas vía correo o de forma presencial:

- URL: https://psc.firma.digital/
- Dirección de contacto: Puerta Oriente 361, Oficina 409, Torre B, Puertas de Chicureo, Colina, Región Metropolitana.
- Correo electrónico: soporte@firma.digital

10. Referencias

Para la elaboración de la presente Política de Certificación y la prestación de los servicios, se han considerado como referencia fundamental las Normas Técnicas y Resoluciones vigentes registradas y publicadas por la Entidad Acreditadora.

Dichos documentos constituyen el marco regulatorio técnico obligatorio para la emisión y gestión de Certificados de Firma Electrónica Avanzada (FEA) y se encuentran disponibles para su consulta en el sitio oficial: **https://www.entidadacreditadora.gob.cl/normas-tecnicas/**

- ETSI TS 102 042 V1.1.1 (2002-04). Technical Specification. Policy requirements for certification authorities issuing public key certificates.
- NCh2805.Of2003 Tecnología de la Información – Requisitos de las políticas de las autoridades certificadoras que emiten certificados de claves públicas.
- ETSI TS 102 042 V1.2.2 (2005-06) .RTS/ESI-000043.Keywords e-commerce, electronic signature, public key, security.
- ETSI TS 102 042 V2.1.1 (2009-05). Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- ETSI TS 102 042 V2.1.2 (2010-04) Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- NCh27002.Of2009 Tecnología de la información – Código de práctica para la gestión de seguridad de la información.
- ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model
- FIPS PUB 140-2: Security Requirements for Cryptographic Modules (mayo 2001).
- NCh.2820/1.Of2003 Tecnología de la información – Técnica de seguridad – Criterio de evaluación de la seguridad de TI – Parte 1: Introducción y modelo general.
- NCh2832.Of2003 Tecnología de la información – Protocolos operacionales de infraestructura de clave pública LDAPv2 para Internet X.509.
- RFC 2559 BOEYEN, S. et al., “Internet X.509 Public Key Infrastructure. Operational Protocols LDAPv2”, Abril 1999.
- RFC 3377 LDAPv3: Technical Specification, September 2002, Lightweight Directory Access Protocol (v3): Technical.