Ministerio de Economía, Fomento y Turismo

Gobierno de Chile

Subsecretaría de Economía y Empresas de Menor Tamaño

Guía de Evaluación
Procedimiento de Acreditación Prestadores de Servicios de Certificación

Servicio de Certificación de Firma Móvil

- Documento Número : EA-106
- Versión : 1.1
- Estado : Versión Final
- Fecha de Emisión : 08/02/2013

Contenido

1. ANTECEDENTES

1.1. RESUMEN

Este documento presenta los detalles del procedimiento de acreditación de los Prestadores de Servicios de Certificación (PSC) establecido por el Ministerio de Economía, Fomento y Turismo (Ex Ministerio de Economía Fomento y Reconstrucción) de Chile en conformidad a la Ley N°19.799 y su Reglamento. Los requisitos que debe cumplir un PSC para obtener la acreditación, aseguran el nivel mínimo de confiabilidad que requiere el sistema.

Como una forma de generar, adicionalmente, compatibilidad con organizaciones equivalentes en otros países, los criterios se basan en estándares internacionales homologados por el organismo normalizador chileno, Instituto Nacional de Normalización (INN) o por fijación, modificación o derogación de norma técnicas según procedimiento indicado en el nuevo Artículo 5°, según modificación del reglamento DS181.

Este documento debería ser usado por un PSC, para identificar los requisitos y estándares que deben cumplir sus procesos de negocios, políticas, recursos, procedimientos y tecnologías para obtener la certificación que lo acredite para emitir certificados digitales de firma electrónica avanzada en conformidad a la Ley N°19.799.

1.2. INTRODUCCIÓN

Para que el país dinamice su economía y alcance un liderazgo en materia tecnológica en la región, que permita acceder a mayores oportunidades de bienestar y progreso para sus ciudadanos, el Gobierno de Chile definió en el año 2000 una Agenda de Impulso de las Nuevas Tecnologías de la Información constituida por cinco áreas de acción: desarrollo de la infraestructura de información, impulso al comercio electrónico, promoción de la industria de contenidos, impulso al uso de nuevas tecnologías en aras de un mejor servicio público, masificación del acceso a Internet y aceleración del aprendizaje social en el uso de redes.

Dando cumplimiento a dicha agenda, el lunes 25 de marzo de 2002 el presidente de la República, S.E. Sr. Ricardo Lagos Escobar promulgó la Ley N°19.799 sobre documento electrónico, firma electrónica y servicios de certificación de dicha firma, cuerpo que regula las operaciones comerciales que se realicen en Chile a través de Internet, con el fin de establecer un marco legal que otorga a los actos y contratos celebrados por medios electrónicos el mismo reconocimiento y protección que gozan los contratos tradicionales, celebrados en formato papel.

La formulación de dicha ley es consecuencia del desarrollo tecnológico alcanzado en el ámbito local y global, donde la criptografía, la certificación y la firma electrónica son utilizadas para proveer privacidad, integridad del contenido, autenticación del origen y no

desconocimiento de la operación, y cuyo propósito fundamental es proveer seguridad tanto en las transacciones realizadas vía Internet como en el intercambio de documentos electrónicos en Intranets, Extranets, redes privadas o cualquier medio de almacenamiento o comunicación electrónico.

Considerando el rol de esta Ley de proveedor de seguridad al mundo Internet, ella resulta ser un pilar fundamental para el desarrollo del gobierno y del comercio electrónico y, dentro de este ámbito, de los medios de pago electrónico.

Del mismo modo la interoperabilidad resulta indispensable en un mundo globalizado, escenario que exige que se asegure la compatibilidad del sistema nacional de firma electrónica con los estándares internacionales (inc. 2° artículo 1° Ley N°19.799).

En este contexto la confianza en las entidades que prestan servicios de certificación, es la base sobre la cual se cimienta el sistema y es el motivo por el cual el proceso de acreditación de los prestadores tiene especial importancia.

En año 2004 se modifica la Ley N°19.799 que incorpora la posibilidad de agregar a los documentos el Sello de Tiempo, dando así una validez legal al documento de cuando este se firma.

El sábado 11 de agosto de 2012 aparece publicado en el Diario Oficial por orden del presidente de la República, S.E. Sr. Sebastián Piñera Echenique, la modificación al Decreto N° 181, de 2002, incorporando principalmente los nuevos estándares de Seguridad asociado a la Firma Electrónica Avanzada y la certificación de dicha firma.

2. CRITERIOS DE ACREDITACIÓN

2.1. OBJETIVO DE LA ACREDITACIÓN

El objetivo de la acreditación es asegurar la existencia de un sistema de certificación de firma electrónica avanzada confiable que asegure su continuidad en el tiempo y que sirva de base para el desarrollo tecnológico del país.

2.2. DEFINICIONES

Los requisitos y obligaciones de acreditación están fijados en la Ley, el Reglamento y sus posteriores modificaciones.

La Entidad Acreditadora sólo evaluará el cumplimiento de los requisitos y obligaciones. No será parte de su función recomendar medidas correctivas o proponer planes para subsanar el incumplimiento de estos requisitos.

Los criterios de acreditación estarán definidos con base en el cumplimiento del conjunto de requisitos y obligaciones definidas por la Ley y el Reglamento vigentes.

Cada requisito será evaluado individualmente, en conformidad a un procedimiento y una escala predefinida.

2.3. CRITERIOS GENERALES DE ACREDITACIÓN

2.3.1. TRANSPARENCIA

El proceso de acreditación pondrá a disposición pública toda la información necesaria requerida para conocer el estado del sistema de certificación acreditado por el Gobierno de Chile, con el propósito de proveer confianza a los usuarios y generar las condiciones y los acuerdos necesarios para el desarrollo de la actividad en conformidad a las normas y acuerdos internacionales que se celebren.

2.3.2. INTEROPERABILIDAD INTERNACIONAL

Los requerimientos del proceso de acreditación deberán fomentar la compatibilidad del sistema nacional de firma electrónica con los estándares internacionales, en la medida que ello sea posible, permitiendo así la interoperabilidad internacional del sistema.

Debemos tener presente también la existencia de otra clase de interoperabilidad, como por ejemplo; la interoperabilidad con los usuarios y en concordancia con los Decretos Supremos 83 y 77.

2.3.3. GRADUALIDAD

Los niveles de exigencia del proceso de acreditación serán graduales y se irán adaptando desde un estado inicial en el que las exigencias apuntarán a cumplir estándares suficientes que provean confianza en el sistema y compatibles con la realidad nacional, hasta el cumplimiento estricto de los estándares internacionales a medida que el desarrollo de la actividad lo requiera.

2.3.4. INDEPENDENCIA

Como una forma de asegurar la independencia de los entes reguladores, la Entidad Acreditadora y los evaluadores no podrán ser partícipes directos del proceso de generación de servicios de certificación ni tener vínculos contractuales con estas organizaciones.

2.3.5. NEUTRALIDAD TECNOLÓGICA

Se considera fundamental promover el desarrollo tecnológico del sistema de certificación y así un mejoramiento de la calidad de los servicios, por lo cual no existirá preferencia hacia una tecnología en particular. Los Prestadores podrán introducir cambios tecnológicos siempre que estos cumplan con la normativa, se notifiquen a la Entidad Acreditadora y sean aprobados por ella.

Nuestra legislación consagra el principio de la neutralidad tecnológica, ello supone no regular un proceso de identificación en sí misma, sino disponer de ella en forma general, creando un ordenamiento común para todos los medios de identificación electrónica, cualquiera que sea el proceso de identificación.

En síntesis, es una regulación abierta que no establece limitantes en el uso de una tecnología en particular, en la medida que cumpla con las condiciones básicas.

2.3.6. PRIVACIDAD

La realización de un proceso de acreditación riguroso requiere de información estratégica o altamente sensible de parte de los Prestadores. Se entiende por información sensible la contemplada en el artículo 2° de la Ley N°19.628 letra g) que señala "*g) Datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual*."

Por lo anterior, la Entidad Acreditadora se compromete a no usar ni divulgar la información entregada por el Prestador, clasificada como confidencial, más que para los fines propios del procedimiento de acreditación. Este compromiso es extensible a todo Organismo y persona que intervenga en el proceso de acreditación.

Lo anterior se debe enmarcar en el contexto de la ley N°19.628 sobre protección de la vida privada. Allí en virtud del artículo 1° que dispone que el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, ello obliga tanto a la Entidad Acreditadora como a los PCS a mantener la debida reserva de la información que gestionen en virtud de sus funciones.

En concordancia con La ley N°19.628 y los artículos 21° y 12° letras b), c), g), h) y j) de la Ley N°19.799

El artículo 21° de la ley N°19.799 señala expresamente que "*La Entidad Acreditadora, así como el personal que actúe bajo su dependencia o por cuenta de ella, deberá guardar la confidencialidad y custodia de los documentos y la información que le entreguen los certificadores acreditados*."

Por otra parte, el artículo 12° de la ley N°19.799, señala "*Son obligaciones del prestador de servicios de certificación de firma electrónica:*

b) 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 Nº 19.628, sobre Protección de la Vida Privada;

c) En el caso de cesar voluntariamente en su actividad, los prestadores de servicios de certificación deberán comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificadas por ellos, de la manera que establecerá el reglamento y deberán, de no existir oposición de estos últimos, transferir los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad;

g) Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Entidad Acreditadora, con una antelación no inferior a un mes cuando vayan a cesar su actividad, y comunicarle el destino que dará a los datos de los certificados, especificando, en su caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto;

h) En caso de cancelación de la inscripción en el registro de prestadores acreditados, los certificadores comunicarán inmediatamente esta circunstancia a cada uno de los usuarios y deberán, de la misma manera que respecto al cese voluntario de actividad, traspasar los datos de sus certificados a otro prestador, si el usuario no se opusiere;

i) Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento"

2.4. ACREDITACIÓN

Se otorgará la acreditación al Prestador de Servicios de Firma Móvil solicitante en los siguientes casos:

1. Si cumple plenamente los requisitos establecidos, de acuerdo a los criterios de evaluación definidos en la Guía de Acreditación de Firma Electrónica Avanzada.

2. Adicionalmente Si cumple plenamente los requisitos establecidos, de acuerdo a los criterios de evaluación definidos en esta Guía Específica de Firma Móvil.

3. Cuando no cumple todos los requisitos, pero son calificados como subsanables por la Entidad Acreditadora, previa aprobación de un plan de medidas correctivas que permita al Prestador de Servicios de Firma Móvil subsanar plenamente los incumplimientos en un plazo razonable.

No se otorgará la acreditación al Prestador de Servicios de Firma Móvil solicitante en el siguiente caso:

1. Cuando no cumple alguno de los requisitos definidos y se determina que no es subsanable o afecta el correcto funcionamiento del sistema o los fines previstos en la Ley para la firma electrónica avanzada.

2.5. CUMPLIMIENTO DE REQUISITOS

El Prestador de Servicios de Firma Móvil deberá demostrar el cumplimiento de los requisitos de acreditación mediante los siguientes medios:

1. Acompañando los antecedentes que exige la Ley, su Reglamento y la Guía de Evaluación a la solicitud de acreditación.

1. Presentando la documentación e información solicitada por la Autoridad Acreditadora dentro de los plazos establecidos en el procedimiento de acreditación y evaluación.

2. Permitiendo el libre acceso a los expertos designados por la Entidad Acreditadora, para la auditoría.

3. Entregando cualquier información adicional pertinente solicitada por la Entidad Acreditadora durante el proceso de acreditación.

Adicionalmente el Prestador de Servicios de Firma Móvil podrá entregar, si lo desea, información que permita reforzar su postulación, la cual podrá ser del siguiente tipo:

4. Documentos descriptivos generados por el PSC que permitan apoyar la comprobación de un requisito.

5. En los casos que sea pertinente y que la Entidad Acreditadora lo autorice, mediante la presentación de una auditoría externa realizada por una consultora independiente.

La presentación de uno o varios de estos medios de prueba dependerá del requisito en particular al que se esté haciendo alusión. La Entidad Acreditadora entregará guías y documentos modelo para orientar el cumplimiento de cada requisito.

2.6. PRELACIÓN DE REQUISITOS

En caso de que existan en esta guía criterios de evaluación discrepantes o contrapuestos con los requerimientos que se establecen en la Ley N°19.799, su Reglamento o las normas técnicas aplicables prevalecerán estos últimos por sobre los dispuestos en esta Guía.

En aquellos casos que la norma técnica definida no especifique aspectos que deban ser evaluados, el Evaluador podrá utilizar referencias o especificaciones que estén reconocidas por la industria. En los casos que esto ocurra se incorporará en la guía de evaluación la individualización del documento utilizado.

2.7. SISTEMA DE ACREDITACIÓN

La Ley N°19.799 y su Reglamento determinan mediante su normativa un sistema de acreditación Prestadores de Servicios de Certificación que involucra las siguientes entidades:

2.7.1. ENTIDAD ACREDITADORA (A)

El proceso de acreditación de un PSC será desarrollado por la Subsecretaría de Economía y Empresas de Menor Tamaño (Ex Subsecretaría de Economía, Fomento y Reconstrucción) quién se puede apoyar en expertos para realizar la evaluación de dichas entidades (Art. 14° Reglamento).

Además, deberá velar porque los requisitos y obligaciones que se observaron al momento de otorgarse la acreditación se mantengan durante la vigencia de la acreditación (Art. 15° Reglamento).

Para ello podrá requerir información y ordenar auditorías a las instalaciones del PSC inspeccionado, sin previo aviso, ya sea personalmente o por medio de las entidades evaluadoras (Art. 15° Reglamento).

La información solicitada por la Entidad Acreditadora deberá ser proporcionada dentro del plazo de 5 días, contado desde la fecha de la solicitud del requerimiento, sin perjuicio del otorgamiento de plazos especiales atendida la información requerida (Art. 15° Reglamento).

2.7.2. ENTIDAD DE NORMALIZACIÓN (B)

El Instituto Nacional de Normalización (INN) a solicitud de la Entidad Acreditadora procederá a la generación u homologación de normas según sea el caso, las que una vez realizado el proceso pasarán a ser parte del conjunto de normas técnicas vigentes.

2.7.3. ENTIDAD EVALUADORA/AUDITORA (C)

Corresponde a una o más instituciones o expertos que cuenten con la capacidad técnica para realizar el proceso de evaluación, las cuales serán designadas por la Entidad Acreditadora, en caso de ser necesario.

El proceso de evaluación y auditoría será el procedimiento por el cual la Entidad Acreditadora verificará el cumplimiento de la Ley y la normativa técnica vigente, tanto para los PSC acreditados como para los que solicitan acreditación, respectivamente.

2.7.4. PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC) (D)

Corresponde a la entidad emisora de certificados de firma electrónica, la cual solicita ser acreditada (Ley 19.799 artículo 1°, letra c) en servicios de Firma Móvil.

2.7.5. REGISTRO DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN ACREDITADOS (E)

Es un registro público que mantiene la Entidad Acreditadora, en el cual están identificados los PSC acreditados.

2.7.6. NORMAS TÉCNICAS (F)

Es el conjunto de normas vigentes que debe cumplir el Prestador de Servicios de Certificación para ser acreditado por la Entidad Acreditadora, además de los requisitos y obligaciones establecidas explícitamente en la Ley y su Reglamento.

En la Figura 1 se presenta el esquema general de la interacción de las entidades/procesos que intervienen en este proceso, actualizado según modificación de Reglamento N°181 (2012).

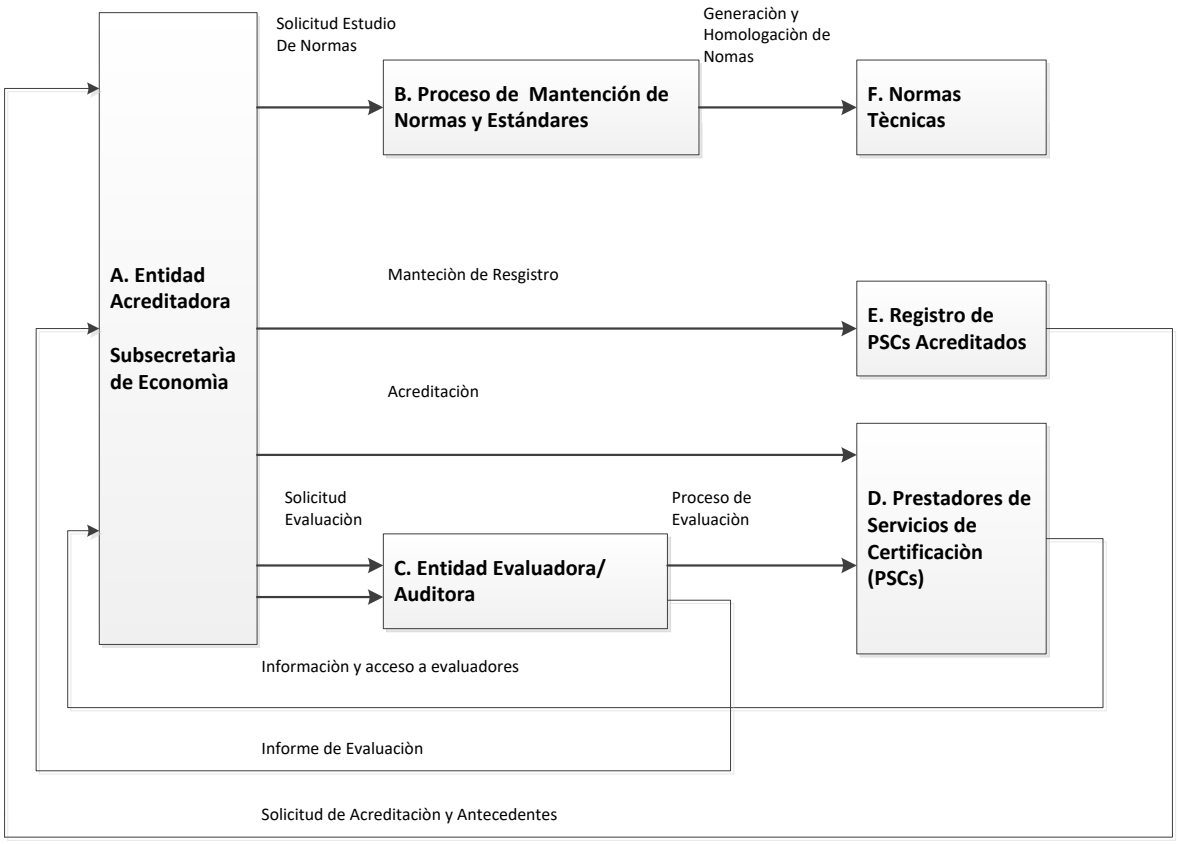


Figura 1: Esquema del sistema de acreditación de PSC.

2.8. PROCEDIMIENTO DE ACREDITACIÓN

El procedimiento de acreditación que se define en la Ley y el Reglamento se describe a continuación y se resume en la Figura 2 (Reglamento Art. 17°):

1. Presentar solicitud de acreditación a la Entidad Acreditadora acompañada del comprobante de pago de los costos de acreditación y los antecedentes que permitan verificar el cumplimiento de lo dispuesto en los párrafos 1° y 2° del Reglamento DS181, exceptuando la póliza de seguro a que hace referencia el artículo 14 de la Ley.

2. La entidad solicitante deberá individualizarse debidamente indicando:
    a. Nombre o razón social de la empresa solicitante
    b. RUT de la empresa solicitante
    c. Nombre del representante legal de la empresa solicitante
    d. RUT del representante legal de la empresa solicitante
    e. Domicilio social
    f. Dirección de correo electrónico

3. El solicitante deberá acompañar al menos los siguientes documentos:
   a. Toda la documentación definida en las Guías de Evaluación para cada uno de los requisitos especificados.
   b. Presentar los procedimientos previstos para asegurar el acceso a los peritos o expertos (Reglamento DS181 Art. 14)
   c. Y adicionalmente, Copia del contrato de los servicios externalizados, si los hay.

4. Verificación de la admisibilidad de la solicitud. La Entidad Acreditadora revisará únicamente que se encuentren presentados todos los antecedentes requeridos. De ser inadmisible la solicitud, dentro de 3° día hábil procederá a comunicar al interesado de dicha situación, pudiendo completar los antecedentes dentro de 15 días, bajo apercibimiento de ser rechazada.

5. Admitida la solicitud, la Entidad Acreditadora procederá a evaluar el cumplimiento de los requerimientos expresados en la Ley, el Reglamento DS181 y su Modificación 2012 y sus disposiciones transitorias. La Prestadora de Servicios de Certificación solicitante deberá facilitar el acceso de los funcionarios o expertos que la Entidad Acreditadora designe para realizar las evaluaciones además de proporcionar cualquier información adicional solicitada por él.

6. Realizada la evaluación la Entidad Acreditadora procederá a pronunciarse sobre si se cumplen los requisitos y obligaciones exigidas en la Ley y el Reglamento DS181 y su Modificación 2012 para otorgar la acreditación dentro de los 90 días siguientes a la Solicitud, prorrogables por razones fundadas.

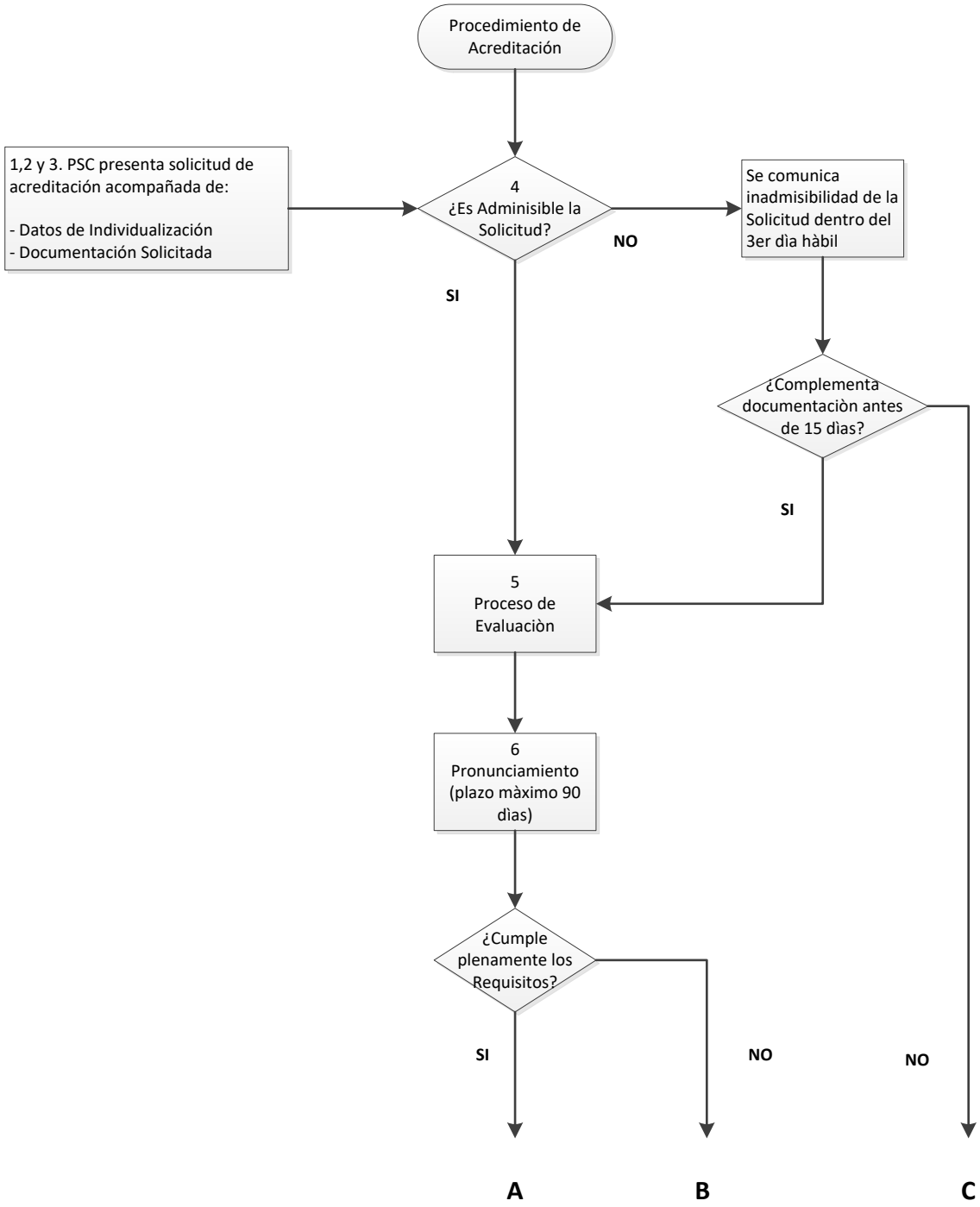
7. En el caso de no cumplir con los requisitos y obligaciones de acreditación definidos por la Ley y el Reglamento DS181 y su Modificación 2012, esto es, que existan requisitos que como resultado de la evaluación se determine que no sean subsanables, dicha Entidad procederá a dictar una resolución en la que rechaza la solicitud de acreditación mencionando los requisitos que se consideran no subsanables.

8. En el caso que la Entidad Acreditadora determine como resultado de la evaluación que los incumplimientos que presenta el PSC solicitante son subsanables y no afectan el correcto funcionamiento del sistema ni los fines previstos en la Ley para la firma electrónica, dicha Entidad procederá a entregar un documento indicando los requisitos incumplidos que se deben subsanar.

9. Una vez recepcionado el plan de medidas correctivas propuesto por el PSC, la Entidad Acreditadora procederá a evaluar dicho plan. En caso de no ser aprobado dicho plan la Entidad Acreditadora procederá a dictar una resolución en la que rechaza la solicitud de acreditación mencionando los requisitos que se consideran no subsanables.

10. En caso de ser favorable la evaluación de acuerdo a los criterios de acreditación definidos en el artículo 17 del Reglamento DS181 y especificados en este documento, la Entidad Acreditadora procederá a informar al Prestador de Servicios de Firma Móvil solicitante que debe presentar la póliza de seguros exigida en el artículo 14 de la Ley, dentro del plazo de 20 días para que su solicitud quede en estado de ser aprobada.

11. Si el PSC cumple con este último requisito dentro del plazo estipulado, la Entidad Acreditadora procederá a acreditar al interesado en el plazo de veinte días contados desde que, a petición del interesado, se certifique que la solicitud se encuentra en estado de resolverse.


Procedimiento de Acreditación
1,2 y 3. PSC presenta solicitud de acreditación acompañada de:
- Datos de Individualización
- Documentación Solicitada
4
¿Es Adminisible la Solicitud?
NO
Se comunica inadmisibilidad de la Solicitud dentro del 3er dìa hàbil
SI
¿Complementa documentaciòn antes de 15 dìas?
SI
5
Proceso de Evaluaciòn
6
Pronunciamiento (plazo màximo 90 dìas)
¿Cumple plenamente los Requisitos?
SI
NO
NO
A
B
C

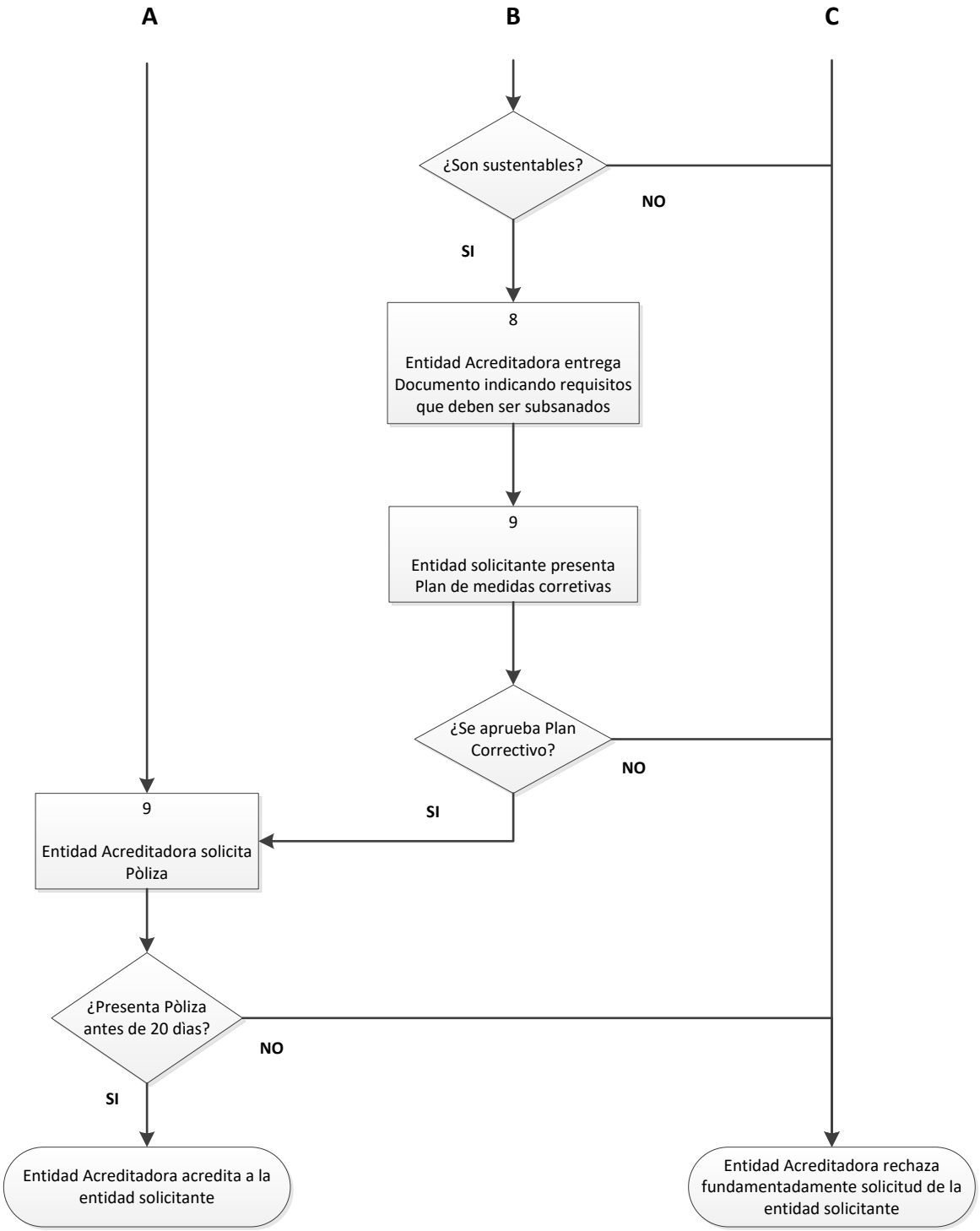


Figura 2: Diagrama de flujos que describe el proceso de acreditación de los PSC de Firma Móvil

2.9. PROCESO DE MANTENCIÓN DE NORMAS TÉCNICAS

El procedimiento de mantención de normas se define en el artículo 5° del Nuevo Reglamento N°181 (2012), el cual se describe a continuación y se resume en la Figura 3.

> *"Artículo 5°. A petición de parte o de oficio, la Entidad Acreditadora podrá iniciar el procedimiento de fijación, modificación o derogación de normas técnicas para la prestación del servicio de certificación de firma electrónica avanzada.*
>
> *Dicho procedimiento se iniciará notificando a cada uno de los prestadores de servicios de certificación acreditados acerca del objeto y propuestas de modificación o fijación de normas técnicas, otorgando un plazo no inferior a 30 días hábiles para que aquellas efectúen las observaciones que estimen pertinentes. Además, la Entidad Acreditadora deberá publicar en su sitio Web, por igual período, el objeto y propuesta de normas técnicas.*
>
> *Las observaciones efectuadas por los prestadores de servicios de certificación acreditados no serán vinculantes para la Entidad Acreditadora.*
>
> *Vencido el plazo para las observaciones, la Entidad Acreditadora evaluará las observaciones recibidas y determinará las normas técnicas que serán fijadas, modificadas o derogadas, las cuales serán puesta a disposición de la ciudadanía para su consulta de acuerdo a lo dispuesto por el artículo 73 de la Ley 20.500, y serán aprobadas mediante resolución fundada del Subsecretario de Economía y Empresas de Menor Tamaño.*
>
> *De ser necesario, se podrá fijar conjuntos alternativos de normas técnicas para la prestación del servicio con el objeto de permitir el uso de diversas tecnologías y medios electrónicos, en conformidad a la Ley y el presente reglamento.*
>
> *Si la fijación, modificación o derogación de normas técnicas relativas a la compatibilidad de documentos electrónicos, técnicas y medios electrónicos con firma electrónica aplicables a los órganos del Estado requiere recursos adicionales o la coordinación de diversos entidades para su implementación, la resolución que aprueba las normas técnicas deberá ser firmada además por los Subsecretarios de Hacienda y del Ministerio Secretaría General de la Presidencia*.".

2.9.1. DIAGRAMA DEL PROCESO DE MANTENCIÓN DE NORMAS TÉCNICAS

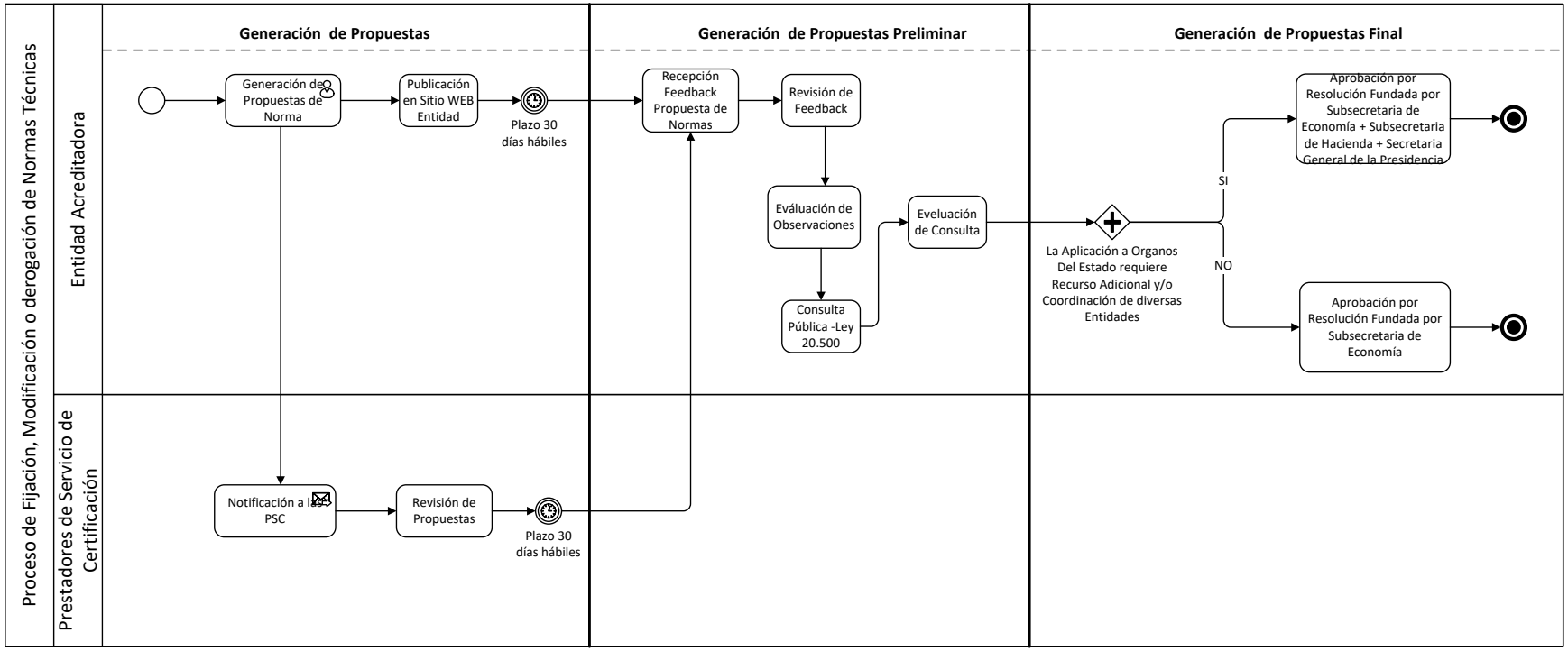


Figura 3: Proceso de Mantención de Normas Técnicas.

3. EVALUACIÓN

3.1. OBJETIVO DE LA EVALUACIÓN

El objetivo general de la evaluación es verificar el cumplimiento de los requisitos y obligaciones que impone la Ley, el Reglamento y la Guía de evaluación al Prestador de Servicios de Certificación que solicita la acreditación.

3.2. ESCALA DE EVALUACIÓN

Cada requisito será evaluado en conformidad a la siguiente escala:

Calificación	Descripción
A	El PSC de Firma Móvil cumple totalmente el requisito exigido.
A-	El PSC de Firma Móvil no cumple totalmente el requisito pero se determina que el incumplimiento es subsanable y no afecta el correcto funcionamiento del sistema ni los fines previstos en la Ley para la firma electrónica avanzada
B	El PSC de Firma Móvil no cumple el requisito y se determina que no es subsanable o afecta el correcto funcionamiento del sistema o los fines previstos en la Ley para la firma electrónica avanzada.

El objetivo de la calificación A- es permitir al PSC de Firma Móvil modificar los aspectos negativos que son subsanables en un corto periodo de tiempo y así optar a la acreditación durante su primera postulación.

3.3. ESQUEMA DE EVALUACIÓN

La verificación del cumplimiento de los requisitos se realizará en conformidad a un procedimiento, que tendrá los siguientes elementos:

1. Revisión de antecedentes.
2. Visitas a las instalaciones para verificar antecedentes, en los casos que sea necesario.
3. Evaluación de la información obtenida.
4. Elaboración de informe.

Para facilitar el proceso de acreditación se han definido clases de requisitos basados en los requerimientos generales descritos en la Ley N°19.799 y su Reglamento. La evaluación permite a la Entidad Acreditadora determinar si el PSC que postula a la acreditación ha

implementado una infraestructura y procedimientos operacionales que provean la necesaria confianza al sistema, y si puede entregar un servicio confiable y duradero.

La Entidad Acreditadora ha considerado necesario para algunos requisitos, acompañar un Anexo de evaluación. El objetivo del Anexo de evaluación es permitir al PSC conocer los requisitos mínimos que debiera cumplir para demostrar a la Entidad Acreditadora el cumplimiento de los requisitos de acreditación.

Los criterios establecidos en este documento evalúan sólo los servicios de Firma Móvil asociado a una Firma Electrónica Avanzada.

3.4. AUDITORIAS

La Entidad Acreditadora realizará inspecciones periódicas para asegurar la conservación en el tiempo del sistema de certificación. Para esto podrá contar con peritos.

3.5. CAMBIOS A LOS CRITERIOS

El contenido de estos criterios puede cambiar en el tiempo, dependiendo de los avances de la tecnología y consideraciones de seguridad nacional. Si existiera alguna duda respecto a la actualización de estos criterios, debe contactarse con la Entidad Acreditadora.

Cualquier PSC acreditado será notificado de los cambios de este documento. Si el cambio es considerado significativo, el proceso de revisión incorporará consultas con la industria y consumidores.

3.6. COSTOS

Todos los costos incurridos en el proceso son responsabilidad de la organización o persona jurídica que solicita la acreditación, los que serán cubiertos con el arancel de acreditación fijado por la Subsecretaría de Economía y Empresas de Menor Tamaño.

3.7. REQUISITOS DE ACREDITACIÓN

Los requisitos mínimos necesarios para que un Prestador de Servicios de Certificación obtenga la acreditación de servicio de Firma Móvil en conformidad a lo expresado en la Ley N°19.799, su Reglamento y las normas técnicas aplicables son los siguientes:

3.7.1. TB TÉCNICOS BÁSICOS

Son aquellos requisitos técnicos específicos contenidos en la Ley N°19.799 y su Reglamento DS181. Estos incluyen los siguientes aspectos:

- Estructura e información del certificado de firma electrónica avanzada.

- Estructura e información de la lista de certificados revocados (CRL)
- Servicios, información y accesibilidad del registro público del PSC de Firma Móvil.
- Modelo de confianza.

3.7.2. PS SEGURIDAD

Son aquellos requisitos que permiten determinar los niveles de seguridad que dispone el PSC para presentar sus servicios. Están relacionados con la valoración de riesgos y amenazas, la implementación de medidas de seguridad, planes de recuperación de desastres y su coherencia con las prácticas y política de certificación.

3.7.3. ET EVALUACIÓN TECNOLÓGICA

Es el conjunto de requisitos relacionados con el cumplimiento de estándares de la plataforma tecnológica de emisión de certificados de firma electrónica avanzada y datos de creación de firma utilizada por el PSC en su actividad.

3.7.4. SF SEGURIDAD FÍSICA

Son los requisitos relacionados con el aseguramiento de áreas restringidas, equipos e información y las condiciones ambientales que permiten mantener el servicio ante amenazas físicas de la infraestructura.

3.7.5. PO POLÍTICA DEL PSC DE FIRMA MÓVIL

Es el conjunto de requisitos relacionados con la implementación de la declaración de prácticas de certificación y la política del certificado de firma móvil.

3.7.6. AD ADMINISTRACIÓN DEL PSC DE FIRMA MÓVIL

Son los requisitos relacionados con la especificación de las operaciones y gestión de certificación y registro, la asignación de funciones y responsabilidades del personal, los planes de entrenamiento, etc.

3.8. TABLA I: RESUMEN REQUISITOS DE ACREDITACIÓN

Requisito	Clase	Nombre	Dependencia	Normas y Anexos	Documentación solicitada
TB05	Tecnológico Básico	Uso de Dispositivos Móviles	Ninguno	ETSI TR 102 203. Anexo 38. Anexo 41.	Documentación de Uso de Firmas Móviles
TB06	Tecnológico Básico	Niveles de protección ofrecido para el proceso de una Firma Móvil	TB05	ETSI TR 102 206. Anexo 37. Anexo 39.	Documento descriptivo de los niveles de protección ofrecido
TB07	Tecnológico Básico	Proceso de generación de Firma Móvil	Ninguno	ETSI TR 102 203. Anexo 36. Anexo 42.	Documento descriptivo de servicio de Firma Móvil
PS01	Seguridad	Documentación y mantención de la política de seguridad	Ninguna	ISO 27.002. Anexo 1. Anexo 2.	Política de Seguridad
PS02	Seguridad	Gestión de Riesgos y Amenazas	PS01	ISO 27.001. ISO 27.005. Anexo 3.	Plan de gestión de Riesgos
PS03	Seguridad	Plan de Continuidad del Negocio y Recuperación de Desastres	PS02	ISO/IEC 27.002. ETSI TS 102 042. BS25.999. Anexo 4. Anexo 18.	1. Plan de Continuidad de Negocios 2. Plan de Recuperación de Desastres
PS04	Seguridad	Plan de un Sistema de Gestión de Seguridad de la Información resultante de PS02 y de acuerdo al marco PS01	PS02	ISO 27001. ISO 27002. Anexo 8. Anexo 9. Anexo 17.	Plan de un Sistema de Gestión de Seguridad de la Información.

Requisito	Clase	Nombre	Dependencia	Normas y Anexos	Documentación solicitada
PS07	Seguridad	Gestión de Incidentes de Seguridad de la Información	PS01	ISO 27.001. Anexo 23. Anexo 25.	Plan de gestión de Incidente de Seguridad de la Información
ET01	Evaluación Tecnológica	Evaluación y Certificación de la Plataforma Tecnológica del Servicio de Firma Móvil	TB, PS03, PS04, PS05	ETSITS 102 042. FIPS 140-2. ISO/IEC 15408. Anexo 35. Anexo 36. Anexo 40. Anexo 43.	Cumplimiento Certificación con estándares
SF01	Seguridad Física	Seguridad Física de la Infraestructura del PSC	PS03	ISO/IEC 27.002. Anexo 19.	Documentación relevante
PO01	Política del PSC de Firma Móvil	Política de Firma Móvil	PS03, ET01	ETSI TS 102 042. RFC 3647. Anexo 6. Anexo 20	Documento de la Política de Firma Móvil
PO02	Política del PSC de Firma Móvil	Declaración de Prácticas de Firma Móvil	PO01	ETSI TS 102 042. RFC 3647. Anexo 7. Anexo 20.	Documento de las Prácticas de Firma Móvil
PO03	Política del PSC de Firma Móvil	Modelo Operacional de la Autoridad de Firma Móvil	PO01	Anexo 40. Anexo 43. Anexo 44.	Documento del modelo operacional de la Autoridad de Firma Móvil
AD01	Administración de la PSC de Firma Móvil	Manual de operaciones de la Autoridad de Firma Móvil	PS03	Anexo 45.	Manual de operaciones de la Autoridad de Firma Móvil

4. REQUISITOS DE ACREDITACIÓN

4.1. REQUISITO TB05 – USO DE DATOS DE FIRMA MÓVIL

4.1.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Uso de Datos de Firma Móvil
Objetivo	Comprobar los aspectos mínimos que disponen la Ley y su Reglamento DS181 con relación a la conformidad con el estándar en el uso de los Datos de Firma Móvil
Descripción	El uso de datos que conforma el Dato de Firma móvil utilizado por el PSC debe estar en conformidad al formato de caso de uso definido en el estándar ETSI TR 102 203
Referencias en Ley N°19.799 o su Reglamento	Modificación Reglamento DS181 (2012)
Dependencias	Ninguna
Estándares de evaluación	ETSI TR 102 203
Documentación solicitada	Ninguna
Evidencias solicitadas	Documentación de Caso de Uso del Dato en el Servicio de Firma Móvil, utilizado por el PSC para apoyar el uso certificado de firma electrónica. Cumplimiento de Requerimiento Obligatorios de Negocio y Funcional del Servicio Firma Móvil

4.1.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	**Evaluación**
Uso del Dato de Firma Móvil utilizado por el PSC	Se verificará que el Caso de Uso del Dato en el Servicio de Firma está de acuerdo según el estándar ETSI TR 102 203. • Cumplimiento de la especificación
Requerimientos de Negocio del Servicio de Firma Móvil utilizado por el PSC	Se verificará que los requerimientos del Negocio obligatorios del Servicio de Firma Móvil está de acuerdo según el estándar ETSI TR 102 203. • Cumplimiento de Requerimientos de Negocio Mandatorios
Requerimientos Funcionales del Servicio de Firma Móvil utilizado por el PSC	Se verificará que los requerimientos Funcionales obligatorios del Servicio de Firma Móvil están de acuerdo según el estándar ETSI TR 102 203. • Cumplimiento de Requerimientos Funcionales Mandatorios

4.2. REQUISITO TB06 –NIVELES DE PROTECCIÓN OFRECIDOS PARA EL PROCESO DE FIRMA MÓVIL

4.2.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Niveles de Protección del Proceso de Firma Móvil
Objetivo	Comprobar los aspectos mínimos que su Reglamento DS181 modificación 2012 con relación a la conformidad con el estándar ETSI TR 102 206
Descripción	Se debe establecer los niveles de protección ofrecidos para el Proceso de Firma Móvil utilizado por el PSC
Referencias en Ley N°19.799 o su Reglamento	ETSI TR 102 206
Dependencias	Ninguna
Estándares de evaluación	Ninguna
Documentación solicitada	Ninguna
Evidencias solicitadas	Documentación de los Niveles de Protección ofrecidos por la PSC para proteger el proceso de Firma Móvil, utilizado por el PSC para apoyar el uso certificado de firma electrónica

4.2.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	**Evaluación**
Marco General de Seguridad de Firma Móvil	Se verificará los elementos que participan en el servicio de firma móvil
Niveles de Protección de Sistema de Creación de Firma Móvil (MSCS)	Se verificará los niveles de protección del proceso de Firma Móvil utilizados por el PSC, en las siguientes componentes del MSCS • DTBS Datos para Ser Firmado • TC Canal Confiable • UN-P Proceso no-confiable • IC Control de Entrada
Niveles de Protección de Aplicación de Creación de Firma Móvil (MSCA)	Se verificará los niveles de protección del proceso de Firma Móvil utilizados por el PSC, en las siguientes componentes del MSCA • SDP Presentación del Documento del Firmante • SAV Visor de Atributo de Firma • SIC Componente de Interacción del Firmante

Aspecto	Evaluación
	• SAC Componente de Autenticación del Firmante • DAC Comunicador MSCD/MSCA • PAC Comunicador MSSP/MSCA
Niveles de Protección de Proveedor del Servicio de Firma Móvil (MSSP)	Se verificará los niveles de protección del proceso de Firma Móvil utilizados por el PSC, en las siguientes componentes del MSSP • DTBSV Verificador de Datos para ser Firmado • DTBSF Formato de Datos para ser Firmado • DHC Componente de Hashing del Dato • SDOC Compositor de Objeto de Dato Firmado • CSPC Componente de Interacción del CSP • SLC Componente de Registro de Firma • PAC Comunicador MSSP/MSCA • MAC Comunicador MSSP/AP
Niveles de Protección de Dispositivo de Creación de Firma Móvil (MSCD)	Se verificará los niveles de protección del proceso de Firma Móvil utilizados por el PSC, en las siguientes componentes del MSCS • UAC Componente de Autenticación del Usuario • SCC Componente de Creación de Firma

4.3. REQUISITO TB07 – PROCESO DE GENERACIÓN DE FIRMA MÓVIL

4.3.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Proceso de Generación de Firma Móvil
Objetivo	Comprobar los aspectos mínimos que disponen la Ley y su Reglamento DS181 modificación 2012 con relación a la conformidad con el estándar en el proceso de firma móvil
Descripción	Se debe establecer el Proceso de Generación ofrecidos para el Proceso de Firma Móvil utilizado por el PSC
Referencias en Ley N°19.799 o su Reglamento	Reglamento DS181
Dependencias	Ninguna
Estándares de Evaluación	Ninguna
Documentación Solicitada	Ninguna
Evidencias solicitadas	Documentación del Proceso de Generación ofrecidos por la PSC para el proceso de Firma Móvil, utilizado por el PSC para apoyar el uso certificado de firma electrónica

4.3.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	**Evaluación**
Descripción General del Servicio	Se verificará el servicio de Firma Móvil Utilizados por el PSC Documento que explicite el servicio general de firma móvil, en aspecto tales como: • descripción general • ámbito de uso • niveles del servicio • métricas del servicio
Descripción del Proceso de Firma Móvil	Se verificará el proceso de firma móvil utilizado por el PSC en lo que respecta Descripción de los Requerimientos del Servicio. • Sensibilización • Adquisición de Firma Móvil • El uso de Firma Móvil • Administración del ciclo de vida de la firma móvil • Servicio al Cliente

Aspecto	**Evaluación**
Descripción Especifica de Servicio firma Móvil	Se verificará el Servicio de firma móvil especifico utilizado por el PSC en lo que respecta Descripción de los Requerimientos del Servicio, según los siguientes aspectos. • Proveedor de Aplicación • Usuario • Servicio de Valor Agregado • Servicio de Gestión de Ciclo de Vida • Servicio al Cliente
Roles y Responsabilidades en el Servicio de Firma Móvil	Se verificará el Servicio de firma móvil los roles identificados en los procesos de las firmas móviles y responsabilidades de las entidades que podrían ser involucradas.

4.4. REQUISITO PS01 – REVISIÓN DE LA EVALUACIÓN DE RIESGOS Y AMENAZAS

4.4.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Revisión de la Evaluación de Riesgos y Amenazas
Objetivo	Determinar la consistencia del análisis de riesgos y amenazas del plan de negocios del PSC de Firma Móvil
Descripción	Dado que el producto principal de un PSC es la "confianza", el requerimiento fundamental para un PSC es demostrar una clara comprensión de las amenazas de seguridad enfrentadas por el negocio y poder mostrar planes efectivos para reducir el riesgo residual a un nivel aceptable. El objetivo principal de un proceso de Gestión del riesgo en una organización debe ser proteger la organización, su capacidad de cumplir con su misión y no impactar en forma significativo los objetivos Organizacionales. La Gestión del Riesgo incluye los siguientes procesos: - Establecimiento del contexto: Se definen los objetivos, alcance y la organización para todo el proceso. - Identificación de riesgos: Consiste en determinar qué puede provocar pérdidas en la organización. - Estimación de riesgos: Utilizar métodos cuantitativos o cualitativos para obtener una cuantificación de los riesgos identificados, teniendo en cuenta los activos, amenazas y salvaguardas. - Evaluación de riesgos: Se comparan los riesgos estimados con los criterios de evaluación y aceptación de riesgos definidos en el establecimiento del contexto - Tratamiento de riesgos: Se define la estrategia para tratar cada uno de los riesgos valorados; reducción, aceptación, evitación o transferencia. - Aceptación de riesgos: Se determinan los riesgos que se decide aceptar y su justificación correspondiente - Comunicación de riesgos: Todos los grupos de interés intercambian información sobre los riesgos. - Monitorización y revisión de riesgos: El análisis de riesgos se actualiza con todos los cambios internos o externos que afectan a la valoración de los riesgos. El resultado debe ser un compromiso razonable entre los costos económicos y operacionales de las medidas de protección, y obtener mejoras en la capacidad de lograr la misión de la organización.

Referencias en Ley Nª19.799 o su Reglamento	Ley N°19.799 Art. 17 a) Reglamento DS181, Art. 16 a. Disposición transitoria
Dependencias	Ninguna
Estándares de evaluación	ISO 27.001, ISO 27.005
Documentación solicitada	Copia del documento correspondiente a la Evaluación de Riesgos

4.4.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	**Evaluación**
Reporte de la valoración de riesgos[1][2]	Verificar que los riesgos considerados sean reales. Verificar que riesgos relevantes no hayan sido omitidos. Verificar la valoración adecuada de los riesgos. Verificar si hay un plan de mantención de la valoración
Estructura del proceso de Gestión de riesgos	Verificar que el proceso de gestión de Riesgos ha sido realizado o auditado por un ente externo independiente y calificado

[1]Guide for Conducting Risk Assessments, Special Publication 800-30 Revision 1, Recommendations of the National Institute of Standards and Technology, September 2012.

[2]ISO/EIC 27.005: 2008, Information technology — Security techniques — Information security risk management, 2008-08-05

4.5. REQUISITO PS02 – POLÍTICA DE SEGURIDAD

4.5.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Documentación y Mantención de la Política de Seguridad de la Información.
Objetivo	Comprobar a través de este documento que la organización tiene claros los objetivos de seguridad relevantes para el negocio y que las instancias de gestión del PSC de Firma Móvil apoyan formalmente esta política.
Descripción	La política de seguridad es una declaración de objetivos de seguridad. Solo contiene objetivos de seguridad que son factibles de lograr a través de acciones, procedimientos y mecanismos implementados por el PSC. Si el PSC externaliza en otra organización algún aspecto de seguridad o confianza, entonces debe indicarse claramente. La política de seguridad deberá cumplir a lo menos con los siguientes requerimientos: • Los objetivos de seguridad deben ser consecuencia de la Evaluación de Riesgos y Amenazas, de forma tal que los objetivos de la política de seguridad y sus defensas asociadas correspondan al nivel de riesgo requerido para que un PSC sea un ente de confianza. • Debe estar basada en las recomendaciones del estándar ISO 27.002 sección 5. • Los objetivos de la política son de alto nivel y no técnicos. Por lo tanto, debe ser lo suficientemente general para permitir alternativas de implementación tecnológica. • Si la complejidad de los objetivos así lo requieren, la política puede estar conformada por más de un documento; esto es, puede haber una política general soportada por políticas específicas. • Los elementos de la política de seguridad que estén incorporados tanto en la Declaración de Prácticas de Certificación (CPS) como la Política de los Certificados de firma electrónica avanzada (CP) deben estar incluidos en este documento. Se recomienda que este documento identifique los objetivos de seguridad relevantes y las amenazas potenciales relacionadas a los servicios suministrados, así como las medidas tomadas para evitar o limitar los efectos de estas amenazas. Adicionalmente, se recomienda que la documentación

	describa las reglas, directivas y procedimientos que indican como son provistos los servicios específicos y las medidas de seguridad asociadas. Para los propósitos de la acreditación de un PSC, algunos de los aspectos más relevantes han sido incorporados en criterios separados para así facilitar el proceso de evaluación y donde estos se detallan completamente. Por ello, este documento puede expresar en forma general aquellos aspectos de la seguridad organizacional que se tratan en documentos específicos.
Referencias en Ley Nº19.799 o su Reglamento	Ley N°19.799 Art. 17 a) Reglamento DS181, Art. 16
Dependencias	PS01
Estándares de evaluación	ISO/IEC 27.002, Sección 5
Documentación solicitada	Copia del documento correspondiente a la Política de Seguridad de Información de la Organización.
Evidencias solicitadas	Auditoría en terreno que permita verificar aspectos relevantes.

4.5.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	**Evaluación**
Conformidad con el estándar ISO 27.002 sección 5.1.1	Verificar que los requerimientos de la sección 5.1.1, están incorporados.
Conformidad con el estándar ISO 27.002 sección 5.1.2	Verificar que se ha incluido un procedimiento de revisión y evaluación periódico de la política de seguridad.
Consistencia entre la política de seguridad y CPS	Verificar la consistencia de la política de seguridad con la CPS.
Consistencia entre la política de seguridad y la CP	Verificar la consistencia de la política de seguridad con la CP de firma avanzada.
Relación entre la Evaluación de Riesgos y la política de seguridad	Verificar que los principales aspectos de la política de seguridad son coherentes con los niveles de riesgo determinados en la evaluación formal de riesgos.

Aspecto	Evaluación
Inclusión de las secciones atingentes indicadas[3] [4]	Verificar que los elementos fundamentales de una política de seguridad están incluidos en el documento.
Claridad de los objetivos de seguridad	Verificar que se establecen objetivos de seguridad claros y relacionados con la protección de los procesos de negocios, activos y servicios del PSC de Firma Móvil.

[3]SANS Institute: Information Security Policy - A Development Guide for Large and Small Companies, http://www.sans.org/reading_room/whitepapers/policyissues/1331.php, 2006

[4]SANS Institute: Information Security Policy Templates. http://www.sans.org/security-resources/policies/

4.6. REQUISITO PS03 – PLAN DE CONTINUIDAD DEL NEGOCIO

4.6.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Plan de Continuidad del Negocio y Recuperación de Desastres
Objetivo	Comprobar a través de este documento que la organización tiene planes establecidos para disminuir a un nivel aceptable el efecto de interrupciones del servicio del PSC de Firma Móvil, mediante una combinación de controles preventivos y planes de contingencia
Descripción	El Plan de Continuidad del Negocio (BCP) y Recuperación de Desastres (DRP), debe describir cómo los servicios serán restaurados en el evento de desastres, una caída de los sistemas o fallas de seguridad. Su objetivo es disminuir a un nivel aceptable el efecto de interrupciones del servicio del PSC de Firma Móvil. Tales planes deben ser mantenidos y probados periódicamente y debieran ser parte integral de los procesos de la organización. En general, para lograr la implantación de proceso de Gestión de Continuidad de negocios se debe alinear con la BS2599 que establece dicho proceso. En particular, el documento describe la prioridad de restauración para asegurar la continuidad de los negocios de terceros que sean dependientes de la operación del PSC de Firma Móvil. Este documento debe ceñirse a los lineamientos dados por: • Estándar ISO 27.002 en su sección 14 y • Estándar ETSI TI 102 042 en su sección 7.4.8 Este documento también deberá describir los procedimientos de emergencia a ser seguidos en a lo menos los siguientes Escenarios: • Desastre que afecte el funcionamiento de los productos de software en el cual el PSC basa sus servicios, • Incidente o posible incidente de seguridad que afecte la operación del sistema en el cual el PSC basa sus servicios, • Compromiso de la llave privada de firma del PSC de Firma Móvil, • Falla de los mecanismos de auditoría, • Falla en el hardware donde se ejecuta el producto en el cual el PSC basa sus servicios (incluyendo servidores, dispositivos criptográficos, dispositivos de seguridad y dispositivos de comunicaciones) Parte del plan de manejo de contingencias es el Análisis de

	Impacto en los Negocios (BIA), siendo esta una evaluación del efecto de las interrupciones no planificadas en el negocio. El plan deberá además incluir mecanismos para la preservación de evidencia de mal uso de los sistemas, cuyo propósito es proporcionar evidencia admisible en una corte judicial en alguna fecha posterior
Referencias en Ley Nº19.799 o su Reglamento	Ley N°19.799 Art. 17 a) Reglamento DS181, Art. 16 a. Disposición transitoria.
Dependencias	PS02 - Revisión de Análisis de Riesgos y Amenazas. PO02 – Declaración de Prácticas de Certificación.
Estándares de evaluación	ISO 27.002, Sección 14 BS25999 o ISO 22301 ETSI TI 102 042, sección 4.7.8
Documentación solicitada	Documento correspondiente al Plan de Continuidad de Negocios y Recuperación ante Desastres Documento de Evaluación de Riesgos
Evidencias solicitadas	Auditoría en Terreno

4.6.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	**Evaluación**
Conformidad con el estándar ISO 27.002 sección 14.1.1 al 14.1.4	Verificar que los requerimientos de la sección 14, están incorporados.
Conformidad con el estándar ISO 27.002 sección 14.1.5	Verificar que se ha incluido un procedimiento de revisión y evaluación periódico de los planes de continuidad de Negocios.
Conformidad con el estándar ETSI TI 102 042 sección 7.4.8	Verificar que el plan incorpora procedimientos especialmente detallados para el caso de compromiso de la llave privada de firma tal como lo indica el estándar ETSI
Relación entre la Evaluación de Riesgos y el BCP y DRP[5] [6] [7]	Verificar que los principales aspectos de los planes son coherentes con los niveles de riesgo determinados en una evaluación formal de riesgos.

[5]ISO 22301:2012, Business Continuity Management.

[6]NIST Special Publication 800-34 Rev.1 Contingency Planning Guide for Federal Information Systems, Mayo 2010

[7]BS 25999-1:2006, Business continuity management. Code of practice.

Aspecto	Evaluación
Bussines Impact[8] Analysis	Verificar la coherencia del Análisis de Impacto en los Negocios, que debe ser parte del plan de manejo de contingencias.
Viabilidad de las facilidades computacionales alternativas	Verificar que las facilidades computacionales alternativas consideradas en el plan, cumplen con los requerimientos mínimos para la operación del PSC de Firma Móvil.
Elementos de auditoría	Verificar que el sistema en el cual el PSC basa sus servicios provee mecanismos de preservación de los elementos de auditoría.

[8] http://www.thebci.org/

4.7. REQUISITO PS04 – PLAN DE SEGURIDAD DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

4.7.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Plan de Seguridad de un Sistema de Gestión de Seguridad de la Información.
Objetivo	Comprobar a través de este documento que la organización tiene un plan de seguridad coherente con su Política de Seguridad, que permita mostrar un nivel de confianza consistente con los objetivos del negocio.
Descripción	El Plan de Seguridad de un Sistema de Gestión de Seguridad de la Información tiene como propósito entregar una descripción de los requerimientos de seguridad de los sistemas y describir los controles desplegados o planificados para satisfacer dichos requerimientos. Adicionalmente, debiera delinear las responsabilidades y conductas esperadas de los individuos que acceden al sistema. Por lo tanto, el Plan de Seguridad de un Sistema de Gestión de Seguridad de la Información debiera describir las acciones operacionales, procedimientos y mecanismos que permitan lograr los objetivos indicados en la Política de Seguridad del PSC, posteriormente esto debe permitir cumplir con un Sistema de Gestión de Seguridad de la Información como lo establece la ISO 27001 El PSC deberá mostrar que su proceso de gestión de la seguridad de la información y la capacidad de administrar las instalaciones está de acuerdo con el Plan de Seguridad. El plan de seguridad tendrá que considerar a lo menos las secciones 5 a 15 del estándar ISO 27002. Sin embargo, en este requisito se evaluarán en particular los siguientes aspectos: • Seguridad Organizacional • Control y clasificación de activos • Administración de las comunicaciones • Control de accesos • Mantención y desarrollo de sistemas Se considera que este Plan es una declaración de intenciones del PSC, por lo que la evaluación bajo este requisito no es una certificación de su nivel de seguridad. El proceso de evaluación bajo este requisito indica el nivel de confiabilidad del PSC si este cumple con el plan de seguridad.

Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799 Art. 17 a) Reglamento Art. 16 a. Disposición transitoria
Dependencias	PS02
Estándares de evaluación	ISO/IEC 27001 ISO/IEC 27002
Documentación solicitada	Copia del documento correspondiente al Plan de Seguridad de Información de la Organización.

4.7.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	**Evaluación**
Relación entre el Plan de Seguridad y los recursos asignados[9]	Verificar que el PSC puede justificar la disponibilidad de los recursos y capacidades para implementar los mecanismos y procedimientos de seguridad.
Relación entre Plan de Seguridad y Evaluación de Riesgos	Verificar que los procedimientos y mecanismos de seguridad permiten lograr el riesgo residual determinado en la Evaluación de Riesgos.
Relación entre Plan de Seguridad y Política de Seguridad	Verificar que los procedimientos y mecanismos de seguridad permiten lograr los objetivos de la Política de Seguridad.
Plan de Seguridad Mantenible	Verificar que el Plan de Seguridad incluye los procedimientos que permiten asegurar que la seguridad del PSC se mantiene en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc.
Relación del Plan de Seguridad con las prácticas y política de certificación	Verificar que los objetivos de seguridad enunciados en la CPS y la Política de Certificados de firma electrónica avanzada se logran a través del Plan de Seguridad.
Requerimientos ISO 27002, sección 6	Verificar que los controles de Organización de la seguridad de la información del estándar ISO 27002 están considerados
Requerimientos ISO 27002, sección 7	Verificar que los controles de Gestión de activosdel estándar ISO 27002 están considerados
Requerimientos ISO 27002, sección 8	Verificar que los controles de Seguridad de Recursos Humanos delestándar ISO 27002 están considerados
Requerimientos ISO 27002, sección 9	Verificar que los controles de Seguridad Física y ambiental del estándar ISO 27002 están considerados
Requerimientos ISO 27002, sección 10	Verificar que los controles de Gestión de las comunicaciones y operaciones del estándar ISO 27002 están considerados

[9]ISO/IEC 27003:2010, Security techniques -- Information security management system implementation guidance.

Aspecto	Evaluación
Requerimientos ISO 27002, sección 11	Verificar que los controles de Controles de Acceso del estándar ISO 27002 están considerados
Requerimientos ISO 27002, sección 12	Verificar que los controles de Adquisición, desarrollo y mantenimiento de los sistemas de información del estándar ISO 27002 están considerados

4.8. REQUISITO PS07 – GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

4.8.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Gestión de Incidentes de Seguridad de la Información
Objetivo	Evaluar los requisitos relacionados con la gestión de incidentes de seguridad de la Información Para ello debe fundamentalmente generar Reporte de los eventos y debilidades de la seguridad de la información y establecer la Gestión de los incidentes y mejoras en la seguridad de la información
Descripción	El PSC debe asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna. Se debieran establecer procedimientos formales de reporte y de la intensificación de un evento. Todos los usuarios empleados contratistas y terceros debieran estar al tanto de los procedimientos para el reporte de los diferentes tipos de eventos y debilidades que podrían tener un impacto en la seguridad de los activos organizacionales. Se les debiera requerir que reporten cualquier evento y debilidad de la seguridad de la información lo más rápidamente posible en el punto de contacto designado. Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información. Se debieran establecer las responsabilidades y procedimientos para manejar de manera efectivo los eventos y debilidades en la seguridad de la información una vez que han sido reportados. Se debiera aplicar un proceso de mejoramiento continuo para la respuesta a, monitoreo, evaluación y la gestión general de los incidentes en la seguridad de la información. Cuando se requiera evidencia, esta se debiera recolectar cumpliendo con los requerimientos legales.
Referencias en Ley N°19.799 o su Reglamento	
Dependencias	PS01
Estándares de evaluación	ISO/IEC 27.002 Information technology – Code of practice for information security management (2005-06-15), Section13

Documentación solicitada	Documentos Descriptivo del Proceso de Gestión de Incidentes de Seguridad de la Información Plan de Gestión de Incidentes de Seguridad de la información Documento descriptivo de la implementación de un sistema de gestión de incidentes de seguridad Reportes de Incidentes de Seguridad de la Información
Evidencias solicitadas	Auditoría en terreno.

4.8.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	**Evaluación**
Relación entre el Plan de Gestión de Incidente y los recursos asignados	Verificar que el PSC dispone de los recursos y capacidades para implementar los mecanismos y procedimientos de seguridad asociado a un Sistema de gestión de Incidentes de Seguridad de la Información.
Relación entre Plan de Gestión de Incidentes y Política de Seguridad	Verificar que los procedimientos y mecanismos de seguridad implementados permiten lograr los objetivos de la política de seguridad.
Relación entre Plan de Gestión de Incidentes y Evaluación de Riesgos	Verificar que los procedimientos y mecanismos de seguridad implementados permiten lograr el riesgo residual determinado en la Evaluación de Riesgos asociados a los incidentes de Seguridad de la Información.
Plan de Gestión de Incidentes mantenible	Verificar que la implementación del Plan Gestión de Incidentes incluye los procedimientos que permiten asegurar que la seguridad del PSC se mantiene en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc.
Aprender de los incidentes en la seguridad de la información(ISO27.002, sección 13.2.2)	Se verificará: Gestión de un incidente en la seguridad de la información según ISO 27.002-Sección 13, Ítem 2.2: Sección 13.2.2Aprender de los incidentes en la seguridad de la información
Recolección de evidencia(ISO27.002, sección 13.2.3)	Se verificará: Gestión de un incidente en la seguridad de la información según ISO 27.002-Sección 13, Ítem 2.3: Sección 13.2.3Recolección de evidencia

4.9. REQUISITO ET01 – EVALUACIÓN DE LA PLATAFORMA TECNOLÓGICA.

4.9.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Evaluación de la Plataforma Tecnológica.
Objetivo	Evaluar los elementos de seguridad de la plataforma tecnológica utilizada para la generación, publicación y administración de certificados de firma electrónica móvil y CRL.
Descripción	Evaluar la seguridad de los elementos que constituyen la plataforma tecnológica del PSC de Firma Móvil. Se debe considerar componentes hardware y software que componen la infraestructura del PSC de Firma Móvil, como asimismo, todos los elementos de apoyo a su operación e interrelación, como protocolos y servicios. Los elementos a considerar son: • Módulo AC (Autoridad de Firma Móvil) • Módulo de Almacenamiento y Publicación de Certificados. • Elementos de administración de logs y auditoría.
Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799 Art. 17 a) y b) Reglamento DS181, Art. 16 a) y b). Disposiciones transitorias
Dependencias	TB01, TB02, TB03, TB04, PS02 y PS03
Estándares de evaluación	FIPS 140-2 ISO/IEC 15408 o equivalente.
Documentación solicitada	Documento descriptivo de la implementación de la infraestructura tecnológica. Este documento debería incluir al menos, planos de interconexión de sistemas, cableado de red de datos, cableado de poder principal y auxiliar, dispositivos de seguridad y control de acceso, y todo aquello relevante que permita demostrar la confiabilidad de la infraestructura tecnológica. Manuales del fabricante de los productos hardware y software relevantes.
Evidencias solicitadas	Documentación del fabricante que acredite el correspondiente nivel de seguridad, y/o de auditores externos.

4.9.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Módulo AC (Autoridad De Firma Móvil)	1. Funcionalidad y operación: • Capacidad para generar certificados con llaves de al menos 2048 bit. • Capacidad suspensión y revocación de certificados. • Capacidad para generar CRLs. • Indicar fecha de publicación y de nueva renovación de la CRL. • Capacidad para generar certificados de firma avanzada. • Capacidad de generar certificados de comunicación segura, entre AC y AR, si corresponde a la arquitectura (CC P2 FTP_ITC.1) • Capacidad de entregar certificados y CRLs a directorios públicos X500. 2. Seguridad. • Existencia de sistema control de acceso para acceder a la generación de certificados (CC P2 FIA_SOS.2) • Existencia de sistema de control de acceso para acceder a los sistemas de administración y auditoria (CC P2 FIA_UAU.2) 3. Ciclo de vida. • Capacidad de suspender y revocar certificados. • Capacidad de revocar certificado raíz y generar uno nuevo. 4. Auditoría. • Capacidad de generar log auditable para administración de contingencia, actividades diarias del personal autorizado y accesos maliciosos (CC P2 FAU_STG.2) 5. Documentación. • Manuales de operación, configuración y puesta en marcha. • Procedimiento de Recuperación ante contingencia.
Módulo de Almacenamiento y Publicación de Certificados	Almacenamiento de certificados en base de datos X500, y publicación a través de protocolos LDAP v2.0 y/o OCSP V1.0.
Elementos de administración de log y auditoría	Debe existir módulos de log y de auditoría, que permitan verificar los intentos de acceso, los accesos y las operaciones dañinas, sean esta intencionadas o no.

4.10. REQUISITO SF01 – SEGURIDAD FÍSICA

4.10.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Seguridad física y ambiental de la infraestructura de la Autoridad de Firma Móvil
Objetivo	Evaluar los requisitos relacionados con el aseguramiento de áreas restringidas, equipos e información y su protección de efectos ambientales.
Descripción	El PSC debe asegurar que el acceso físico a los servicios que manejan información sensible estén controlados y los riesgos físicos para los activos estén reducidos a su valor residual. Los accesos físicos a las áreas de servicios concernientes a la generación de certificados, entrega de dispositivos seguros a titulares, servicios de gestión de revocación y al área de residencia de servidores del PSC de Firma Móvil, deben ser limitados a individuos debidamente autorizados y deben asegurar que no habrá accesos no autorizados. Los controles deben ser implementados de manera de evitar las pérdidas, daños o compromiso de los activos propios de la actividad del negocio y el compromiso o robo de información. La protección física deberá ser alcanzada a través de la creación de perímetros de seguridad definidos alrededor de los las áreas deservicios de generación de certificados, provisión de dispositivos seguros y gestión de revocación. Cualquier parte de los servicios compartida con otra organización debe estar fuera del perímetro de seguridad. Los controles de seguridad físicos y ambientales deben ser implementados para proteger los servicios que entregan los recursos de sistemas propios, los servicios utilizados para soportar su operación y contra la suspensión no autorizada de servicios externos. La política de seguridad física y ambiental del PSC de Firma Móvil en lo concerniente a los sistemas de generación de certificados, provisión de dispositivos seguros a los titulares y gestión de revocación debe contemplar al menos de los siguientes aspectos: • Controles físico de acceso • Protección y recuperación ante desastres naturales • Protección contra robos, forzamiento y entrada • Medidas de protección en caso de incendios •Medidas ante falla de servicios de soporte (electricidad,

	telecomunicaciones, etc.) • Medidas en caso de fallas estructurales o de las redes húmedas • Servicio técnico para los servicios básicos
Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799, Artículo 17.- a), Reglamento DS181, Art. 16 a., Disposición Transitoria, Primera, Seguridad
Dependencias	PO02
Estándares de evaluación	ETSI 102 042 V2.1.2 (2010-4), 7.4.4 Physical and environment security. ISO/IEC 27.002 Information technology – Code of practice for information security management (2005-06-15), Section 9
Documentación solicitada	Análisis de riesgos del PSC de Firma Móvil. Política de certificación del certificado de firma digital avanzada. Declaración de prácticas de certificación. Plan de Seguridad de Sistemas Documento descriptivo de la implementación de seguridad física
Evidencias solicitadas	Auditoría a las instalaciones del PSC de Firma Móvil

4.10.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	**Evaluación**
Perímetro de seguridad física(ISO27.002, sección 9.1.1)	Se verificará: Evaluación de Seguridad Física según ISO 27.002-Sección 9, Ítem 1.1: Sección 9.1.1 Perímetro de seguridad física
Controles de acceso físico (ISO27.002, sección 9.1.2)	Se verificará: Evaluación de Seguridad Física según ISO 27.002-Sección 9, Ítem 1.2: Sección 9.1.2 Controles de acceso físico
Seguridad de oficinas, recintos e instalaciones (ISO27.002, sección 9.1.3)	Se verificará: Evaluación de Seguridad Física según ISO 27.002-Sección 9, Ítem 1.3: Sección 9.1.3 Seguridad de oficinas, recintos e instalaciones
Protección contra amenazas externas y ambientales (ISO27.002, sección 9.1.4)	Se verificará: Evaluación de Seguridad Física según ISO 27.002-Sección 9, Ítem 1.4: Sección 9.1.4 Protección contra amenazas externas y ambientales
Trabajo en áreas seguras(ISO27.002, sección 9.1.5)	Se verificará: Evaluación de Seguridad Física según ISO 27.002-Sección 9, Ítem 1.5: Sección 9.1.5 Trabajo en áreas seguras

Aspecto	Evaluación
Áreas de carga, despacho y acceso público (ISO27.002, sección 9.1.6)	Se verificará: Evaluación de Seguridad Física según ISO 27.002-Sección 9, Ítem 1.6: Sección 9.1.6 Áreas de carga, despacho y acceso público
Ubicación y protección de los equipos (ISO27.002, sección 9.2.1)	Se verificará: Evaluación de Seguridad Física según ISO 27.002-Sección 9, Ítem 2.1: Sección 9.2.1 Ubicación y protección de los equipos
Ubicación y protección de los equipos (ISO27.002, sección 9.2.1)	Se verificará: Evaluación de Seguridad Física según ISO 27.002-Sección 9, Ítem 2.1: Sección 9.2.1 Ubicación y protección de los equipos
Servicios de suministro (ISO27.002, sección 9.2.2)	Se verificará: Evaluación de Seguridad Física según ISO 27.002-Sección 9, Ítem 2.2. Sección 9.2.2 Servicios de suministro
Seguridad del cableado (ISO27.002, sección 9.2.3)	Se verificará: Evaluación de Seguridad Física según ISO 27.002-Sección 9, Ítem 2.3: Sección 9.2.3 Seguridad del cableado
Mantenimiento de los equipos (ISO27.002, sección 9.2.4)	Se verificará: Evaluación de Seguridad Física según ISO 27.002-Sección 9, Ítem 2.4: Sección 9.2.4 Mantenimiento de los equipos
Seguridad de los equipos fuera de las instalaciones(ISO27.002, sección 9.2.5)	Se verificará: Evaluación de Seguridad Física según ISO 27.002-Sección 9, Ítem 2.5: Sección 9.2.5 Seguridad de los equipos fuera de las instalaciones
Seguridad en la reutilización o eliminación de los equipos (ISO27.002, sección 9.2.6)	Se verificará: Evaluación de Seguridad Física según ISO 27.002-Sección 9, Ítem 2.6: Sección 9.2.6 Seguridad en la reutilización o eliminación de los equipos
Retiro de activos (ISO27.002, sección 9.2.7)	Se verificará: Evaluación de Seguridad Física según ISO 27.002-Sección 9, Ítem 2.7: Sección 9.2.7 Retiro de activos

4.11. REQUISITO PO01 – POLÍTICA DE FIRMA MÓVIL

4.11.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Política de Firma Móvil.
Objetivo	Comprobar que La Política de Firma Móvil (PFM) contiene los aspectos relevantes de Seguridad y están acorde a la Política de Seguridad del PSC.
Descripción	Este requisito es relevante no sólo para el usuario cliente sino que para todas las entidades involucradas, incluyendo quienes usan un servicio de Firma Móvil. Se verificarán a lo menos los siguientes aspectos: • La Política de Firma Móvil, debe entregar la confianza necesaria para que el uso Firma Móvil en forma electrónica, se ciña a la forma de operar recomendada. • La Política de Firma Móvil deberá permitir la interoperabilidad con otro Autoridad de PSC de Firma Móvil. • Las Prácticas de Firma Móvil deberán establecer como el PSC entrega la confianza establecida en la Política Firma Móvil
Referencias en Ley N°19.799 o su Reglamento	Reglamento DS181
Dependencias	PS03
Estándares de evaluación	ISO/EIC 27002
Documentación solicitada	Documento conteniendo la Política de Firma Móvil
Evidencias solicitadas	Auditoría a la PSC según ISO 27002: Sección 3

4.11.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	**Evaluación**
Clientes	La PSC deberá indicar a quién se le puede utilizar sus Datos en en el servicio de Firma Móvil.
Procedimiento de registro	Se verifica el registro del solicitante. La autenticación, verificación de su identidad en forma de acuerdo a la política para verificar los datos del usuario, y de acuerdo a los niveles de protección requeridos.
Usos del Dato de Firma Móvil	La PSC deberá indicar los propósitos para el cual fue usado el Datos en el servicio de Firma Móvil y sus limitaciones.
Obligaciones	Descripción de las obligaciones que contraen las entidades involucradas en la utilización del servicio de Firma Móvil.

Aspecto	**Evaluación**
Declaración de las garantías, seguros y responsabilidades de las partes.	Concordancia de las Políticas de Firma Móvil con los procedimientos operacionales.
Privacidad y Protección de los datos	Verificación de las políticas de privacidad y protección de datos usados en el servicio de Firma Móvil. Que estas políticas sean las apropiadas para el servicio de firma Móvil, pero que sean publicadas y de conocimiento del cliente.

4.12. REQUISITO PO02 – DECLARACIÓN DE PRÁCTICAS DE FIRMA MÓVIL.

4.12.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Declaración de Prácticas de Firma Móvil
Objetivo	Verificar que el PSC de Firma Móvil disponga de un documento, que señale los procedimientos de operación tanto para usarlos en el Servicio de Firma Móvil como el marco de aplicación de los mismos.
Descripción	Los elementos principales que debe contener la Declaración de Práctica de Firma Móvil, son las delimitaciones de responsabilidad y las obligaciones tanto del PSC de Firma Móvil, como del solicitante a ser identificado digitalmente. Además debe quedar explícito, tanto el ciclo de vida de los datos del servicio de Firma Móvil, desde su uso hasta el término de su vida útil, como el ciclo de vida del PSC de Firma Móvil, desde el inicio hasta el fin del mismo.
Referencias en Ley N|19.799 o su Reglamento	Reglamento DS181 modificación 2012
Dependencias	PO01
Estándares de evaluación	
Documentación solicitada	Documentación de las prácticas de Firma Móvil.
Evidencias solicitadas	Auditoría a la PSC Firma Móvil respecto a la Declaración de Práctica de Firma Móvil

4.12.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	**Evaluación**
Existencia del documento de prácticas de Firma Móvil	Verificar que exista documentación de las Declaración de prácticas de Firma Móvil y que esté debidamente publicada.
Las obligaciones y responsabilidades del PSC: Confidencialidad de la información de los solicitantes /protección de datos.	Verificar que exista una declaración de las obligaciones y deberes del PSC de Firma Móvil. Existencia de procedimientos de protección de la información de los solicitantes del servicio de Firma Móvil

Aspecto	Evaluación
Las obligaciones y responsabilidades del solicitante a identificar digitalmente.	Verificar que existan definiciones de los deberes y obligaciones de los usuarios (solicitantes del servicio de Firma Móvil)
Ciclo de vida del uso de Datos del Servicio de Firma Móvil	Verificar que existan procedimientos que definan el ciclo de vida de los datos usados en el servicio de Firma Móvil. Deberes y procedimientos del PSC de Firma Móvil para el uso de Datos en el Servicio firma Móvil
Ciclo de vida del PSC de Firma Móvil.	Verificar que exista la documentación de procedimientos de finalización del giro de la PSC de Firma Móvil, en el que se incluyan los procedimientos de término y de traspaso a otro PSC u organismo que asuma la responsabilidad de mantener la continuidad de los servicios
Controles de Seguridad técnica	Verificar la existencia de las medidas de seguridad adoptadas por el PSC de Firma Móvil para proteger sus datos de uso de Datos en el servicio de firma móvil.
Controles de seguridad no técnica	Verificar la existencia de controles utilizados por la PSC de Firma Móvil para asegurar las funciones de uso de datos en el servicio de firma móvil, autentificación de solicitantes, auditoria y almacenamiento de información relevante.

4.13. REQUISITO PO03 – MODELO OPERACIONAL DE LA PSCDE FIRMA MÓVIL

4.13.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Modelo Operacional de la Autoridad de Firma Móvil del PSC.
Objetivo	Comprobar a través de la documentación presentada que el modelo operacional cumple con los requerimientos y obligaciones en relación con la confiabilidad e interoperabilidad en la forma de operar y prestar los servicios de firma móvil en un PSC.
Descripción	El modelo operacional deberá responder a lo menos a las siguientes preguntas: • Cuales son los servicios prestados por la PSC de Firma Móvil. • Como se interrelacionan los diferentes servicios • En que lugares se operará. • Que tipos de Datos en el servicio de firma móvil se usarán • Cómo se pretende hacer esto, incluyendo servicios externalizados. • Como se protegerán los activos
Referencias en Ley N°19.799 o su Reglamento	Reglamento DS181 modificación 2012
Dependencias	PO02
Estándares de evaluación	N/A
Documentación solicitada	Descripción del modelo operacional de PSC de Firma Móvil
Evidencias solicitadas	Auditoría en terreno. Auditoría a la PSC según Controles de Documentación Operacional

4.13.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	**Evaluación**
Consistencia del documento	Se verificará que el documento incluya todas las partes atingentes del documento tipo
Resumen Ejecutivo	Se verificará que el resumen incluya: a. Un resumen coherente del contenido del documento b. La historia de la empresa. c. Relaciones comerciales con proveedores de insumos o servicios para sus operaciones.

Aspecto	**Evaluación**
Componentes del sistema	Se verificará que el modelo comprenda los siguientes aspectos: a. Interfaces con el Servicio de Firma Móvil b. Implementación de elementos de seguridad c. Procesos de administración d. Sistema de directorios e. Procesos de auditoría y respaldo f. Bases de Datos g. Privacidad h. Entrenamiento del personal
Plan de Auditoría	Se verificará que el modelo considere la auditoría de lo siguiente: a. Seguridad y dispositivos de seguridad b. Restricciones del personal c. Interfaces de administración d. Procedimientos de recuperación de desastres e. Procedimientos de respaldo
Seguridad	Se verificará que el modelo incluya los requerimientos de: a. La seguridad física de las instalaciones. b. Seguridad del personal. c. Nivel de seguridad del módulo criptográfico.

4.14. REQUISITO AD01 – MANUAL DE OPERACIONES DE LA PSCDE FIRMA MÓVIL

4.14.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Manual de Operaciones de la Autoridad de Firma Móvil del PSC.
Objetivo	Comprobar a través de la documentación presentada que los aspectos operacionales mínimos con relación a los requisitos de confiabilidad e interoperabilidad en la forma de operar y prestar los servicios de la PSC de Firma Móvil.
Descripción	El propósito del manual es describir la administración diaria y las prácticas operacionales de la PSC de Firma Móvil y debería ser la guía que garantice que las directrices primarias de la Política de Firma Móvil están implementadas operacionalmente. Para mejorar la comunicación de esta información al personal de operaciones y a los evaluadores, pueden usarse gráficos, diagramas de flujo funcionales, líneas de tiempo, etc. El manual de operaciones de la PSC de Firma Móvil deberá tener a lo menos las siguientes características: • Deberá ser consistente con la Política de Firma Móvil. • Deberá incluir la interacción entra los usuarios y el servicio de Firma Móvil. • Deberá describir los controles de seguridad física, de red, del personal y de procedimientos. • Deberá incluir los procedimientos adoptados para el manejo de las Base de Datos
Referencias en Ley N°19.799 o su Reglamento DS181 y Modificación 2012	Reglamento DS181
Dependencias	PS03
Estándares de evaluación	
Documentación solicitada	Manual de operaciones PSC de Firma Móvil
Evidencias solicitadas	Auditoría en terreno

4.14.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Nómina y descripción de cargos	Nómina de los cargos de personal, con la descripción de las responsabilidades y los procedimientos en que los empleados realizan sus funciones en el servicio de Firma Móvil.
Referencias de los cargos en los planes de la PSC de Firma Móvil	Referencia del personal en los planes de continuidad del negocio y los planes de recuperación de desastres y emergencia en el servicio de Firma Móvil
Planes de Contingencia	Descripción de los planes de contingencia.
Descripción de las operaciones	Descripción detallada de los siguientes procedimientos: • Uso de Datos en el Servicio de Firma Móvil • Almacenamiento de Datos en el Servicio de Firma Móvil • Medidas de control de acceso • Procedimientos de respaldo y recuperación
Actualización de CPS y CP	Procedimiento de actualización de la Declaración de Prácticas y Política de PSC de Firma Móvil
Servicios del PSC de Firma Móvil	Descripción de los servicios del PSC de Firma Móvil
Interacción Servicio – Usuarios	El documento cubre la interacción entre la Servicio de Firma Móvil y los Usuarios de Datos en el servicio de Firma Móvil

5. BIBLIOGRAFÍA

1) Legal

- 2002; LEY-19.799; "LEY SOBRE DOCUMENTOS ELECTRÓNICOS, FIRMA ELECTRÓNICA Y SERVICIOS DE CERTIFICACIÓN DE DICHA FIRMA", Fecha Publicación: 12.04.2002, Fecha Promulgación: 25.03.2002

- 2002; DTO-181; REGLAMENTO DE LA LEY 19.799 SOBRE DOCUMENTOS ELECTRONICOS, FIRMA ELECTRONICA Y LA CERTIFICACION DE DICHA FIRMA; Fecha de Publicación : 17.08.2002; Fecha de Promulgación : 09.07.2002

- 2007; MODIFICA LEY-19.799; "LEY SOBRE DOCUMENTOS ELECTRÓNICOS, FIRMA ELECTRÓNICA Y SERVICIOS DE CERTIFICACIÓN DE DICHA FIRMA", Fecha Inicio Vigencia 12-11-2007

- 2012; MODIFICA DECRETO SUPREMO 181, DE 09 DE JULIO DE 2002, DEL MINISTERIO DE ECONOMÍA, FOMENTO Y TURISMO, QUE APRUEBA REGLAMENTO DE LA LEY Nº 19.799 SOBRE DOCUMENTOS ELECTRÓNICOS, FIRMA ELECTRÓNICA Y LA CERTIFICACIÓN DE DICHA FIRMA

2) Prácticas de Certificación:

- ETSI TS 102 042 V2.3.1 (2012-11) - 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.

3) Seguridad:

- 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.

- NCh2829.Of.2003 Tecnología de la Información - Requisitos de Seguridad para Módulos Criptográficos.

4) Estructura de Certificados:

- ISO/IEC 9594-8: 2005 Information Technology - Open Systems Interconnection - The Directory Attribute Certificate Framework. Correccion 2:2009.

- ITU-T - X.690 - Information technology – ASN.1 encoding rules Specification of BER, CER, DER

- NCh2798.Of2003 Tecnología de la Información - Reglas de codificación ASN.1 Especificación de las reglas de codificación básica (BER) de las reglas de codificación canónica (CER) y de las reglas de codificación distinguida (DER).

5) Repositorio de Información:

- 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. (Lo reemplaza RFC 3494)

- RFC 3377 LDAPv3: Technical Specification, September 2002, Lightweight Directory Access Protocol (v3): Technical. (Lo reemplaza RFC 4510)

6) Sellado de Tiempo/Time Stamping:

- ETSI TS 102 023 V1.2.2 (2008-10) - Policy requirements for time-stamping authorities

- ETSI TS 101 861 V1.4.1 (2011-07) - Time stamping profile

- ISO/IEC 18014-1:2008 Information technology - Security techniques - Time-stamping services - Part 1: Framework.
- ISO/IEC 18014-2:2009 Information technology - Security techniques - Time-stamping services - Part 2: Mechanism producing independent tokens.
- ISO/IEC 18014-3:2009 Information technology - Security techniques - Time-stamping services - Part 3: Mechanisms producing linked tokens.
- RFC 3161 Internet X.509 Public Key Infrastructure Time – Stamp Protocol (TSP)
- RFC 5816 ESSCertIDv2 Update for RFC 3161
- RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs)
- NIST Special Publication 800-102 - Recommendation for Digital Signature Timeliness

7) DNI Electrónico y su Identidad Biométrica:

- ISO/ 19.785, ISO 19.794-2 Formatos de cabecera y datos de referencia.
- ISO 7816-4, ISO 7816-11 Para la definición de los comandos de la tarjeta.
- ANSI X.9.84 - 2003 - Reconocimiento de firmas, huellas digitales.
- ISO/IEC 27N2949 - Condiciones de los sistemas biométricos para la industria de servicios financieros.
- ISO/IEC 19784-1:2005, también conocido como BioAPI 2.0. Conexión entre dispositivos biométricos y diferentes tipos de aplicaciones, interfaz de programación de aplicaciones biométricas (API).
- ISO/IEC 19785-1:2006 Common Biometric Exchange Formats Framework - formatos comunes de intercambio de archivos biométricos.

8) Servicios de firma móvil:

- ETSI TS 102 207 V1.1.3 (2003-08) - Specifications for Roaming in Mobile Signature Services
- ETSI TR 102 206 V1.1.3 (2003-08) - Security Framework
- ETSI TR 102 203 V1.1.1 (2003-05) - Business and Functional Requirements
- ETSI TS 102 204 V1.1.4 (2003-08) - Web Service Interface

9) Especificaciones Técnicas:

- ETSI TS 101 733 V2.1.1 (2012-03) - CMS Advanced Electronic Signatures (CAdES)
- ETSI TS 101 903 V1.4.2 (2010-12) - XML Advanced Electronic Signatures (XAdES)
- ETSI TS 102 778 V1.1.1 (2009-04) - CMS Profile based on ISO 32000-1
- ETSI TS 102 778-1 V1.1.1 (2009-07) - Part 1 PAdES Overview - a framework document for PAdES
- ETSI TS 102 778-2 V1.2.1 (2009-07) - Part 2 PAdES Basic - Profile based on ISO 32000-1
- ETSI TS 102 778-3 V1.2.1 (2010-07) - Part 3 PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles
- ETSI TS 102 778-4 V1.1.2 (2009-12) - Part 4 PAdES Long Term - PAdES-LTV Profile
- ETSI TS 102 176-1 V2.1.1 (2011-07) - Part 1 Hash functions and asymmetric algorithms
- ETSI TR 102 038 V1.1.1 (2002-04) - XML format for signature policies
- ETSI TR 102 041 V1.1.1 (2002-02) - Signature Policies Report

- ETSI TR 102 045 V1.1.1 (2003-03) - Signature policy for extended business model
- ETSI TR 102 272 V1.1.1 (2003-12) - ASN.1 format for signature policies
- RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
- RFC 3125 - Electronic Signature Policies
- RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol
- RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 5652 - Cryptographic Message Syntax (CMS)
- ITU-T - X.680 - Information technology – Abstract Syntax Notation One (ASN.1) Specification of basic notation

6. GLOSARIO

Castellano

Sigla	Descripción
AC	Autoridad Certificadora
AIN	Análisis de Impacto en el Negocio
AR	Autoridad de Registro
CSI	Comité de Seguridad de la Información
DPC	Declaración de Prácticas de Certificación
DPI	Derechos de Propiedad Intelectual
EA	Entidad Acreditadora
ICP	Infraestructura de Clave Pública
LCR	Lista de Certificados Revocados
PC	Política de Certificación
PCN	Plan de Continuidad del Negocio
PRD	Plan de Recuperación ante Desastres
PSC	Prestador de Servicios de Certificación
SGSI	Sistema de Gestión de Seguridad de la Información
TI	Tecnología de la Información
TUC	Tiempo Universal Coordinado

Inglés

Acronym	Meaning
ANSI	American National Standards Institute
ASN	Abstract Syntax Notation
BCP	Business Continuance Plan
BDB	Biometric Data Block
BFP	Biometric Function Provider
BIA	Business Impact Analysis
BIR	Biometric Information Register
BS	British Standards Institution
BSP	Biometric Service Provider
CA	Certification Authority
CBEFF	Common Biometric Exchange Formats Framework
CC	Common Criteria
CP	Certification Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DMZ	De-Militarized Zone

DRP	Disaster Recovery Plan
EAL	Evaluation Assurance Level
EE	End Entity
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IPR	Intelectual Property Rights
ISC	Information Security Comitee
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standard and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infraestructure
PKIX	X.509-based PKI
RA	Register Authority
RFC	Request for Comment
SPI	Service Provider Interface
TS	Time Stamping
TSA	Time Stamping Authority
TSDM	Trusted Software Development Methodology
TSL	Trust Service Status List
UTC	Universal Time Coordinated
VA	Validation Authority