Servicios de certificación asociados a la

Firma Electrónica Avanzada

Guía para inspección anual de Prestadores de Servicios de Certificación

Ministerio de Economía, Fomento y Turismo

Gobierno de Chile

Subsecretaría de Economía y Empresas de Menor Tamaño

- Documento Número : EA-104
- Versión : 2.1
- Estado : Versión Final
- Fecha de Emisión : 08/02/2013

Contenido

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 N°19.799 *sobre documento electrónico, firma electrónica y servicios de certificación de dicha firma*, cuerpo que regula las operaciones comerciales que se realicen en Chile a través de Internet, con el fin de establecer un marco legal que otorga a los actos y contratos celebrados por medios electrónicos el mismo reconocimiento y protección que gozan los contratos tradicionales, celebrados en formato papel.

La formulación de dicha ley es consecuencia del desarrollo tecnológico alcanzado en el ámbito local y global, donde la *criptografía*, la *certificación* y la *firma electrónica* son utilizadas para proveer privacidad, integridad del contenido, autenticación del origen y no desconocimiento de la operación, y cuyo propósito fundamental es proveer seguridad tanto en las transacciones realizadas vía Internet como en el intercambio de documentos electrónicos en Intranets, Extranets, redes privadas o cualquier medio de almacenamiento o comunicación electrónico.

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

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

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

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

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

2. MARCO GENERAL PARA LA INSPECCIÓN ANUAL DE ENTIDADES ACREDITADAS

2.1. OBJETIVO

El objetivo de la inspección anual a los prestadores de servicios de certificación es verificar que se mantiene un sistema de servicios de certificación asociados a la firma electrónica avanzada confiable, que asegure su continuidad en el tiempo.

2.2. CAUSALES DE PÉRDIDA DE LA ACREDITACIÓN

El Reglamento de la Ley N°19.799 señala en su artículo 26 que la acreditación de los certificadores se dejará sin efecto por las siguientes causas:

a) Por solicitud del prestador acreditado de servicios de certificación, ante la Entidad Acreditadora.

b) Por pérdida de las condiciones que sirvieron de fundamento a su acreditación, la que será calificada por los funcionarios o expertos que la Entidad Acreditadora ocupe para el cumplimiento de la facultad inspectora.

c) Por incumplimiento grave o reiterado de las obligaciones que establece la Ley y su Reglamento.

2.3. PARTICIPANTES

La Ley N°19.799 y su Reglamento determinan mediante su normativa el sistema de acreditación e inspección anual de Prestadores de Servicios de Certificación, que para el segundo caso involucra las siguientes entidades:

2.3.1. ENTIDAD ACREDITADORA

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

Además, deberá velar porque los requisitos y obligaciones que se observaron al momento de otorgarse la acreditación se mantengan durante la vigencia de la acreditación (Art. 15 Reglamento). Para ello podrá requerir información y ordenar auditorías a las instalaciones del PSC inspeccionado, sin previo aviso, ya sea personalmente o por medio de las entidades evaluadoras (Art. 15 Reglamento).

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

2.3.2. ENTIDAD EVALUADORA

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

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

2.3.3. PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC)

Corresponde a la entidad emisora de certificados de Firma Electrónica Avanzada y servicios de certificación asociados:

- Sello de Tiempo
- Biometría
- Firma Móvil

2.4. PROCEDIMIENTO DE INSPECCIÓN ANUAL

El procedimiento de inspección anual se describe a continuación:

1. La Entidad Acreditadora por medio de resolución fijará dentro del primer trimestre de cada año el arancel de los costos de la acreditación y el arancel de supervisión.

2. El arancel de supervisión deberá ser pagado por cada prestador acreditado de servicios de certificación dentro de los 90 días siguientes a la fecha de la resolución que los fija. (Reglamento Art. 24).

3. Una vez cumplido, cada PSC presentará a la Entidad Acreditadora el comprobante de pago de los costos de supervisión anual, individualizándose debidamente mediante la siguiente información:

    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

4. Para dar inicio a la supervisión anual, la Entidad Acreditadora solicitará al PSC entregar los siguientes documentos:

   a. Procedimiento previsto para asegurar el acceso a los peritos o expertos (Reglamento Art. 14).
   b. Si los hay, copia de los contratos de servicios externalizados con fecha posterior a su acreditación o a la última inspección anual realizada.
   c. Toda la documentación definida en las Guías de Evaluación para Acreditación, para cada uno de los requisitos especificados, que hubieren sufrido modificación desde la fecha de su acreditación a la fecha de la inspección, o entre una inspección y la siguiente.

5. La Entidad Acreditadora revisará que se encuentren presentados todos los antecedentes requeridos.

6. Recibidos todos los antecedentes, la Entidad Acreditadora procederá a evaluar el cumplimiento de los requerimientos expresados en la Ley, el Reglamento y sus disposiciones transitorias. El Prestador 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 éstos.

7. Realizada la evaluación, la Entidad Acreditadora procederá a pronunciarse sobre si se cumplen los requisitos y obligaciones exigidas en la Ley, el Reglamento y las correspondientes Guías de Evaluación para Acreditación, para mantener la acreditación.

8. La Entidad Acreditadora podrá dejar sin efecto la acreditación mediante resolución fundada, por las causales previstas en el artículo 26 del Reglamento de la Ley N°19.799. Dicha resolución deberá ordenar la cancelación de la inscripción del certificador del registro público que lleve la Entidad Acreditadora. En los casos de las letras b) y c) de dicho artículo, la resolución deberá ser adoptada previo traslado de cargos y audiencia del afectado, para lo cual la Entidad Acreditadora dará un plazo de 5 días hábiles. Recibidos éstos la Entidad Acreditadora deberá resolver fundadamente dentro del plazo de 15 días, prorrogables por el mismo período, por motivos fundados.

9. En el caso que la Entidad Acreditadora determine como resultado de la inspección 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 y solicitará al PSC entregue un plan de medidas correctivas y los plazos establecidos para ello.

10. 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 según se indica en el punto 8.

11. En caso de ser favorable la evaluación, la Entidad Acreditadora procederá a informar al Prestador de Servicios de Certificación de la mantención de la inscripción del certificador en el registro público que lleve la Entidad Acreditadora.

3. EVALUACIÓN

3.1. REQUISITOS EVALUADOS

Los requisitos evaluados en la inspección anual son los mismos señalados en la última versión oficial de las Guías de Acreditación, disponibles en el sitio Web de la Entidad Acreditadora http://www.entidadacreditadora.gob.cl/

En caso de que existan en dichas Guías, criterios de evaluación discrepantes o contrapuestos con los requerimientos que se establecen en la Ley N°19.799, su Reglamento, o las normas técnicas aplicables, prevalecerán los anteriores por sobre los dispuestos en ellas.

3.2. CUMPLIMIENTO DE REQUISITOS

El Prestador de Servicios de Certificación deberá demostrar la mantención del cumplimiento de los requisitos de acreditación mediante los siguientes medios:

1. Acompañando la actualización de los antecedentes presentados al momento de su acreditación si estos hubieren sufrido modificaciones desde esa fecha al momento de la inspección anual, o entre una inspección anual y la siguiente.

2. Presentando la documentación e información adicional solicitada por la Entidad Acreditadora durante el proceso de inspección anual, dentro de los plazos establecidos en cada solicitud.

3. Permitiendo el libre acceso a los expertos nombrados por la Entidad Acreditadora para la inspección anual.

3.3. ESQUEMA DE EVALUACIÓN

La verificación del cumplimiento de los requisitos se realizará en conformidad a 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.

3.4. 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.

3.5. 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 evaluados, debe contactarse con la Entidad Acreditadora, Subsecretaría de Economía y Empresas de Menor Tamaño.

4. BIBLIOGRAFÍA

1) Legal

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

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

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

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

2) Prácticas de Certificación:

- ETSI TS 102 042 V2.3.1 (2012-11) - Policy requirements for certification authorities issuing public key certificates

- NCh2805.Of2003 Tecnología de la Información - Requisitos de las políticas de las autoridades certificadoras que emiten certificados de claves públicas.

3) Seguridad:

- NCh27002.Of2009 Tecnología de la información - Código de práctica para la gestión de seguridad de la información.

- ISO/IEC 15408-1:2009 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

- FIPS PUB 140-2: Security Requirements for Cryptographic Modules (mayo 2001).

- NCh.2820/1.Of2003 Tecnología de la información - Técnica de seguridad - Criterio de evaluación de la seguridad de TI - Parte 1: Introducción y modelo general.

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

4) Estructura de Certificados:

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

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

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

5) Repositorio de Información:

- NCh2832.Of2003 Tecnología de la información - Protocolos operacionales de infraestructura de clave pública LDAPv2 para Internet X.509.

- RFC 2559 Boeyen, S. et al., Internet X.509 Public Key Infrastructure. Operational Protocols LDAPv2, abril 1999. (Lo reemplaza RFC 3494)

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

6) Sellado de Tiempo/Time Stamping:

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

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

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

7) DNI Electrónico y su Identidad Biométrica:

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

8) Servicios de firma móvil:

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

9) Especificaciones Técnicas:

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

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