Situación Firma Electrónica Avanzada en Chile

Gobierno de Chile

Participantes

- Mario Lemus Varas

  Encargado de la Entidad Acreditadora de Firma Electrónica Avanzada

  Ministerio de Economía de Chile

  MLemus@economia.cl
- Sebastian Gómez Fiedler

  Asesor Legal

  Subdepto. Derecho Internacional

  Departamento Jurídico

  Ministerio de Relaciones Exteriores de Chile

  SAGomez@direcon.gob.cl

Gobierno de Chile

MARCO LEGAL

Ley 19799

- Publicada el 12 de abril de 2002
- Última versión: 10 de octubre de 2014
- Ministerio de Economía, Fomento y Reconstrucción
- Subsecretaría de Economía, Fomento y Reconstrucción.
- ”Sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma”
- Disponible en línea desde la Biblioteca del Congreso Nacional de Chile: http://bcn.cl/1uw9n

Decreto Supremo 181

- Publicado el 17 de agosto de 2002
- Última versión al 27 de febrero de 2014
- Aprueba Reglamento de la Ley 19.799 sobre documentos electrónicos, Firma Electrónica y la Certificación de dicha firma
- Disponible en línea desde la Biblioteca del Congreso Nacional de Chile: http://bcn.cl/1xm85

Gobierno de Chile

NORMAS TÉCNICAS

Prácticas de Certificación

- ETSI TS 102 042 V1.1.1 (2002-04).Technical Specification. Policy requirements for certification authorities issuing public key certificates.
- NCh2805.Of2003 Tecnología de la Información – Requisitos de las políticas de las autoridades certificadoras que emiten certificados de claves públicas.
- ETSI TS 102 042 V1.2.2 (2005-06).RTS/ESI-000043.Keywords e- commerce, electronic signature, public key, security.
- ETSI TS 102 042 V2.1.1 (2009-05).Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- ETSI TS 102 042 V2.1.2 (2010-04) Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

Seguridad de la Información

- 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.

Estructura de Certificados

- ISO/IEC 9594 – 8: 2005 Information Technology – Open Systems Interconnection – The Directory Attribute Certificate Framework. Correccion 2:2009.
- ITU – T Rec.X.690 (2002) / ISO/IEC 8825-1:2002. ASN.1 Basic Encoding Rules.
- 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).

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

Sellado de Tiempo

- ETSI TS 102 023, v.1.2.1 y v.1.2.2.Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- ETSI TS 101 861 V1.3.1 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) (2001), RFC 5816 (update), ANSI ASC X 9.95.
- RFC 3628 Requirements for Times Stamping Authorities.
- NIST Special publication 800-102, Sept.2009.

DNI Electrónico e 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).
- Common Biometric Exchange File Format – formatos comunes de intercambio de archivos biométricos.

Gobierno de Chile

ENTIDAD ACREDITADORA

https://www.entidadacreditadora.gob.cl

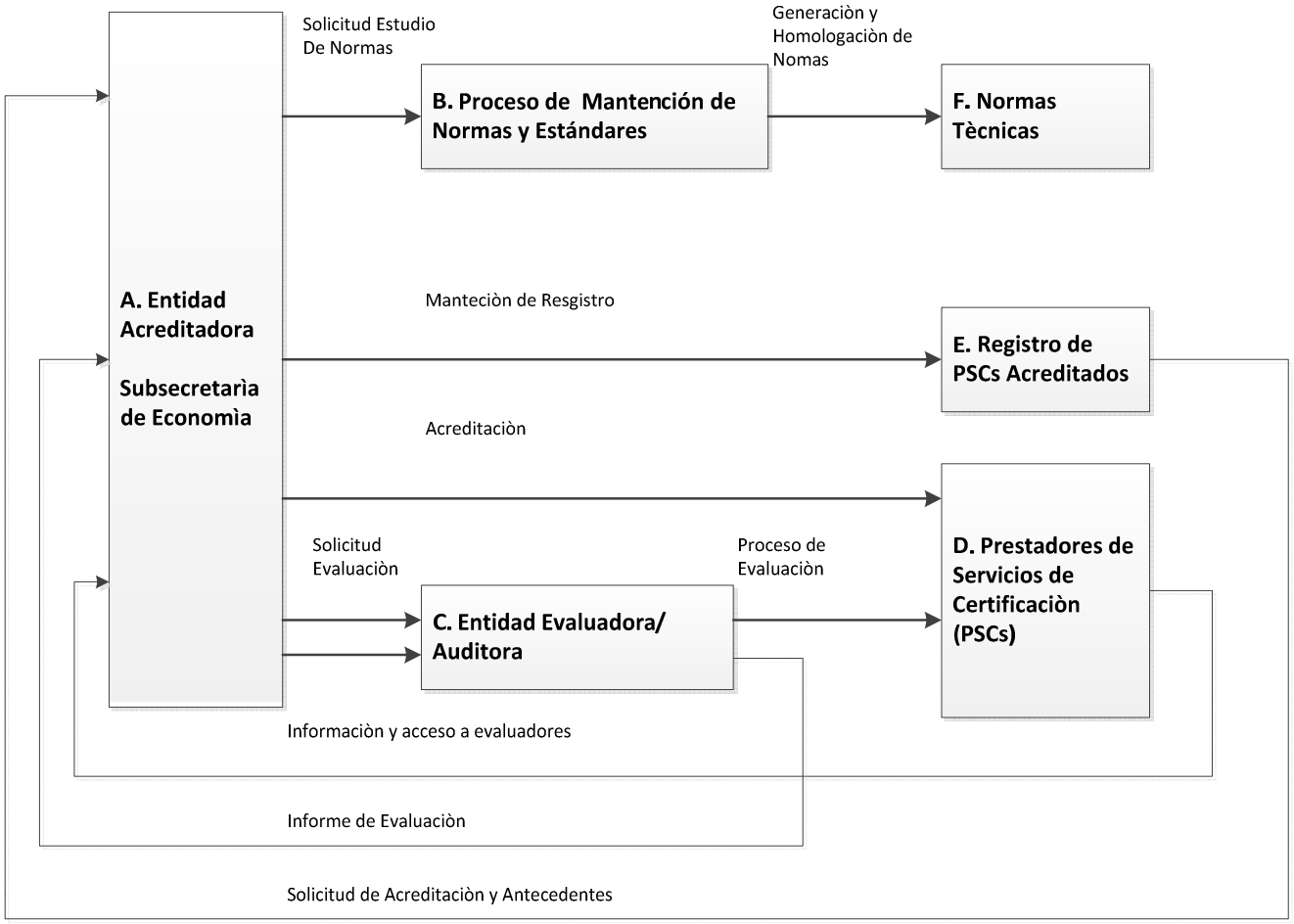
Entidad Acreditadora

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

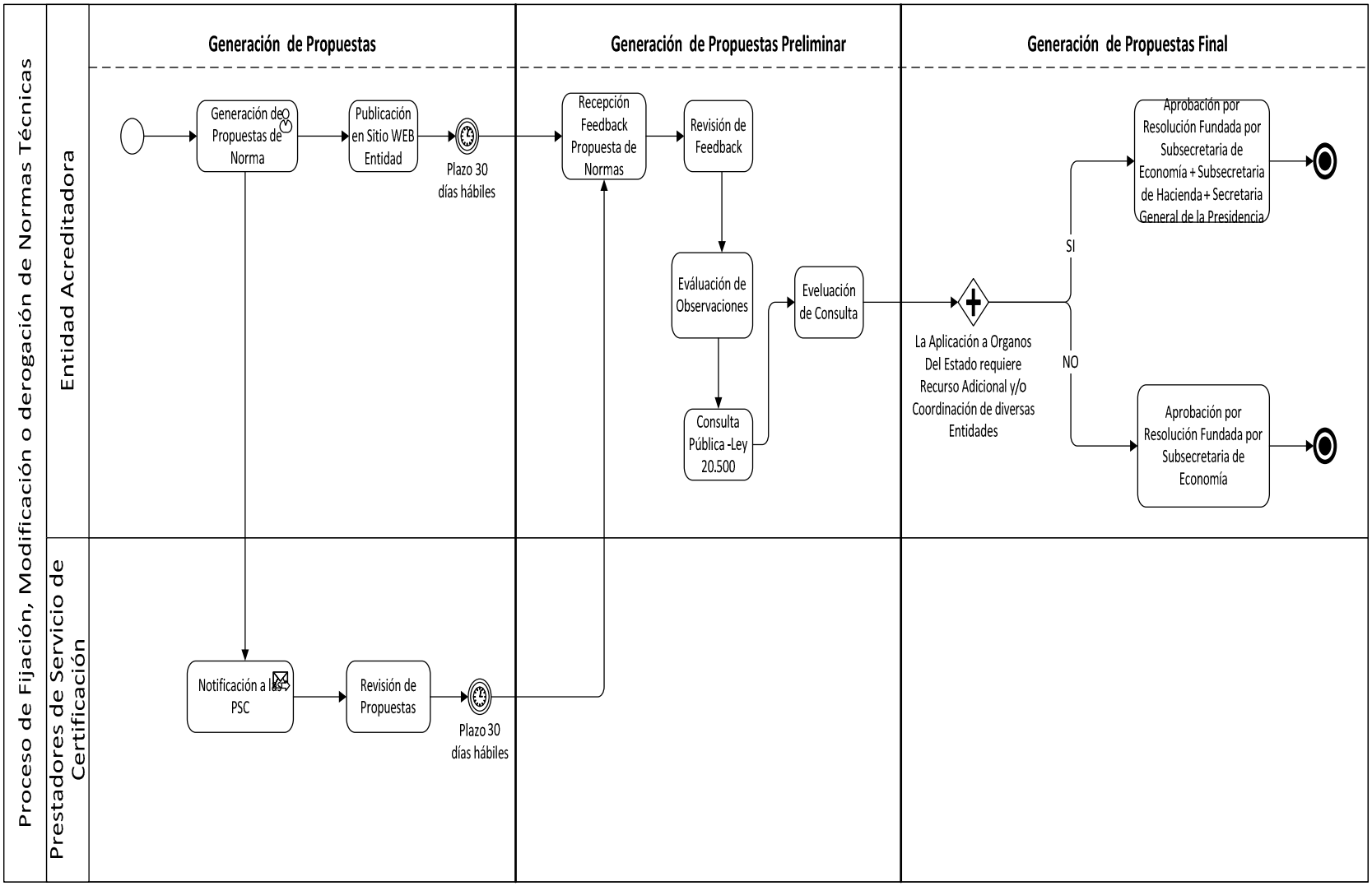
Entidad Acreditadora

- 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).

Esquema del proceso de acreditación



Proceso de actualización de normas técnicas



Gobierno de Chile

GUÍAS DE ACREDITACIÓN

Acreditación

- Se otorgará la acreditación al Prestador de Servicios de Certificación solicitante en los siguientes casos:

1. Si cumple plenamente los requisitos establecidos, de acuerdo a los criterios de evaluación definidos en esta Guía.
2. Cuando no cumple todos los requisitos, pero son calificados como subsanables por la Entidad Acreditadora, previa aprobación de un plan de medidas correctivas que permita al Prestador de Servicios de Certificación subsanar plenamente los incumplimientos en un plazo razonable.

- No se otorgará la acreditación al Prestador de Servicios de Certificación solicitante en el siguiente caso:

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

Evaluación

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.

Guías de Acreditación

- Orden de prelación

1. Firma Electrónica Avanzada
2. Sellado de Tiempo
3. Biometría (minucias)
4. Firma Móvil

Gracias.

Gobierno de Chile

www.gob.cl