Servicios de Certificación de Firma Electrónica Avanzada

Guía de Evaluación
Procedimiento de Acreditación Prestadores de Servicios de Certificación

Ministerio de Economía Fomento y Reconstrucción

CHILE

Versión 1.0

Septiembre de 2002

INTEC CHILE

Servicios de Certificación de Firma Electrónica Avanzada

Guía de Evaluación
Procedimiento de Acreditación Prestadores de Servicios de Certificación

- **Documento Número : EA-003**
- **Versión : 1.0**
- **Estado : Provisional**
- **Fecha de Emisión : 30/09/2002**

Contacto : Patricio Escobar R. (Intec)
pescobar@intec.cl
56 2 2428212

Ministerio de Economía Fomento y Reconstrucción
CHILE

Servicios de Certificación de Firma Electrónica Avanzada

Guía de Acreditación
Procedimiento de Acreditación Prestadores de Servicios de Certificación

CONTENIDO

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 Reconstrucción de Chile en conformidad a la Ley 19799 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)

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 19.799.

PRIMERA PARTE

1 ANTECEDENTES

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 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 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.

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.

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 y el Reglamento.

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.

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 el sistema nacional de firma electrónica con los estándares internacionales, en la medida que ello sea posible, permitiendo así la interoperabilidad internacional del sistema.

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 participes 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.

2.3.6 PRIVACIDAD

La realización de un proceso de acreditación riguroso requiere de información estratégica o altamente sensible de parte de los Prestadores. 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.

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.

2.5 CUMPLIMIENTO DE REQUISITOS

El Prestador de Servicios de Certificación deberá demostrar el cumplimiento de los requisitos de acreditación mediante los siguiente medios:

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

2. Presentando la documentación e información solicitada por la Autoridad 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 guías y documentos modelo para orientar el cumplimiento de cada requisito.

2.6 PRELACIÓN DE REQUISITOS

En caso de que existan en esta guía criterios de evaluación discrepantes o contrapuestos con los requerimientos que se establecen en la Ley 19799, 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 19799 y su Reglamento determinan mediante su normativa un sistema de acreditación Prestadores de Servicios de Certificación que involucra las siguientes entidades:

2.7.1 ENTIDAD ACREDITADORA (A)

El proceso de acreditación de PSCs será desarrollado por la 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 auditorias 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 PSCs acreditados como para los que solicitan acreditación, respectivamente.

2.7.4 PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSCS) (D)

Corresponde a la entidad emisora de certificados de firma electrónica, la cual solicita ser acreditada (Ley 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 PSCs 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 que intervienen en este proceso.

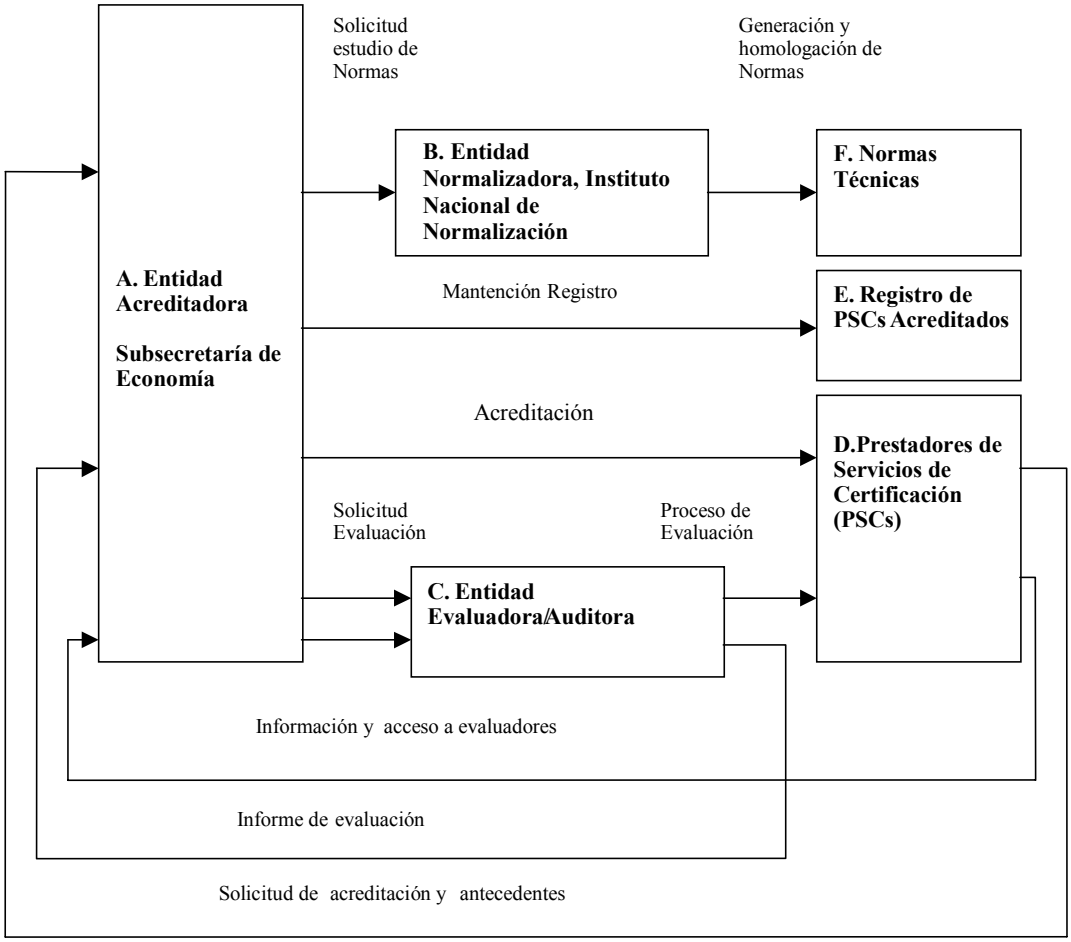


Figura 1: Esquema del sistema de acreditación de PSC.

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 Fig. 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:

1. Toda la documentación definida en las Guías de Evaluación para cada uno de los requisitos especificados.
2. Presentar los procedimientos previstos para asegurar el acceso a los peritos o expertos (Reglamento Art. 14)
3. Y adicionalmente, Copia del contrato de los servicios externalizados, si los hay.

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

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

6. Realizada la evaluación la Entidad Acreditadora procederá a pronunciarse sobre si se cumplen los requisitos y obligaciones exigidas en la Ley y el

Reglamento para otorgar la acreditación dentro de los 90 días siguientes a la Solicitud, prorrogables por razones fundadas.

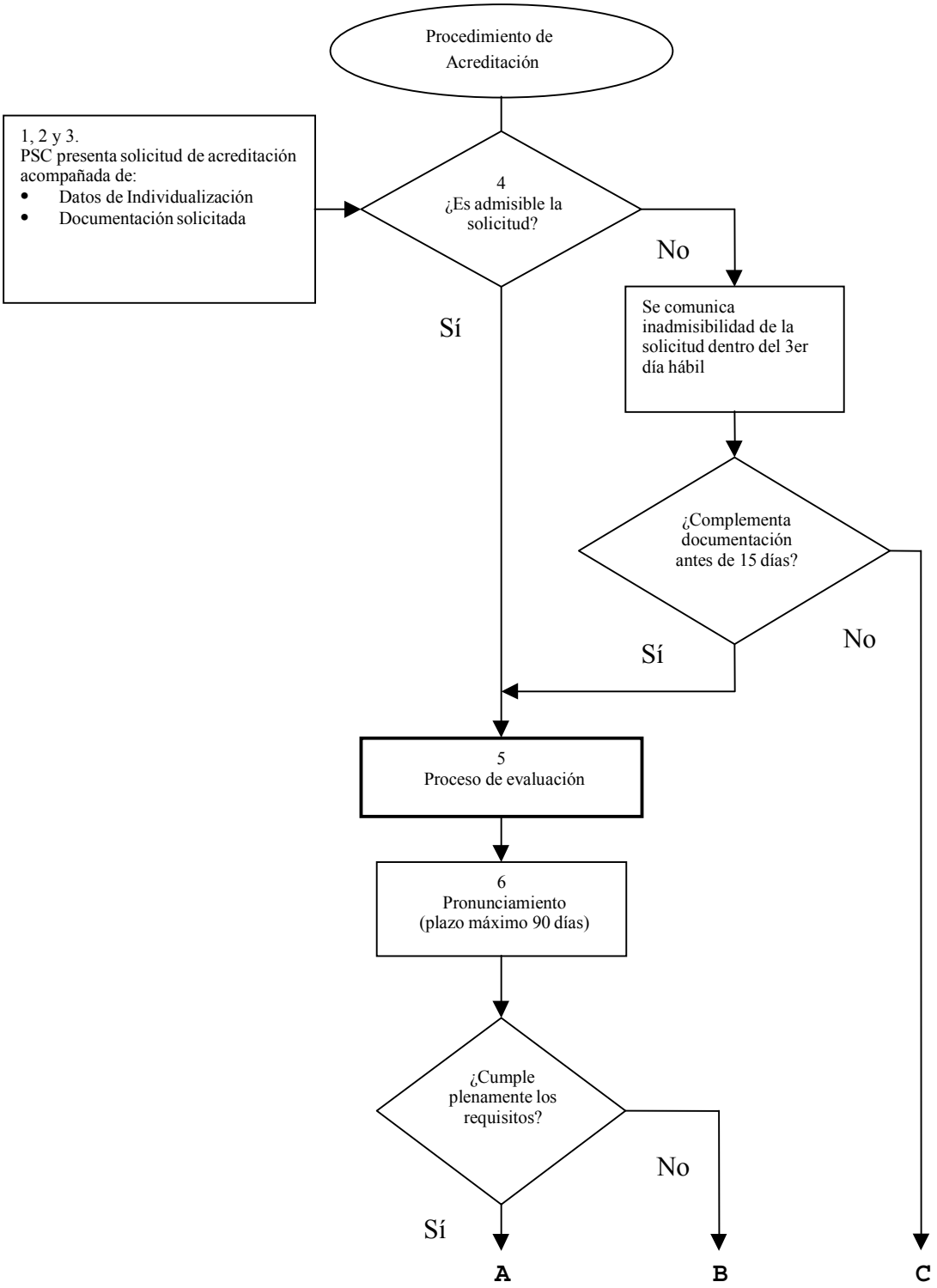
7. En el caso de no cumplir con los requisitos y obligaciones de acreditación definidos por la Ley y el Reglamento, esto es, que existan requisitos que como resultado de la evaluación se determine que no sean subsanables, dicha Entidad procederá a dictar una resolución en la que rechaza la solicitud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


Procedimiento de Acreditación
1, 2 y 3.
PSC presenta solicitud de acreditación acompañada de:
• Datos de Individualización
• Documentación solicitada
4
¿Es admisible la solicitud?
No
Sí
Se comunica inadmisibilidad de la solicitud dentro del 3er día hábil
¿Complementa documentación antes de 15 días?
Sí
No
5
Proceso de evaluación
6
Pronunciamiento
(plazo máximo 90 días)
¿Cumple plenamente los requisitos?
No
Sí
A
B
C

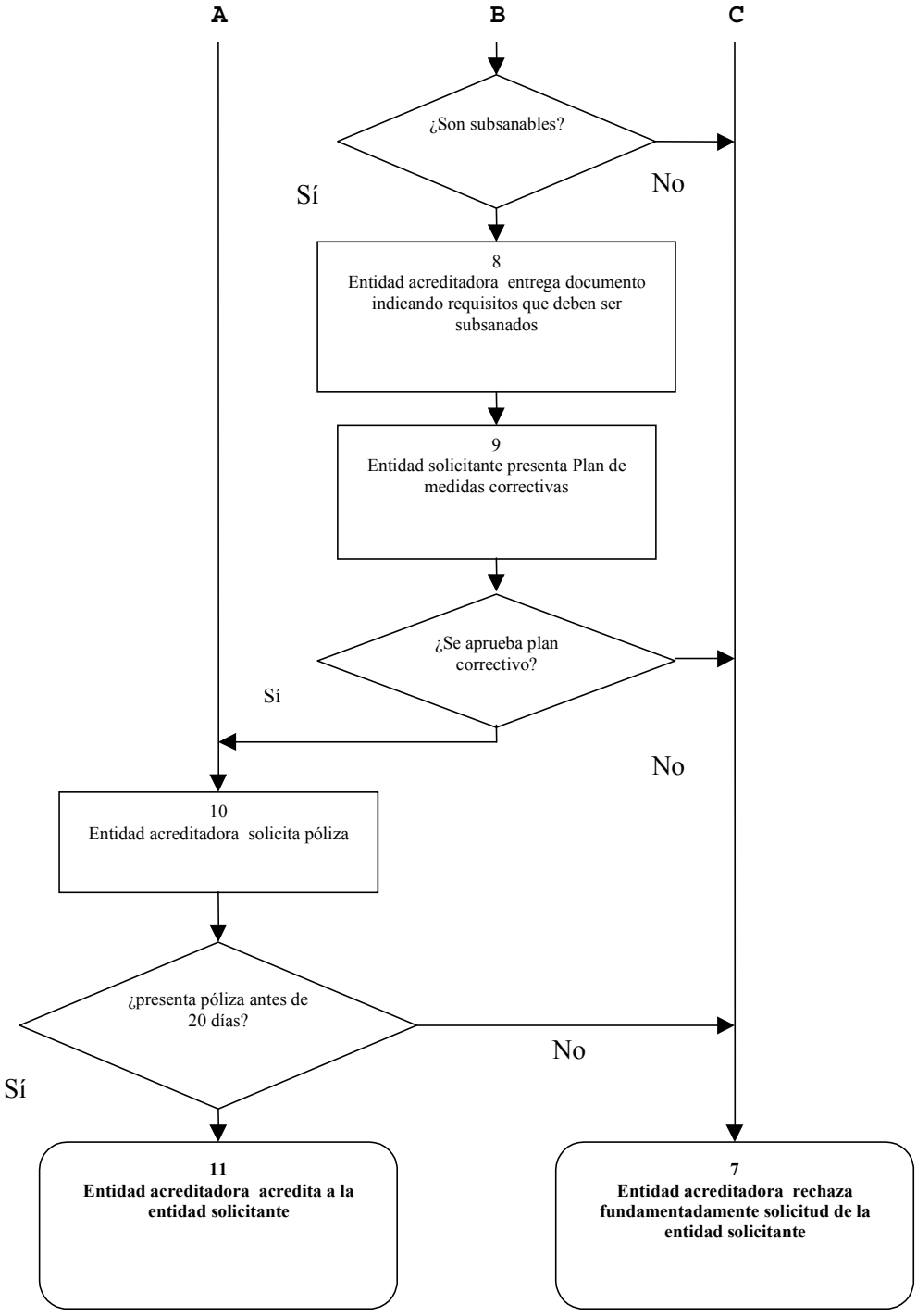


Figura 2: Diagrama de flujos que describe el proceso de acreditación de los PSCs.

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 y el Reglamento 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 19799 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.

Cada requisito se acompaña de una guía de evaluación. El objetivo de las guías 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 autentificar 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 Subsecretaría de Economía Fomento y Reconstrucción.

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 Fomento y Reconstrucción.

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 19799, 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 auditorias 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 registro o durante la vigencia del certificado respectivamente.

3.7.4 TB TÉCNICOS BÁSICOS

Son aquellos requisitos técnicos específicos contenidos en la Ley 19799 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)
- 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 SF SEGURIDAD FÍSICA

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

3.7.8 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

Requisito	Clase	Nombre	Dependencia	Normas y Guías	Documentación Solicitada
AS01	Admisibilidad	Requisitos de Admisibilidad	Ninguna	Ley 19799 y su Reglamento Guía AS01	
RG01	Requerimientos Generales	Requerimientos generales de la Ley 19799 y su Reglamento.	Ninguna	Ley 19799 y su Reglamento Guía RG01	
LE01	Legales	Aspectos Legales y de Privacidad	Ninguno	Ley 19628, 19799 y su Reglamento Guía LE01	Documento de la Política de Privacidad. Constitución de sociedad vigente.
TB01	Tecnológico Básico	Estructura e información del certificado de firma avanzada	Ninguno	Ley 19799 y su Reglamento, ISO/IEC 9594-8 Guía TB01	Certificado tipo de firma electrónica avanzada vigente
TB02	Tecnológico Básico	Estructura e información de la lista de certificados revocados (CRL)	Ninguno	Ley 19799 y su Reglamento, ISO/IEC 9594-8 Guía TB02	Lista tipo de certificados revocados vigente(CRL)
TB03	Tecnológico Básico	Servicios, información y accesibilidad del sistema público de acceso electrónico del PSC. Acceso a certificados emitidos por el PSC.	Ninguno	Ley 19799 y su Reglamento, ISO/IEC 9594-8 Guía TB03	Documento descriptivo de los servicios y la dirección electrónicas vigentes donde se pueden acceder.
TB04	Tecnológico Básico	Modelo de confianza	Ninguno	Ley 19799 y su Reglamento, ISO/IEC 9594-8 Guía TB04	Documento descriptivo.
PS01	Seguridad	Documentación y mantención de la Política de Seguridad	Ninguna	Guía PS01	Política de Seguridad.
PS02	Seguridad	Revisión del Análisis de Riesgos y Amenazas	PS01	Guía PS02	Documento de la valoración de riesgos
PS03	Seguridad	Plan de Continuidad del Negocio y Recuperación de Desastres	PS02	ISO/IEC 17799 ETSI TS 102 042 Guía PS03	1. Plan de Continuidad de Negocios 2. Plan de Recuperación de Desastres

Requisito	Clase	Nombre	Dependencia	Normas y Guías	Documentación Solicitada
PS04	Seguridad	Plan de Seguridad de Sistemas y Administración de llaves resultante de PS02 y de acuerdo al marco de PS01	PS02	Guía PS04	Plan de Seguridad de Sistemas
PS05	Seguridad	Evaluación de la Implementación del Plan de Seguridad de Sistemas	PS03	Guía PS05	Informe auditor independiente
PS06	Seguridad	Evaluación del Plan de Administración de Llaves	PS04	ETSI TS 102 042 Guía PS06	Informe auditor independiente
ET01	Evaluación Tecnológica	Evaluación y Certificación de la Plataforma Tecnológica del PSC	TB, PS03, PS04, PS05	ITSEC 102 042, FIPS 140-1 o ISO/IEC 15408 Guía ET01	Cumplimiento Certificación con estándares
SF01	Seguridad Física	Seguridad física de la infraestructura del PSC	PS04	ISO/IEC 17799 o ETSI TS 102 042 Guía SF01	Documentación relevante
PO01	Política del PSC	Política de los Certificados de Firma Avanzada	PS03, PS05, PS06, ET01, SF01	ETSI TS 102 042 Guía PO01	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 o RFC 2527 Guía PO02	Documento de las Prácticas de Certificación para Firma Electrónica Avanzada
PO03	Política del PSC	Modelo Operacional de la PSC	PO01	Guía PO03	Documento del Modelo Operacional de la AC
PO04	Política de la PSC	Modelo Operacional de la Autoridad de Registro de la PSC	PO01	Guía PO04	Documento del Modelo Operacional de la AR
AD01	Administración de la PSC	Manual de Operaciones del PSC	PS03	Guía AD01	Manual de Operaciones de la AC
AD02	Administración de la PSC	Manual de Operaciones de la Entidad de Registro del PSC	PS04	Guía AD02	Manual de Operaciones de la AR
PE01	Examen del personal	Evaluación completa de los perfiles del personal al nivel Altamente Confiable	PO04	ISO 17799 ETSI TS 102 042 Guía PE01	Documentación relevante
PE02	Examen del personal	Evaluación del Oficial de Seguridad de la Instalación (o IT Security Manager)	PE01	ISO 17799 Guía PE02	Documentación relevante

SEGUNDA PARTE

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 19799 o su Reglamento	Ley 19799, Artículo 12. f) y 18. Reglamento Art. 2 y 18
Dependencias	Ninguna
Estándares de evaluación	N/A
Documentación solicitada	• Solicitud de acreditación conteniendo los datos de individualización del PSC: 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 • Copia de 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 Reconstrucción.

4.2 REQUISITO RG01 – REQUERIMIENTOS GENERALES

4.2.1 INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Requerimientos generales de la Ley 19799 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	Se verificará que el PSC cumple con los aspectos generales del procedimiento de acreditación, definidos la Ley 19799 y su Reglamento. Entre otros, se verificarán los siguientes aspectos: • 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 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 19799 o su Reglamento	Ley 19799, 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 solicitadas	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 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 19799 o su Reglamento	Ley 19799, 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	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. Ultimo balance auditado de la persona jurídica 6. Documento de la Política de Privacidad
Evidencias solicitadas	Documentación que pruebe que la persona jurídica tiene domicilio en Chile y certificado del registro de comercio.

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 de la cédula 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 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 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.

4.4 TB REQUISITOS TECNOLÓGICOS BÁSICOS

4.4.1 IDENTIFICACIÓN CLASE DE REQUISITO

Código	TB
Nombre	Implementación de Requerimientos Tecnológicos Básicos.
Descripción general	Son aquellos requisitos tecnológicos específicos contenidos en la Ley 19799 y su Reglamento o que se deriven directamente de ellos.

4.4.2 REQUISITOS ESPECÍFICOS DE LA CLASE TB

TB01	Estructura e información del certificado de firma electrónica avanzada.
TB02	Estructura e información de la lista de certificados revocados (CRL)
TB03	Servicios, información y accesibilidad del sistema público de acceso electrónico del PSC.
TB04	Modelo de confianza.

4.5 REQUISITO TB01 – ESTRUCTURA CERTIFICADOS

4.5.1 INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Estructura e información del certificado de firma electrónica avanzada.
Objetivo	Comprobar los aspectos mínimos que dispone 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	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: • 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 19799 o su Reglamento	Ley 19799, 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
Evidencia solicitada	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.

4.5.2 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.

Aspecto	Evaluación
Lectura y reconocimiento del contenido mínimo cuando existen atributos adicionales en el certificado de firma electrónica avanzada emitido por el PSC	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 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.

[1] RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, (Obsoletes 2459), R. Housley, W. Polk, W. Ford, D. Solo , April 2002.

4.6 REQUISITO TB02 – ESTRUCTURA CRL

4.6.1 INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Estructura e información de la lista de certificados revocados (CRL)
Objetivo	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.
Descripción	La lista de certificados revocados de firma electrónica avanzada (CRL) debería contener la información y estructura que especifica el estándar ISO/IEC 9594-8. 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. Ya que la lista podría ser almacenada y transmitida en medios inseguros, debería estar debidamente firmada por el PSC emisor.
Referencias en Ley 19799 o su Reglamento	Reglamento, Primera Disposición Transitoria, Estructura de Certificados.
Dependencias	TB01
Estándares de evaluación	ISO/IEC 9594-8
Documentación solicitada	Política de certificación del certificado de firma electrónica avanzada del PSC.
Evidencias solicitadas	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.

4.6.2 ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Contenido Mínimo	Se verificará que la CRL contenga al menos la siguiente información: • Versión. Debe tener el valor 2 • Algoritmo de firma. Este campo debe contener la identificación del algoritmo de firma utilizado[2]. • 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 mas 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.
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.

[2] RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, (Obsoletes 2459), R. Housley, W. Polk, W. Ford, D. Solo , April 2002.

4.7 REQUISITO TB03 – REGISTRO DE ACCESO PÚBLICO

4.7.1 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	Se verificará que el PSC interesado: • 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 16. • 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 19799 o su Reglamento	Ley 19799 Artículos 11, 12 letras b y d, 16, 17 letras b y d, 23 inciso 1° 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: • 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.

4.7.2 ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Existencia y contenido mínimo del sitio de información pública.	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: • 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.
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 del sitio tanto internos como externos.

4.8 REQUISITO TB04 – MODELO DE CONFIANZA

4.8.1 INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Modelo de confianza.
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.
Referencias en Ley 19799 o su Reglamento	Reglamento Art. 32 inciso 2°.
Dependencias	TB01
Estándares de evaluación	N/A
Documentación solicitada	Documento en el que se describe el modelo de confianza utilizado por el PSC para lograr el objetivo o alternativamente la Política de Certificación si contiene dicho punto.
Evidencia solicitada	Ninguna

4.8.2 ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Modelo de confianza	Se evaluará si el modelo de confianza adoptado permite cumplir con el objetivo planteado (Anexo 14)
Efectividad	Se verifica el mecanismo utilizado para implementar el modelo de confianza en forma práctica.

4.9 REQUISITO PS01 – REVISIÓN DE LA EVALUACIÓN DE RIESGOS Y AMENAZAS

4.9.1 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	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. La Evaluación de Riesgos es parte de un proceso más amplio denominado Administración del Riesgo. El objetivo principal de un proceso de administración del riesgo en una organización debe ser proteger la organización y su capacidad de cumplir con su misión, y no sólo sus activos IT. La Administración del Riesgo incluye tres procesos: - Valoración de los riesgos, el cual incluye la identificación y evaluación de los riesgos e impactos de los riesgos, y medidas recomendadas para reducirlos. - Disminución de los riesgos, el cual se refiere a la priorización, implementación y mantención de las medidas de reducción de riesgo apropiadas recomendadas por el proceso de valorización de riesgos. Este proceso conduce a la definición de un Plan de Seguridad, PS04. - Mantención, que corresponde al proceso de evaluación continua para adecuar el proceso de valoración de riesgos a condiciones cambiantes del entorno o del negocio. 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. Se recomienda que un proceso similar al descrito en los documentos indicados en las referencias se siga para realizar el proceso de evaluación de riesgos. El reporte de la valoración de los riesgos debe ceñirse a la estructura indicada en el Anexo B, de la referencia 3. Un ejemplo se muestra en el Anexo 3 de esta Guía.

Referencias en Ley 19799 o su Reglamento	Ley 19799 Art. 17 a) Reglamento Art. 16 a. Disposición transitoria
Dependencias	Ninguna
Estándares de evaluación	N/A
Documentación solicitada	Copia del documento correspondiente a la Evaluación de Riesgos

4.9.2 ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	**Evaluación**
Reporte de la valoración de riesgos[3 y 4]	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 valoración de riesgos	Verificar la valoración a sido realizado o auditado por un ente externo independiente y calificado

[3] Risk Management Guide for information Technology Systems, Special Publication 800-30, Recommendations of the National Institute of Standards and Technology, October 2001.

[4] HANDBOOK 3, RISK MANAGEMENT, Version 1.0, Australian Communications-Electronic Security Instruction 33 (ACSI 33).

4.10 REQUISITO PS02 – POLÍTICA DE SEGURIDAD

4.10.1 INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Documentación y Mantención de la Política de Seguridad de la Información.
Objetivo	Comprobar a través de este documento que la organización tiene claros los objetivos de seguridad relevantes para el negocio y que las instancias de gestión del PSC apoyan formalmente esta política.
Descripción	La política de seguridad es una declaración de objetivos de seguridad. Solo contiene objetivos de seguridad que son factibles de lograr a través de acciones, procedimientos y mecanismos implementados por el PSC. Si el PSC externaliza en otra organización algún aspecto de seguridad o confianza, entonces debe indicarse claramente. La política de seguridad deberá cumplir a lo menos con los siguientes requerimientos: • Los objetivos de seguridad deben ser consecuencia de la Evaluación de Riesgos y Amenazas, de forma tal que los objetivos de la política de seguridad y sus defensas asociadas correspondan al nivel de riesgo requerido para que un PSC sea un ente de confianza. • Debe estar basada en las recomendaciones del estándar ISO 17799 sección 3, los cuales se transcriben en el Anexo 1 de esta guía de evaluación. • Los objetivos de la política son de alto nivel y no técnicos. Por lo tanto, debe ser lo suficientemente general para permitir alternativas de implementación tecnológica. • Si la complejidad de los objetivos así lo requieren, la política puede estar conformada por más de un documento; esto es, puede haber una política general soportada por políticas específicas. • Los elementos de la política de seguridad que estén incorporados tanto en la Declaración de Prácticas de Certificación (CPS) como la Política de los Certificados de firma electrónica avanzada (CP) deben estar incluidos en este documento. Se recomienda que este documento identifique los objetivos de seguridad relevantes y las amenazas potenciales relacionadas a los servicios suministrados, así como las medidas tomadas para evitar o limitar los efectos de estas amenazas. Adicionalmente, se recomienda que la documentación describa las

	reglas, directivas y procedimientos que indican como son provistos los servicios específicos y las medidas de seguridad asociadas. En el Anexo 2 de esta Guía se describen los principales aspectos que una política de seguridad debe considerar. Para los propósitos de la acreditación de un PSC, algunos de los aspectos más relevantes han sido incorporados en criterios separados para así facilitar el proceso de evaluación y donde estos se detallan completamente. Por ello, este documento puede expresar en forma general aquellos aspectos de la seguridad organizacional que se tratan en documentos específicos.
Referencias en Ley 19799 o su Reglamento	Ley 19799 Art. 17 a) Reglamento Art. 16
Dependencias	PS01
Estándares de evaluación	ISO/IEC 17799
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.

4.10.2 ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Conformidad con el estándar ISO 17799 sección 3.1.1	Verificar que los requerimientos de la sección 3.1.1 descritos en el Anexo 1, están incorporados.
Conformidad con el estándar ISO 17799 sección 3.1.2	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 atingentes indicadas[5,6] en el Anexo 2 de esta Guía	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 relacionados con la protección de los procesos de negocios, activos y servicios del PSC.

[5] Internet Security Policy: A Technical Guide, by the National Institute of Standards and Technologies (NIST) http://csrc.nist.gov/nissc/1997/panels/isptg/bagwill/html/

[6] Information Security Policies Made Easy, by Charles Cresson Wood, 8th Ed., Baseline Software, 2001. http://www.baselinesoft.com

4.11 REQUISITO PS03 – PLAN DE CONTINUIDAD DEL NEGOCIO

4.11.1 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	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. 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. Este documento debe ceñirse a los lineamientos dados por: • Estándar ISO 17799 en su sección 11 y • Estándar ETSI TI 102 042 en su sección 7.4.8 Este documento también deberá describir los procedimientos de emergencia a ser seguidos en a lo menos los siguientes eventos: • 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) Parte del plan de manejo de contingencias es el Análisis de Impacto en los Negocios (BIA), siendo esta una evaluación del efecto de las interrupciones no planificadas en el negocio. El plan deberá además incluir mecanismos para la preservación de evidencia de mal uso de los sistemas, cuyo propósito es proporcionar evidencia admisible en una corte judicial en alguna fecha posterior.

Referencias en Ley 19799 o su Reglamento	Ley 19799 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 17799 ETSI TI 102 042
Documentación solicitada	Documento correspondiente al Plan de Continuidad de Negocios y Recuperación ante Desastres Documento de Evaluación de Riesgos
Evidencias solicitadas	Ninguna

4.11.2 ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	**Evaluación**
Conformidad con el estándar ISO 17799 sección 11.1.1 al 11.1.3	Verificar que los requerimientos de la sección 11 indicados en el Anexo 1 de esta Guía, están incorporados.
Conformidad con el estándar ISO 17799 sección 11.1.5	Verificar que se ha incluido un procedimiento de revisión y evaluación periódico de la política de seguridad.
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, reproducido en el Anexo 4 de esta Guía.
Relación entre la Evaluación de Riesgos y el PCN y PRD[7,8,9].	Verificar que los principales aspectos de los planes son coherentes con los niveles de riesgo determinados en una evaluación formal de riesgos.
Bussines Impact Analysis[10]	Verificar la coherencia del Análisis de Impacto en los Negocios, que debe ser parte del plan de manejo de contingencias.

[7] NIST ITL Bulletin June 2002, Contingency Planning Guide for Information Systems.
[8] NIST Special Publication 800-34 Contingency Planning Guide for Information Systems, June 2002.
[9] NIST Special Publication 800-30 Risk Management Guide.
[10] http://www.businesscontinuityworld.com/toolkit.htm

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.

4.12 REQUISITO PS04 – PLAN DE SEGURIDAD DE SISTEMAS

4.12.1 INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Documentación y Mantención del Plan de Seguridad del Sistema de Información.
Objetivo	Comprobar a través de este documento que la organización tiene un plan de seguridad coherente con su Política de Seguridad, que permita mostrar un nivel de confianza consistente con los objetivos del negocio.
Descripción	El Plan de Seguridad tiene como propósito entregar una descripción de los requerimientos de seguridad de los sistemas y describir los controles desplegados o planificados para satisfacer dichos requerimientos. Adicionalmente, debiera delinear las responsabilidades y conductas esperadas de los individuos que acceden al sistema. Por lo tanto, el Plan de Seguridad de Sistemas debiera describir las acciones operacionales, procedimientos y mecanismos que permitan lograr los objetivos indicados en la Política de Seguridad del PSC. El plan de seguridad tendrá que considerar a lo menos las secciones 4 a 10 del estándar ISO 17799. Sin embargo, en este requisito se evaluarán en particular los siguientes aspectos: • Seguridad Organizacional • Control y clasificación de activos • Administración de las comunicaciones • Control de accesos • Mantención y desarrollo de sistemas Se considera que este Plan es una declaración de intenciones del PSC, por lo que la evaluación bajo este requisito no es una certificación de su nivel de seguridad. El proceso de evaluación bajo este requisito indica el nivel de confiabilidad del PSC si este cumple con el plan de seguridad.
Referencias en Ley 19799 o su Reglamento	Ley 19799 Art. 17 a) Reglamento Art. 16 a. Disposición transitoria
Dependencias	PS02
Estándares de evaluación	ISO/IEC 17799
Documentación solicitada	Copia del documento correspondiente al Plan de Seguridad de Información de la Organización.

4.12.2 ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Relación entre el Plan de Seguridad[11,12] y los recursos asignados	Verificar que el PSC puede justificar la disponibilidad de los recursos y capacidades para implementar los mecanismos y procedimientos de seguridad.
Relación entre Plan de Seguridad y Evaluación de Riesgos	Verificar que los procedimientos y mecanismos de seguridad permiten lograr el riesgo residual determinado en la Evaluación de Riesgos.
Relación entre Plan de Seguridad y Política de Seguridad	Verificar que los procedimientos y mecanismos de seguridad permiten lograr los objetivos de la Política de Seguridad.
Plan de Seguridad mantenible	Verificar que el Plan de Seguridad incluye los procedimientos que permiten asegurar que la seguridad del PSC se mantiene en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc.
Relación del Plan de Seguridad con las prácticas y política de certificación	Verificar que los objetivos de seguridad enunciados en la CPS y la Política de Certificados de firma electrónica avanzada se logran a través del Plan de Seguridad.
Requerimientos ISO 17799, sección 4	Verificar que los controles de Seguridad Organizacional del estándar ISO 17799 están considerados (indicados en el Anexo 1 de esta Guía)
Requerimientos ISO 17799, sección 5	Verificar que los controles de Control y Clasificación de Activos del estándar ISO 17799 están considerados (indicados en el Anexo 1 de esta Guía)
Requerimientos ISO 17799, sección 6	Verificar que los controles de Seguridad del Personal del estándar ISO 17799 están considerados (indicados en el Anexo 1 de esta Guía)
Requerimientos ISO 17799, sección 7	Verificar que los controles de Seguridad Ambiental y Física del estándar ISO 17799 están considerados (indicados en el Anexo 1 de esta Guía)
Requerimientos ISO 17799, sección 8	Verificar que los controles de Administración de Operaciones y Comunicaciones del estándar ISO 17799 están considerados (indicados en el Anexo 1 de esta Guía)
Requerimientos ISO 17799, sección 9	Verificar que los controles de Controles de Acceso del estándar ISO 17799 están considerados (indicados en el Anexo 1 de esta Guía)

[11] NIST SP800-18, Guide for Developing Security Plans for Information Technology Systems.
[12] NIST SP800-26 Self Assessment Guide IT Systems Review.

Requerimientos ISO 17799, sección 10	Verificar que los controles de Mantención y Desarrollo de Sistemas del estándar ISO 17799 están considerados (indicados en el Anexo 1 de esta Guía)
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.

4.13 REQUISITO PS05 – IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD DE SISTEMAS

4.1.1 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	El PSC deberá mostrar que sus procedimientos de administración de la seguridad y la capacidad de administrar las instalaciones de acuerdo con el Plan de Seguridad.
	Se evaluarán:
	• 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 17799. En particular los planes correspondientes a los siguientes aspectos:
	  • Seguridad Organizacional
	  • Control y clasificación de activos
	  • Administración de las comunicaciones
	  • Control de accesos
	  • Mantención y desarrollo de sistemas
	La evaluación combinará entrevistas con el personal del PSC y auditorias que incluirán visitas a las instalaciones del PSC para verificar la implementación práctica del plan.

Referencias en Ley 19799 o su Reglamento	Ley 19799 Art. 17 a) y b) Reglamento Art. 16 a) y b). Disposiciones transitorias
Dependencias	PS03, PS04 y ET01
Estándares de evaluación	ISO17799.
Documentación solicitada	Documento descriptivo de la implementación del Plan de Seguridad de los Sistemas de Información de la Organización.
Evidencias solicitadas	Auditoría en terreno

4.13.1 ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación
Relación entre el Plan de Seguridad[13,14] 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 17799, sección 4	Verificar que los controles de Seguridad Organizacional recomendados por el estándar ISO 17799 están implementados (indicados en el Anexo 1 de esta Guía)
Requerimientos ISO 17799, sección 5	Verificar que los controles de Control y Clasificación de Activos recomendados por el estándar ISO 17799 están implementados (indicados en el Anexo 1 de esta Guía)
Requerimientos ISO 17799, sección 6	Verificar que los controles de Seguridad del Personal recomendados por el estándar ISO 17799 están implementados (indicados en el Anexo 1 de esta Guía)
Requerimientos ISO 17799, sección 7	Verificar que los controles de Seguridad Ambiental y Física recomendados por el estándar ISO 17799 están implementados (indicados en el Anexo 1 de esta Guía)
Requerimientos ISO 17799, sección 8	Verificar que los controles de Administración de Operaciones y Comunicaciones recomendados por el estándar ISO 17799 están implementados (indicados en el Anexo 1 de esta Guía)
Requerimientos ISO 17799, sección 9	Verificar que los controles de Controles de Acceso recomendados por el estándar ISO 17799 están implementados (indicados en el Anexo 1 de esta Guía)

[13] NIST SP800-18, Guide for Developing Security Plans for Information Technology Systems.
[14] NIST SP800-26 Self Assessment Guide IT Systems Review.

Requerimientos ISO 17799, sección 10	Verificar que los controles de Mantención y Desarrollo de Sistemas recomendados por el estándar ISO 17799 están implementados (indicados en el Anexo 1 de esta Guía)
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 colectada durante el proceso de registro.

4.14 REQUISITO PS06 – PLAN DE ADMINISTRACIÓN DE LLAVES

4.14.1 INDIVIDUALIZACIÓN DEL REQUISITO

Nombre	Implementación y Mantención 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	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 especifico para su administración (ETSI TS 102 042 sección 7.2) Contenido de este plan:
	• Documentación del ciclo de vida completo de las llaves criptográficas, esto es:
	  • 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 19799 o su Reglamento	Ley 19799 Art. 17 a) Reglamento Art. 16 a. Disposición transitoria
Dependencias	PS02 y PS04
Estándares de evaluación	ETSI TS 102 042 y FIPS 140-1
Documentación solicitadas	Documento descriptivo de la implementación del Plan de Administración de Llaves Criptográficas de la Organización.
Evidencias	Auditoría en terreno

4.14.2 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.
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 140-1 nivel 2 (o Common Criteria EAL 3) en sus elementos de seguridad e implementación de los algoritmos criptográficos estándares.

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 y CRLs.
Descripción	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. Los elementos a considerar son: • 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 19799 o su Reglamento	Ley 19799 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 140-1, ISO/IEC 15408 o equivalente.
Documentación solicitada	Documento descriptivo de la implementación de la infraestructura tecnológica. Este documento debería incluir al menos, planos de interconexión de sistemas, cableado de red de datos, cableado de poder principal y auxiliar, dispositivos de seguridad y control de acceso, y todo aquello relevante que permita demostrar la confiabilidad de la infraestructura tecnológica. Manuales del fabricante de los productos hardware y software relevantes.
Evidencias solicitadas	Documentación del fabricante que acredite el correspondiente nivel de seguridad, y/o de auditores externos.

4.15.2 ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	**Evaluación**
Módulo criptográfico.	1. Funcionalidad y operación: • Generar pares de llave privada y pública con largo llaves de al menos 1024bit (CC P2 FCS_COP.1) • Capacidad de firma y cifrado (CC P2 FCS_CKM.2) 2. Seguridad. • 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. 3. Ciclo de vida. • Capacidad de respaldar la llave privada, en forma segura. • Capacidad de recuperar la llave privada de back-up. 4. Auditoría. • Capacidad de generar log auditable para administración de contingencia y accesos maliciosos. 5. Documentación. • Manuales de operación, configuración y puesta en marcha. • Procedimiento de Recuperación ante contingencia.
Módulo AC (Autoridad Certificadora)	1. Funcionalidad y operación: • Capacidad para generar certificados con llaves de al menos 1024 bit. • Capacidad suspensión y revocación de certificados. • Capacidad para generar CRLs. • Indicar fecha de publicación y de nueva renovación de la CRL. • Capacidad para generar certificados de firma avanzada. • Capacidad de generar certificados de comunicación segura, entre AC y AR, si corresponde a la arquitectura (CC P2 FTP_ITC.1) • Capacidad de entregar certificados y CRLs a directorios públicos X500. 2. Seguridad. • Existencia de sistema control de acceso para acceder a la generación de certificados (CC P2 FIA_SOS.2) • Existencia de sistema de control de acceso para acceder a los sistemas de administración y auditoria (CC P2

	FIA_UAU.2) 3. Ciclo de vida. • Capacidad de suspender y revocar certificados. • Capacidad de revocar certificado raíz y generar uno nuevo. 4. Auditoría. • Capacidad de generar log auditable para administración de contingencia, actividades diarias del personal autorizado y accesos maliciosos (CC P2 FAU_STG.2) 5. Documentación. • Manuales de operación, configuración y puesta en marcha. • Procedimiento de Recuperación ante contingencia.
Módulo de AR (Autoridad de Registro)	1.- Funcionalidad y operación: • Capacidad de recibir requerimientos de certificados (CC P2 FCS_CKM.2) • Solicitar certificado a la AC. 2.- Seguridad. • 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 auditoria. 3.- Ciclo de vida. • Capacidad de suspender y revocar certificados. • Capacidad de revocar certificado raíz y generar uno nuevo. 4.- Auditoría. • Capacidad de generar log auditable para administración de contingencia y accesos maliciosos. 5.- Documentación. • Manuales de operación, configuración y puesta en marcha. • Procedimiento de Recuperación ante contingencia.
Módulo de Almacenamiento y Publicación de Certificados	Almacenamiento de certificados en base de datos X500, y publicación a través de protocolos LDAP v2.0 y/o OCSP V1.0.
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 esta 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	El PSC debe asegurar que el acceso físico a los servicios que manejan información sensible estén controlados y los riesgos físicos para los activos estén reducidos a su valor residual. Los accesos físicos a las áreas de servicios concernientes a la generación de certificados, entrega de dispositivos seguros a titulares, servicios de gestión de revocación y al área de residencia de servidores del PSC, deben ser limitados a individuos debidamente autorizados y deben asegurar que no habrá accesos no autorizados. Los controles deben ser implementados de manera de evitar las pérdidas, daños o compromiso de los activos propios de la actividad del negocio y el compromiso o robo de información. La protección física deberá ser alcanzada a través de la creación de perímetros de seguridad definidos alrededor de los las áreas 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. Los controles de seguridad físicos y ambientales deben ser implementados para proteger los servicios que entregan los recursos de sistemas propios, los servicios utilizados para soportar su operación y contra la suspensión no autorizada de servicios externos. La política de seguridad física y ambiental del PSC en lo concerniente a los sistemas de generación de certificados, provisión de dispositivos seguros a los titulares y gestión de revocación debe contemplar al menos de los siguientes aspectos: • Controles físico de acceso • Protección y recuperación ante desastres naturales • Protección contra robos, forzamiento y entrada • Medidas de protección en caso de incendios • Medidas ante falla de servicios de soporte (electricidad, telecomunicaciones, etc.) • Medidas en caso de fallas estructurales o de las redes

	húmedas • Servicio técnico para los servicios básicos
Referencias en Ley 19799 o su Reglamento	Ley 19799, Artículo 17.- a), Reglamento Art. 16 a., Disposición Transitoria, Primera, Seguridad
Dependencias	PO02
Estándares de evaluación	ETSI 102 042 V1.1.1 (2002-4), 7.4.4 Physical and environment security. ISO/IEC 17799 Information technology – Code of practice for information security management (2000-12-01), 7
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**
Seguridad física del perímetro (ISO 17799, sección 7.1.1)	Se verificará que existan perímetros claramente definidos y eficientes en torno a las áreas sensibles o críticas. Se verificará que las barreras de entrada a los perímetros implementadas son suficientemente fuertes y bien ubicadas para proteger a un nivel razonable dichas áreas y en conformidad al análisis de riesgo efectuado por el PSC. En particular se verificará que las áreas donde se ubican los sistemas de generación de certificados y gestión de revocación de manejo de certificados estén debidamente protegidos mediante puertas y paredes firmes, chapas seguras, controles de acceso, y alarmas de seguridad e incendio.

Aspecto	**Evaluación**
Controles físicos de entrada (ISO 17799, sección 7.1.2)	Se verificará que las áreas seguras sean protegidas por controles de entrada apropiados que aseguren que sólo personal autorizado tenga acceso permitido. En particular se verificará que existan procedimientos definidos y prácticas para asegurar que el acceso a la información sensible o a los servicios de información en proceso sea restringido sólo a personal autorizado y mediante controles de autentificación de al menos dos factores. El acceso de visitas a las áreas críticas, debe requerir de la autorización del oficial de seguridad del perímetro, el visitante debe estar claramente identificado en todo momento con una credencial mientras se encuentre dentro del perímetro y se debe dejar registrado las actividades del visitante con la hora y fecha de su ingreso y salida. Por último se verificará que exista un procedimiento regular de actualización de la autorización de acceso al personal a las áreas restringidas.
Seguridad de oficinas, salas y servicios básico (ISO 17799, sección 7.1.3)	Las áreas seguras deberían ser oficinas cerradas o algunas salas dentro del perímetro de seguridad físico, los cuales deberían ser cerradas y contener gabinetes cerrados o seguros. La selección y diseño de un área segura debería tomar en cuenta la posibilidad de daño por fuego, fluidos, explosión desordenes civiles, y otras formas de desastres naturales o causadas por el hombre. Los servicios claves deben situarse en lugares alejados del acceso o atención de público. Los elementos de soporte tales como fax o fotocopias deben ser instalados dentro de las áreas seguras que lo requieran de tal manera de evitar que la demanda por el acceso a ellos comprometa la seguridad de la información. El material impreso en desuso, debe ser destruido sin posibilidad de recuperación antes de ser desechado. Las puertas y ventanas deben ser bloqueadas y aseguradas cuando no se están utilizando y se debe instalar protección externa en las ventanas. Deben instalarse y mantenerse operativos sistemas de detección de intrusos en todas las puertas y ventanas del perímetro de seguridad. Las salas desocupadas dentro del perímetro deben estar todo el tiempo con el sistema de detección de intrusos activado. La gestión de los servicios de procesamiento de información del PSC debe estar físicamente separada del resto de los servicios.

Aspecto	Evaluación
Trabajo en áreas seguras (ISO 17799, sección 7.1.4)	Se verificará la existencia de los procedimientos y prácticas de seguridad del personal dentro del perímetro de seguridad definido, las que al menos deben contemplar las siguientes prácticas: - El personal debe conocer los procedimientos y prácticas de seguridad definidas dentro del área segura. - El trabajo sin supervisión en áreas seguras debe definirse para evitar problemas de seguridad y prevenir oportunidades que puedan derivar en actividades maliciosas. - Las áreas vacías deben ser bloqueadas y revisadas periódicamente. - El personal de servicios de soporte que no es parte del personal estable del PSC, sólo debe poder acceder a las áreas restringidas en caso de ser necesario. El acceso de este personal debe ser autorizado y monitoreado. - No se debe permitir ningún equipo de grabación, tanto visual como sonoro dentro del perímetro de seguridad.
Separación entre áreas de trabajo y de carga y descarga (ISO 17799, sección 7.1.5)	Se verificará que las áreas de recepción de insumos y salida de basura o cualquier elemento de desecho producido como parte de la operación sean controladas y separadas del área de procesamiento de la información para evitar el acceso no autorizado. Los requerimientos de seguridad para las áreas de atención al cliente deben ser determinados a partir de una evaluación de riesgos. Se verificará que el personal que acceda a las áreas externas de la recepción de insumos y entrega de materiales o desechos esté debidamente controlado. Se verificará que el personal no autorizado, no pueda acceder a través de estas áreas a los perímetros definido de seguridad. Se verificará que las puertas externas de las áreas mencionadas sean seguras cuando las puertas internas se encuentren abiertas. Se verificará que existan procedimientos y prácticas para inspeccionar el material e insumos entrante en busca de potenciales peligros antes de ser trasladado desde la zona de ingreso al punto de uso.
Resguardo y protección del equipamiento (ISO 17799, sección 7.2.1)	Se verificará que el equipamiento sea instalado y protegido para reducir los riesgos de amenazas y peligros ambientales, y oportunidades de accesos no autorizados.

Aspecto	Evaluación
Energía (ISO 17799, sección 7.2.2)	Se verificará que los equipos estén protegidos de fallas y anomalías la alimentación eléctrica. Se verificará especialmente que los equipos sensibles cuenten con unidades de suministro no interrumpible de energía (UPS) y que la instalación cuente con una unidad de generación de energía de respaldo para los equipos y servicios críticos para la operación del PSC.
Seguridad del cableado (ISO 17799, sección 7.2.3)	Se verificará que el cableado de energía y comunicaciones que se emplean para el transporte de datos o soportan los servicios de información se proteja contra intercepción y daños. Las líneas de potencia y comunicaciones al interior de los servicios de información sensibles deben están bajo el piso si es posible o alternativamente con una protección adecuada. El cableado de red debe ser protegido de la intercepción o daño no autorizado. Las líneas de potencia deben estar separadas de las líneas de datos evitar interferencias.
Mantención del equipamiento (ISO 17799, sección 7.2.4)	El equipamiento sensible debe ser correctamente mantenido para asegurar su continua disponibilidad e integridad. El mantenimiento de los equipos se debe realizar de acuerdo a las especificaciones e intervalos recomendados por el fabricante. Los equipos deben ser reparados fuera de las instalaciones del PSC sólo por personal de mantenimiento autorizado. Se debe guardar registro de todas las sospechas de mal funcionamiento o fallas reales y de todos los mantenimientos preventivos y correctivos de los equipos sensibles para la operación del PSC.
Seguridad del equipamiento portátil (ISO 17799, sección 7.2.5)	Se verificará que existan procedimientos y prácticas que eviten que ningún equipo portátil contenga información sensible y que si existieran por alguna razón justificada equipos portátiles que contengan información o procesos críticos de la operación del PSC o información privada de los titulares de los certificados nunca salgan del perímetro de seguridad designado para ellos.
Seguridad del equipamiento en desuso o reutilizado (ISO 17799, sección 7.2.6)	Se verificará que existan procedimientos y prácticas que eviten que equipos a ser reutilizados o en desuso contengan información sensible. Los disquetes, discos duros y otros medios de almacenamiento magnético u óptico que dejen de prestar servicio dentro de los perímetros de seguridad deben ser formateados y/o destruidos antes de salir del perímetro.

Aspecto	**Evaluación**
Política de escritorio y pantalla limpios (ISO 17799, sección 7.3.1)	Se verificará si la empresa ha adoptado la política de “escritorio limpio” y “pantalla limpia” como práctica conocida que permita reducir los riesgos de acceso no autorizado, perdidas o daños de la información durante o fuera el horario normal de trabajo.
Extracción de información o equipos (ISO 17799, sección 7.3.2)	Se verificará que existan procedimientos y prácticas conocidos que eviten que equipos, información o software salgan de los perímetros de seguridad sin autorización.

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	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. Se verificarán a lo menos los siguientes aspectos: • 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 19799 o su Reglamento	Ley 19799, 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	Ninguna

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.
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 subscriptor.
Suspensión y revocación del certificado	Verificar bajo que circunstancias un certificado es suspendido o revocado, y quién puede pedir dichos actos.

4.18 REQUISITO PO02 – DECLARACIÓN DE PRACTICAS 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 19799 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. (Ver Anexo 9)
Referencias en Ley 19799 o su Reglamento	Reglamento Art. 6 y 16
Dependencias	PO01
Estándares de evaluación	RFC 2527 ETSI TS 102 042
Documentación solicitada	Documentación de las prácticas de certificación.
Evidencias solicitadas	Ninguna

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 19799, articulo 6, el cual se detalla en el Anexo 7 de esta Guía.
Existencia del documento de prácticas de certificación	Verificar que exista documentación de las practicas de certificación y que esté debidamente publicada.

Aspecto	Evaluación
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.
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, autentificación de titulares, emisión de certificados, suspensión y revocación de certificados, auditoria 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: • 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 19799 o su Reglamento	Ley 19799, 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.

4.19.2 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 10 de esta Guía.
Resumen Ejecutivo	Se verificará que el resumen incluya: a. Un resumen coherente del contenido del documento b. La historia de la empresa. c. Relaciones comerciales con proveedores de insumos o servicios para sus operaciones.
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 auditoria 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 dispone 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	El modelo operacional deberá responder a: • 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. 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.
Referencias en Ley 19799 o su Reglamento	Ley 19799, 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 Anexo11 de esta Guía.
Resumen Ejecutivo	Verificar que el resumen ejecutivo sea coherente con el contenido del documento.
Componentes del	Se verificará que el modelo comprenda los siguientes aspectos:

Aspecto	**Evaluación**
sistema	a. Interfaces con CA b. Implementación de dispositivos de seguridad c. Procesos de administración d. Procesos de auditoria 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	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. El manual de operaciones de la AC deberá tener a lo menos las siguientes características: • 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 19799 o su Reglamento	Ley 19799, 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 2527
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.
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: • 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	• 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:
	• 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:
	  • 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 19799 o su Reglamento	Ley 19799, Artículo 14 y 15. Reglamento, Art. 2, 5, 10, 11, 20, 23, 24, 25 y 26
Dependencias	PS04
Estándares de evaluación	RFC 2527
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	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. El dispositivo seguro entregado al titular debe firmar internamente el documento sin ser jamás accesible la llave privada del titular. 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. El dispositivo seguro debe contar con mecanismos que inhabiliten el dispositivo en caso de reiterados intentos fallidos de acceso. El PSC debe entregar al titular herramientas, aplicaciones e instrucciones para que el titular pueda firmar en forma segura.
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.
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	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: a) Que tenga la calificación técnica o profesional requerida para el cargo o función que desempeña. b) Que tenga la experiencia mínima requerida para el cargo y función que desempeña. c) Que no posea antecedentes penales o comerciales que lo inhabiliten. d) Que esté instruido en los procedimientos mínimos de seguridad que debe guardar en su función. Se evaluará el procedimiento que utiliza el PSC para reclutar, seleccionar, evaluar y contratar personal crítico. 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. El personal de operaciones y sistemas no debería tener acceso a funciones de confianza, hasta que todos sus antecedentes hayan sido razonablemente verificados. El personal que maneje información sensible, deberá ser personal de planta, y que existan contratos de confidencialidad que se extiendan mas allá de la vigencia del contrato del empleado y/o empresa externa.
Referencias en Ley 19799 o su Reglamento	Ley 19799 Artículo 17, c)
Dependencias	PS02
Estándares de evaluación	ISO 17799 y 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 de la Instalación.
Objetivo	Verificar la capacidad técnica y los antecedentes del Oficial de Seguridad empleado por el PSC
Descripción	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: 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. b) Que no posea antecedentes penales o comerciales que lo inhabiliten. Se evaluará el procedimiento que utiliza el PSC para reclutar, evaluar y seleccionar al Oficial de Seguridad. Se evaluará el procedimiento y las fuentes que utiliza el PSC para comprobar los antecedentes del Oficial de Seguridad. 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.
Referencias en Ley 19799 o su Reglamento	Ley 19799 Artículo 17, c)
Dependencias	PS02
Estándares de evaluación	Ninguno
Documentación solicitada	Currículum del Oficial de Seguridad, incluyendo referencias. Procedimientos de seguridad aplicado en la contratación del Oficial de Seguridad y comprobación de antecedentes comerciales y penales.

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

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.

ANEXOS

ANEXO 1: CONTROLES DEL ESTÁNDAR ISO/IEC 17799, SECCIONES 3 A 11, APLICABLES COMO REQUISITOS DE ACREDITACIÓN DE PSCS EN CHILE.

3. Política de Seguridad de la Información.

3.1.1 Documentación de la política de seguridad

Un documento de política debería ser aprobado por la administración, y publicado y comunicado a todo el personal. Como mínimo, debería incluir las siguientes recomendaciones:

- *Una definición de seguridad de la información, sus objetivos y alcances generales y la importancia de la seguridad como un mecanismo habilitador del intercambio de información.*
- *Una declaración de la intención de la administración, apoyando los objetivos y principios de la seguridad de la información.*
- *Una breve explicación de la (o las) política de seguridad, principios, estándares y requerimientos a cumplir que sean de particular importancia para la organización, como por ejemplo:*
  - *Cumplimiento con requerimientos legales o contractuales*
  - *Requerimientos de educación en seguridad*
  - *Prevención y detección de virus u otros tipos de software dañino*
  - *Administración de la continuidad del negocio*
  - *Consecuencias de la violación de la política de seguridad*
- *Una definición de responsabilidades generales y específicas para administrar la seguridad de información, incluyendo el reporte de incidentes de seguridad.*
- *Referencias a documentación de apoyo a la política, ej. políticas de seguridad más detalladas y procedimientos para sistemas de información específicos, o roles de seguridad con los cuales los usuarios deben cumplir.*

3.1.2 Evaluación y actualización

La política debería tener un encargado que es responsable por su mantención y revisión de acuerdo a un proceso de revisión predefinido. Este proceso debería asegurar que se realiza una revisión en respuesta a cualquier cambio que afecte las bases de la evaluación original de riesgos, ej. incidentes de seguridad relevantes, nuevas vulnerabilidades o cambios en la infraestructura técnica u organizacional. Deberían además estar programadas revisiones periódicas de los siguientes aspectos:

- *Efectividad de la política, demostrada por la naturaleza, número e impacto de los incidentes de seguridad registrados.*
- *Costo e impacto de los controles en la eficiencia del negocio.*
- *Efectos de cambios en la tecnología.*

4. *Seguridad Organizacional*

4.1 Infraestructura de seguridad de la Información: Tiene como objetivo administrar la infraestructura de seguridad de la información dentro de la Organización

- *Management information security forum (4.1.1);*
- *Allocation of information security responsibilities (4.1.3)*
- *Authorization process for information processing facilities (4.1.4)*
- *Specialist information security advice (4.1.5)*
- *Independent review of information security (4.1.7)*

4.2 Seguridad en el acceso de terceras partes: Tiene como objetivo mantener la seguridad de las facilidades de procesamiento de la información y activos de información de la Organización cuando son accedidos por terceras partes.

- *Identification of risks from third party access (4.2.1)*
- *Security requirements in third party contracts (4.2.2)*

4.3 Externalización: Tiene como objetivo mantener la seguridad de la información cuando la responsabilidad del procesamiento de la información a sido externalizada a otra organización.

- *Security requirements in outsourcing contracts (4.3.1)*

5. *Control y Clasificación de Activos*

5.1 Contabilización de los activos: Tiene por objetivo mantener una protección apropiada de los activos de la organización.

- *Inventory of assets (5.1.1)*

5.2 Clasificación de la Información: Tiene por objetivo asegurar que los activos de información reciben un nivel de protección apropiado

- *Classification guidelines (5.2.1)*
- *Information labeling and handling (5.2.2)*

6. *Seguridad de Personal*

6.1 Seguridad en la definición de puestos de trabajo y contratación: Tiene por objetivo reducir los riesgos de errores humanos, robos, fraudes o mal uso de las facilidades.

- *Including security in job responsibilities (6.1.1)*
- *Personnel screening and policy (6.1.2)*
- *Confidentiality agreements (6.1.3)*
- *Terms and conditions of employment (6.1.4)*

6.2 Entrenamiento de Usuarios: Tiene por objetivo asegurar que los usuarios tengan conciencia de las amenazas y precauciones a/con la seguridad de información y tengan el conocimiento que le permita apoyar la política de seguridad corporativa durante su trabajo normal.

- *Information security education and training (6.2.1)*

6.3 Respuesta frente a incidentes de seguridad y fallas: Tiene por objetivo minimizar los daños provenientes de incidentes de seguridad y fallas, y aprender de dichos incidentes.

- *Reporting security incidents (6.3.1)*
- *Reporting security weaknesses (6.3.2)*
- *Reporting software malfunctions (6.3.3)*
- *Learning from incidents (6.3.4)*
- *Disciplinary process (6.3.5)*

7. Seguridad Física y Ambiental

7.1 Areas seguras: Tiene por objetivo prevenir accesos no autorizados, daños e interferencias a la información e infraestructura del negocio.

- *Physical security perimeter (7.1.1)*
- *Physical entry controls (7.1.2)*
- *Securing offices, rooms and facilities (7.1.3)*
- *Working in secure areas (7.1.4)*
- *Isolated delivery and loading areas (7.1.5)*

7.2 Seguridad de equipamiento: Tiene por objetivo prevenir pérdidas, daños o compromiso de activos e interrupciones a las actividades del negocio.

- *Equipment sitting and protection (7.2.1)*
- *Power supplies (7.2.2)*
- *Cabling security (7.2.3)*
- *Equipment maintenance (7.2.4)*
- *Security of equipment off-premises (7.2.5)*
- *Secure disposal or reuse of equipment (7.2.6)*

7.3 Controles generales: Tiene por objetivo prevenir compromiso o robo de información y facilidades de procesamiento de la información.

- *Clear desk and clear screen policy (7.3.1)*
- *Removal of property (7.3.2)*

8. Administración de Operaciones y Comunicaciones

8.1 Procedimientos operacionales y responsabilidades: Tiene por objetivo asegurar la operación segura y correcta de las facilidades de procesamiento de la información.

- *Documented operating procedures (8.1.1)*
- *Operational change control (8.1.2)*
- *Incident management procedures (8.1.3)*
- *Segregation of duties (8.1.4)*
- *Separation of development and operational facilities (8.1.5)*

8.2 Planificación y aceptación de sistemas: Tiene por objetivo minimizar los riesgos de fallas de sistemas.

- *Capacity planning (8.2.1)*
- *System acceptance (8.2.2)*

8.3 Protección contra software malicioso: Tiene por objetivo proteger la integridad del software y la información.

- *Controls against malicious software (8.3.1)*

8.4 Mantención interna: Tiene por objetivo mantener la integridad y disponibilidad del procesamiento de la información y comunicaciones.

- *Information backup (8.4.1)*
- *Operator logs (8.4.2)*
- *Fault logging (8.4.3.)*

8.5 Administración de redes: Tiene por objetivo asegurar la protección de información en redes de datos y la protección de la infraestructura que las provee.

- *Network controls (8.5.1)*

8.6 Seguridad y manejo de medios de almacenamiento: Tiene por objetivo prevenir el daño a los activos e interrupciones a las actividades del negocio.

- *Management of removable computer media (8.6.1)*
- *Disposal of media (8.6.2)*
- *Information handling procedures (8.6.3)*
- *Security of system documentation (8.6.4)*

8.7 Intercambios de información y software: Tiene por objetivo prevenir la pérdida, modificación o mal uso de información intercambiada entre organizaciones.

- *Information and software exchange agreements (8.7.1)*
- *Security of media in transit (8.7.2)*
- *Security of electronic mail (Security Risks and email policy) (8.7.4)*
- *Security of electronic office systems 8.7.5)*
- *Publicly available systems (8.7.6)*

9. Control de Acceso a los Sistemas

9.1 Requerimientos del negocio respecto al control de acceso: Tiene por objetivo controlar el acceso a la información.

- *Access control policy (9.1.1)*

9.2 Administración del acceso de usuarios: Tiene por objetivo prevenir el acceso no autorizado a los sistemas de información.

- *User registration (9.2.1)*
- *Privilege management (9.2.2)*
- *User responsibilities (9.2.3)*

9.3 Responsabilidades de los usuarios: Tiene por objetivo prevenir el acceso no autorizado de usuarios.

- *Password use (9.3.1)*
- *Unattended user equipment (9.3.2)*

9.4 Control de acceso a las redes de datos: Tiene por objetivo asegurar la protección de los servicios de redes.

- *Policy on use of networked services (9.4.1)*
- *User authentication for external connections (9.4.3)*
- *Node authentication (9.4.4)*
- *Remote diagnostic port protection (9.4.5)*
- *Segregation in networks (9.4.6)*

- *Network connection control (9.4.7)*
- *Network routing control (9.4.8)*
- *Security of network services (9.4.9)*

9.5 Control de acceso a los sistemas operativos: Tiene por objetivo prevenir accesos no autorizados a los computadores.

- *Terminal logon procedures (9.5.2)*
- *User identification and authentication (9.5.3)*
- *Password management system (9.5.4)*
- *Use of system utilities (9.5.5)*
- *Terminal timeout (9.5.7)*
- *Limitation of connection time (9.5.8)*

9.6 Monitoreo de uso y acceso a los sistemas: Tiene por objetivo detectar actividades no autorizadas.

- *Event logging (9.6.1)*
- *Clock synchronization (9.6.2)*

9.7 Acceso remoto y computación móvil: Tiene por objetivo asegurar la seguridad de la información cuando se usa computación móvil y facilidades de tele trabajo.

- *Mobile computing (9.7.1)*
- *Teleworking (9.7.2)*

10. Desarrollo y mantención de sistemas

10.1 Requerimientos de seguridad de los sistemas informáticos: Tiene por objetivo asegurar que la seguridad es incorporada en las aplicaciones del negocio.

- *Security requirements analysis and specification (10.1.1)*

10.2 Seguridad en las aplicaciones: Tiene por objetivo prevenir la pérdida, modificación o mal uso de los datos de los usuarios por las aplicaciones.

- *Input data validation (10.2.1)*
- *Control of internal processing (10.2.2)*
- *Message authentication (10.2.3)*
- *Output data validation (10.2.4)*

10.3 Control criptográfico: Tiene por objetivo proteger la confidencialidad, autenticidad e integridad de la información.

- *Policy on the use of cryptographic controls (10.3.1)*
- *Encryption (10.3.2)*
- *Digital signatures (10.3.3)*
- *Non-repudiation services (10.3.4)*
- *Key management (10.3.5)*

10.4 Seguridad de los sistemas de archivos: Tiene por objetivo asegurar que los proyectos IT y las actividades que lo soportan son conducidos de manera segura. Acceso a los sistemas de archivos debería ser controlado.

- *Control of operational software (10.4.1)*
- *Protection of system test data (10.4.2)*
- *Access control to program source library (10.4.3)*

10.5 Seguridad en el desarrollo y procesos de soporte: Tiene por objetivo mantener la seguridad de los datos y software de las aplicaciones.

- *Change control procedures (10.5.1)*
- *Technical review of operating system changes (10.5.2)*
- *Restriction on changes to software packages (10.5.3)*
- *Covert channels and Trojan code (10.5.4)*
- *Outsourced software development (10.5.5)*

11. *Administración de la continuidad del negocio.*

11.1.1 Proceso de administración de la continuidad del negocio

Debe haber un proceso administrado para desarrollar y mantener la continuidad del negocio en todos los ámbitos de la organización. Debe conjugar todos los elementos claves del manejo de la continuidad del negocio descrito a continuación:

- *Clarificar los riesgos a los cuales la organización se enfrenta en términos de su probabilidad de ocurrencia y de su impacto, incluyendo una identificación y priorización de procesos críticos del negocio.*
- *Clarificar el impacto que las interrupciones probablemente tendrán en el negocio (es importante que se encuentren soluciones para manejar incidentes pequeños, así como incidentes serios que pueden amenazar la viabilidad de la organización), y establecer los objetivos de negocios de las facilidades de procesamiento de la información.*
- *Considerar la contratación de los seguros adecuados que pueden formar parte del proceso de continuidad del negocio.*
- *Formular y documentar una estrategia de continuidad del negocio consistente con los objetivos y prioridades concordados del negocio.*
- *Formular y documentar planes de continuidad del negocio en concordancia con la estrategia definida.*
- *Actualización y prueba periódica de los planes y procesos definidos.*
- *Asegurar que la administración de la continuidad del negocio esté incorporada en los procesos y estructura de la organización. La responsabilidad de coordinar el proceso de administración de la continuidad del negocio debería ser asignada en un nivel adecuado de la organización, ej. en el comité de seguridad de la información.*

11.1.2 Continuidad del negocio y análisis de impactos

La continuidad del negocio debería comenzar con la identificación de eventos que pueden causar interrupciones en los procesos del negocio, ej. falla de equipos, inundaciones e incendios. Esto debiera ser seguido por una *evaluación de riesgos* para determinar el impacto de esas interrupciones (tanto en términos de magnitud del daño y periodo de recuperación) Ambas actividades debieran ser efectuadas involucrando completamente a los dueños de los procesos y recursos del negocio. Esta evaluación considera todos los procesos del negocio y no está limitada a las facilidades de procesamiento de la información.

Dependiendo de los resultados de la evaluación de riesgos, un plan estratégico debería desarrollarse para determinar la aproximación global a la continuidad del negocio. Una vez que este plan ha sido creado, debe ser ratificado por las instancias de gestión de la organización.

11.1.3 Documentación e implementación de planes de continuidad

Los planes deberían desarrollarse para mantener o restaurar las operaciones del negocio en el lapso de tiempo requerido después de la interrupción de, o falla de, los procesos críticos del negocio. El proceso de planificación de la continuidad del negocio debería considerar lo siguiente:

- *Identificar y acordar todas las responsabilidades y procedimientos de emergencia.*
- *Implementar procesos de emergencia que permitan la recuperación y restauración en los lapsos de tiempo requeridos.*
- *Documentar los procesos y procedimientos concordados.*
- *Entrenar adecuadamente al personal a cargo respecto de los procedimientos y procesos de emergencia incluyendo la administración de la crisis.*
- *Actualización y pruebas de los planes.*

El proceso de planificación debería focalizarse en los objetivos del negocio, ej. restaurar servicios específicos para los clientes en un lapso de tiempo aceptable. Los servicios y recursos que posibilitarán este objetivo deberían ser considerados, incluyendo personal, recursos que no sean de procesamiento de la información, así como acuerdos de uso de facilidades alternativas de procesamiento de la información.

11.1.5 Pruebas, mantención y reevaluación de planes de continuidad del negocio.

11.1.5.1 Prueba de los planes

Los planes de continuidad del negocio pueden fallar en el momento de utilizarlos, a menudo por suposiciones incorrectas, omisiones o cambios en el equipamiento o el personal. Deberían por lo tanto probarse periódicamente para asegurar que ellos están actualizados y son efectivos. Tales pruebas deberían también asegurar que todos los miembros del grupo de recuperación y personal relevante están al tanto de los planes.

El cronograma de pruebas del plan de continuidad del negocio debería indicar como y cuando cada elemento del plan debería ser probado. Se recomienda probar frecuentemente los elementos individuales del plan. Diferentes técnicas deberían ser utilizadas para proveer la seguridad de que el plan funcionará en la vida real. Estos deberían incluir:

- Pruebas de escritorio de diferentes escenarios (discutiendo las acciones de recuperación del negocio usando interrupciones representativas)
- Simulaciones (particularmente para entrenar a la gente en sus roles de administración de la crisis después del incidente)
- Pruebas de recuperación tecnológica (asegurando que los sistemas de información pueden ser restauradas efectivamente)
- Pruebas de recuperación en un sitio alternativo (ejecutando los procesos de negocios en paralelo con las operaciones de recuperación lejos el sitio principal)
- Pruebas del proveedor de facilidades y servicios (asegurando que los servicios y productos externalizados proveerán los requerimientos contratados)
- Recuperación completa (probando que la organización, personal, equipos, facilidades y procesos pueden subsanar la interrupción)

11.1.5.2 Mantención y reevaluación del plan.

Los planes de continuidad del negocio deberían ser mantenidos mediante revisiones y actualizaciones periódicas para asegurar su efectividad en el tiempo. Procedimientos deberían ser incluidos en el programa de administración del cambio en la organización para asegurar que los temas de continuidad del negocio son tratados adecuadamente.

Debería designarse un responsable de las revisiones periódicas del plan. La identificación de cambios en la estrategia de negocios que aun no estén reflejadas en el plan de continuidad del negocio debería ser seguida de una actualización adecuada del plan. Este proceso formal de control cambios debería asegurar que los planes actualizados son distribuidos y reforzados por revisiones periódicas del plan total.

Ejemplos de situaciones que podrían necesitar una actualización de los planes incluyen la adquisición de equipamiento nuevo, o actualizaciones de sistemas operativos y cambios en:

- *Personal*
- *Direcciones y números de teléfono*
- *Estrategia de negocios*
- *Ubicaciones, facilidades, recursos*
- *Normativas y leyes*
- *Contratistas, proveedores y clientes clave*
- *Nuevos procesos o eliminación de procesos*
- *Riesgo (operacional y financiero)*

ANEXO 2: DOCUMENTO ESTÁNDAR DE UNA POLÍTICA DE SEGURIDAD.

Una política de seguridad puede estar divida en a lo menos las secciones descritas a continuación. Cada sección debería incorporar a lo menos los cuatro aspectos siguientes:

1. Una declaración resumida de dicho aspecto particular de la política, que indica que debe suceder sin indicar como se realiza.
2. Identificación de la persona o comité responsable de establecer la política.
3. Identificación de la persona o comité responsable de implementar la política.
4. Referencias que apuntan a las guías de implementación, recomendaciones detalladas o políticas relacionadas.

Organización. Detalla las relaciones y responsabilidades respecto a la seguridad en la organización. Describe como se formula la política de seguridad, con especial énfasis en cuales grupos formales, staff o proceso consultivo es requerido por la organización antes de promulgar la política. Describe la relación con instituciones externas que tienen una responsabilidad en proveer asesoría y soporte en seguridad. Describe las relaciones (si las hay) con proveedores de servicios u otras instituciones con las que se requiere cooperación en materias de seguridad, o hace referencia a documentos legales que detallen estas relaciones. Describe quienes son los responsables en realizar revisiones o auditorias de seguridad de los sistemas de información.

Evaluación de riesgos. Incluye una referencia a la evaluación de riesgos que formará la base de la política de seguridad. En lo posible se debe incluir un resumen de esta evaluación en un anexo de la política.

Control de Acceso. Especifica los niveles de clasificación de la confidencialidad e importancia de la información que será manipulada o que podría ser accesada por el personal autorizado de los sistemas de información de la organización. Esta sección debiera detallar algunos objetivos para controlar el acceso a información clave (esto es, el bosquejo de una “matriz de control de acceso”) Los principales dueños de la información deberían también ser identificados, cuando sea adecuado.

Seguridad de Personal (relacionado son seguridad IT) Especifica los requerimientos de selección del personal de seguridad y como estos serán logrados. En caso de no ser necesaria una selección formal de seguridad, esta sección detalla la política de verificación indirecta de antecedentes del personal para asegurar que personal no adecuado sea empleado en posiciones de confianza. Proveer directrices bajo las cuales personal, contratistas, consultores y/o auditores pueden acceder a las dependencias de la organización, darle acceso a información de los sistemas internos, etc. También es importante un plan mediante el cual al personal se le da acceso de superusuario o acceso privilegiado a los sistemas especificados. Acceso privilegiado se define como un acceso mediante el cual el usuario tiene la posibilidad de cambiar elementos claves de la configuración del sistema, tener acceso a elementos de auditoría o información relacionada, o tener acceso a datos, archivos o cuentas pertenecientes a otros usuarios. Esta sección también debería detallar las responsabilidades asociadas con el uso de los sistemas de la organización y los requerimientos que permitan asegurar que los usuarios estén conscientes de sus responsabilidades y efectos de las contravenciones.

Seguridad Física. Especifica los objetivos de seguridad física incluyendo, pero no limitado a, eliminación de elementos en desuso, guardias, alarmas de seguridad física, tiempos de

respuesta, llaves físicas, y estructura de la seguridad física de todas las dependencias relevantes.

Seguridad de Comunicaciones y Redes. Especifica como las conexiones de red con otras organizaciones son aprobadas y administradas. Debería indicar además los requerimientos de seguridad para cualquier otro medio de comunicación.

Mantención de equipos y su desecho. Especifica los objetivos de la política tendientes a asegurar la integridad de los sistemas hardware y software cuando un equipo es reemplazado, decomisado o sometido a mantención. La política debe establecer si al personal no seleccionado bajo criterios de seguridad le es permitido realizar mantención del equipamiento y en caso de ser permitido como se realizaría. La manipulación, control y desecho de medios de almacenamiento son también componentes importantes de la política global de seguridad.

Control de Cambios y Configuración. Especifica los entes responsables de la aprobación de cambios a los sistemas, y los procesos mediante los cuales deberían aprobarse estos cambios. Debería designarse supervisores del proceso de cambio.

Planificación de Contingencias. Especifica los objetivos críticos de la administración para un plan de contingencia. Debe establecerse una relación clara entre la evaluación de riesgos y lo objetivos del plan de contingencia, tal que los objetivos de la política de contingencia correspondan al nivel de riesgo estimado. La política debe definir un “incidente” y una “caída de sistemas” y un encargado responsable de la declaración de un incidente y una caída de sistemas. Un incidente no necesariamente puede generar una caída de sistemas, pero puede requerir una evaluación del responsable. Una guía de la política respecto a los tiempos de recuperación para los diferentes niveles de caída de sistemas puede ser apropiado. Alguna guía para el régimen de pruebas y reporte de estado de los sistemas de respaldo también puede requerirse. Esta sección puede incluir una referencia al Plan de Continuidad de Negocios.

Respuesta a Incidentes. Contiene definiciones claras de los tipos de incidentes que son probables de ocurrir, de forma que un plan documentado pueda ser derivado para alertar a la administración respecto a la respuesta esperada. Deberían especificarse objetivos de seguridad para reportes en tiempo real e incluirse requerimientos de como la administración ejecutiva debería involucrase. Especifica la(s) autoridad(es) responsable de iniciar investigaciones internas y el esquema de investigación de un incidente. También es útil incluir la referencia a un plan de control de fraudes y los criterios mediante los cuales la autoridad responsable iniciará una investigación formal o policial de un incidente. Referencias específicas a las medidas antivirus y la respuesta frente a incidentes virales debería incluirse.

Auditorias y Detección de Intrusiones. Especifica los objetivos de la detección de intrusiones, incorporando los requerimientos para la administración y mantención de herramientas y técnicas de detección de intrusiones, y administración y revisión de trazas para auditoría. Debería haber una asociación entre los objetivos de la detección de intrusiones y los objetivos del componente de respuesta frente a incidentes.

Medios de Almacenamiento. Especifica los objetivos de la administración de medios de almacenamiento conteniendo datos clasificados. Esto incluye la administración de medios para respaldo y recuperación.

ANEXO 3: EJEMPLO DE VALORACIÓN DE RIESGOS

NOTAS:

1. Esta valoración se provee solo como un EJEMPLO, para propósitos de guía.
2. Los datos ingresados en esta tabla han sido clasificados por el nivel de la "Prioridad de la Contramedida" (columna 7)

Columna 1	Columna 2	Columna 3	Columna 4	Columna 5	Columna 6	Columna 7
Identificación del Activo	Amenaza al Activo	Probabilidad de la Amenaza	Daño, de ocurrir la amenaza	Riesgo resultante	Riesgo requerido	Prioridad de la Contramedida
1. Protección de correo interno sensible	Distribución inadvertida de correos sensibles a destinatarios externos	Muy alta	Serio	Extremo	Nulo	5
2. Confiabilidad de sitio web relacionado con comercio electrónico	Falla accidental de equipos o suministro eléctrico	Media	Grave	Crítico	Nulo	4
3. Disponibilidad de servicio de correo externo	Ataque al servidor de correos tipo denegación de servicios (DoS)	Extrema	Dañino	Crítico	Bajo	3
	Ataque al servidor de correos tipo "Mail Bomb"	Muy alta	Dañino	Crítico	Bajo	3
4. Veracidad de la base de datos de información de clientes (CID)	Acceso no autorizado y fuga de información	Baja	Serio	Alto	Nulo	3

5. Desecho seguro de medios de almacenamiento con información redundante.	Compromiso accidental de información sensible.	Baja	Serio	Alto	Nulo	3
6. Control de acceso seguro a los paneles y sistemas de distribución eléctrica o cualquiera de sus componentes (excluyendo UPS)	Caída de poder no deseada debido a conexión accidental en el sistema de distribución	Baja	Grave	Alto	Bajo	2
7. Veracidad de la información pública disponible en el sitio web	Pérdida de confianza o buena fe debido a "hacking" de una página web	Alta	Menor	Medio	Bajo	1
8. Acceso seguro a los servicios de red interna por personal autorizado, desde redes externas.	Pérdida del token criptográfico o llaves requeridas para acceder a los canales seguros	Muy baja	Serio	Medio	Bajo	1

ANEXO 4: ESTÁNDAR ETSI TI 102 042 SECCIÓN 7.4.8: ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO Y MANEJO DE INCIDENTES.

El PSC debe asegurar que las operaciones deben restaurarse tan pronto como sea posible ante la ocurrencia de un desastre, incluyendo el caso del compromiso de la llave privada utilizada para la firma de certificados.

NOTA 1: Otras situaciones de desastre incluyen la falla de componentes críticos de los sistemas del PSC, incluyendo hardware y software.

En particular:

a) El plan de continuidad de negocios del PSC deberá considerar como un desastre el compromiso o sospecha de compromiso de la llave privada de firma del PSC y los procesos de recuperación deben estar disponibles y probados.

b) A continuación de un desastre el PSC deberá, en la medida que sea posible, tomar las medidas que eviten su repetición.

c) En el caso de compromiso de su llave privada, el PSC deberá como mínimo tomar las siguientes medidas:

a. Informar del compromiso a todos los subscriptores y sus contrapartes así como a los otros PSCs con quienes tiene acuerdos de interoperabilidad, certificación cruzada u otras formas de colaboración;
b. Indicar que los certificados e información del estado de revocación emitidos usando la llave del PSC puede no ser válida.

NOTA 2: Se recomienda que cuando otro PSC, con la cual se tiene un acuerdo de colaboración, es informado del compromiso de la llave privada, este debiera revocar cualquier certificado de CA que ha sido emitido por el PSC comprometido.

ANEXO 5: REQUERIMIENTOS TÍPICOS DE SEGURIDAD PARA UN REPOSITORIO PÚBLICO DE UN PSC

1. Un repositorio de certificados y CRLs de acceso público debería cumplir los siguientes requerimientos:

   01.01 La utilización de sistemas confiables para almacenar certificados en una forma verificable de manera que:
   - 01.01.1 Sólo personal o procesos autorizados puedan realizar cambios y entradas.
   - 01.01.2 La autenticidad de la información debe ser posible de verificar (en el caso de los certificados digitales, esto se autosustenta al estar firmados)
   - 01.01.3 Los certificados deberán estar disponibles 24 horas al día, 7 días a la semana.

   01.02 En caso de fallar el sistema de distribución de certificados, el tiempo de caída del servicio no deberá superar al establecido en las prácticas de certificación

   01.03 Los certificados deberán estar disponibles de manera pública e internacional. Los medios por los cuales se hagan públicos los certificados deberán cumplir con el requerimiento de interoperabilidad. Es aceptada la utilización de LDAPv2 - descrito en RFC 2559.

2. Una configuración típica que cumpliría estos requerimientos sería:

   - Estructura de directorio LDAP (iPlanet o equivalente)
   - Residente en sistema operativo securizado o verificado por auditor independiente, tal que provea Common Criteria nivel EAL3/EAL4 o TCSEC C2/B1.
   - Aplicación periódica de parches distribuidos por el fabricante (ej. cada 2 meses)
   - Servidor de alta disponibilidad incluyendo como mínimo doble fuente de poder, doble interfaz de red, discos en configuración RAID.
   - Conexión Internet con disponibilidad mínima del 99%
   - Servidor ubicado en la zona DMZ de un cortafuego
   - Disponibilidad mínima de alimentación eléctrica del 99.7%
   - Etc.

ANEXO 6: PAUTA PARA UNA POLÍTICA DE CERTIFICACIÓN

Cuando una autoridad certificadora o PSC emite un certificado, ésta entrega una declaración al titular del certificado, que una llave pública particular está ligada a una entidad particular (persona, en el caso de los certificados de firma avanzada) Los diferentes certificados son emitidos bajo políticas y prácticas diferentes para distintos propósitos. Las políticas de los certificados de llave pública en X.509 se definen como "un conjunto de reglas declaradas que indican la aplicabilidad de un certificado para una comunidad particular o clase de aplicación con requerimientos de seguridad comunes"

Dada la importancia que tiene la política de certificación para establecer la confianza en un certificado de llave pública, es fundamental que la PC (política de certificación) sea entendida no solo por el titular, sino también, por quien recibe el certificado para verificar una firma electrónica.

La política de certificación constituye la base para la interoperabilidad ya que PSCs con distintas Prácticas de Certificación (CPS) pueden tener Políticas de Certificados (CPs) similares para obtener interoperabilidad.

Los tópicos indicados más adelante entregan una guía de los temas y aspectos que debiera contener una Política de Certificación.

1.INTRODUCCION

1.0 CONCEPTOS

1.0.1 Política de Certificado

1.0.2 Declaración de las Prácticas Certificación

1.0.3 Relación entre la Política de Certificado y la Declaración de las Prácticas Certificación

1.1 IDENTIFICACION

1.2 COMUNIDAD Y APLICABILIDAD

1.3 ENTIDADES ADMINISTRATIVAS

1.3.0 Autoridad certificadora raíz

1.3.1 *Autoridades certificadoras*

1.3.2 Autoridades de Registro

1.3.3 Entidades finales

1.3.4 Aplicabilidad

1.4 DETALLES DE LOS CONTACTOS

1.4.1 Direcciones de contactos para las PSC

1.4.1.1 Entidades administrativas

1.4.1.2 Autoridad certificadora raíz

1.4.1.3 Autoridad certificadora

1.4.1.4 Autoridades de registro

1.4.2 Persona de Contacto

1.4.3 Persona que determina la aplicabilidad de la *Declaración de las Prácticas Certificación* para la Política del Certificado

2. REQUERIMIENTOS GENERALES

2.1 OBLIGACIONES

2.1.0 Obligaciones de la PSC raíz (RCA)

2.1.1 Obligaciones de la AC

2.1.1.1 Emisión de Certificados

2.1.1.2 Administración de llaves

2.1.1.3 Directorios de Certificados y listas de Revocación

2.1.1.4 General

2.1.2 Obligaciones de la AR autoridad de registro

2.1.3 Obligaciones del Subscriptor

2.1.3.1 Obligaciones del titular de la llave

2.1.3.2 Obligaciones de la Organización

2.1.4 Obligaciones de terceros

2.1.5 Obligaciones de los repositorios

2.2 RESPONSABILIDADES LEGALES

2.2.0.1 Responsabilidades generales

2.2.0.2 Responsabilidades al bien común

2.2.0.3 Fuerza mayor

2.2.0.4 Responsabilidad de la PSC raíz

2.2.1 Responsabilidad de la AC

2.2.2 Responsabilidad de la AR

2.2.3 Responsabilidad del subscriptor

2.2.4 Responsabilidad de terceros

2.2.5 Responsabilidad del repositorio

2.3 RESPONSIBILIDAD FINANCIERA

2.3.1 Relaciones fiduciarias

2.3.2 Procesos administrativos

2.4 INTERPRETACION Y RESGUARDOS LEGALES

2.4.1 Ley gobernante y Jurisdicción

2.4.2 Divisibilidad, sobrevivencia, consorcio

2.4.2.1 Divisibilidad

2.4.2.2 Sobrevivencia

2.4.2.3 Consorcios

2.4.3 Procedimientos para resolver disputas

2.4.4 Estructuras del Contrato aplicables

2.5 Honorarios

2.5.1 Honorarios por emisión y renovación de certificados

2.5.2 Honorarios por acceso a certificados

2.5.3 Honorarios por acceso a información de listas de revocación o estatus

2.5.4 Honorarios por otros servicios como información sobre las políticas

2.5.5 Política de reembolso

2.5.6 Información para titulares

2.6 PUBLICACION Y REPOSITORIOS

2.6.1 Publicación de la información de la AC

2.6.2 Frecuencia de la publicación

2.6.3 Controles de acceso

2.6.4 Repositorios

2.7 AUDITORIAS DE ACREDITACION

2.7.1 Frecuencia de las auditorías de acreditación

2.7.2 Identidad y calificaciones del auditor

2.7.3 Relaciones entre el auditor y los auditados

2.7.4 Tópicos cubiertos por la auditoría
2.7.5 Acciones a tomar como resultado de deficiencias encontradas
2.7.6 Comunicación de los resultados
2.8 PRIVACIDAD Y PROTECCION DE LOS DATOS
2.8.1 Tipos de información a proteger
2.8.1.0 Información en-confidencia
2.8.1.1 Información confidencial
2.8.1.2 Información personal
2.8.1.3 Otra información protegida
2.8.2 Tipos de información que puede ser entregada
2.8.2.1 Información del Certificado
2.8.3 Entrega de información sobre la revocación o suspensión del certificado
2.8.4 Entrega de información a funcionarios de la corte
2.8.5 Entrega de información como parte de un proceso civil
2.8.6 Entrega de información a petición del titular
2.8.7 Entrega de información bajo otras circunstancias
2.9 DERECHOS DE PROPIEDAD INTELECTUAL

3. IDENTIFICACION Y AUTENTICACION
3.1 REGISTRO INICIAL
3.1.1 Tipos de nombres
3.1.2 Necesidad que los nombres sean significativos
3.1.3 Reglas para interpretar los nombres
3.1.4 Exclusividad de los nombres
3.1.5 Procedimiento por disputa de nombres
3.1.6 Reconocimiento, autenticación y rol de marcas registradas
3.1.7 Método para probar la posesión de la llave privada
3.1.8 Verificación - general
3.1.9 Verificación de la identidad de la Organización
3.1.10 Verificación de la identidad del titular
3.1.11 Verificación del estado organizacional del titular
3.2 REEMISIÓN DE LA LLAVE
3.3 REEMISIÓN DE LA LLAVE LUEGO DE UNA REVOCACIÓN – SIN COMPROMISO DE LA LLAVE
3.4 REQUERIMIENTO DE REVOCACION

4. REQUISISTOS OPERATIONALES
4.0 MANUALES OPERACIONALES
4.1 SOLICITACION DE CERTIFICADO
4.1.1 Registro
4.1.2 Labores de AC y AR
4.2 EMISIÓN DE CERTIFICADOS
4.3 ACEPTACIÓN DE CERTIFICADO
4.4 SUSPENSION Y REVOCACION DE CERTIFICADO
4.4.1 Circunstancias de revocación
4.4.2 Quién puede requerir una revocación
4.4.3 Procedimiento de revocación
4.4.4 Período de gracia de la revocación
4.4.5 Circunstancias para la suspensión
4.4.6 Quién puede pedir la suspensión
4.4.7 Procedimiento de suspensión

4.4.8 Limite de la suspensión
4.4.9 Frecuencia de emisión de la CRL
4.4.10 Requisitos para comprobar la CRL
4.4.11 Comprobar el estado de revocación en línea
4.4.12 Requisitos para verificar la revocación en línea
4.4.13 Otras formas de avisos de revocación
4.4.14 Verificar requisitos para otras formas de avisos de revocación
4.4.15 Requisitos especiales para la reemisión de llave comprometida

4.5 PROCEDIMEINTOS DE SEGURIDAD Y AUDITORIA
4.6 ARCHIVO DE REGISTROS
4.7 CONVERSIÓN DE LLAVES
4.8 COMPROMISO Y RECUPERACION DE DESASTRES
4.9 TÉRMINO DE AR, AC Ó PSC

5. CONTROLES DE PERSONAS, FÍSICOS Y DE PROCEDIMIENTOS

5.0 GENERAL
5.0.1 Políticas de Seguridad
5.0.2 Revisión de riesgos de seguridad
5.0.3 Plan de Seguridad
5.1 CONTROLES FISICOS
5.2 CONTROLES DE PROCEDIMIENTOS
5.2.1 Roles de confianza
5.2.2 Número de personas por actividad
5.2.3 Identificación y autenticación para cada rol
5.3 CONTROLES DEL PERSONAL
5.3.1 Calificaciones, experiencia, y requisitos de espacio
5.3.2 Procedimientos para verificar experiencia
5.3.3 Requisitos de entrenamiento
5.3.4 Requisitos y frecuencia de reentrenamientos
5.3.5 Rotación de personal
5.3.6 Sanciones para acciones no autorizadas
5.3.7 Requisitos para contratar personal
5.3.8 Documentación provista al personal

6. CONTROLES DE SEGURIDAD TECNICA

6.0 PLAN DE ADMINISTRACION DE LLAVES
6.1 INTALACION Y GENERACION DE PARES DE LLAVES
6.1.1 Generación del par de llaves
6.1.2 Entrega de la llave privada
6.1.3 Entrega de la llave publica al emisor del certificado
6.1.4 Entrega de la llave publica de la PSC
6.1.5 Largo de llaves
6.1.6 Generación de parámetros para la llave pública
6.1.7 Verificación de la calidad de los parámetros
6.1.8 Generación de llave por Hardware/software
6.1.9 Propósitos de la llave (como X.500 v3)
6.2 PROTECCION DE LA LLAVE PRIVADA
6.2.1 Estándares para el módulo criptográfico
6.2.2 Private Key (n out of m) multi-person control
6.2.3 Respaldo de la llave privada
6.2.4 Archivo de la llave privada

ANEXO 7: ELEMENTOS DE UNA EVALUACIÓN DE UN PLAN DE SEGURIDAD

La evaluación es una valoración de los siguientes aspectos:

- ¿Existe un administrador de la seguridad IT en terreno?
- ¿Tiene el administrador de seguridad IT un conocimiento adecuado de su rol, consistente con aquel descrito en el Plan de Seguridad y el Manual de Operación?
- ¿Está el personal de soporte operacional que se identifica en el Plan de Seguridad disponible en terreno?
- ¿Tiene el personal de soporte un conocimiento adecuado de su rol, consistente con aquel descrito en el Plan de Seguridad y el Manual de Operación?
- ¿Es el conjunto de usuarios privilegiados del sistema AC o AR consistente con el conjunto de usuarios privilegiados descritos en el plan de seguridad?
- Está la infraestructura computacional y de red instalada y operando de acuerdo a lo descrito en ¿El Plan de Seguridad, el Manual de Operaciones, la Declaración de Prácticas de Certificación y el Plan de Continuidad de Negocios y Recuperación ante Desastres?
- ¿Están los mecanismos de seguridad y procedimientos descritos en el Plan de Seguridad instalados y configurados o implementados de acuerdo con el Plan? Se verificará principalmente:
    - Mecanismos de control de acceso
    - Captura y revisión de datos de auditoría
    - Monitoreo de incidentes de seguridad
    - Administración de incidentes y procedimientos de respuesta ante incidentes
    - Mantención y uso de la información acerca de vulnerabilidades de las instalaciones de la AC o AR
    - Plan de administración de llaves criptográficas
    - Administración de cuentas de usuarios
    - Control de media removible
    - Respaldo y recuperación de datos y sistemas, incluyendo almacenamiento de segundas copias fuera de las instalaciones
    - Control de inventario, incluyendo procedimientos de registro para controlar ubicación y acceso de los activos críticos.
    - Administración del FW Internet
    - Procedimientos y mecanismos que tengan un rol relevante en reducir las amenazas a las operaciones de la AC o AR.

- Provee la confianza mediante la comprobación en terreno de que la seguridad operacional del PSC se mantendrá en el tiempo dadas las condiciones siguientes:
    - ¿Después que el grupo evaluador se ha retirado?
    - ¿Después de cambios en las amenazas de seguridad, personal, servicios ofrecidos, tecnología e infraestructura?

ANEXO 8: ELEMENTOS DE UNA REEVALUACIÓN DE UN PLAN DE SEGURIDAD

La reevaluación es una valoración de los siguientes aspectos:

- ¿Ha sido actualizada la Política de Seguridad con algún nuevo objetivo de seguridad producto de cambios en los servicios o certificados ofrecidos?
- ¿Se requiere una revisión del requisito PS01?
- Hay evidencias de revisiones de la Valoración de ¿Riesgos y Amenazas, incluyendo un análisis de amenazas cambiantes y las implicaciones de cualquier cambio en los servicios ofrecidos y la infraestructura?
- ¿Se requiere una revisión del requisito PS02?
- Se ha modificado el Plan de Seguridad para incluir cualquier procedimiento de seguridad nuevo debido a cambios en la Política de Seguridad y en la Valoración de Riesgos y Amenazas
- ¿Se requiere una revisión del requisito PS04?
- Cuales han sido los resultados en el tiempo de los siguientes procedimientos regulares:
    - Revisión de los logs de auditoría
    - Detección de incidentes de seguridad
    - Administración y respuesta frente a incidentes de seguridad
    - Administración de llaves criptográficas
    - Revisión de la administración de configuración
    - Scanning de vulnerabilidades de seguridad
    - Scanning de código malicioso (virus, etc.)
    - Administración de cuentas de usuarios
    - Administración de procedimientos de control de acceso
    - Procedimientos de respaldo y restauración de datos (incluyendo el resultado de ejercicios de recuperación donde sea aplicable)
    - Procedimientos de mantención
    - Revisión de la integridad del sistema
    - Procedimientos de transferencia de datos
    - Procedimientos de control de traslado de dispositivos de respaldo
    - Procedimientos de control de ubicación e inventario

- ¿Cuales han sido los resultados de oportunidades de entrenamiento y educación del personal de sistemas y operaciones?
- ¿Es capaz de demostrar el personal de sistemas y operaciones su capacidad de llevar a cabo sus roles, consistente con lo descrito en el Plan de Seguridad y los Manuales de Operaciones?
- ¿Esta el PSC siendo operado de acuerdo a los planes descritos en el Plan de Seguridad, el Manual de Operaciones, la Declaración de Prácticas de Certificación y el Plan de Continuidad de Negocios y Recuperación de Desastres?

ANEXO 9: REGLAMENTO LEY 19799 – ARTICULO 6

Las prácticas de certificación consisten en una descripción detallada de las normas o prácticas que el prestador de servicios de certificación declara convenir en la prestación de sus servicios de certificación.

Dichas prácticas deberán contener al menos:

a) Introducción, en la que se deberá identificar el conjunto de provisiones, tipo de entidades y aplicaciones para las cuales las prácticas han sido definidas. Dicha introducción deberá contener, un resumen de las prácticas de certificación de que se trate mencionando tanto la entidad que suscribe el documento, como los usuarios.
b) Provisiones generales, debiendo contener información sobre obligaciones, responsabilidades, cumplimiento de auditorias, confidencialidad, y derechos de propiedad intelectual, con relación a todas las partes involucradas.
c) Identificación y autentificación, debiendo describirse los procesos de autentificación aplicados a los solicitantes de certificados, los procesos para autentificar a las partes cuando piden suspensión y/o revocación de certificado.
d) Requerimientos operacionales, debiendo contener información operacional para los procesos de solicitud de certificado, emisión de certificados, suspensión y revocación de certificados, procesos de auditoria de seguridad, almacenamiento de información relevante, cambios de datos de creación de firma electrónica, recuperación de compromisos, casos de fuerza mayor y caso fortuito, y procedimiento de término del prestador de servicios de certificación.
e) Controles de procedimiento, personal y físicos, debiendo describirse los controles de seguridad no técnicos utilizados por el prestador de servicios de certificación para asegurar las funciones de generación de datos de creación de firma electrónica, autentificación de usuarios, emisión de certificados, suspensión y revocación de certificados, auditoria y almacenamiento de información relevante.
f) Controles de seguridad técnica, debiendo señalarse las medidas de seguridad adoptadas por el prestador de servicios de certificación para proteger sus datos de creación de firma electrónica.
g) Perfiles de certificados y del registro de acceso público, debiendo especificar el formato del certificado y del registro de acceso público.
h) Especificaciones de administración, debe contener como la política de certificación está contenida en la práctica, los procedimientos para cambiar la política, publicar y notificar.

ANEXO 10: PAUTA DE MODELO OPERACIONAL DE LA AC DE UN PSC

Este documento provee una guía para que un PSC documente el modelo de operaciones de la AC.

El modelo de operaciones es uno de los primeros documentos que debieran ser preparados al iniciar sus actividades un PSC. El cual debería presentar una visión general de cómo interaccionarán los diferentes elementos constituyentes de un PSC. Cubriendo aspectos operacionales, técnicos, legales, de seguridad y administración.

Algunas de las secciones de esta guía pueden no aplicar a todos los PSC y la organización postulante debería presentar en la documentación aspectos que reflejen su circunstancia particular.

Resumen ejecutivo

Presentar una visión general de las operaciones de la PSC. Debiera responder a las siguientes preguntas:
¿Cuál es el producto y servicio?
¿Desde donde se operará?
¿A quien se proveerá de certificados?
¿Quién estará involucrado en las operaciones?

Historia de la empresa

Descripción breve de los orígenes de la organización, relaciones con los proveedores de tecnología y otras empresas asociadas.

Relaciones Comerciales

Proveer un resumen de las relaciones comerciales de la compañía en relación con las operaciones de la PKI.
Si las operaciones involucran otras empresas, describir la relación con estas.

Prefacio del documento

Describe el propósito y alcance del documento.
Descripción de los tópicos que cubre el documento y sus anexos.

Componentes del sistema

Describe cuales son las partes funcionales del PSC, en sus distintos modos de operación.

Los componentes que se describen son los necesarios para operar el PSC y pueden incluir, pero no están limitados a: Interfaces entre la AC y AR, componentes de hardware y software.

Administración

Incluye las referencias a las políticas para los clientes, filosofía operacional, elementos estratégicos y de interrelación.

Se deben incluir detalles operacionales, como horarios de atención, personal requerido, infraestructura, etc.

Se puede incluir organigrama de la empresa.

Directorio

Declarar brevemente:

Estándar que utilice el directorio, por ejemplo x.500 LDAP

La información incluida en el directorio

Como afectan las revocaciones al directorio

Bases de datos de la AC

Describir brevemente la información que incluyen las bases de datos de la AC. Por ejemplo:
Registro de ingreso y egreso a los sistemas

Registro de la creación de certificados

Detalles de los certificados

Detalles de las revocaciones.

Otros subsistemas

Cualquier otra información de subsistemas que pueda aplicar:

Cuando se genera el par de llaves, quien realiza esta función (AC/AR/ titular) Si el titular genera las llaves, indicar por cual medio y describir la tecnología utilizada.

Medios de comunicación entre la AC y AR. Cuales son las relaciones y dependencias entre ellas.

Diagramas de los procesos pueden apoyar las descripciones.

Generación de llaves en la AC

Si aplica, describir el proceso de generación de llaves. Detalle de los mecanismos de protección de acceso para la generación de llaves.

Generación de Certificados

Mostrar como opera la cadena de jerarquía. Incluir referencias al certificado raíz y las relaciones con otras AC si aplica. Por ejemplo, en caso de existir AC subordinadas.

Operaciones de la AC

Este punto debiera describir brevemente otros aspectos sensibles a la seguridad o de naturaleza sensible a las operaciones de la PSC y que no hayan sido descritos anteriormente.

Procedimientos de recuperación de datos

Describir brevemente la frecuencia de los respaldos y los procedimientos almacenamiento que se seguirán.

Planes de Auditoria

Describir cuales son los componentes del plan de auditoria de la organización en, por ejemplo:
Dispositivos de seguridad
Seguridad
Restricciones del personal
Interfaces de administración

Recuperación de desastres

Descripción de la estrategia para recuperación de desastres incluyendo:

Definición de roles y responsabilidades
Ejercicios de práctica para la recuperación de desastres, con cuanta frecuencia se realizan.
Respaldos en cinta, frecuencia, tipo de respaldo (por ejemplo incremental o total)
Reiniciar el sistema
Procesos de auditoria y generación de reportes.

Seguridad

Esta sección debe describir brevemente todos los aspectos de seguridad que están involucrados en las operaciones de la AC y AR. Los detalles de estos aspectos pueden ser referenciados a otros documentos presentados.

Seguridad de las instalaciones

Provee la descripción física del lugar donde operara la AC y AR. Puede incluir referencias a otros documentos o procesos de certificación con los cuales cumpla.

Seguridad del Personal

Provee descripción de los requerimientos de seguridad para el personal de la organización, como por ejemplo:

Referencia a que puestos pueden entrar en zonas restringidas
Plan de entrenamiento para el personal
Zonas restringidas para el personal
Registro de ingresos
Control de ingreso

Nivel de Seguridad del módulo criptográfico

Describe los productos y tecnología que se está utilizando para realizar las operaciones de la PSC, en particular el módulo criptográfico de la AC.

ANEXO 11: PAUTA DE MODELO OPERACIONAL DE LA AR DE UN PSC

Este documento provee una guía para que un PSC documente el modelo de operaciones de la AR.
El modelo de operaciones es uno de los primeros documentos que debieran ser preparados al iniciar sus actividades un PSC. El cual debería presentar una visión general de cómo interaccionarán los diferentes elementos constituyentes de un PSC. Cubriendo aspectos operacionales, técnicos, legales, de seguridad y administración.

Algunas de las secciones de esta guía pueden no aplicar a todos los PSC y la organización postulante debería presentar en la documentación aspectos que reflejen su circunstancia particular.

Resumen ejecutivo

Debería presentar una visión general de las operaciones de la AR. Debiera y responder a las siguientes preguntas:

¿Cuál es el producto y servicio?
¿Desde donde se operará?
¿A quien se proveerá de certificados?
¿Quién estará involucrado en las operaciones?

Historia de la empresa

Descripción breve de los orígenes de la organización, relaciones con los proveedores de tecnología y otras empresas asociadas.

Relaciones Comerciales

Proveer un resumen de las relaciones comerciales de la compañía en relación con las operaciones de la PKI.
Si las operaciones involucran otras empresas, describir la relación con estas.

Prefacio del documento

Describe el propósito y alcance del documento.
Descripción de los tópicos que cubre el documento y sus anexos.

Componentes del sistema

Describe cuales son los componentes funcionales de la AR, en sus distintos modos de operación.

Los componentes que se describen son los necesarios para operar el PSC y pueden incluir, pero no están limitados a: Interfaces entre la AC y AR, componentes de hardware y software.

Administración

Incluye las referencias a las políticas para los clientes, filosofía operacional, elementos estratégicos y de interrelación.

Se deben incluir detalles operacionales, como horarios de atención, personal requerido, infraestructura, etc.

Se puede incluir organigrama de la empresa.

Bases de datos de la AR

Describir brevemente la información que incluyen las bases de datos de la AR. Por ejemplo:
Registro de ingreso y egreso a los sistemas

Registro de la creación de certificados

Detalles de los certificados

Detalles de las revocaciones.

Otros subsistemas

Cualquier otra información de subsistemas que pueda aplicar.

Como se registran los usuarios para obtener un certificado

El medio utilizado para registrar, por ejemplo: electrónico, cara a cara, etc.

Que procesos se utilizan para registrar la identidad, y por quien.

Cuando se genera el par de llaves, quien realiza esta función (AC/AR/ titular) Si el titular genera las llaves, indicar por cual medio y describir la tecnología utilizada.

Medios de comunicación entre la AR y AC. Cuales son las relaciones y dependencias entre ellas.

Generación de llaves por el cliente

Proveer detalles de:

La forma en que se generan las llaves

Como se comunica la AR y la AC una vez generadas las llaves

Protección del mecanismo de generación de llaves**.**

Operaciones de la AR

Este punto debiera describir brevemente otros aspectos sensibles a la seguridad o de naturaleza sensible a las operaciones de la AR y que no hayan sido descritos anteriormente.

Planes de Auditoria

Describir brevemente cuales son los componentes del plan de auditoria de la organización en, por ejemplo:

Dispositivos de seguridad

Seguridad

Restricciones del personal y

Interfaces de administración

Procedimientos de respaldo y recuperación

Describir brevemente la frecuencia de los respaldos, los procedimientos de auditoria y almacenamiento que se seguirán.

Recuperación de desastres

Descripción breve de la estrategia para recuperación de desastres incluyendo:

Definición de roles y responsabilidades

Ejercicios de práctica para la recuperación de desastres, con cuanta frecuencia se realizan.

Respaldos en cinta, frecuencia, tipo de respaldo (por ejemplo incremental o total)

Reiniciar el sistema

Procesos de auditoria y generación de reportes.

Privacidad y entrenamiento

Describir brevemente:
Las provisiones tomadas para proteger la información personal recolectada como evidencia de la identidad en el proceso de registro AR.

Plan de entrenamiento del personal, en temas relacionados con el manejo de información privada y confidencial.

Seguridad

Esta sección debe describir brevemente todos los aspectos de seguridad que están involucrados en las operaciones de la AR. Los detalles de estos aspectos pueden ser referenciados a otros documentos presentados.

Seguridad de las instalaciones

Provee la descripción física del lugar donde operara la AR. Puede incluir referencias a otros documentos o procesos de certificación con los cuales cumpla.

Seguridad del Personal

Provee descripción de los requerimientos de seguridad para ele personal de la organización, como por ejemplo:

Referencia a que puestos pueden entrar en zonas restringidas

Plan de entrenamiento para el personal

Zonas restringidas para el personal

Registro de ingresos

Control de ingreso

Nivel de Seguridad del módulo criptográfico

Describe los productos y tecnología que se esta utilizando para realizar las operaciones de la PSC, incluyendo el módulo criptográfico de la AR, si lo hay, y el dispositivo donde almacenará las llaves el titular.

ANEXO 12: PAUTA DE MANUAL DE OPERACIONES DE UNA AC.

El propósito de este documento es describir las secciones tipo de un manual de operaciones describiendo las acciones diarias de la AC en el PSC. Gráficos y diagramas funcionales se deben incluir para el mejor entendimiento de las operaciones por parte de sus empleados.

Los aspectos del manual de operaciones relacionados con la seguridad, plan de recuperación de errores y plan de continuidad del negocio pueden ser referenciados en este documento y nos es preciso incluirlos en detalle.

Introducción

Visión general del sistema

Provee de una descripción del sistema y un diagrama esquemático de la PKI, incluyendo la interacción entre la AC y la AR.

Roles y responsabilidades en la AC

Describe los roles y responsabilidades de los empleados del PSC.

Estructura administrativa

Provee de un diagrama organizacional indicando la estructura administrativa y operacional.

Provisiones generales

Repositorios y publicaciones

Describe como operan las publicaciones y los directorios, incluyendo:

- Como se publican las prácticas de certificación y políticas de los certificados.
- Publicación de los certificados
- Publicación del estado de los certificados
- Frecuencia de las publicaciones
- Control de acceso a los objetos publicados, incluida la CP
- Definiciones de las CP, certificados, CRL, Estado de los certificados

Auditorias

Describe:

- Frecuencia de las auditorías
- Identidad y calificaciones de los auditores (asegura no tener conflicto de intereses)
- Tópicos a ser cubiertos por las auditorías
- Acciones a realizar cuando la auditoría encuentra fallas
- Resultados de las auditorías

Confidencialidad y Privacidad

Presenta:

- Tipo de información que se mantiene confidencial
- Como se protege la información
- Tipos de información no confidencial

- Política de entrega de información en caso de juicios civiles y penales
- Otro tipo de entrega de información

Requerimientos operacionales de la AC

Los aspectos mínimos a incluir son:

- Horas de operación y continuidad del negocio
- Administración de certificados
- Procedimientos de seguridad y auditoria
- Archivo de fichas
- Compromisos y recuperación de fallas
- Término de una AC subordinada

Controles de Seguridad

Controles de seguridad física de las instalaciones

El manual de operaciones debe describir en este capítulo los procedimientos atingentes a la seguridad físicas descritos en el Plan de Seguridad, incluyendo:

- Controles de seguridad física
- Administración de seguridad física

Procedimientos en los cambios de las especificaciones

Eventualmente se podrá requerir cambiar las prácticas de certificación o las políticas de los certificados. Describir como se realizan estos procesos.

Procedimientos para cambiar la documentación

Describe como se administran los accesos lógicos. Quién autoriza los cambios y quién realiza los cambios a los documentos.

Control de accesos lógicos

El control de accesos lógicos debe estar referenciado al Plan de Seguridad.

Administración de configuraciones

Describe el control de versiones de software, hardware, y bases de datos.

Almacenamiento y recuperación de archivos (papelería)

Describe los procedimientos de archivo de documentación

Compromiso de la PKI

Describe o referencia los procedimientos al Plan de Recuperación de desastres y continuidad del negocio.

Control de medios magnéticos removibles

Procedimientos de Almacenamiento

Destrucción de material clasificado

Manejo de incidentes

Referencia los procedimientos al Plan de Recuperación de desastres y continuidad del negocio.

Controles de Generación y uso de llaves

Describe los procedimientos de generación del par de llaves y su instalación

- Generación de las llaves
- Largo de llaves
- Generación de los parámetros para la llave pública
- Generación de la llave por Hardware/Software
- Renovación de llaves
- Protección de la llave privada
- Estándares para el módulo criptográfico
- Destrucción de la llave privada
- Otros aspectos de la administración de llaves y certificados
- Archivo de llaves públicas
- Períodos de vida útil de las llaves pública y privada
- Prácticas de seguridad

Perfiles de los certificados y CRL

Describe o hace referencia a otros documentos donde se especifican los contenidos de las CRL y Certificados, incluyendo sus perfiles y extensiones.

Administración de las especificaciones

Describe como se administra la mantención y cambios de la CSP y CP, incluyendo

- Cambios en la especificación
- Aprobación de la CPS
- Publicación de las políticas CP y CPS

ANEXO 13: PAUTA DE MANUAL DE OPERACIONES DE UNA AR

El propósito de este documento es describir las secciones tipo de un manual de operaciones describiendo las acciones diarias de la AR en el PSC. Gráficos y diagramas funcionales se deben incluir para el mejor entendimiento de las operaciones por parte de sus empleados.

Los aspectos del manual de operaciones relacionados con la seguridad, plan de recuperación de errores y plan de continuidad del negocio pueden ser referenciados en este documento y nos es preciso incluirlos en detalle.

Introducción

Visión general del sistema

Provee de una descripción del sistema y un diagrama esquemático de la PKI, incluyendo la interacción entre la AC y la AR. Los procesos de registro, generación de llaves, entrega de los certificados, y certificación de identidad del titular.

Roles y responsabilidades en la AR

Describe los roles y responsabilidades de los empleados del PSC

Estructura administrativa

Provee de un diagrama organizacional indicando la estructura administrativa y operacional

Provisiones generales

Auditorias

Describe:

- Frecuencia de las auditorias
- Identidad y calificaciones de los auditores (asegura no tener conflicto de intereses)
- Tópicos a ser cubiertos por las auditorias
- Acciones a realizar cuando la auditoría encuentra fallas
- Resultados de las auditorias

Confidencialidad y Privacidad

Presenta:

- Tipo de información que se mantiene confidencial
- Como se protege la información
- Tipos de información no confidencial
- A quien se le informa de la revocación de certificados
- A petición del titular que información se puede entregar
- Política de entrega de información en caso de juicios civiles y penales
- Otro tipo de entrega de información

Identificación y Autenticación

Presenta procedimientos para identificar al titular antes de emitir el certificado.
Como se autentifican las personas que piden una revocación o reemisión de certificados.

Registro inicial

Este proceso debe contener a lo menos los siguientes pasos: Registro del titular, verificación de su identidad, recolección de antecedentes y archivo de los mismos.

Reemisión de llaves

Requerimiento de revocación

Requerimiento de suspensión (si aplica)

Requerimientos operacionales de la AR

Los aspectos mínimos a incluir son:

Horas de operación y continuidad del negocio
Administración de certificados
Procedimientos de seguridad y auditoria
Archivo de fichas
Compromisos y recuperación de fallas
Término de una AR

Controles de seguridad

Controles de seguridad física de las instalaciones

El manual de operaciones debe describir en este capítulo los procedimientos atingentes a la seguridad físicas descritos en el Plan de Seguridad, incluyendo:

Controles de seguridad física
Administración de seguridad física

Procedimientos en los cambios de las especificaciones

Eventualmente se podrá requerir cambiar las prácticas de certificación o las políticas de los certificados. Describir como se realizan estos procesos.

Procedimientos para cambiar la documentación

Describe como se administran los accesos lógicos. Quién autoriza los cambios y quién realiza los cambios a los documentos.

Control de accesos lógicos

Los procedimientos de control de accesos lógicos deben estar referenciados al Plan de Seguridad.

Administración de configuraciones

Describe el control de versiones de software, hardware, y bases de datos.

Almacenamiento y recuperación de archivos (papelería)

Describe los procedimientos de archivo de documentación

Control de medios magnéticos removibles

Procedimientos de Almacenamiento

Destrucción de material clasificado

Manejo de incidentes

Referencia los procedimientos al Plan de Recuperación de desastres y continuidad del negocio.

Controles de Generación y uso de llaves

Generación del par de llaves y su instalación
Generación de las llaves
Entrega de la llave privada
Entrega de la llave pública a los usuarios
Largo de llaves
Generación de los parámetros para la llave pública
Generación de la llave por Hardware/Software
Renovación de llaves
Protección de la llave privada
Estándares para el token criptográfico
Destrucción de la llave privada
Otros aspectos de la administración de llaves y certificados
Activación y desactivación de las llaves
Archivo de llaves públicas
Períodos de vida útil de las llaves pública y privada
Prácticas de seguridad

Administración de las especificaciones

Describe como se administra la mantención y cambios de la CSP y CP, incluyendo

Cambios en la especificación
Aprobación de la CPS
Publicación de las políticas CP y CPS

ANEXO 14: MODELO DE CONFIANZA

El modelo de confianza es el esquema por el cual un usuario de un certificado de firma electrónica avanzada emitido por un Prestador de Servicios de Certificación acreditado puede confiar en dicho certificado.

El esquema definido por la Ley 19799 y el reglamento deja en manos al prestador de servicios de certificación implementar el mecanismo por el cual un usuario que confíe en él, pueda confiar en cualquier otro prestador de servicios de certificación acreditado (Reglamento artículo 26 inciso 2°)

Para esto la Subsecretaría de Economía Fomento y Reconstrucción generará un archivo firmado mediante firma electrónica por el funcionario público responsable, conteniendo los certificados de todos los prestadores de servicios de certificación acreditados por esta subsecretaría el cual estará disponible para cualquiera que los solicite.

El mecanismo propuesto consiste en que cada prestador de servicios de certificación mantenga en su repositorio de acceso público los certificados de todos los prestadores acreditados de tal manera que los usuarios que confíen en él puedan instalar en sus aplicaciones estos certificados. El método debe incluir mecanismos de seguridad para evitar que se puedan reemplazar los certificados en el repositorio o durante su transmisión sin que ello no pueda ser detectado por el usuario.

BIBLIOGRAFÍA

1.- LEY-19799, "LEY SOBRE DOCUMENTOS ELECTRÓNICOS, FIRMA ELECTRÓNICA Y SERVICIOS DE CERTIFICACIÓN DE DICHA FIRMA
Fecha Publicación : 12.04.2002
Fecha Promulgación : 25.03.2002
Organismo : Ministerio de Economía, Fomento y Reconstrucción; Subsecretaría de Economía, Fomento y Reconstrucción

2.- REGLAMENTO LEY-19799 VERSIÓN FINAL 11/06/2002

GLOSARIO

Castellano

PSC	Prestador de Servicios de Certificación
LCR	Lista de Certificados Revocados
PC	Política del Certificado
DPC	Declaración de Prácticas de Certificación
AC	Autoridad de Certificación
AR	Autoridad de Registro
ICP	Infraestructura de Clave Pública
PCN+	Política del Certificado Normalizado con requerimiento de uso de dispositivo usuario seguro.
PCN	Plan de Continuidad del Negocio
PRD	Plan de Recuperación de Desastres

Inglés

CSP	Certification Service Provider
CRL	Certificate Revocate List
CP	Certificate Policy
CPS	Certification Practice Statements
CA	Certification Authority
RA	Registration Authority
PKI	Public Key Infrastructure
NCP+	Normalized Certificate Policy requiring use of a secure user device
BCP	Business Continuity Plan
DRP	Disaster Recovery Plan