

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 Electrónica Avanzada

- Documento Número : EA-103
- Versión : 2.1
- Estado : Versión Final
- Fecha de Emisión : 08/02/2013

NOTA: Este documento no podrá ser, ni en su totalidad ni en parte alguna, reproducido o almacenado en un sistema electrónico, o transmitido en forma o medio alguno, ya sea electrónico, mecánico, fotocopia, grabación u otros, sin previo consentimiento del Ministerio de Economía Fomento y Reconstrucción de la República de Chile.

Contenido

1.	ANTECEDENTES	7
1.1.	RESUMEN	7
1.2.	INTRODUCCIÓN	7
2.	CRITERIOS DE ACREDITACIÓN	9
2.1.	OBJETIVO DE LA ACREDITACIÓN	9
2.2.	DEFINICIONES.....	9
2.3.	CRITERIOS GENERALES DE ACREDITACIÓN	9
2.3.1.	TRANSPARENCIA	9
2.3.2.	INTEROPERABILIDAD INTERNACIONAL	9
2.3.3.	GRADUALIDAD.....	10
2.3.4.	INDEPENDENCIA.....	10
2.3.5.	NEUTRALIDAD TECNOLÓGICA	10
2.3.6.	PRIVACIDAD.....	10
2.4.	ACREDITACIÓN	12
2.5.	CUMPLIMIENTO DE REQUISITOS.....	12
2.6.	PRELACIÓN DE REQUISITOS	13
2.7.	SISTEMA DE ACREDITACIÓN.....	13
2.7.1.	ENTIDAD ACREDITADORA (A).....	13
2.7.2.	ENTIDAD DE NORMALIZACIÓN (B)	14
2.7.3.	ENTIDAD EVALUADORA/AUDITORA (C)	14
2.7.4.	PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC) (D)	14
2.7.5.	REGISTRO DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN ACREDITADOS (E)..	14
2.7.6.	NORMAS TÉCNICAS (F).....	14
2.8.	PROCEDIMIENTO DE ACREDITACIÓN	15
2.9.	PROCESO DE MANTENCIÓN DE NORMAS TÉCNICAS	20

2.9.1.	Diagrama del Proceso de Mantenimiento de Normas Técnicas.....	21
3.	EVALUACIÓN	22
3.1.	OBJETIVO DE LA EVALUACIÓN	22
3.2.	ESCALA DE EVALUACIÓN.....	22
3.3.	ESQUEMA DE EVALUACIÓN	22
3.4.	AUDITORIAS.....	23
3.5.	CAMBIOS A LOS CRITERIOS	23
3.6.	COSTOS.....	23
3.7.	REQUISITOS DE ACREDITACIÓN	23
3.7.1.	AS REQUISITOS DE ADMISIBILIDAD.....	23
3.7.2.	RG REQUISITOS GENERALES.....	24
3.7.3.	LE ASPECTOS LEGALES Y DE PRIVACIDAD.....	24
3.7.4.	TB TÉCNICOS BÁSICOS.....	24
3.7.5.	PS SEGURIDAD.....	24
3.7.6.	ET EVALUACIÓN TECNOLÓGICA	24
3.7.7.	SF SEGURIDAD FÍSICA	24
3.7.8.	PO POLÍTICA DEL PSC.....	25
3.7.9.	AD ADMINISTRACIÓN DEL PSC.....	25
3.7.10.	PE EXAMEN DEL PERSONAL.....	25
3.8.	TABLA I: RESUMEN REQUISITOS DE ACREDITACIÓN DE FIRMA ELECTRÓNICA AVANZADA 26	
4.	REQUISITOS DE ACREDITACIÓN	30
4.1.	REQUISITO AS01 – REQUISITOS DE ADMISIBILIDAD	30
4.1.1.	INDIVIDUALIZACIÓN DEL REQUISITO	30
4.1.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	31
4.2.	REQUISITO RG01 – REQUERIMIENTOS GENERALES.....	32

4.2.1.	INDIVIDUALIZACIÓN DEL REQUISITO	32
4.2.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	33
4.3.	REQUISITO LE01 – ASPECTOS LEGALES Y DE PRIVACIDAD	34
4.3.1.	INDIVIDUALIZACIÓN DEL REQUISITO	34
4.3.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	34
4.4.	REQUISITO TB01 – ESTRUCTURA CERTIFICADOS	36
4.4.1.	INDIVIDUALIZACIÓN DEL REQUISITO	36
4.4.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	37
4.5.	REQUISITO TB02 – ESTRUCTURA CRL y SERVICIO OCSP.....	39
4.5.1.	INDIVIDUALIZACIÓN DEL REQUISITO	39
4.5.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	40
4.6.	REQUISITO TB03 – REGISTRO DE ACCESO PÚBLICO.....	41
4.6.1.	INDIVIDUALIZACIÓN DEL REQUISITO	41
4.6.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	42
4.7.	REQUISITO TB04 – MODELO DE CONFIANZA.....	43
4.7.1.	INDIVIDUALIZACIÓN DEL REQUISITO	43
4.7.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	43
4.8.	REQUISITO PS01 – REVISIÓN DE LA EVALUACIÓN DE RIESGOS Y AMENAZAS	44
4.8.1.	INDIVIDUALIZACIÓN DEL REQUISITO	44
4.8.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	45
4.9.	REQUISITO PS02 – POLÍTICA DE SEGURIDAD	46
4.9.1.	INDIVIDUALIZACIÓN DEL REQUISITO	46
4.9.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	47
4.10.	REQUISITO PS03 – PLAN DE CONTINUIDAD DEL NEGOCIO.....	48
4.10.1.	INDIVIDUALIZACIÓN DEL REQUISITO	48
4.10.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	49

4.11.	REQUISITO PS04 – PLAN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	51
4.11.1.	INDIVIDUALIZACIÓN DEL REQUISITO	51
4.11.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	52
4.12.	REQUISITO PS05 – PLAN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	54
4.12.1.	INDIVIDUALIZACIÓN DEL REQUISITO	54
4.12.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	55
4.13.	REQUISITO PS06 – PLAN DE ADMINISTRACIÓN DE LLAVES	56
4.13.1.	INDIVIDUALIZACIÓN DEL REQUISITO	56
4.13.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	57
4.14.	REQUISITO PS07 – GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN....	59
4.14.1.	INDIVIDUALIZACIÓN DEL REQUISITO	59
4.14.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	60
4.15.	REQUISITO ET01 – EVALUACIÓN DE LA PLATAFORMA TECNOLÓGICA.....	62
4.15.1.	INDIVIDUALIZACIÓN DEL REQUISITO	62
4.15.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	63
4.16.	REQUISITO SF01 – SEGURIDAD FÍSICA	65
4.16.1.	INDIVIDUALIZACIÓN DEL REQUISITO	65
4.16.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	66
4.17.	REQUISITO PO01 – POLÍTICA DE CERTIFICADOS DE FIRMA AVANZADA.....	68
4.17.1.	INDIVIDUALIZACIÓN DEL REQUISITO	68
4.17.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	68
4.18.	REQUISITO PO02 – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN.	70
4.18.1.	INDIVIDUALIZACIÓN DEL REQUISITO	70
4.18.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	70

4.19.	REQUISITO PO03 – MODELO OPERACIONAL DE LA AUTORIDAD CERTIFICADORA.....	72
4.19.1.	INDIVIDUALIZACIÓN DEL REQUISITO	72
4.19.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	72
4.20.	REQUISITO PO04 – MODELO OPERACIONAL DE LA AUTORIDAD DE REGISTRO (AR) ...	74
4.20.1.	INDIVIDUALIZACIÓN DEL REQUISITO	74
4.20.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	74
4.21.	REQUISITO AD01 – MANUAL DE OPERACIONES DE AUTORIDAD CERTIFICADORA	76
4.21.1.	INDIVIDUALIZACIÓN DEL REQUISITO	76
4.21.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	76
4.22.	REQUISITO AD02 – MANUAL DE OPERACIONES DE LA AUTORIDAD DE REGISTRO	78
4.22.1.	INDIVIDUALIZACIÓN DEL REQUISITO	78
4.22.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	79
4.23.	REQUISITO PE01 – EXAMEN DEL PERSONAL.....	81
4.23.1.	INDIVIDUALIZACIÓN DEL REQUISITO	81
4.23.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	82
4.24.	REQUISITO PE02 – EXAMEN DEL PERSONAL.....	83
4.24.1.	INDIVIDUALIZACIÓN DEL REQUISITO	83
4.24.2.	ASPECTOS ESPECÍFICOS A EVALUAR.....	84
5.	BIBLIOGRAFÍA.....	85
6.	GLOSARIO	90

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 N° 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 Certificación solicitante en los siguientes casos:

1. Si cumple plenamente los requisitos establecidos, de acuerdo a los criterios de evaluación definidos en esta Guía.
2. 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 Certificación subsanar plenamente los incumplimientos en un plazo razonable.

No se otorgará la acreditación al Prestador de Servicios de Certificación 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 Certificación 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.
2. Presentando la documentación e información solicitada por la Entidad Acreditadora dentro de los plazos establecidos en el procedimiento de acreditación y evaluación.
3. Permitiendo el libre acceso a los expertos designados por la Entidad Acreditadora, para la auditoría.
4. Entregando cualquier información adicional pertinente solicitada por la Entidad Acreditadora durante el proceso de acreditación.

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

5. Documentos descriptivos generados por el PSC que permitan apoyar la comprobación de un requisito.
6. 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 Anexos 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 de 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 N°19.799 artículo 1°, letra c).

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).

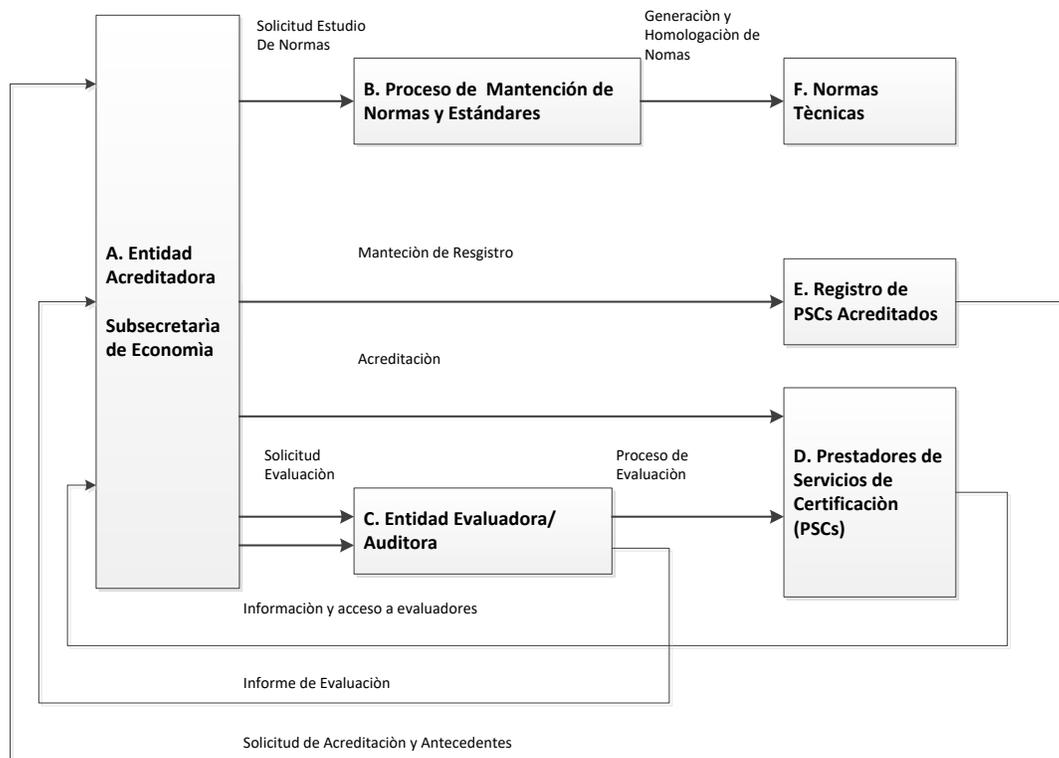


Figura 1: Esquema del sistema de acreditación de PSC.

2.8. PROCEDIMIENTO DE ACREDITACIÓN

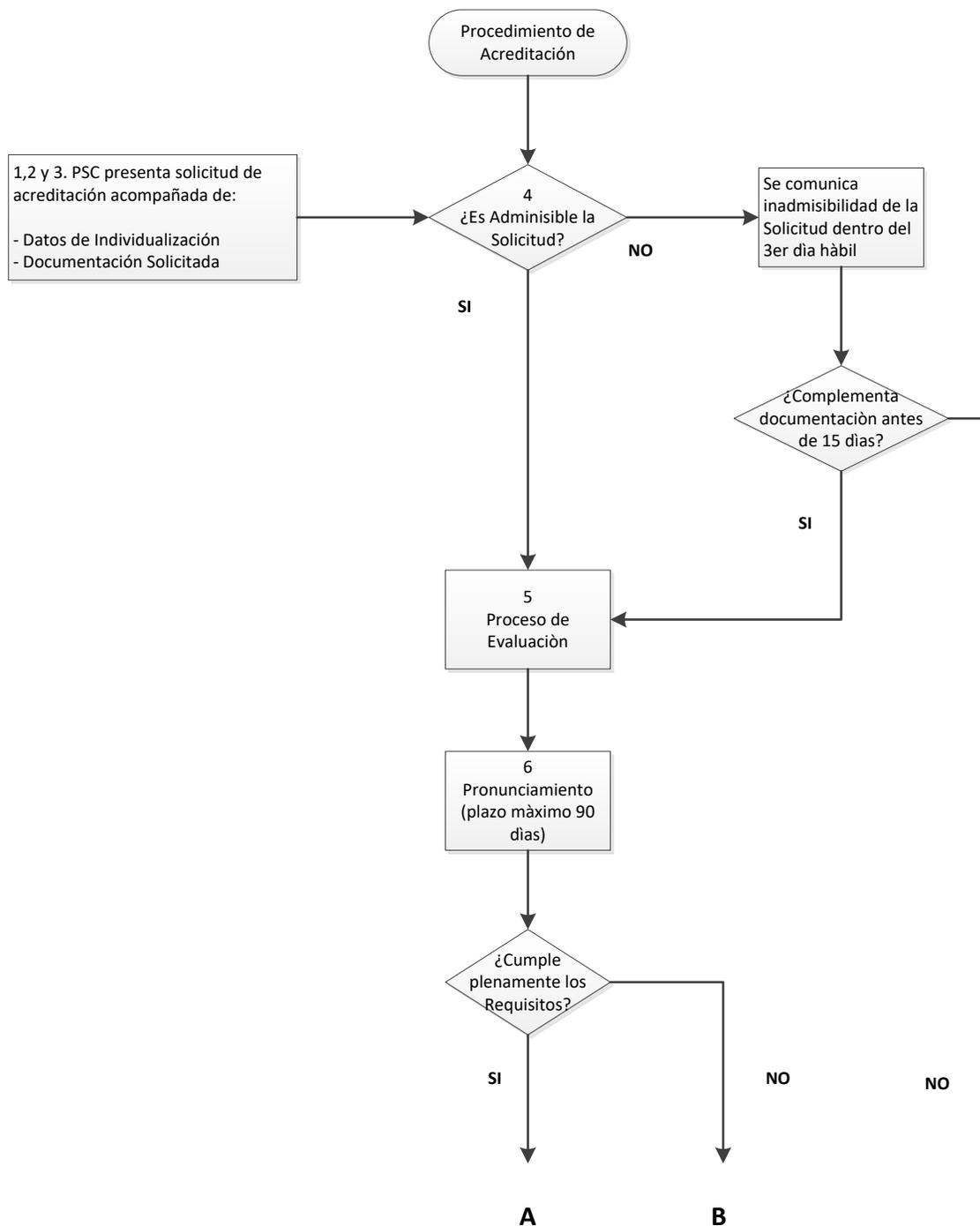
El procedimiento de acreditación que se define en la Ley y el Reglamento se describe a continuación y se resume en la Figura 2 (Reglamento Art. 17°):

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, 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 la Guía de Evaluación para cada uno de los requisitos especificados.
 - b. Presentar los procedimientos previstos para asegurar el acceso a los peritos o expertos (Reglamento 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 inadmisibles 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, sus disposiciones transitorias y la Guía de Evaluación. 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, el Reglamento y la Guía de Evaluación 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, 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 y especificados en este documento, la Entidad Acreditadora procederá a informar al Prestador de Servicios de Certificación 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.



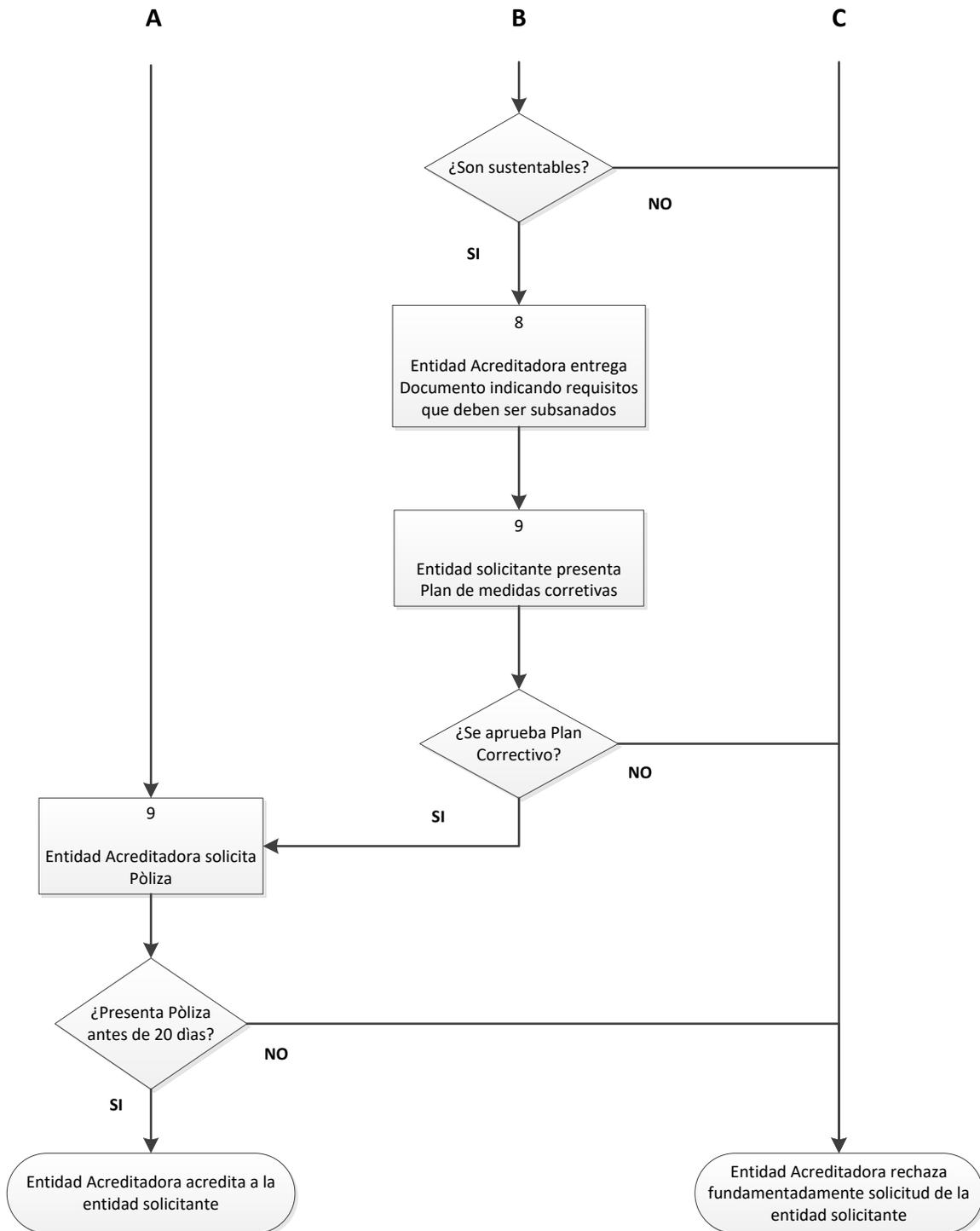


Figura 2: Diagrama de flujos que describe el proceso de acreditación de los PSC.

2.9. PROCESO DE MANTENCIÓN DE NORMAS TÉCNICAS

El procedimiento de mantenimiento 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 diversas 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 Mantenimiento de Normas Técnicas

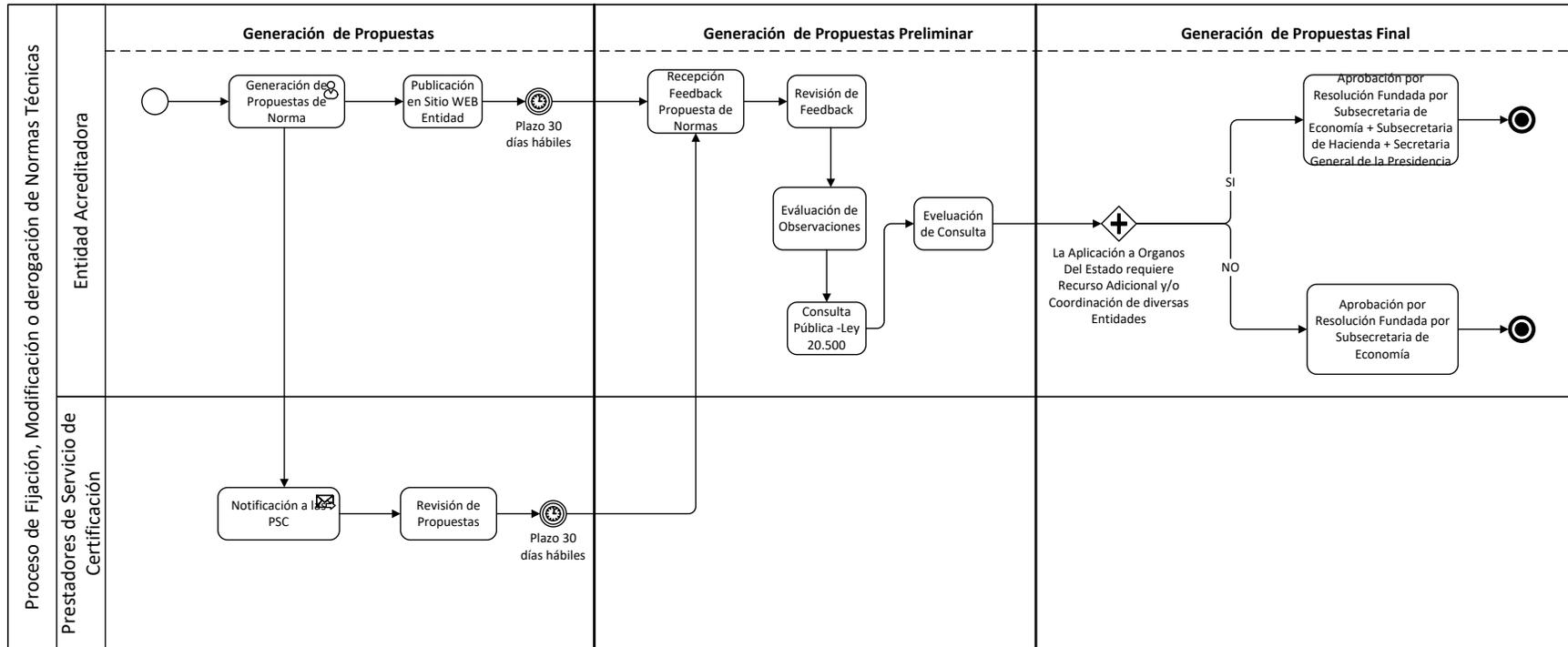


Figura 3: Proceso de Mantenición de Normas Técnicas.

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 cumple totalmente el requisito exigido.
A-	El PSC 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 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 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 la emisión de certificados digitales para autenticar una persona que actúa en representación de sí misma o de una persona natural o jurídica.

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 en conformidad a lo expresado en la Ley N°19.799, su Reglamento y las normas técnicas aplicables son los siguientes:

3.7.1. AS REQUISITOS DE ADMISIBILIDAD

Son aquellos requisitos previos necesarios para iniciar el procedimiento de evaluación del PSC, los que incluyen la presentación de la solicitud de acreditación, entrega de la documentación solicitada, entrega del comprobante de pago de los costos de acreditación y el cumplimiento del plazo establecido para la entrega de documentación faltante en caso de ser necesario.

3.7.2. RG REQUISITOS GENERALES

Son todos aquellos relacionados con el cumplimiento de plazos y procedimientos de acreditación, tales como auditorías en terreno, entrega de información adicional solicitada por evaluadores, etc.

3.7.3. LE ASPECTOS LEGALES Y DE PRIVACIDAD

Son los relacionados con la comprobación de la documentación legal solicitada, tales como personalidad jurídica vigente, contratos con proveedores de servicios, seguros de responsabilidad, resguardo de la información privada entregada por los solicitantes y titulares de certificados de firma electrónica avanzada al PSC durante el proceso de registro o durante la vigencia del certificado respectivamente, conforme a las disposiciones de la ley N°19.628 de Protección de la Vida Privada y los estándares de seguridad de la información que sean pertinente para su correcta protección, tales como la norma ISO 27.001.

3.7.4. TB TÉCNICOS BÁSICOS

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

- Estructura e información del certificado de firma electrónica avanzada.
- Estructura e información de la lista de certificados revocados (CRL)
- Servicio de estado del certificado (OCSP)
- Servicios, información y accesibilidad del registro público del PSC.
- Modelo de confianza.

3.7.5. 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.

3.7.6. 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.

3.7.7. SE 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.

3.7.8. PO POLÍTICA DEL PSC

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

3.7.9. AD ADMINISTRACIÓN DEL PSC

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.

3.7.10. PE EXAMEN DEL PERSONAL

Son los requisitos relacionados con los requerimientos del personal que maneja información sensible y del oficial de seguridad.

3.8. TABLA I: RESUMEN REQUISITOS DE ACREDITACIÓN DE FIRMA ELECTRÓNICA AVANZADA

Requisito	Clase	Nombre	Dependencia	Normas y Anexos	Documentación solicitada
AS01	Admisibilidad	Requisitos de Admisibilidad	Ninguna	Ley N°19.799 y su reglamento.	
RG01	Requerimientos Generales	Requerimientos Generales de la ley 19.799 y su Reglamento	Ninguna	Ley N°19.799 y su reglamento.	
LE01	Legales	Aspectos legales y de Privacidad	Ninguno	Ley N°19628. Ley N°19.799 y su Reglamento. Anexo 28.	Documento de la Política de Privacidad. Evaluación de Privacidad de Sitio Web. Constitución de sociedad vigente.
TB01	Tecnológico Básico	Estructura e información del certificado de firma avanzada	Ninguno	Ley N°19.799 y su reglamento. ISO/IEC 9594-8.	Certificado tipo de firma electrónica avanzada vigente
TB02	Tecnológico Básico	Estructura e información de la lista de certificador revocados (CLR). Consulta y Respuesta del Estado de Certificado vía servicio OCSP.	Ninguno	Ley N°19.799 y su reglamento. ISO/IEC 9594-8. Anexo 26.	Lista tipo de certificados revocados vigentes (CRL). Servicio de Estado de Certificado OCSP.
TB03	Tecnológico Básico	Servicios, información y accesibilidad del sistema público de acceso electrónico del PSC. Acceso a certificados emitidos por el PSC	Ninguno	Ley N°19.799 y su reglamento. ISO/IEC 9594-8. Anexo 5.	Documento descriptivo de los servicios y las dirección electrónicas vigentes donde se pueden acceder

Requisito	Clase	Nombre	Dependencia	Normas y Anexos	Documentación solicitada
TB04	Tecnológico Básico	Modelo de confianza	Ninguno	Ley N°19.799 y su reglamento. ISO/IEC 9594-8. ETSI TS 102 231. Anexo 16. Anexo 27.	Documento descriptivo. Información de acuerdo a formato TSL.
PS01	Seguridad	Documentación y mantención de la política de seguridad	Ninguna	ISO 27002. Anexo 1. Anexo 2.	Política de Seguridad
PS02	Seguridad	Gestión de Riesgos y Amenazas	PS01	ISO 27001. ISO 27005. Anexo 3.	Plan de gestión de Riesgos
PS03	Seguridad	Plan de Continuidad del Negocio y Recuperación de Desastres	PS02	ISO/IEC 27002. ETSI TS 102 042. BS25999. Anexo 4. Anexo 18.	Plan de Continuidad de Negocios. Plan de Recuperación de Desastres.
PS04	Seguridad	Plan de un Sistema de Gestión de Seguridad de la Información y Administración de llaves resultante de PS02 y de acuerdo al marco PS01	PS02	ISO 27001. ISO 27002. Anexo 17.	Plan de un Sistema de Gestión de Seguridad de la Información
PS05	Seguridad	Evaluación de la Implementación del Plan de un Sistema de Seguridad de la Información	PS04	Anexo 8. Anexo 9.	Informe auditor independiente.

Requisito	Clase	Nombre	Dependencia	Normas y Anexos	Documentación solicitada
PS06	Seguridad	Evaluación del Plan de Administración de llaves	PS04	ETSI TS 102 042. Anexo 21. Anexo 22.	Informe auditor independiente.
PS07	Seguridad	Gestión de Incidentes de Seguridad de la Información	PS01	ISO 27001. Anexo 23. Anexo 25.	Plan de gestión de Incidente de Seguridad de la Información.
ET01	Evaluación Tecnológica	Evaluación y Certificación de la Plataforma Tecnológica de PSC	TB, PS03, PS04, PS05.	ETSITS 102 042. FIPS 140-2. ISO/IEC 15408. Anexo 11.	Cumplimiento Certificación con estándares.
SF01	Seguridad Física	Seguridad Física de la Infraestructura del PSC	PS04	ISO/IEC 27002. ETSI TS 102 042. Anexo 19.	Documentación relevante.
PO01	Política del PSC	Política de los Certificados de Firma Avanzada	PS03, PS05, PS06, ET01, SF01.	ETSI TS 102 042. RFC 3647. Anexo 6. Anexo 20.	Documento de la Política de Certificado de Firma Electrónica Avanzada.
PO02	Política del PSC	Declaración de Prácticas de Certificación	PO01, AD01, AD02, PE02.	ETSI TS 102 042. RFC 3647. Anexo 7. Anexo 10. Anexo 20.	Documento de las Prácticas de Certificación para Firma Electrónica Avanzada.
PO03	Política del PSC	Modelo Operacional de la PSC	PO01	Anexo 11. Anexo 12. Anexo 24.	Documento del modelo operacional de la AC.
PO04	Política del PSC	Modelo Operacional de la Autoridad de Registro de la PSC	PO01	Anexo 11. Anexo 13. Anexo 24.	Documento del modelo operacional de la AR.

Requisito	Clase	Nombre	Dependencia	Normas y Anexos	Documentación solicitada
AD01	Administración de la PSC	Manual de operaciones PSC	PS03	Anexo 14.	Manual de operaciones de la AC.
AD02	Administración de la PSC	Manual de Operaciones de la Entidad de Registro del PSC	PS04	Anexo 15.	Manual de operaciones de la AR.
PE01	Examen del Personal	Evaluación completa de los perfiles del personal al nivel Altamente Confiable	PO04	ISO 27002. ETSI TS 102 042.	Documentación Relevante.
PE02	Examen del Personal	Evaluación del Oficial de Seguridad de la Instalación (o IT Security Manager)	PE01	ISO 27002.	Documentación Relevante.

4. REQUISITOS DE ACREDITACIÓN

4.1. REQUISITO AS01 – REQUISITOS DE ADMISIBILIDAD

4.1.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Requisitos de admisibilidad del PSC en el proceso de acreditación
Objetivo	Comprobar que el Prestador de Servicios de Certificación (PSC) cumpla con la entrega a la Entidad Acreditadora, al momento de entregar la solicitud de acreditación, de la documentación y el pago del arancel necesario para iniciar el procedimiento.
Descripción	Los requisitos de admisibilidad son aquellos requisitos previos necesarios para iniciar el procedimiento de evaluación del PSC, los que incluyen la presentación de la solicitud de acreditación, entrega de la documentación solicitada, entrega del comprobante de pago de los costos de acreditación y el cumplimiento del plazo establecido para la entrega de documentación faltante en caso de ser necesario.
Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799, Artículo 12. f) y 18. Reglamento Art. 2 y 18
Dependencias	Ninguna
Estándares de evaluación	N/A
Documentación solicitada	<ul style="list-style-type: none">• Solicitud de acreditación conteniendo los datos de individualización del PSC:<ul style="list-style-type: none">a.- Nombre o razón social de la empresa solicitanteb.- RUT de la empresa solicitantec.- Nombre del representante legal de la empresa solicitanted.- RUT del representante legal de la empresa solicitantee.- Domicilio socialf.- Dirección de correo electrónico• Copia de los contrato de los servicios externalizados por la empresa (Reglamento Art. 2), si los hay.• Presentar los procedimientos previstos para asegurar el acceso a los peritos (Reglamento Art. 14)• Adicionalmente toda la documentación especificada en las guías de evaluación para cada uno de los requisitos del proceso de evaluación.
Evidencias solicitadas	Comprobante de pago del arancel de acreditación.

4.1.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Entrega de Documentación solicitada.	Se comprueba que el PSC entregue, al momento de la solicitud de acreditación, toda la documentación solicitada. No se evaluará el contenido de ella.
Entrega de Comprobante de pago de acreditación.	Entrega del comprobante de pago del arancel de acreditación, emitido por Ministerio de Economía, Fomento y Turismo.

4.2. REQUISITO RG01 – REQUERIMIENTOS GENERALES

4.2.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Requerimientos generales de la Ley N°19.799 y su Reglamento
Objetivo	Comprobar que el PSC que solicita la acreditación cumple con los aspectos generales que dispone o se derivan de la Ley y su Reglamento relacionados con los procedimientos necesarios para evaluar si cumple con los requisitos, si es capaz de entregar un servicio de certificación y si presenta evidencias que permitan asegurar su permanencia y continuidad en el negocio.
Descripción	<p>Se verificará que el PSC cumple con los aspectos generales del procedimiento de acreditación, definidos la Ley N°19.799 y su Reglamento. Entre otros, se verificarán los siguientes aspectos:</p> <ul style="list-style-type: none"> • Cumplimiento de procedimientos y plazos definidos por la Entidad Acreditadora. • Libre acceso a los funcionarios o expertos, debidamente identificados, enviados por la Entidad Acreditadora durante el procedimiento de acreditación o auditoría en terreno. • Entrega de información adicional solicitada por la Entidad Acreditadora a través de los funcionarios o expertos debidamente identificados. • Que una vez producido el pronunciamiento de la Entidad Acreditadora, y este es favorable, el PSC contrate y mantenga un seguro, dentro del plazo de 20 días, que cubra su eventual responsabilidad civil, para indemnizar al titular en caso de negligencia o responsabilidad propia, por un monto equivalente a cinco mil unidades de fomento, como mínimo, tanto por los certificados propios como por aquellos homologados por ella.
Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799, Artículos 14, 17 e), 18, 20 y 23 inciso 10° Reglamento Artículos 12, 16 e. y 17
Dependencias	AS01
Estándares de evaluación	N/A
Documentación solicitada	Procedimiento interno para inspección de la Entidad Acreditadora.
Evidencias solicitadas	Póliza de seguro vigente

4.2.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Procedimiento	Cumplimiento de procedimientos y plazos definidos por la Entidad Acreditadora.
Acceso	Libre acceso a los funcionarios o expertos, debidamente identificados, enviados por la Entidad Acreditadora durante el procedimiento de acreditación o la auditoría.
Información	Entrega de información adicional solicitada por la Entidad Acreditadora a través de los funcionarios o expertos debidamente identificados.
Plazo de la entrega de la póliza de seguro de responsabilidad civil	El PSC deberá presentar una póliza de responsabilidad civil según se especifica en el artículo 12 del Reglamento, dentro de los 20 días posteriores a la certificación de que el interesado cumple los requisitos y obligaciones para ser acreditado.

4.3. REQUISITO LE01 – ASPECTOS LEGALES Y DE PRIVACIDAD

4.3.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Requisitos legales y consideraciones de privacidad de la información de los titulares
Objetivo	Comprobar que el Prestador de Servicios de Certificación que solicita la acreditación cumple con los requisitos legales, de privacidad y de calidad de servicios en conformidad a la Ley N°19.799, su Reglamento y otras normativas complementarias aplicables.
Descripción	El PSC interesado debe presentar la documentación necesaria para demostrar al menos lo siguiente: Que es una persona jurídica constituida según la legislación vigente en Chile o en el país que corresponda y que tiene domicilio en Chile.
Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799, Artículo 11, 12 a), f) y j), 17 y 23 inciso 1° a 10° Reglamento Art. 2
Dependencias	Ninguna
Estándares de evaluación	N/A
Documentación solicitada	<ol style="list-style-type: none"> 1. Copia autorizada ante notario de la cédula RUT de la entidad solicitante. 2. Copia fiel de la escritura de constitución de la sociedad, con extracto debidamente inscrito y publicado, con vigencia. 3. Poderes de él o los representantes legales de la entidad solicitante, en el caso que no consten en los estatutos sociales. 4. Iniciación de actividades en la Unidad de Impuestos Internos que tiene jurisdicción sobre el lugar en que se encuentra el domicilio del solicitante. 5. Último balance auditado de la persona jurídica 6. Documento de la Política de Privacidad
Evidencias solicitadas	<p>Documentación que pruebe que la persona jurídica tiene domicilio en Chile y certificado del registro de comercio.</p> <p>Informe de Evaluación de Privacidad de Sitio Web.</p>

4.3.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Personalidad Jurídica	Se verificará la validez y vigencia de la personalidad jurídica del solicitante, mediante la revisión y comprobación de la escritura presentada y sus certificados.

Domicilio	Se verificará que el solicitante tenga domicilio en Chile, mediante la revisión y comprobación del RUT del solicitante y documentos o auditorias que prueben que realiza sus actividades en el país durante el período que declara.
Giro de la empresa	Se comprobará que el giro de la empresa sea compatible con la actividad de Prestador de Servicios de Certificación.
Capital	Se verificará que la entidad jurídica solicitante posea el respaldo financiero necesario que asegure su permanencia en el tiempo y su responsabilidad con los usuarios y receptores de certificados de firma electrónica avanzada. (Se tomará como referencia el capital social solicitado por el SII)
Privacidad de la Información	Se verificará que en los contratos con los titulares existan cláusulas que definan la responsabilidad del prestador en cuanto a proteger la privacidad de la información entregada por el titular y las prácticas que implementa para asegurar este objetivo.
Prácticas no discriminatorias	Se verificará que la Política del Certificado, la Declaración de Prácticas de Certificación y los contratos, no incorporen cláusulas discriminatorias en contra de los titulares o partes que confían.
Publicidad y servicios no contratados.	Se verificará que el Prestador de Servicios de Certificación no incorpore cláusulas que obliguen al titular a recibir publicidad o servicios no deseados y que no puedan ser rechazados si se desea contratar servicios de certificación digital de firma electrónica avanzada.
Concordancia con Ley N°19.496 sobre Protección de los Derechos de los Consumidores.	Revisar que en los contratos de adhesión que el titular de certificados de firma electrónica avanzada contrae con el prestador no contenga cláusulas que puedan contradecir o ignorar la Ley de Protección de los Derechos de los Consumidores.
Concordancia con Ley N°19.628 sobre Protección de la Vida Privada.	Revisar que en los contratos de adhesión que el usuario de certificados de firma electrónica avanzada contrae con el prestador no existen cláusulas que puedan contradecir o ignorar la Ley de Protección de la Vida Privada.
Evaluación de Privacidad del Sitio Web	Revisar que el Sitio Web cumple con los elementos de Privacidad de los usuarios y que estos no puedan contradecir o ignorar la Ley de Protección de la Vida Privada.

4.4. REQUISITO TB01 – ESTRUCTURA CERTIFICADOS

4.4.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Estructura e información del certificado de firma electrónica avanzada.
Objetivo	Comprobar los aspectos mínimos que disponen la Ley y su Reglamento con relación a la conformidad con el estándar, contenidos mínimos, incorporación del RUT, límites y atributos del certificado de firma electrónica avanzada.
Descripción	<ol style="list-style-type: none"> 1. La estructura de datos que conforma el certificado de firma avanzada emitido por el PSC debe estar en conformidad al estándar ISO/IEC 9594-8. 2. El certificado de firma avanzada emitido por el PSC debe contener al menos las siguientes menciones: <ul style="list-style-type: none"> • Un código de identificación único del certificado; • Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada; • Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y su rol único tributario, y • Su plazo de vigencia. 3. El PSC debe incorporar en sus certificados el RUT propio y del titular de acuerdo a la estructura e identificadores que se especifican en el Reglamento. 4. Los PSC deben indicar en forma explícita, que el certificado emitido corresponde a una política de certificados de firma electrónica avanzada. Esta indicación debe quedar inserta en el campo Certificate Policies de las extensiones del certificado del formato X.509 versión 3. Su texto debe ser: "Certificado para firma electrónica avanzada". 5. El PSC interesado debe estructurar los certificados de firma electrónica avanzada que emite de forma que los atributos adicionales que introduce con el fin de incorporar límites al uso del certificado no impidan la lectura de las menciones señaladas en el artículo 22° del reglamento ni su reconocimiento por terceros. 7. Los límites de uso que se incorporen en los certificados de firma electrónica avanzada que emite deben ser reconocibles por terceros. 8. Los datos de creación de firma del PSC acreditado para

	emitir certificados de firma electrónica avanzada no deben ser utilizados para certificados emitidos bajo otras políticas.
Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799, Artículo 14. y 15.- Reglamento, Art. 22 y. 23, Reglamento Disposición Transitoria Primera, Segunda y Tercera.
Dependencias	Ninguna
Estándares de evaluación	ISO/IEC 9594-8 ITU-T X.690
Documentación solicitada	Ninguna
Evidencias solicitadas	Certificado tipo de firma electrónica avanzada, emitido por el PSC en evaluación y certificado de firma electrónica de la AC que los emite, ambos en formato binario.

4.4.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Conformidad con el estándar ISO/IEC 9594-8	Se verificará que la estructura básica del certificado esté en conformidad a la norma y que la gramática utilizada tanto en la estructura básica como en las extensiones obligatorias para incluir el RUT, puedan ser leídos por cualquier aplicación que cumpla dicho el estándar.
Contenido básico del certificado de firma electrónica avanzada emitido por el PSC	Se verificará que el certificado contiene la siguiente información: a) Un código de identificación único del certificado; b) Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada; c) Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y su rol único tributario, y d) Su plazo de vigencia.
Método de incorporación del RUT	Se verificará que el PSC incorpore en sus certificados el RUT propio y del titular de acuerdo a la estructura, sintaxis e identificadores que se especifican en el Reglamento.
Lectura y reconocimiento del contenido mínimo cuando existen atributos adicionales	Se verificará que el PSC estructure sus certificados de firma electrónica avanzada de forma que los atributos adicionales que introduzca con el fin de incorporar límites al uso del certificado, si los hay, no impidan la lectura de las menciones señaladas en el artículo 28° del Reglamento ni su

Aspecto	Evaluación
en el certificado de firma electrónica avanzada emitido por el PSC	reconocimiento por terceros.
Reconocimiento de límites de uso del certificado de firma electrónica avanzada por terceros	Se verificará que el PSC estructure sus certificados de firma electrónica avanzada de forma que los límites de uso, si los hay, sean reconocibles por terceros.
Uso de clave pública acreditada	Se verificará que los datos de creación de firma del PSC acreditado para emitir certificados de firma electrónica avanzada no sean utilizados para certificados emitidos bajo otras políticas.
Algoritmos de firma	Se verificará que el PSC utilice algoritmos de firma estándares de la industria ¹ que provean el adecuado nivel de seguridad tanto para su propia firma como para la firma del titular.
Largos de llaves	Se verificará que el PSC utilice largos de llave pública y privada tales que provean el nivel de seguridad prevaleciente en la industria tanto para su propia firma como para la firma del titular.
Funciones Hash	Se verifica que el PSC utilice funciones Hash estándares de la industria, para el proceso de firma, que provean el adecuado nivel de seguridad tanto para su propia firma como para la firma del titular.

¹IETF RFC 5280, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile., (Obsoletes 3280), D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, Mayo 2008.

4.5. REQUISITO TB02 – ESTRUCTURA CRL y SERVICIO OCSP

4.5.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Estructura e información de la lista de certificados revocados (CRL) y del Servicio en línea de estado de los Certificados (OCSP)
Objetivo	<p>Verificar que las listas de certificados revocados de firma electrónica avanzada tengan el formato y contenido especificado en el estándar, y permita al usuario identificar plenamente al PSC emisor de la CRL.</p> <p>Verificar el estado de los certificados de firma electrónica avanzada tengan el formato y contenido especificado en el estándar, y permita al usuario identificar plenamente el estado del certificado emitido por la PSC emisor.</p>
Descripción	<p>La lista de certificados revocados de firma electrónica avanzada (CRL) debería contener la información y estructura que especifica el estándar ISO/IEC 9594-8.</p> <p>Este estándar especifica que la lista debería contener al menos la identificación del emisor, fecha de su emisión e identificación de los certificados revocados a dicha fecha.</p> <p>Ya que la lista podría ser almacenada y transmitida en medios inseguros, debería estar debidamente firmada por el PSC emisor.</p> <p>El servicio en línea de estado de los certificados (OCSP) debería contener la información y estructura que especifica el estándar RFC 2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol” actualizada según RFC 6277 “Online Certificate Status Protocol Algorithm Agility”</p>
Referencias en Ley N°19.799 o su Reglamento	Reglamento, Primera Disposición Transitoria, Estructura de Certificados.
Dependencias	TB01
Estándares de evaluación	ISO/IEC 9594-8 RFC 2560 y RFC 6277
Documentación solicitada	Política de certificación del certificado de firma electrónica avanzada del PSC.
Evidencias solicitadas	<p>Lista de certificados revocados de firma electrónica avanzada (CRL) emitida por el PSC en evaluación y el certificado de firma electrónica de la AC que la emite.</p> <p>Respuesta a Consulta de Estado de Certificado al Servicio OCSP de la PSC.</p>

4.5.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Contenido Mínimo	<p>Se verificará que la CRL contenga al menos la siguiente información:</p> <ul style="list-style-type: none"> • Versión. Debe tener el valor 2 • Algoritmo de firma. Este campo debe contener la identificación del algoritmo² de firma utilizado. • Nombre del emisor. Este campo debe contener el nombre de la entidad que emitió y firmó la lista de certificados revocados. • Fecha actual. Este campo debe contener la fecha y hora en que fue emitida la lista de certificados revocados (CRL) • Próxima actualización. Se debería incluir en este campo la fecha en que, a más tardar, se emitirá la próxima lista de certificados revocados. • Certificados revocados. En este campo se deben incluir los números de serie de los certificados revocados por el emisor, indicando además la fecha y hora de revocación correspondiente. <p>Se verificará que el Servicio OSCP del PSC este implementado de acuerdo al estándar RFC 2560 en sus mecanismo de:</p> <ul style="list-style-type: none"> • Petición de Validación • Respuesta a la Validación
Comprobación de firma	Se verificará que la lista de certificados revocados esté debidamente firmada por el PSC emisor.
Mecanismo de suspensión de certificados	Se verificará que la lista de certificados revocados puede incluir la información necesaria para indicar el estado de suspensión de un certificado.
Mecanismo de Petición de Validación y Respuesta a la Validación	Se verificará que el servicio OCSP tenga implantado los mecanismos de Petición de Validación y Respuesta a la Validación

²IETF RFC 5280, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile., (Obsoletes 3280), D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, Mayo 2008..

4.6. REQUISITO TB03 – REGISTRO DE ACCESO PÚBLICO

4.6.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Servicios, contenido y accesibilidad electrónica del sistema público de información del PSC.
Objetivo	Asegurar el acceso a información relevante descriptiva del sistema por parte de los titulares y terceros.
Descripción	<p>Se verificará que el PSC interesado:</p> <ul style="list-style-type: none"> • Garantice la existencia de un servicio seguro de consulta remota de un registro de certificados emitidos, en el que quede constancia de los certificados emitidos indicando si el mismo se encuentra vigente, revocado o suspendido, si le ha sido traspasado de otro prestador de servicios de certificación acreditado o es homologado. • Provea acceso al registro público de certificados a los titulares y partes interesadas por medios electrónicos de manera continua y regular. • Use sistemas y productos confiables que garanticen la seguridad de su sistema de difusión de información. • Cuente con procedimientos para informar a los titulares las características generales de los procesos de creación y verificación de firma electrónica, así como de las reglas sobre prácticas de certificación y las demás que el PSC se comprometa a utilizar en la prestación del servicio. • Tenga procedimientos para dejar sin efecto temporal o definitivamente (suspender o revocar) los certificados, fundados en, a lo menos, una de las causas o circunstancias que indica la Ley en el artículo 16º. • Cuente con procedimientos para publicar y actualizar en su(s) sitio(s) de difusión de información de acceso electrónico, las resoluciones de la Entidad Acreditadora que le afecten. Esto debe realizarse como mínimo en los sitios de dominio público registrados durante el proceso de acreditación. Además, debe incluirse la Política (CP) y Declaración de Prácticas de Certificación (CPS)
Referencias en Ley Nª19.799 o su Reglamento	Ley Nª19.799 Artículos 11, 12 letras b y d, 16, 17 letras b y d, 23 inciso 1º Reglamento Artículos 2, 7, 16 b y d, 27, 28, 29, 30.
Dependencias	Ninguna
Estándares de Evaluación	N/A
Documentación solicitada	Documento descriptivo que contenga al menos la siguiente información:

	<ul style="list-style-type: none"> • Individualización del sitio de acceso electrónico, • Descripción de la tecnología, • Disponibilidad, accesibilidad, conexión, esquemas y diagramas de funcionamiento, • Medidas de seguridad.
Evidencias solicitadas	Sitio de acceso electrónico operativo con las funcionalidades descritas.

4.6.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Existencia y contenido mínimo del sitio de información pública.	<p>El PSC debe mantener un sitio de acceso electrónico, en el cual mantenga la información relevante para los titulares y las partes que confían. Debe contener al menos los siguientes documentos:</p> <ul style="list-style-type: none"> • Registro de certificados emitidos, indicando código de identificación único del certificado y su estado (vigente, suspendido o revocado) • Copia de la Lista de certificados revocados (CRL) actualizada cada 24 horas. • Si es pertinente, indicar si el certificado ha sido traspasado de otro prestador de servicios de certificación acreditado o ha sido homologado. • Acceso seguro a los titulares para realizar la revocación o suspensión de certificados vigentes. • Política del certificado de firma electrónica avanzada. • Declaración de sus Prácticas de Certificación. • Resoluciones de la Entidad Acreditadora que le afecten. • Servicio de consulta en línea de estado de un certificado (OCSP)
Disponibilidad de la información pública	Se debe asegurar una disponibilidad del sitio no menor al 99%. Para esto se verificará la existencia de mecanismos redundantes o alternativos de conexión y sitios de emergencia que se levanten manual o automáticamente en caso de desastres.
Seguridad	Se debe proteger la integridad y disponibilidad de la información mediante el uso de tecnología y medidas de seguridad tanto físicas como lógicas que reduzcan los riesgos y consecuencias de ataques maliciosos en contra de los sitios tanto internos como externos.

4.7. REQUISITO TB04 – MODELO DE CONFIANZA

4.7.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Modelo de confianza y TSL
Objetivo	Verificar que el PSC provea a los titulares de certificados de firma electrónica avanzada emitidos por él, de un mecanismo de confianza que le permita comprobar la validez de cualquier certificado de firma electrónica avanzada que reciba.
Descripción	El certificado de firma electrónica avanzada emitido por un prestador de servicios de certificación acreditado deberá permitir a su receptor verificar, en forma directa o mediante consulta electrónica, todos los certificados de firma electrónica avanzada que reciba, con la finalidad de comprobar la validez del mismo. De esta forma es factible asegurar la interoperabilidad en el sistema y la propagación de la confianza depositada por el titular en su PSC hacia el resto del sistema. Se debe poder consultar a la Entidad Acreditadora por el documento en formato TSL que indica los servicios y PSC acreditadas
Referencias en Ley Nº19.799 o su Reglamento	Reglamento Art. 32 inciso 2°.
Dependencias	TB01
Estándares de evaluación	ETSI TS 102 231
Documentación solicitada	Documento en el que se describe el modelo de confianza utilizado por el PSC para lograr el objetivo o alternatively la Política de Certificación si contiene dicho punto. Información entregada de acuerdo a TSL que indica las PSC y sus servicios acreditados según norma ETSI TS 102 231
Evidencias solicitadas	Información TSL de acuerdo a la norma ETSI TS 102 231

4.7.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Modelo de confianza	Se evaluará si el modelo de confianza adoptado permite cumplir con el objetivo planteado
Efectividad	Se verifica el mecanismo utilizado para implementar el modelo de confianza en forma práctica.
TSL	Se evaluará la implantación de TSL de acuerdo a la norma

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

4.8.1. 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
Descripción	<p>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.</p> <p>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.</p> <p>La Gestión del Riesgo incluye los siguientes procesos:</p> <ul style="list-style-type: none"> - 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. <p>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.</p>

Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799 Art. 17 a) Reglamento Art. 16 a. Disposición transitoria
Dependencias	Ninguna
Estándares de evaluación	ISO 27001, ISO 27005
Documentación solicitada	Copia del documento correspondiente a la Evaluación de Riesgos

4.8.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Reporte de la valoración de riesgos ³⁴	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

³Guide for Conducting Risk Assessments, Special Publication 800-30 Revision 1, Recommendations of the National Institute of Standards and Technology, September 2012.

⁴ISO/EIC 27005: 2008, Information technology — Security techniques — Information security risk management, 2008-08-05

4.9. REQUISITO PS02 – POLÍTICA DE SEGURIDAD

4.9.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Documentación y Mantenimiento 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 apoyan formalmente esta política.
Descripción	<p>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.</p> <p>La política de seguridad deberá cumplir a lo menos con los siguientes requerimientos:</p> <ul style="list-style-type: none"> • 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 27002 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. <p>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.</p> <p>Adicionalmente, se recomienda que la documentación describa las reglas, directivas y procedimientos que indican</p>

	como son provistos los servicios específicos y las medidas de seguridad asociadas.
Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799 Art. 17 a) Reglamento Art. 16
Dependencias	PS01
Estándares de evaluación	ISO/IEC 27002, 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.

4.9.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Conformidad con el estándar ISO 27002 sección 5.1.1	Verificar que los requerimientos de la sección 5.1.1 están incorporados.
Conformidad con el estándar ISO 27002 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.
Inclusión de las secciones atinentes indicadas ⁵⁶	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.

⁵SANS Institute: Information Security Policy - A Development Guide for Large and Small Companies, 2006

⁶SANS Institute: Information Security Policy Templates. <http://www.sans.org/security-resources/policies/>

4.10. REQUISITO PS03 – PLAN DE CONTINUIDAD DEL NEGOCIO

4.10.1. 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, mediante una combinación de controles preventivos y planes de contingencia
Descripción	<p>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. Tales planes deben ser mantenidos y probados periódicamente y debieran ser parte integral de los procesos de la organización.</p> <p>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.</p> <p>Este documento debe ceñirse a los lineamientos dados por:</p> <ul style="list-style-type: none"> • Estándar ISO 27002 en su sección 14 y • Estándar ETSI TI 102 042 en su sección 7.4.8 <p>Este documento también deberá describir los procedimientos de emergencia a ser seguidos en a lo menos los siguientes Escenarios:</p> <ul style="list-style-type: none"> • 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, • 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) <p>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.</p> <p>El plan deberá además incluir mecanismos para la</p>

	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 N°19.799 o su Reglamento	Ley N°19.799 Art. 17 a) Reglamento Art. 16 a. Disposición transitoria.
Dependencias	PS02 - Revisión de Análisis de Riesgos y Amenazas. PO02 - Declaración de Prácticas de Certificación.
Estándares de evaluación	ISO 27002, 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

4.10.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Conformidad con el estándar ISO 27002 sección 14.1.1 al 14.1.4	Verificar que los requerimientos de la sección 14 indicados, están incorporados.
Conformidad con el estándar ISO 27002 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 ⁷⁸⁹	Verificar que los principales aspectos de los planes son coherentes con los niveles de riesgo determinados en una evaluación formal de riesgos.
Business Impact ¹⁰ Analysis	Verificar la coherencia del Análisis de Impacto en los Negocios, que debe ser parte del plan de manejo de contingencias.

⁷ISO 22301:2012, Business Continuity Management.

⁸NIST Special Publication 800-34 Rev.1 Contingency Planning Guide for Federal Information Systems, Mayo 2010

⁹BS 25999-1:2006, Business continuity management. Code of practice.

¹⁰<http://www.thebci.org/>

Aspecto	Evaluación
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.
Elementos de auditoría	Verificar que el sistema en el cual el PSC basa sus servicios provee mecanismos de preservación de los elementos de auditoría.

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

4.11.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Documentación y Mantenimiento del 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	<p>El Plan 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.</p> <p>Por lo tanto, el Plan de Seguridad de Sistemas 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</p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • Seguridad Organizacional • Control y clasificación de activos • Administración de las comunicaciones • Control de accesos • Mantenimiento y desarrollo de sistemas <p>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.</p>
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.

4.11.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Relación entre el Plan de Seguridad y los recursos asignados ¹¹	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 Mantenable	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 activos del estándar ISO 27002 están considerados
Requerimientos ISO 27002, sección 8	Verificar que los controles de Seguridad de Recursos Humanos del estándar 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
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

¹¹ISO/IEC 27003:2010, Security techniques -- Information security management system implementation guidance.

Aspecto	Evaluación
Administración de llaves criptográficas	Verificar que el Plan de Seguridad contiene un Plan de Administración de Llaves Criptográficas para todo el ciclo de vida de estas llaves.
Protección del repositorio de acceso público	Verificar que el Plan de Seguridad contiene medidas especiales de protección del repositorio público de certificados.
Protección de información privada	Verificar que el plan incluye medidas de protección de información privada colectada durante el proceso de registro.

4.12. REQUISITO PS05 – PLAN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

4.12.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Implementación del Plan de Seguridad de los Sistemas de Información de la Organización.
Objetivo	Comprobar que la organización tiene implementado un plan de seguridad coherente con su Política de Seguridad, que permita mostrar un nivel de confianza consistente con los objetivos del negocio.
Descripción	<p>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.</p> <p>Se evaluarán:</p> <ul style="list-style-type: none"> • Acciones operacionales, procedimientos y mecanismos que permiten lograr los objetivos indicados en el Plan de Seguridad del PSC. • Controles desplegados o planificados para satisfacer dichos requerimientos. • Que estos controles sean coherentes con los requerimientos del estándar ISO 27002. En particular los planes correspondientes a los siguientes aspectos: <ul style="list-style-type: none"> • Seguridad Organizacional • Control y clasificación de activos • Administración de las comunicaciones • Control de accesos • Mantenimiento y desarrollo de sistemas <p>La evaluación combinará entrevistas con el personal del PSC y auditorías que incluirán visitas a las instalaciones del PSC para verificar la implementación práctica del plan.</p>
Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799 Art. 17 a) y b) Reglamento Art. 16 a) y b). Disposiciones transitorias
Dependencias	PS03, PS04 y ET01
Estándares de evaluación	ISO 27001 ISO 27002
Documentación solicitada	Documento descriptivo de la implementación del Plan de Seguridad de los Sistemas de Información de la Organización
Evidencias solicitadas	Auditoría en terreno

4.12.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Relación entre el Plan de Seguridad ¹² y los recursos asignados	Verificar que el PSC dispone de los recursos y capacidades para implementar los mecanismos y procedimientos de seguridad.
Relación entre Plan de Seguridad 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 Seguridad y Evaluación de Riesgos	Verificar que los procedimientos y mecanismos de seguridad implementados permiten lograr el riesgo residual determinado en la Evaluación de Riesgos.
Plan de Seguridad mantenible	Verificar que la implementación del 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 prácticas y la política de certificación	Verificar que los objetivos de seguridad enunciados en la CPS y la Política de Certificados de Firma 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 implementados
Requerimientos ISO 27002, sección 7	Verificar que los controles de Gestión de activos del estándar ISO 27002 están implementados
Requerimientos ISO 27002, sección 8	Verificar que los controles de Seguridad de Recursos Humanos del estándar ISO 27002 están implementados
Requerimientos ISO 27002, sección 9	Verificar que los controles de Seguridad Física y ambiental del estándar ISO 27002 están implementados
Requerimientos ISO 27002, sección 10	Verificar que los controles de Gestión de las comunicaciones y operaciones del estándar ISO 27002 están implementados
Requerimientos ISO 27002, sección 11	Verificar que los controles de Controles de Acceso del estándar ISO 27002 están implementados
Requerimientos ISO 27002, sección 12	Verificar que los controles de Adquisición, desarrollo y mantenimiento de los sistemas de información del estándar ISO 27002 están implementados
Protección del repositorio de acceso público	Verificar que la implementación del Plan de Seguridad contiene medidas especiales de protección del repositorio público de certificados.
Protección de información privada	Verificar que la implementación del plan incluye medidas de protección de información privada recolectada durante el proceso de registro.

¹²ISO/IEC 27003:2010, Security techniques -- Information security management system implementation guidance.

4.13. REQUISITO PS06 – PLAN DE ADMINISTRACIÓN DE LLAVES

4.13.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Implementación y Mantenimiento del Plan de Administración de Llaves Criptográficas
Objetivo	Comprobar que la organización implementa un plan de administración del ciclo de vida de sus llaves criptográficas coherente con su política de seguridad, que permita mostrar un nivel de confianza consistente con los objetivos del negocio.
Descripción	<p>Las llaves criptográficas son la base de una infraestructura de llaves públicas (PKI), siendo el elemento principal a resguardar y administrar por el PSC, y por lo tanto requiere de un plan específico para su administración (ETSI TS 102 042 sección7.2) Contenido de este plan:</p> <ul style="list-style-type: none"> • Documentación del ciclo de vida completo de las llaves criptográficas, esto es: <ul style="list-style-type: none"> • Generación de las llaves de la autoridad certificadora de firma electrónica avanzada del PSC • Almacenamiento, respaldo y recuperación de la llave privada de la AC de firma electrónica avanzada • Distribución de la llave pública de la AC de firma electrónica avanzada • Uso de la llave privada por parte de la AC de firma electrónica avanzada • Término del ciclo de vida de la AC de firma electrónica avanzada • Administración del ciclo de vida del hardware criptográfico utilizado por la AC. • Servicios de administración de las llaves de los titulares suministradas por la AC (generación de llave y renovación después de vencimiento) • Preparación de los dispositivos seguros de los usuarios. • A su vez el plan debe ser consistente con la Política de los Certificados de firma electrónica avanzada.
Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799 Art. 17 a) Reglamento Art. 16 a. Disposición transitoria
Dependencias	PS02 y PS04
Estándares de evaluación	ETSI TS 102 042 FIPS 140-2

Documentación solicitada	Documento descriptivo de la implementación del Plan de Administración de Llaves Criptográficas de la Organización.
Evidencias solicitadas	Auditoría en terreno

4.13.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Relación entre el Plan de Administración de Llaves y los recursos asignados	Verificar que el PSC dispone de los recursos y capacidades adecuados para implementar el plan de administración de llaves.
Relación entre Plan de Administración de Llaves y Evaluación de Riesgos	Verificar que los procedimientos y mecanismos de administración de llaves implementados permiten lograr el riesgo residual determinado en la Evaluación de Riesgos
Plan de Administración de Llaves mantenible	Verificar que los procedimientos implementados de acuerdo al Plan de Administración de Llaves posibilitan que la seguridad de las llaves se mantiene en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc.
Relación del Plan de Administración de Llaves con las prácticas y política de certificación	Verificar que los objetivos de seguridad enunciados en la CPS y la Política de Certificados de Firma Avanzada se logran a través de la implementación del Plan de Administración de Llaves.
Requerimientos ETSI TS 102 042, sección 7.2.1	Verificar que los requerimientos de Generación de Llaves de la AC, del estándar ETSI TS 102 042 están considerados.
Requerimientos ETSI TS 102 042, sección 7.2.2	Verificar que los requerimientos de Almacenamiento, Respaldo y Recuperación, del estándar ETSI TS 102 042 están considerados.
Requerimientos ETSI TS 102 042, sección 7.2.3	Verificar que los requerimientos de Distribución de la llave pública de la AC, del estándar ETSI TS 102 042 están considerados.
Requerimientos ETSI TS 102 042, sección 7.2.5	Verificar que los requerimientos de Uso de Llave de la AC, del estándar ETSI TS 102 042 están considerados.
Requerimientos ETSI TS 102 042, sección 7.2.6	Verificar que los requerimientos de Fin del Ciclo de Vida de la Llave de la AC, del estándar ETSI TS 102 042 están considerados.
Requerimientos ETSI TS 102 042, sección 7.2.7	Verificar que los requerimientos de Administración del hardware criptográfico del estándar ETSI TS 102 042 están considerados.

Aspecto	Evaluación
Nivel de seguridad del dispositivo seguro de los usuarios	Verificar que el dispositivo seguro de los usuarios cumple como mínimo con los requerimientos del estándar FIPS 140-2 nivel 2 (o Common Criteria EAL 3) en sus elementos de seguridad e implementación de los algoritmos criptográficos estándares.

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

4.14.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Implementación de la gestión de incidentes de seguridad de la información
Objetivo	<p>Evaluar los requisitos relacionados con la gestión de incidentes de seguridad de la Información.</p> <p>Para ello debe fundamentalmente generar reportes 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.</p>
Descripción	<p>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.</p> <p>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.</p> <p>Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.</p> <p>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.</p> <p>Cuando se requiera evidencia, esta se debiera recolectar cumpliendo con los requerimientos legales.</p>
Referencias en Ley N°19.799 o su Reglamento	N/A
Dependencias	PS01
Estándares de evaluación	ISO/IEC 27002 Information technology – Code of practice for information security management (2005-06-15), Sección13

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

4.14.2. 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.
Reporte de eventos en la seguridad de la información(ISO 27002, sección13.1.1)	Se verificará Gestión de un incidente en la seguridad de la información según ISO 27002-Sección 13, Ítem 1.1: Sección 13.1.1 Reporte de eventos en la seguridad de la información
Reporte de las debilidades en la seguridad (ISO 27002, sección 13.1.2)	Se verificará: Gestión de un incidente en la seguridad de la información según ISO 27002-Sección 13, Ítem 1.2: Sección 13.1.2Reporte de las debilidades en la seguridad
Responsabilidades y procedimientos (ISO 27002, sección 13.2.1)	Se verificará: Gestión de un incidente en la seguridad de la información según ISO 27002-Sección 13, Ítem 2.1: Sección 13.2.1 Responsabilidades y procedimientos
Aprender de los incidentes en la seguridad de la información(ISO 27002, sección 13.2.2)	Se verificará: Gestión de un incidente en la seguridad de la información según ISO 27002-Sección 13, Ítem 2.2: Sección 13.2.2Aprender de los incidentes en la seguridad de la información

Aspecto	Evaluación
Recolección de evidencia(ISO 27002, sección 13.2.3)	Se verificará: Gestión de un incidente en la seguridad de la información según ISO 27002-Sección 13, Ítem 2.3: Sección 13.2.3Recolección de evidencia

4.15. REQUISITO ET01 – EVALUACIÓN DE LA PLATAFORMA TECNOLÓGICA.

4.15.1. 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 avanzada, CRL y OCSP.
Descripción	<p>Evaluar la seguridad de los elementos que constituyen la plataforma tecnológica del PSC. Se debe considerar componentes hardware y software que componen la infraestructura PKI del PSC, como asimismo, todos los elementos de apoyo a su operación e interrelación, como protocolos y servicios.</p> <p>Los elementos a considerar son:</p> <ul style="list-style-type: none"> • Módulo criptográfico. • Módulo AC (Autoridad Certificadora) • Módulo AR (Autoridad de Registro) • Módulo de Almacenamiento y Publicación de Certificados. • Protocolos de comunicación entre AC y AR. • 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 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	<p>Documento descriptivo de la implementación de la infraestructura tecnológica.</p> <p>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.</p> <p>Manuales del fabricante de los productos hardware y software relevantes.</p>
Evidencias solicitadas	Documentación del fabricante que acredite el correspondiente nivel de seguridad, y/o de auditores externos.

4.15.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Módulo criptográfico.	<p>1. Funcionalidad y operación:</p> <ul style="list-style-type: none"> • Generar pares de llave privada y pública con largo llaves de al menos 2048bit (CC P2 FCS_COP.1) • Capacidad de firma y cifrado (CC P2 FCS_CKM.2) <p>2. Seguridad.</p> <ul style="list-style-type: none"> • Existencia de sistema control de acceso para acceder a la llave privada. • Existencia de controles de acceso para acceder a funcionalidades de firma y cifrado. <p>3. Ciclo de vida.</p> <ul style="list-style-type: none"> • Capacidad de respaldar la llave privada, en forma segura. • Capacidad de recuperar la llave privada de back-up. <p>4. Auditoría.</p> <ul style="list-style-type: none"> • Capacidad de generar log auditable para administración de contingencia y accesos maliciosos. <p>5. Documentación.</p> <ul style="list-style-type: none"> • Manuales de operación, configuración y puesta en marcha. • Procedimiento de Recuperación ante contingencia.
Módulo AC (Autoridad Certificadora)	<p>1. Funcionalidad y operación:</p> <ul style="list-style-type: none"> • Capacidad para generar certificados con llaves de al menos 2048 bit. • Capacidad de suspensión y revocación de certificados. • Capacidad para generar CRL. • Indicar fecha de publicación y de nueva renovación de la CRL. • Servicios OCSP • 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 CRL a directorios públicos X500. <p>2. Seguridad.</p> <ul style="list-style-type: none"> • 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) <p>3. Ciclo de vida.</p> <ul style="list-style-type: none"> • Capacidad de suspender y revocar certificados. • Capacidad de revocar certificado raíz y generar uno nuevo. <p>4. Auditoría.</p> <ul style="list-style-type: none"> • Capacidad de generar log auditable para administración de

Aspecto	Evaluación
	contingencia, actividades diarias del personal autorizado y accesos maliciosos (CC P2 FAU_STG.2) 5. Documentación. <ul style="list-style-type: none"> • Manuales de operación, configuración y puesta en marcha. • Procedimiento de Recuperación ante contingencia.
Módulo de AR (Autoridad de Registro)	1.- Funcionalidad y operación: <ul style="list-style-type: none"> • Capacidad de recibir requerimientos de certificados (CC P2FCS_CKM.2) • Solicitar certificado a la AC. 2.- Seguridad. <ul style="list-style-type: none"> • Existencia de sistema control de acceso para acceder a la generación de certificados. • Existencia de sistema de control de acceso para acceder a los sistemas de administración y auditoría. 3.- Ciclo de vida. <ul style="list-style-type: none"> • Capacidad de suspender y revocar certificados. • Capacidad de revocar certificado raíz y generar uno nuevo. 4.- Auditoría. <ul style="list-style-type: none"> • Capacidad de generar log auditable para administración de contingencia y accesos maliciosos. 5.- Documentación. <ul style="list-style-type: none"> • 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.
Protocolos de comunicación entre AR y AC	Capacidad de generar certificados de comunicación segura, entre AC y AR, si corresponde a la arquitectura, utilizando un protocolo estándar de la industria (CC P2 FTP_ITC.1)
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 estas intencionadas o no.

4.16. REQUISITO SF01 – SEGURIDAD FÍSICA

4.16.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Seguridad física y ambiental de la infraestructura del PSC
Objetivo	Evaluar los requisitos relacionados con el aseguramiento de áreas restringidas, equipos e información y su protección de efectos ambientales.
Descripción	<p>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.</p> <p>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, deben ser limitados a individuos debidamente autorizados y deben asegurar que no habrá accesos no autorizados.</p> <p>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 las áreas de servicios 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.</p> <p>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.</p> <p>La política de seguridad física y ambiental del PSC 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:</p> <ul style="list-style-type: none"> • 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.)

	<ul style="list-style-type: none"> • 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 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 27002 Information technology – Code of practice for information security management (2005-06-15), Section 9
Documentación solicitada	Análisis de riesgos del PSC. 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

4.16.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Perímetro de seguridad física(ISO 27002, sección 9.1.1)	Se verificará: Evaluación de Seguridad Física según ISO 27002- Sección 9, Ítem 1.1: Sección 9.1.1 Perímetro de seguridad física
Controles de acceso físico (ISO 27002, sección 9.1.2)	Se verificará: Evaluación de Seguridad Física según ISO 27002- Sección 9, Ítem 1.2: Sección 9.1.2 Controles de acceso físico
Seguridad de oficinas, recintos e instalaciones (ISO 27002, sección 9.1.3)	Se verificará: Evaluación de Seguridad Física según ISO 27002- Sección 9, Ítem 1.3: Sección 9.1.3 Seguridad de oficinas, recintos e instalaciones
Protección contra amenazas externas y ambientales (ISO 27002, sección 9.1.4)	Se verificará: Evaluación de Seguridad Física según ISO 27002- Sección 9, Ítem 1.4: Sección 9.1.4 Protección contra amenazas externas y ambientales
Trabajo en áreas seguras(ISO 27002, sección 9.1.5)	Se verificará: Evaluación de Seguridad Física según ISO 27002- Sección 9, Ítem 1.5: Sección 9.1.5 Trabajo en áreas seguras
Áreas de carga, despacho y acceso público (ISO 27002, sección 9.1.6)	Se verificará: Evaluación de Seguridad Física según ISO 27002- Sección 9, Ítem 1.6: Sección 9.1.6 Áreas de carga, despacho y acceso público

Aspecto	Evaluación
Ubicación y protección de los equipos (ISO 27002, sección 9.2.1)	Se verificará: Evaluación de Seguridad Física según ISO 27002- Sección 9, Ítem 2.1: Sección 9.2.1 Ubicación y protección de los equipos
Ubicación y protección de los equipos (ISO 27002, sección 9.2.1)	Se verificará: Evaluación de Seguridad Física según ISO 27002- Sección 9, Ítem 2.1: Sección 9.2.1 Ubicación y protección de los equipos
Servicios de suministro (ISO 27002, sección 9.2.2)	Se verificará: Evaluación de Seguridad Física según ISO 27002- Sección 9, Ítem 2.2. Sección 9.2.2 Servicios de suministro
Seguridad del cableado (ISO 27002, sección 9.2.3)	Se verificará: Evaluación de Seguridad Física según ISO 27002- Sección 9, Ítem 2.3: Sección 9.2.3 Seguridad del cableado
Mantenimiento de los equipos (ISO 27002, sección 9.2.4)	Se verificará: Evaluación de Seguridad Física según ISO 27002- Sección 9, Ítem 2.4: Sección 9.2.4 Mantenimiento de los equipos
Seguridad de los equipos fuera de las instalaciones (ISO 27002, sección 9.2.5)	Se verificará: Evaluación de Seguridad Física según ISO 27002- 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 (ISO 27002, sección 9.2.6)	Se verificará: Evaluación de Seguridad Física según ISO 27002- Sección 9, Ítem 2.6: Sección 9.2.6 Seguridad en la reutilización o eliminación de los equipos
Retiro de activos (ISO 27002, sección 9.2.7)	Se verificará: Evaluación de Seguridad Física según ISO 27002- Sección 9, Ítem 2.7: Sección 9.2.7 Retiro de activos

4.17. REQUISITO PO01 – POLÍTICA DE CERTIFICADOS DE FIRMA AVANZADA

4.17.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Política de Certificados de Firma Electrónica Avanzada.
Objetivo	Comprobar que La Política de Certificados de Firma Electrónica Avanzada contiene los aspectos mínimos dispuestos en la Ley y su Reglamento.
Descripción	<p>Este requisito es relevante no sólo para el titular del certificado sino que para todas las entidades involucradas, incluyendo quienes reciben un documento firmado electrónicamente.</p> <p>Se verificarán a lo menos los siguientes aspectos:</p> <ul style="list-style-type: none"> • La Política de Certificados de Firma Electrónica Avanzada, debe entregar la confianza necesaria para que los documentos firmados en forma electrónica por el titular de un certificado, que se ciña a la forma de operar recomendada, sean equivalentes a una firma holográfica en las circunstancias que indica la Ley. • La Política de Certificados de Firma Avanzada deberá permitir la interoperabilidad con otro PSC. • Las Prácticas de Certificación deberán establecer como el PSC entrega la confianza establecida en la Política de Certificados de Firma Avanzada.
Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799, Artículo 14 y 15. Reglamento, Art. 2, 5, 10, 11, 20, 23, 24, 25 y 26
Dependencias	TB01, TB02, TB03, TB04
Estándares de evaluación	ETSI TS 102 042
Documentación solicitada	Documento conteniendo la Política de Certificados de Firma Electrónica Avanzada
Evidencias solicitadas	Auditoría a la PSC

4.17.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Titulares	La CP deberá indicar a quién se le puede otorgar un certificado de firma avanzada.
Procedimiento de registro	Se verifica el registro del titular. La autenticación, verificación de su identidad en forma fehaciente y forma de política para verificar el nombre del titular. Para que el certificado pueda ser utilizado para firma avanzada.

Aspecto	Evaluación
Usos del certificado	La CP deberá indicar los propósitos para el cual fue emitido el certificado y sus limitaciones.
Obligaciones CA, RA, titular y receptor	Descripción de las obligaciones que contraen las entidades involucradas en la emisión y utilización de un certificado de firma avanzada.
Declaración de las garantías, seguros y responsabilidades de las partes.	Concordancia de las Prácticas de certificación y políticas de certificados con los procedimientos operacionales.
Privacidad y Protección de los datos	Verificación de las políticas de privacidad y protección de datos. Que estas políticas sean las apropiadas para la firma electrónica, pero que sean publicadas y de conocimiento del suscriptor.
Suspensión y revocación del certificado	Verificar bajo qué circunstancias un certificado es suspendido o revocado, y quién puede pedir dichos actos.

4.18. REQUISITO PO02 – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN.

4.18.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Declaración de Prácticas de certificación
Objetivo	Verificar que el PSC disponga de un documento, que señale los procedimientos de operación tanto para otorgar certificados de firma electrónica avanzada como el marco de aplicación de los mismos, según lo establece la Ley N°19.799 y su reglamento.
Descripción	Los elementos principales que debe contener la práctica de certificación de firma electrónica avanzada, son las delimitaciones de responsabilidad y las obligaciones tanto del PSC, como del sujeto a ser identificado digitalmente. Además debe quedar explícito, tanto el ciclo de vida de los certificados, desde su solicitud hasta el término de su vida útil, como el ciclo de vida del PSC, desde el inicio hasta el fin del mismo.
Referencias en Ley N°19.799 o su Reglamento	Reglamento Art. 6 y 16
Dependencias	PO01
Estándares de evaluación	RFC 3647 ETSI TS 102 042
Documentación solicitada	Documentación de las prácticas de certificación.
Evidencias solicitadas	Auditoría a la PSC

4.18.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Verificar estructura	Verificar que la CPS contiene a lo menos los tópicos indicados en el Reglamento de la Ley N°19.799, artículo 6°
Existencia del documento de prácticas de certificación	Verificar que exista documentación de las prácticas de certificación 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. Existencia de procedimientos de protección de la información de los solicitantes.

Aspecto	Evaluación
Las obligaciones y responsabilidades del titular a identificar digitalmente.	Verificar que existan definiciones de los deberes y obligaciones de los usuarios (solicitantes de identificación digital)
Ciclo de vida de los certificados: Emisión / Revocación/Suspensión /Expiración /Renovación.	Verificar que existan procedimientos que definan el ciclo de vida de los certificados. Deberes y procedimientos del PSC para emitir / revocar / suspender / renovar certificados de firma avanzada y definiciones sobre la expiración de los certificados.
Ciclo de vida del PSC.	Verificar que exista la documentación de procedimientos de finalización del giro del PSC, 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, en tanto existan certificados vigentes.
Controles de Seguridad técnica	Verificar la existencia de las medidas de seguridad adoptadas por el PSC para proteger sus datos de creación de firma electrónica avanzada.
Controles de seguridad no técnica	Verificar la existencia de controles utilizados por el PSC para asegurar las funciones de generación de datos de creación de firma electrónica, autenticación de titulares, emisión de certificados, suspensión y revocación de certificados, auditoría y almacenamiento de información relevante.

4.19. REQUISITO PO03 – MODELO OPERACIONAL DE LA AUTORIDAD CERTIFICADORA

4.19.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Modelo Operacional de la Autoridad Certificadora (AC) del PSC.
Objetivo	Comprobar a través de la documentación presentada que el modelo operacional cumple con los requerimientos y obligaciones que dispone la Ley y su Reglamento en relación con la confiabilidad e interoperabilidad en la forma de operar y prestar los servicios de la Autoridad Certificadora (AC) en un PSC.
Descripción	El modelo operacional deberá responder a lo menos a las siguientes preguntas: <ul style="list-style-type: none"> • Cuales son los servicios prestados por la AC del PSC. • Como se interrelacionan los diferentes servicios • En que lugares se operará. • Que tipos de certificados se entregarán • Cómo se pretende hacer esto, incluyendo servicios externalizados. • Como se protegerán los activos
Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799, Artículo 23 Reglamento, Art. 21
Dependencias	PO02
Estándares de evaluación	N/A
Documentación solicitada	Descripción del modelo operacional de la PSC (AC)
Evidencias solicitadas	Auditoría en terreno. Auditoría a la PSC sobre Controles de Documentación, Operación y Acceso Público de una PSC

4.19.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Consistencia del documento	Se verificará que el documento incluya todas las partes atinentes del documento tipo descrito en los Anexos de esta Guía.
Resumen Ejecutivo	Se verificará que el resumen incluya: <ol style="list-style-type: none"> Un resumen coherente del contenido del documento La historia de la empresa. 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 AR b. Implementación de elementos de seguridad c. Procesos de administración d. Sistema de directorios para los certificados e. Procesos de auditoría y respaldo f. Bases de Datos g. Privacidad h. Entrenamiento del personal
Proceso de Certificación	Se verificará que el modelo considere la generación de llaves para el titular de acuerdo a las políticas de certificación.
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.

4.20. REQUISITO PO04 – MODELO OPERACIONAL DE LA AUTORIDAD DE REGISTRO (AR)

4.20.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Modelo Operacional de la Autoridad de Registro (AR)
Objetivo	Comprobar los aspectos mínimos que disponen la Ley y su Reglamento con relación a conformidad con los requisitos de confiabilidad e interoperabilidad en la forma de operar y prestar sus servicios.
Descripción	<p>El modelo operacional deberá responder a:</p> <ul style="list-style-type: none"> • Cuales son los servicios de registro prestados por el PSC. • En que lugares se ofrecerán dichos servicios. • Que tipos de certificados se entregarán. • Cómo se pretende hacer esto, incluyendo los servicios externalizados. <p>Según el artículo 25 del reglamento y la norma técnica ETSI TS 102 042 se entiende que el Prestador de Servicios de Certificación tiene la obligación de generar y entregar en forma segura la llave privada del titular de un certificado de firma electrónica avanzada emitido por él, asegurándose además de la fiabilidad del dispositivo seguro y los mecanismos que el titular utiliza para firmar.</p>
Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799, Artículo 23 Reglamento, Art. 21
Dependencias	PO03
Estándares de evaluación	ETSI TS 102 042
Documentación solicitada	Descripción del modelo operacional de la AR
Evidencias solicitadas	Auditoría en terreno.

4.20.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Consistencia del documento	Se verificará que el documento incluya todas las partes atingentes del documento tipo descrito en el Anexo de esta Guía.
Resumen Ejecutivo	Verificar que el resumen ejecutivo sea coherente con el contenido del documento.

Aspecto	Evaluación
Componentes del sistema	Se verificará que el modelo comprenda los siguientes aspectos: a. Interfaces con CA b. Implementación de dispositivos de seguridad c. Procesos de administración d. Procesos de auditoría y respaldo e. Bases de Datos f. Privacidad g. Entrenamiento del personal
Proceso de Certificación	Se verificará que el modelo de registro del titular provea una identificación unívoca del titular y el modelo de uso de la llave privada provea la confianza requerida en el sistema.
Plan de Auditoría	Se verificará que el modelo de la AR incluya auditoría de lo siguiente: a. Dispositivos de seguridad b. Seguridad c. Restricciones del personal d. Interfaces de administración e. Procedimientos de recuperación de desastres f. Procedimientos de respaldo
Seguridad	Se verificará que el modelo de la AR incluya lo siguiente: a. Descripción de la seguridad física de las instalaciones. b. Seguridad del personal.

4.21. REQUISITO AD01 – MANUAL DE OPERACIONES DE AUTORIDAD CERTIFICADORA

4.21.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Manual de Operaciones de la Autoridad Certificadora del PSC.
Objetivo	Comprobar a través de la documentación presentada que los aspectos operacionales mínimos que dispone la Ley y su Reglamento con relación a los requisitos de confiabilidad e interoperabilidad en la forma de operar y prestar los servicios de la Autoridad Certificadora (AC) de un PSC.
Descripción	<p>El propósito del manual es describir la administración diaria y las prácticas operacionales de la AC y debería ser la guía que garantice que las directrices primarias de la Política de Certificación 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.</p> <p>El manual de operaciones de la AC deberá tener a lo menos las siguientes características:</p> <ul style="list-style-type: none"> • Deberá ser consistente con la Política de Certificación. • Deberá incluir la interacción entra la AC y la AR. • Deberá describir los controles de seguridad física, de red, del personal y de procedimientos. • Deberá incluir los procedimientos adoptados para el manejo de llaves públicas y privadas
Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799, Artículo 14. - y 15. - Reglamento, Art. 2, 5, 10, 11, 20, 23, 24, 25 y 26
Dependencias	PS04
Estándares de evaluación	ETSI TS 102 042 RFC 3647
Documentación solicitada	Manual de operaciones PSC (AC)
Evidencias solicitadas	Auditoría en terreno

4.21.2. 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.

Aspecto	Evaluación
Referencias de los cargos en los planes de la PSC	Referencia del personal en los planes de continuidad del negocio y los planes de recuperación de desastres y emergencia.
Planes de Contingencia	Descripción de los planes de contingencia.
Descripción de las operaciones	Descripción detallada de los siguientes procedimientos: <ul style="list-style-type: none"> • Generación de pares de llaves • Publicación de la CRL • Publicación de la información del certificado • Distribución de llaves y certificados • Renovación de certificados • Renovación de certificados luego de una revocación • Medidas de control de acceso • Procedimientos de respaldo y recuperación
Actualización de CPS y CP	Procedimiento de actualización de la Declaración de Prácticas de Certificación y Política de certificados de firma avanzada.
Servicios de la AC	Descripción de los servicios de la AC
Interacción AC - AR	El documento cubre la interacción entre la AC y AR

4.22. REQUISITO AD02 – MANUAL DE OPERACIONES DE LA AUTORIDAD DE REGISTRO

4.22.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Manual de Operaciones de la Autoridad de Registro (AR)
Objetivo	Comprobar a través de la documentación presentada los aspectos operacionales mínimos que dispone la Ley y su Reglamento con relación a los requisitos de confiabilidad e interoperabilidad de la opera el PSC para realizar las funciones de Autoridad de Registro.
Descripción	<ul style="list-style-type: none"> • El manual de operaciones deberá describir como operará el servicio de registro del PSC y su administración diaria. Entre otros aspectos debería tener las siguientes características: <ul style="list-style-type: none"> • Deberá ser consistente con las políticas de certificación. • Deberá describir el plan de entrenamiento de los empleados. • Deberá incluir la forma en que se verifica la identidad de las personas. • Deberá incluir procedimientos de entrega y uso de la llave privada por los titulares de los certificados. Según el artículo 25 del Reglamento y la norma ETSI TS 102 042 se entiende que el PSC tiene la obligación de generar y entregar en forma segura la llave privada del titular de un certificado de firma electrónica avanzada emitido por él, asegurándose además de la fiabilidad del dispositivo seguro y los mecanismos que el titular utiliza para firmar. • Deberá incluir la metodología adoptada para manejar los temas de: <ul style="list-style-type: none"> • Análisis de riesgos • Plan de recuperación de desastres • Plan de seguridad • Deberá incluir la interacción entre las unidades internas que cumplen la función de AC y AR
Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799, Artículo 14 y 15. Reglamento, Art. 2, 5, 10, 11, 20, 23, 24, 25 y 26
Dependencias	PS04
Estándares de evaluación	RFC 3647
Documentación solicitada	Manual de Operaciones de la AR Manual técnico de los dispositivos seguros de firma electrónica avanzada
Evidencias solicitadas	Auditoría en terreno

4.22.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Nómina y descripción de cargos	Nómina de los cargos de personal empleado, con la descripción de los procedimientos operacionales y la forma en que los empleados realizan sus funciones.
Procedimiento de registro	Se verifica el registro del titular. La autenticación, verificación de su identidad y forma de política para verificar el nombre del titular.
Entrega segura de los datos de creación de firma	El PSC debe tener implementados procedimientos y prácticas que permitan entregar en forma personal y segura los datos de creación de firma al titular del certificado.
Dispositivo seguro y mecanismos de firma del titular	<p>PSC debe tener implementados procedimientos y prácticas que aseguren que una vez entregados los datos de creación de firma sólo el titular tenga control de ellos.</p> <p>El dispositivo seguro entregado al titular debe firmar internamente el documento sin ser jamás accesible la llave privada del titular.</p> <p>El mecanismo de control de acceso a la llave privada sólo debe ser conocido por el titular al momento de la entrega del dispositivo y en lo posible modificable por el mismo titular, antes de ser utilizado por primera vez.</p> <p>El dispositivo seguro debe contar con mecanismos que inhabiliten el dispositivo en caso de reiterados intentos fallidos de acceso.</p> <p>El PSC debe entregar al titular herramientas, aplicaciones e instrucciones para que el titular pueda firmar en forma segura.</p>
Capacitación y servicio al titular.	El PSC debe tener implementados procedimientos de capacitación que permitan al titular manejar en forma segura e informada el dispositivo de firma, y además mantener un servicio de atención para responder y solucionar dudas de los usuarios.
Referencias de los cargos en los planes de contingencia del PSC	Referencia del personal en los planes de continuidad del negocio y los planes de recuperación de desastres y contingencia.
Planes de Contingencia	Descripción de los planes de emergencia.

Aspecto	Evaluación
Descripción de las operaciones	Descripción detallada de los siguientes eventos: 1. Procedimiento seguro de suspensión y revocación de certificados 2. Medidas de control de acceso 3. Procedimientos de respaldo y recuperación
Interacción entre AR y PSC	El documento cubre los procedimientos que involucren la interacción entre la AC y AR

4.23. REQUISITO PE01 – EXAMEN DEL PERSONAL

4.23.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Evaluación de los perfiles del personal que maneja o tiene acceso a sistemas y/o información sensible.
Objetivo	Verificar que el PSC emplea personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión, con el fin de minimizar los riesgos de errores humanos, robos o mal uso de los atributos del cargo.
Descripción	<p>Se evaluará en conformidad al análisis de riesgos del PSC que el personal que maneja o tiene acceso a sistemas e información sensible cumpla al menos con las siguientes condiciones:</p> <p>a) Que tenga la calificación técnica o profesional requerida para el cargo o función que desempeña.</p> <p>b) Que tenga la experiencia mínima requerida para el cargo y función que desempeña.</p> <p>c) Que no posea antecedentes penales o comerciales que lo inhabiliten.</p> <p>d) Que esté instruido en los procedimientos mínimos de seguridad que debe guardar en su función.</p> <p>Se evaluará el procedimiento que utiliza el PSC para reclutar, seleccionar, evaluar y contratar personal crítico.</p> <p>Se evaluará el procedimiento que utiliza el PSC para comprobar los antecedentes del personal crítico antes de contratarlo y el procedimiento para chequear antecedentes del personal contratado.</p> <p>El personal de operaciones y sistemas no debería tener acceso a funciones de confianza, hasta que todos sus antecedentes hayan sido razonablemente verificados.</p> <p>El personal que maneje información sensible, deberá ser personal de planta, y que existan contratos de confidencialidad que se extiendan más allá de la vigencia del contrato del empleado y/o empresa externa.</p>
Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799 Artículo 17, c)
Dependencias	PS02
Estándares de evaluación	ISO 27002 ETSI TS 102 042

Documentación solicitada	Perfiles de los cargos que manejan información o sistemas sensibles Currículos de las personas que ocupan los cargos y funciones sensibles Procedimientos de seguridad aplicados en la contratación y seguimiento de los antecedentes comerciales y penales del personal de la empresa
Evidencias solicitadas	Identificación del personal calificado como crítico, durante la visita del evaluador designado por la Entidad Acreditadora, en la forma que él lo solicite (Presentación de RUT, foto, huella digital, etc.)

4.23.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Antecedentes profesionales del personal crítico	Se verificarán los antecedentes profesionales y la experiencia del personal crítico que trabaja para el PSC, verificando la concordancia de los perfiles en cada cargo y función, con el análisis de riesgos.
Capacitación del personal crítico en aspectos de seguridad acorde a su función y cargo	Se verificará que el personal crítico esté capacitado en las prácticas de seguridad que debe observar de acuerdo a su cargo y función.
Antecedentes comerciales del personal crítico	Se verificarán los antecedentes comerciales del personal crítico.
Antecedentes penales del personal crítico	Se verificarán los antecedentes penales del personal crítico.
Procedimiento de contratación del personal crítico	Se evaluará el procedimiento definido por el PSC para la contratación del personal crítico.
Procedimiento de verificación de antecedentes del personal crítico	Se evaluará el procedimiento definido por el PSC para comprobar los antecedentes del personal crítico una vez seleccionado.

4.24. REQUISITO PE02 – EXAMEN DEL PERSONAL

4.24.1. INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Evaluación del Oficial de Seguridad (OS) de la Instalación.
Objetivo	Verificar la capacidad técnica y los antecedentes del Oficial de Seguridad empleado por el PSC
Descripción	<p>El Oficial de Seguridad debe velar por el diseño, implantación y cumplimiento de los procedimientos y prácticas de seguridad en las instalaciones del PSC. Esta función demanda que el perfil del Oficial y los procedimientos de reclutamiento, evaluación, selección, y verificación de antecedentes penales y comerciales de este personal deben cumplir un alto estándar de exigencia. En particular se debe comprobar que el Oficial cumpla al menos los siguiente requisitos:</p> <p>a) Que tenga la calificación profesional en el ámbito de la seguridad tanto lógica como física. El perfil recomendado como mínimo es Ingeniero Informático o equivalente con certificación y/o experiencia de al menos 5 años en el ámbito de la seguridad informática.</p> <p>b) Que no posea antecedentes penales o comerciales que lo inhabiliten.</p> <p>Se evaluará el procedimiento que utiliza el PSC para reclutar, evaluar y seleccionar al Oficial de Seguridad.</p> <p>Se evaluará el procedimiento y las fuentes que utiliza el PSC para comprobar los antecedentes del Oficial de Seguridad.</p> <p>Adicionalmente, se evaluarán las cláusulas contractuales, de modo que aseguren que la vigencia de compromisos de no divulgación de información más allá de la vigencia de los contratos, en caso de cesación del profesional en el cargo.</p>
Referencias en Ley N°19.799 o su Reglamento	Ley N°19.799 Artículo 17, c)
Dependencias	PS02
Estándares de evaluación	Ninguno
Documentación solicitada	Currículum del Oficial de Seguridad, incluyendo referencias. Procedimientos de seguridad aplicados en la contratación del Oficial de Seguridad y comprobación de antecedentes comerciales y penales.

Evidencias solicitadas	<p>Certificados que acrediten el perfil profesional emitidos por entidades reconocidas u homologadas por el Ministerio de Educación o bien por referentes de la industria.</p> <p>Certificado de antecedentes comerciales.</p> <p>Certificado de antecedentes penales.</p> <p>Entrevista con el Oficial de Seguridad</p>
------------------------	--

4.24.2. ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Antecedentes profesionales del OS	Se verificarán los antecedentes profesionales y curriculares del OS presentados por el PSC.
Antecedentes comerciales del OS	Se verificarán los antecedentes comerciales del OS.
Antecedentes penales del OS	Se verificarán los antecedentes penales del OS.
Procedimiento de contratación del OS	Se evaluará el procedimiento definido por el PSC para la contratación del OS.
Procedimiento de verificación de antecedentes del OS	Se evaluará el procedimiento definido por el PSC para comprobar los antecedentes del OS una vez seleccionado.

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 (CAAdES)
- 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 Continuanance 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	Intellectual 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