ACEPTA

Empresas
a velocidad
digital

PO01

Declaración de Políticas de Certificación

Enero de 2014

RESPONSABLES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Certificación y Seguridad	- Gerente de Certificación y Seguridad - Oficina técnica. - Fiscalía	Gerente General

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
Declaración de Políticas de Certificación - PO01	1.0	Primera versión	23-01-2014
Declaración de Políticas de Certificación - PO01	1.1	Actualización proveedor de Data Center	04-03-2015
Declaración de Políticas de Certificación - PO01	2.0	Segunda versión	29-06-2016
Declaración de Políticas de Certificación - PO01	4.0	Revisión anual	01-10-2016
Declaración de Políticas de Certificación - PO01	4.1	Ajustes Perú	04-01-2017
Declaración de Políticas de Certificación - PO01	4.2	Ajuste a punto 3.4 (revocación por parte de la empresa)	29-05-2017
Declaración de Políticas de Certificación - PO01	5.0	Revisión anual	01-10-2017
Declaración de Políticas de Certificación - PO01	5.1	Posibilidad de realizar la operación de registro y validación en base a clave única del SRCeI	07-11-2017
Declaración de Políticas de Certificación - PO01	6.0	Revisión anual	01-10-2018
Declaración de Políticas de Certificación - PO01	7.0	Revisión anual	01-10-2019

CLASIFICACIÓN DEL DOCUMENTO

NIVEL DE CRITICIDAD: Baja **NIVEL DE CONFIDENCIALIDAD: Pública**
NOTA DE CONFIDENCIALIDAD: Se encuentra disponible ante su solicitud. ESTE DOCUMENTO NO PUEDE SER REPRODUCIDO, DISTRIBUIDO, COMUNICADO, TRANSMITIDOO ALMACENADO, TOTAL O PARCIALMENTE, EN CUALQUIER FORMA O POR CUALQUIER MEDIO, SIN EL PREVIO CONSENTIMIENTO POR ESCRITO DE ACEPTA.

CONTROL DE DIFUSIÓN

AUTOR/ES: Gerencia de Certificación y Seguridad
DISTRIBUCIÓN: • Sitio web • Ministerio de Economía

REFERENCIAS

Documentos Internos	
Título	**Nombre del archivo**
Documentos Externos	
• Ley N° 19.799, Ley 19.496 y Ley 19.628. (Chile) • Ley N° 27.269, Ley 29.733 (Perú) • Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Reconstrucción • DECRETO SUPREMO 019 (Perú) • Guías-de-Evaluación-Procedimientos-de-Acreditación-v2.1 (Chile) • Estándares Internacionales considerados en el Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Reconstrucción	

ÍNDICE

1. Introducción

1.1 Presentación

Este documento presenta la Política de Certificación (CP, por su sigla en inglés Certification Policy) de Acepta para los certificados de firma electrónica. Estas son una descripción de los procedimientos que Acepta declara convenir en la prestación de sus servicios de certificación, cuando emite y gestiona certificados de firma electrónica en su calidad de Prestador de Servicios de Certificación (PSC). Además, se incluyen las normas a seguir por quienes comprueban fehacientemente la identidad de los solicitantes de certificados de firma electrónica avanzada (Autoridad de Registro).

La Política de Certificación referida en este documento se utilizará para la emisión de certificados de firma electrónica, generados por Acepta y que se emitirán sobre dispositivo seguro de creación de firma. Mediante los certificados emitidos por Acepta y los dispositivos seguros de creación de firma, que se indican en esta Política de Certificación, se generarán firmas electrónicas reconocidas por las terceras partes.

Cabe indicar que la presente Declaración de Políticas de Certificación se ha generado siguiendo las especificaciones del documento RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" propuesto por Network Working Group para este tipo de documentos. Tales políticas son las que se prosigue en detallar, y están disponibles en el Sitio WEB de Acepta (www.acepta.com) para conocimiento público.

Esta Política de Certificación asume el manejo de conceptos básicos de Infraestructura de Clave Pública, certificado y firma digital, en caso contrario se recomienda estudiar estos conceptos, previo a continuar con la lectura del presente documento.

1.1.1 Sobre las Políticas de Certificación

Las políticas de certificación aquí descritas establecen el ciclo de vida de los servicios que provee Acepta, que como antes se ha mencionado incluyen desde la gestión de la solicitud de certificado, la verificación y validación de la información proporcionada, pasando por la emisión, uso, administración de los certificados, su revocación y su renovación. Es decir son aquellas políticas que dan seguridad y confianza a los certificados y servicios provistos por Acepta.

1.1.2 Alcance

El alcance de la Declaración de Políticas de Certificación (CP) detalla las condiciones de los servicios de certificación que presta Acepta para la emisión de sus certificados de firma electrónica.

1.1.3 Referencias

La presente Declaración de Políticas de Certificación se ha generado siguiendo las especificaciones del documento RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" propuesto por Network Working Group para este tipo de documentos.

1.2 Identificación

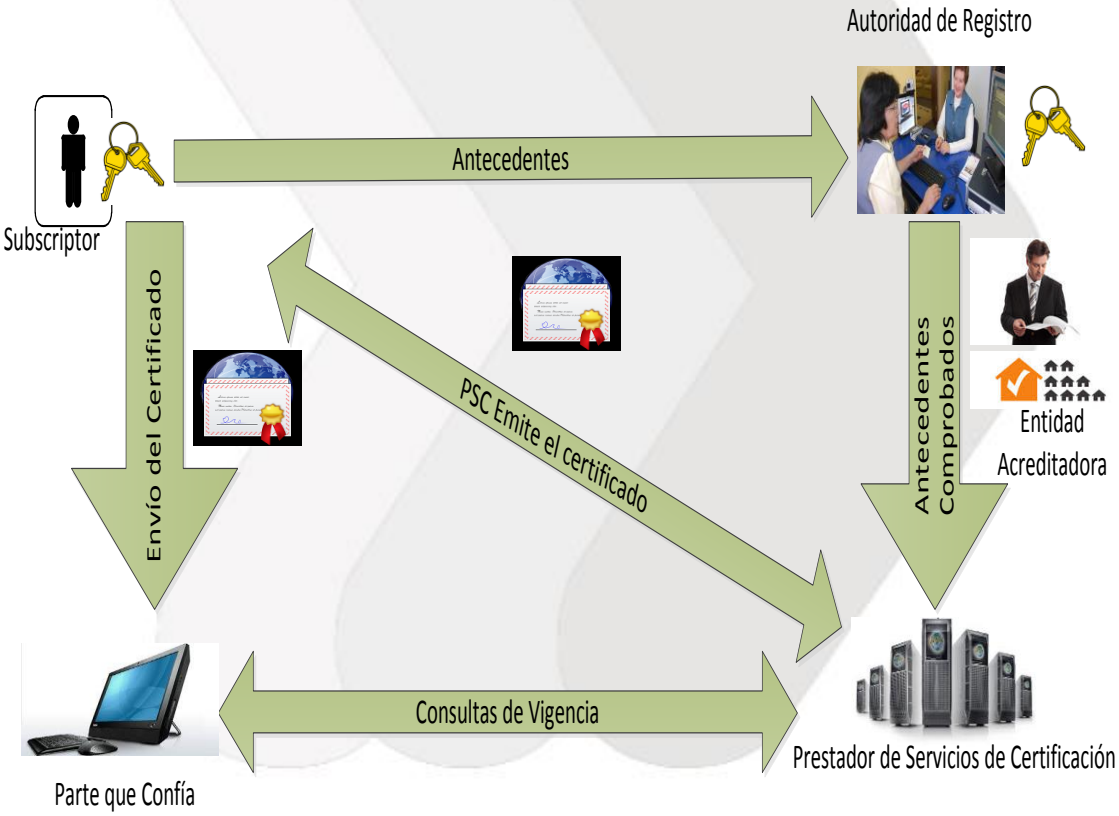
El presente documento se denomina “Políticas de Certificado de Firma Electrónica Avanzada de Acepta”, las que internamente se citan como CP o CP-FA y están registradas con el número único internacional (OID) 1.3.6.1.4.1.6891.3.

Acepta tiene asignado el identificador (OID) 1.3.6.1.4.1.6891, el cual está registrado en la Internet Assigned Number Authority (IANA). Este número identifica únicamente a Acepta en un contexto global.

En las CPS de Acepta, sección “1.2 Identificación”, se presenta la lista completa de OIDs administrados por Acepta.

1.3 Comunidad y Aplicabilidad

Los servicios de certificados de firma electrónica o clave pública de Acepta están insertos en una infraestructura en que se relacionan distintas entidades. Básicamente existen 5 tipos: Prestador de Servicios de Certificación (PSC), Autoridades de Registro (AR), Suscriptor, terceras partes que confían en los certificados y Entidad acreditadora. La siguiente figura muestra dicha relación:



1.3.1 Comunidad de usuarios

- **Solicitante:** Son las personas que concurren a Acepta a solicitar un certificado de firma electrónica avanzada, completan el formulario de solicitud y proveen todos los antecedentes que exige la ley y esta CPS para comprobar fehacientemente su identidad.
- **Suscriptores:** Son las personas titulares de los datos de creación de firma a quienes le corresponde o está asociada la clave pública informada en los certificados de firma electrónica

avanzada. Los suscriptores son personas naturales, sin perjuicio que puedan concurrir en la suscripción documental en nombre propio o en la representación de alguna persona jurídica.

- **Autoridad de registro**: La recepción y procesamiento de las solicitudes de certificados es realizada por la "Autoridades de Registro" (AR) de Acepta, sea que lo haga directamente o a través de un mandatario especialmente designado para tal objeto. La Autoridad de Registro debe realizar la comprobación fehaciente de la identidad de los solicitantes de certificados de firma electrónica avanzada. En caso que sea un tercero el que actúe, en calidad de mandatario de Acepta, como Autoridad de Registro, la actividad deberá desarrollarla dando pleno cumplimiento al contrato de mandato y a esta Declaración de Prácticas de Certificación.
- **Prestador de Servicios de Certificación ("PSC")**: Es la entidad prestadora de los servicios de certificación de firma electrónica avanzada, de conformidad a la ley, en particular, a lo previsto en la Ley 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma (Chile) o Ley 27.269 (Perú), que en este caso es Acepta.
- **Tercera parte que confía**: Es el receptor de un certificado de firma electrónica avanzada. Normalmente, junto con el certificado este tercero recibe un documento electrónico que se encuentra suscrito con la firma electrónica avanzada del suscriptor. La parte que confía debe contar con mecanismos que le permitan validar si se trata de un certificado auténtico y si este certificado se encontraba vigente en el momento en que se produjo la suscripción documental.
- **Entidad Acreditadora:** La Subsecretaría de Economía, que de conformidad con lo dispuesto en la Ley 19.799 el Prestador de Servicios de Certificación de Firma Electrónica debe demostrarle que cuenta con las instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados de firma electrónica avanzada, permitiendo su inscripción en el registro de certificadores acreditados. En el caso de Perú, el DECRETO SUPREMO 019, designa INDECOPI para esta función.

Los usuarios que utilicen los certificados - emitidos directamente por Acepta o por alguna de sus autoridades certificadoras acreditadas - antes de solicitar dichos certificados - deben conocer y estar en conformidad con lo establecido en estas CPS y en las CP correspondientes al tipo de certificado.

1.4 Aplicabilidad de los certificados

Los Certificados emitidos por Acepta se utilizarán únicamente conforme a la función y finalidad que tengan establecida en la presente Declaración de Políticas de Certificación, en las correspondientes Prácticas de Certificación y de conformidad con lo dispuesto en la Ley 19.799 (Chile) y su reglamento o Ley 27.269 (Perú) y su reglamento.

1.4.1 Tipos y usos de los certificados

Acepta emite distintos tipos de certificados, definiendo cada tipo un nivel de seguridad, restricciones y requerimientos específicos respecto a las medidas tomadas para la autentificación de la entidad suscriptora del certificado, mecanismos de emisión, revocación y utilización de los certificados. Los usuarios o suscriptores deberán elegir la clase de certificado que más se ajuste a sus necesidades.

El conjunto de normas que regulan la aplicabilidad de los distintos tipos de certificados, en determinados ambientes y comunidades se denomina “Política de Certificados” o CP. Acepta posee una política de certificado para cada tipo de certificado emitido.

Los certificados de firma electrónica avanzada de persona natural, son emitidos por Acepta para soportar las siguientes necesidades de seguridad:

1. **Autentificación:** proporciona suficientes garantías respecto a la identidad del suscriptor del certificado, al requerirse la presencia del suscriptor junto con su Cédula Nacional de Identidad e imponer que el almacenamiento de la llave privada sea en un dispositivo especializado y acreditado según la norma internacional FIPS-140 nivel 2.
2. **Integridad de mensajes:** los mensajes firmados con certificado de firma electrónica avanzada permiten validar si el contenido de mensaje ha sido alterado en el tiempo transcurrido desde su generación.
3. **Firmas digitales:** las firmas digitales producidas con certificados de firma electrónica avanzada ofrecen los medios de respaldo para demostrar fehacientemente, incluso en tribunales, la autenticidad de un mensaje o documento electrónico.
4. **Privacidad:** Los certificados de firma electrónica avanzada permiten cifrar mensajes de forma que al ser transmitidos sean visibles sólo por el remitente correspondiente. Sin embargo, Acepta recomienda usar otros certificados para estos fines, con una duración de al menos 10 años. La expiración o revocación de los certificados de firma electrónica avanzada no provocan consecuencias con las firmas electrónicas generadas en forma previa al término de la vigencia del certificado, pero en el caso de mensajes cifrados, se genera un problema al expirar el certificado, ya que este se debe conservar durante todo el período de tiempo en el que se desee poder descifrar los mensajes protegidos.

1.4.2 Limitaciones de Usos y Prohibiciones

Los Certificados de firma electrónica avanzada emitidos por Acepta se utilizarán únicamente conforme a los usos y finalidades que tengan establecida en este documento y en las correspondientes Prácticas de Certificación, y de acuerdo a la normativa chilena y/o peruana vigente y a los convenios internacionales ratificados por estos Estados. Cualquier uso diferente del autorizado por ley e indicado en estas prácticas está expresamente prohibido. En consecuencia, será responsabilidad del Suscriptor el uso no autorizado o indebido que éste haga del mismo

Asimismo, queda expresamente prohibido alterar en cualquier forma los certificados emitidos por Acepta, los que solo serán válidos en la forma suministrada por Acepta.

1.4.3 Contenido de los Certificados

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

1.5 Detalle de los contactos y administración de la CA

Cualquier consulta respecto a las normas contenidas en este documento, puede ser realizada en la siguiente dirección:

- **Nombre**: Acepta.com S.A.
- **Dirección de e-mail**: contacto_cys@acepta.com
- **Dirección**: Av. Providencia 1760, piso 8, Providencia, Santiago de Chile
- Código Postal: 7500498
- **Número telefónico**: (+56-2) 27149590

1.6 Definiciones y Acrónimos

El A efectos del documento de Políticas de Certificación, las expresiones que se pasan a indicar a continuación tendrán el alcance y/o significado que se pasa a indicar en cada caso:

- **Prestador de Servicios de Certificación:** Es aquella entidad que en conformidad con la legislación vigente emite certificados de firma electrónica avanzada.
- **Autoridad de Registro:** Es Acepta personalmente o representada a través de un mandatario, para la comprobación fehaciente de la identidad de los solicitantes de certificados.
- **Certificado:** Certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica
- **Certificado raíz:** Certificado cuyo suscriptor es Acepta y pertenece a la jerarquía que Acepta presenta como Prestador de Servicios de Certificación.
- **Clave:** Secuencia de símbolos.
- **Datos de creación de firma:** Son datos únicos que el suscriptor utiliza para crear la Firma electrónica y que se encuentran inequívocamente unidos a la clave pública contenida en el certificado de firma electrónica avanzada..
- **Clave Pública:** Son los datos que se utilizan para verificar la Firma electrónica y que se encuentran inequívocamente unidos a los datos de creación de firma.
- **Declaración de Prácticas de Certificación:** Declaración de Acepta, respecto a aquellas prácticas, a nivel de sistemas y de personal, que en base a sus buenas prácticas dan seguridad y confianza a los certificados y servicios provistos pro Acepta.
- **Firma electrónica avanzada:** Aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría
- **Listas de Revocación de Certificados:** registro de acceso público de certificados, en el que quedará constancia de los certificados que han perdido su vigencia por haber sido revocados.
- **Número de serie de Certificado:** Valor entero y único que está asociado inequívocamente con un certificado expedido por Acepta.
- **OCSP (Online Certificate Status Protocol):** Protocolo informático que permite la comprobación del estado de un certificado en el momento en que éste es utilizado.
- **Prestador de Servicios de Certificación (PSC):** Es aquella entidad que en conformidad con la legislación, emite certificados de firma electrónica.

- **Política de Certificación:** Es el conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad en particular y/o clase de aplicación con requerimientos de seguridad comunes. Es el documento que completa la Declaración de Prácticas de Certificación, estableciendo las condiciones de uso y los procedimientos seguidos por Acepta para emitir Certificados.
- **SHA-1: Secure Hash Algorithm** (algoritmo seguro de resumen –hash-). Desarrollado por el NIST- El algoritmo consiste en tomar mensajes de menos de 2^{64} bits y generar un resumen de 160 bits de longitud. La probabilidad de encontrar dos mensajes distintos que produzcan un mismo resumen es teóricamente nula. Por este motivo se usa para asegurar la Integridad de los documentos durante el proceso de Firma electrónica.
- **SHA-2: Secure Hash Algorithm** (algoritmo seguro de resumen –hash-). Desarrollado por el NIST- El algoritmo consiste en tomar mensajes de menos de 2^{64} bits y generar un resumen de 256 bits de longitud.
- **Solicitante:** Persona que solicita la emisión de un certificado de firma electrónica avanzada dando cumplimiento a las exigencias establecidas en la Ley y en esta Declaración de Prácticas de Certificación.
- **Suscriptor:** Es la persona cuya identidad personal ha quedado vinculada a los datos de creación de firma, a través de una clave pública certificada por el Prestador de Servicios de Certificación Acepta.
- **Terceras partes que confían:** Aquellas personas que voluntariamente depositan su confianza en un certificado de Acepta, comprobando la validez y vigencia del certificado según lo descrito en esta Declaración de Prácticas de Certificación y en las Políticas de Certificación asociadas a cada tipo de certificado.
- **X.509:** Estándar desarrollado por la UIT, que define el formato electrónico básico para certificados electrónicos.

Acrónimos

- AC: Autoridad Certificadora
- ACR: Autoridad Certificadora Raíz
- AFIS: Automated Fingerprint Identification System
- AR: Autoridad de Registro
- CA: Certification Authority
- CP: Certificate Policy
- CP-FA: Políticas de Certificado de Firma Electrónica Avanzada
- CPS: Certification Practice Statement
- CRL: Certificate Revocation List
- FIPS: Federal Information Processing Standard
- HSM: Hardware Security Module
- IANA: Internet Assigned Number Authority
- IETF: Internet Engineering Task Force
- ITU: international Telecommunication Union
- KEY USAGE: En este contexto es el uso que se da al Certificado
- NFPA: National Fire Protection Association
- NIST: Instituto Nacional de Estándares y Tecnología
- OCSP: On-line Certificate Status Protocol
- OID: Object Identifier
- PKCS#10: Certification Request Syntax Specification

- PSC: Prestador de Servicios de Certificación
- PIN: personal Identification Number
- PKI: Public Key Infrastructure
- RA: Registration Authority
- RSA: Algoritmo de Encriptación
- SII: Servicio de Impuestos Internos
- UIT: Unión Internacional de Telecomunicaciones
- X.500: Serie de estándares computacionales

2 Requerimientos Generales

2.1 Obligaciones

Acepta, en su calidad de Prestador de Servicios de Certificación se obliga ejecutar sus actividades de certificación acorde con las Prácticas de certificación asociadas a cada tipo de certificador. Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.1.1 Obligaciones de la AC Raíz (ACR)

El certificado raíz de Acepta, permite firmar aquellos certificados de las entidades que de él son subordinadas. Es así como el certificado raíz de Acepta es sobre el cual se basa el modelo de confianza de toda la jerarquía de entidades intermedias que ha emitido Acepta, ya que los certificados de estas entidades intermedias, en este caso Acepta ha generado para sí misma dichos certificados intermedios, son firmados por la raíz misma.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.1.2 Obligaciones de la Autoridad de Registro (AR) y la Autoridad Certificadora (AC)

Cada AR y/o PSC acreditado deberá cumplir las normas y ser consistente con lo establecido en el documento de Prácticas de Certificación de cada tipo de certificado.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.1.3 Obligaciones del Solicitante

Los solicitantes de certificados a Acepta, se obligan a conocer las políticas y prácticas de certificación, entregar antecedentes fidedignos al momento de la solicitud, notificar cambios que en ellos ocurran y finalmente suscribir el contrato de servicios.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.1.4 Obligaciones del Suscriptor de la llave

Los suscriptores de certificados a Acepta, se obligan a conocer las políticas y prácticas de certificación, conocer el alcance del certificado, proporcionar antecedentes fidedignos, notificar cambios en dichos antecedentes y finalmente pagar la tarifa del servicio.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.1.5 Obligaciones los Usuarios

Los usuarios de certificados emitidos por Acepta, o cualquier entidad que deposite su confianza en dichos certificados deberá comprobar el estado de los certificados y conocer el propósito y alcance del certificado.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.1.6 Confianza en las Firmas y Certificados

Las partes que consideren confiar en las firmas y certificados emitidos por Acepta deberán tener conocimiento de las normas legales que sigue el Proveedor de Servicios de Certificación, deberán verificar la autenticidad de la firma, deberán asegurar el estado de esta firma, deberán acotar la confianza al uso definido para el certificado emitido, deberán verificar su validez y finalmente deberán tomar conocimiento de las consecuencias en que se incurre al aceptar y usar los certificados en que se confía.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.1.7 Obligaciones de los Repositorios

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.2. Responsabilidad del PSC

Acepta solo será responsable de los daños y perjuicios que en el ejercicio de la actividad de certificación de firma electrónica ocasione y, en ningún caso será responsable del uso incorrecto, indebido o fraudulento de los certificados de firma electrónica emitidos ni de cualquier daño indirecto o imprevisto que resulte de su uso.

Acepta será responsable de los daños y perjuicios que en el ejercicio de su actividad de certificación de firma electrónica ocasione, debiendo demostrar que actuó con la debida diligencia.

Será responsabilidad de los usuarios adoptar las medidas de prevención usuales a la actividad computacional para evitar daños y perjuicios originados por el uso o incapacidad de uso de los certificados de firma electrónica.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.2.1 Responsabilidad Pecuniaria

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.2.2 Fuerza Mayor

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.2.3 Responsabilidad de la AC y AR

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.3 Ley Aplicable y Resolución de Conflictos

Acepta declara efectuar sus actividades en conformidad con los principios generales de la legislación chilena y o peruana (según corresponda) y dando cumplimiento a todas y cada una de las leyes aplicables a las actividades desarrolladas por Acepta.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.4 Publicación y Repositorios

Acepta publica en su sitio Web en www.acepta.com, las prácticas de certificación por ella utilizadas, así como las políticas de certificado (CP) pertinentes a cada tipo de certificado emitido, las cuales están a disposición de los usuarios sin cargo alguno.

La información respecto al estado de vigencia y validez de los certificados emitidos por Acepta, se encuentra disponible en el sitio Web de Acepta.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.5 Privacidad y Protección de los Datos Personales

Las Políticas de Privacidad de Acepta se encuentran publicadas en el sitio web de Acepta www.acepta.com.

2.5.1 Tipos de Información a Proteger

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.5.2 Tipos de Información que puede ser entregada

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.5.3 Información del Certificado

Los certificados de firma electrónica avanzada emitidos por Acepta están en conformidad con el formato X.509v3 definido en ITU-T X.509v3 y las recomendaciones de la IETF RFC-3280.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.5.4 Entrega de Información sobre la Revocación o Suspensión del Certificado

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.5.5 Entrega de Información en virtud de un Procedimiento Judicial y/o Administrativo

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.5.6 Entrega de Información a Petición del Titular

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

2.6 Derechos de Propiedad Intelectual e Industrial

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

3 Identificación y Autenticación

Tanto las políticas como las prácticas implementadas por Acepta en la validación de la identidad del solicitante de un certificado son presentadas en el documento de políticas escrito para cada tipo de certificado.

3.1 Registro Inicial

3.1.1 Registro de Nombres

Todos los suscriptores de contratos requieren un nombre distintivo como se menciona en el estándar X.500, el cual es registrado en un campo del certificado. Del mismo modo se registrará el RUN o RUT, en caso de emitirse el certificado a una persona natural o a una persona jurídica según corresponda.

Se considerará como válido, en el caso de los nombres, cualquiera que sea aceptado por el Servicio de Registro Civil e Identificación o en el Registro de personas Jurídicas.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

3.1.2 Verificación General

Acepta, como parte del proceso de emisión de certificados, procederá a verificar la identidad de la persona a la cual se asociará el certificado. Para esto el solicitante se presentará ante un operador de registro, o a quien Acepta determine para ejecutar esta función (Servicio de Registro Civil e Identificación o Notarios), quien estará encargado de verificar la identidad de este versus la cédula de identidad presentada.

Respecto a la dirección de correo electrónico del suscriptor, Acepta informa que no garantiza que esta dirección de correo esté vinculada con el suscriptor del certificado, por lo que la confianza en que esta dirección recae sólo en la parte confiante. Acepta, garantiza que la dirección electrónica de correo contenida en el certificado, ha sido aportada por el suscriptor al momento de formalizar su solicitud.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

3.2 Reemisión de la Llave

No aplica

3.3 Reemisión de la Llave luego de una Revocación

No aplica

3.4 Requerimiento de Revocación

El proceso de solicitud de revocación viene definido por la Política de Certificación aplicable a cada tipo de certificado. La política de identificación para las solicitudes de revocación acepta los siguientes métodos de identificación:

- Solicitud del titular del certificado (en caso de emisión a persona natural) o solicitud del representante legal actual de la empresa o del titular del certificado a revocar (en caso que el certificado esté emitido para un cargo de dicha empresa).

- Por oficio de Acepta ante sospecha fundada de compromiso en la clave privada de un suscriptor.
- Presencial con una identificación similar a la primera solicitud de certificado (ver 3.1.2).
- Por medio electrónico, en que el titular debe enviar a Acepta un e-mail firmado con firma electrónica avanzada, siendo la casilla de destino admin-revocaciones@acepta.com.
- Por carta certificada, en caso de revocar su certificado de firma electrónica y no desear continuar con el servicio, adjuntando además fotocopia de su carnet de identidad.

La revocación tendrá lugar cuando Acepta constate alguna de las circunstancias especificadas en la Declaración de Prácticas de Certificación (CPS) de Acepta.

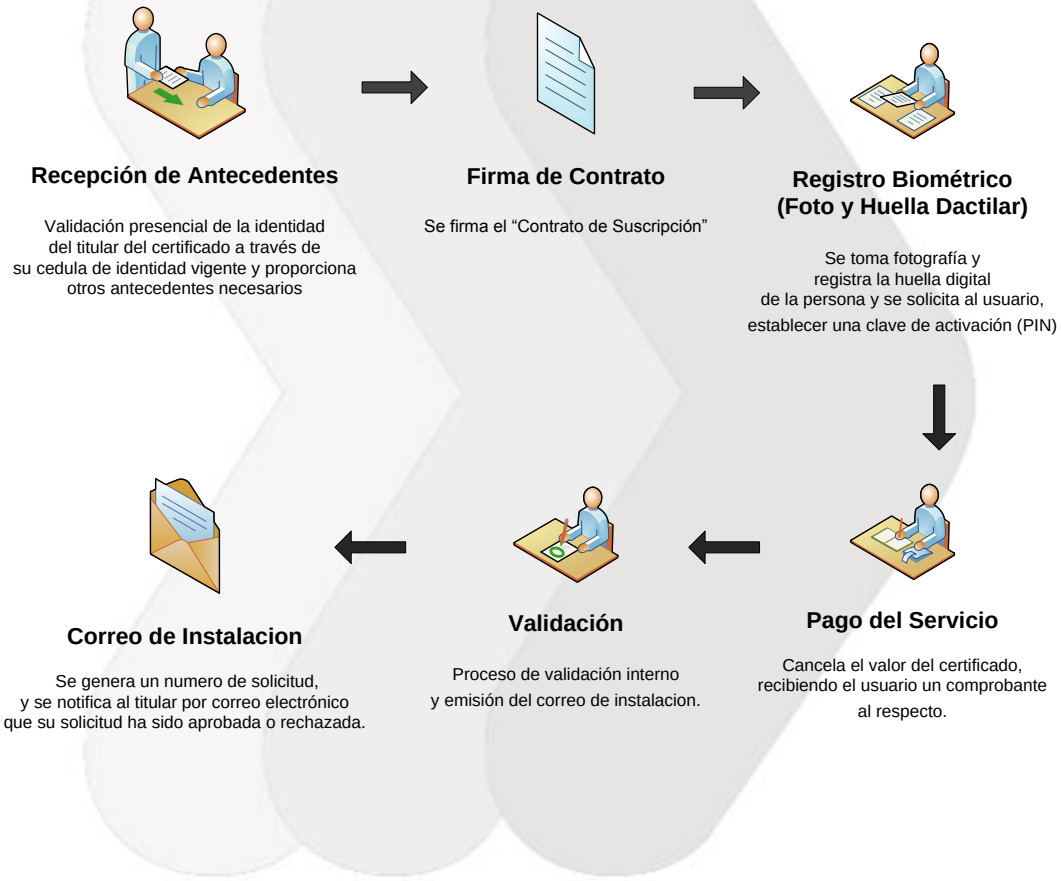
4 Requisitos Operacionales

Las especificaciones de este capítulo son complementadas en el documento de declaración de prácticas de certificación.

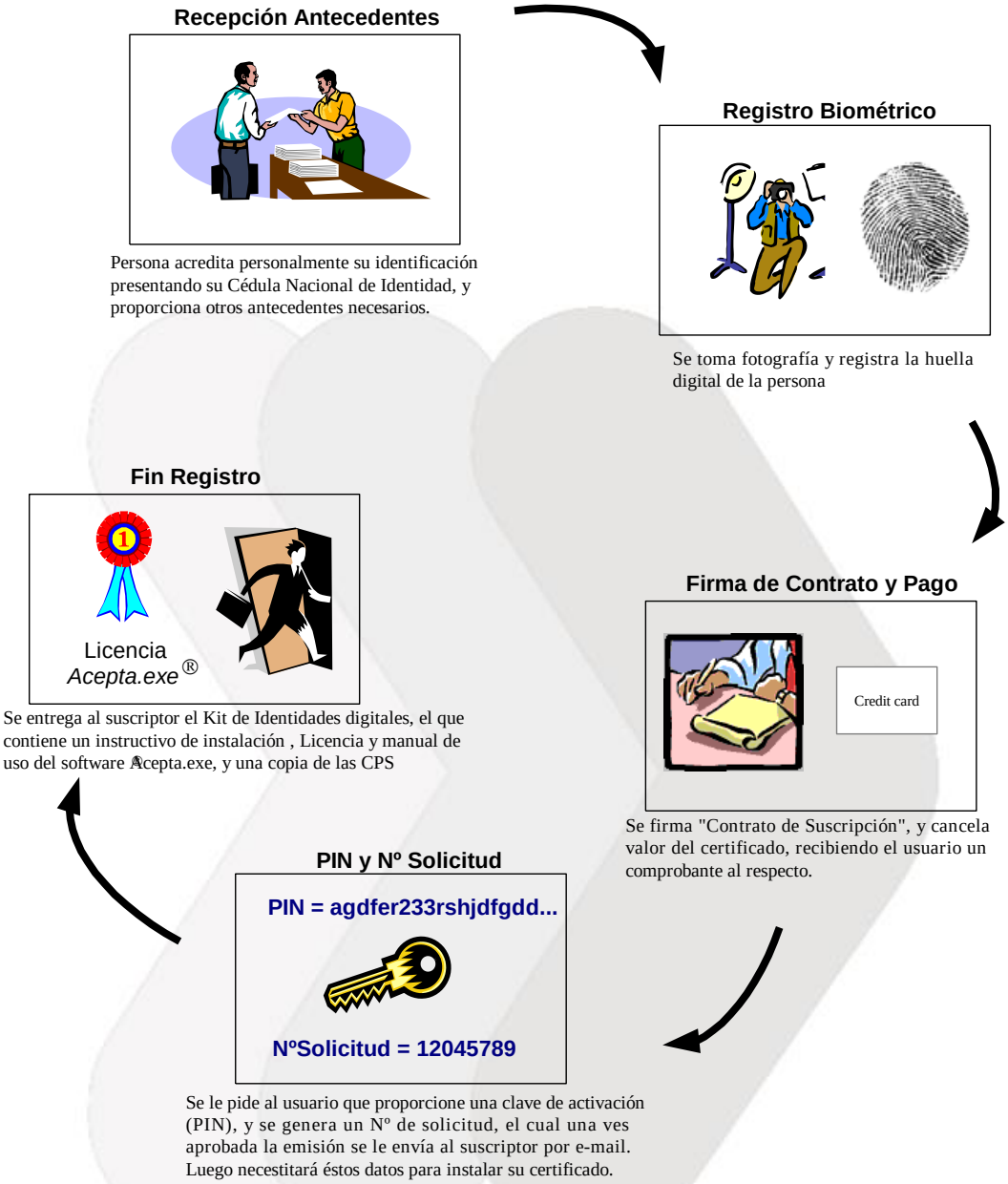
4.1 Manuales Operacionales

Para cumplir las labores de registro inicial, validación y emisión de certificados de firma, Acepta cuenta con manuales operacionales los cuales guían a los operadores de registro y validación en las labores asociadas a su rol. En estos documentos se describen los requisitos operativos pertinentes a las etapas de certificación, conducentes a la obtención de un certificado de persona de firma electrónica avanzada. Además, se describe el mecanismo de revocaciones y/o suspensiones.

El siguiente diagrama muestra el proceso de registro



Un mayor detalle para este proceso, se presenta en la siguiente figura:



4.2 Solicitud de Certificado

La solicitud de certificados de firma electrónica avanzada puede ser hecha a través de cualquier medio. La exigencia de Acepta es que se realice un registro presencial, después del cual se contará con los siguientes datos del solicitante:

- RUN: Rol Único Nacional emitido por el Servicio de Registro Civil e Identificación.
- Nombres y apellidos, tal como aparecen en la cédula de identidad o pasaporte. Por razones de compatibilidad con X.509v3, las letras acentuadas son reemplazadas por letras sin acento y las "ñ" son reemplazadas por "n".
- Dirección de correo electrónica.
- Título o profesión, tal como aparece en la cédula de identidad.

Si el registro presencial es hecho por un operador de registro de Acepta, se capturan los siguientes datos:

- Imagen escaneada de la cédula de identidad por ambos lados.
- Foto del solicitante.
- Contrato de suscripción, con firma manuscrita e impresión dactilar.

Si el registro presencial es hecho por un funcionario del Registro Civil, se envían los siguientes datos a Acepta:

- RUN
- Nombres
- Fecha de nacimiento
- Foto en formato digital
- Impresión dactilar en formato digital
- Digitalización de firma manuscrita
- Copia de un comprobante en papel firmado en forma manuscrita por el solicitante

En caso de que el solicitante cuente con una Clave Única emitida por el Servicio de Registro Civil, el proceso de registro y validación (proceso de responsabilidad de la Autoridad de Registro de ACEPTA), podrá ser reemplazado por la captura de los datos civiles del solicitante, estando la verificación de identidad del solicitante dada de facto por la relación de confianza con el emisor de esta clave única.

Si la solicitud de registro fue hecha por el suscriptor, pero la validación presencial es efectuada por un notario; una vez recibida la carta certificada por parte del notario, se procederá a validar la solicitud versus la carta en cuanto a:

- RUN
- Nombres
- Fecha de nacimiento
- Firma
- Fotocopia de cédula de identidad

Respecto a la contraseña de activación, su generación dependerá de quién es quien realiza el registro presencial, es así como:

- Si el registro presencial es hecho por un operador de registro de Acepta, entonces el solicitante debe digitar 2 veces una contraseña de activación. La contraseña de activación es almacenada usando una transformación hashing, por lo que ninguna persona o proceso de Acepta tiene acceso a la contraseña digitada por el usuario.
- Si el registro presencial es realizado por un funcionario del Registro Civil, entonces la contraseña de activación es generada en forma aleatoria por el sistema y se le entrega al solicitante impresa en un comprobante asociado a la solicitud. Esta contraseña es enviada de manera cifrada a Acepta.
- Si la solicitud de registro es efectuada por el solicitante, y validada por el notario, entonces la contraseña se generará cuando el solicitante ingrese sus datos al formulario electrónico.

A fin de apoyar el proceso de certificación, se solicita además los siguientes datos:

- Datos de contacto
- Información de pago

La recopilación de los antecedentes del individuo, en caso de realizarse por el operador de registro, se realiza por medio del software desarrollado por Acepta denominado Registro.exe©, el cual se encarga de adjuntar toda la información necesaria, y posteriormente enviar dicha información al Prestador de Servicios de Certificación, para su validación y emisión del certificado requerido.

El programa Registro.exe©, realiza toda su operación de una manera segura. Cada operador que utilice el programa debe firmar electrónicamente todos los datos capturados con un certificado de firma electrónica, emitida por Acepta, para dichos fines. Los datos de registro firmados por un operador de registro se denominan solicitud electrónica de firma avanzada. Las solicitudes son enviadas de manera cifrada a Acepta, lo que garantiza que se mantiene la autenticidad, integridad y confidencialidad de dicha información durante todo el proceso.

En caso de realizarse por el Servicios de Registro Civil e Identificación, dicha solicitud será desarrollada a través del servicio de emisión de Cédulas y Pasaportes que este Servicio posee. Finalmente en el caso de las solicitudes cursadas a través de notarios, la información será ingresada a través de una página web provista por Acepta.

4.2.1 Validación y aprobación de certificados

Las menciones exigidas por la Ley 19.799 (Chile) o Ley 27.269 (Perú), para los certificados de firma electrónica avanzada deben ser comprobados fehacientemente por Acepta, por un notario o por un funcionario del Servicio de Registro Civil e Identificación de Chile o RENIEC, según corresponda.

Luego que los antecedentes del suscriptor son remitidos a Acepta, se procede a su validación central, necesaria para verificar la consistencia de dichos antecedentes en relación con la solicitud de certificado correspondiente. Para ello, un operador de validación recupera y revisa las solicitudes pendientes, corroborando la siguiente información:

a. Cuando el registro presencial fue hecho por un operador de registro

- Verifica que la información del nombre y RUN asociados a la solicitud correspondan con las copias electrónicas de la Cédula Nacional de Identidad.

- Verifica que el nombre, RUN, y dirección de e-mail de la solicitud correspondan a los datos estipulados en la copia electrónica del contrato del suscriptor.
- Verifica que la copia electrónica del contrato de suscripción esté debidamente firmada y con impresión dactilar, y que dicha firma corresponda a la de la Cedula Nacional de Identidad.

b. Cuando el registro presencial fue hecho por un funcionario del Registro Civil

- Verifica que los datos recibidos estén completos y no tengan problemas de formato.

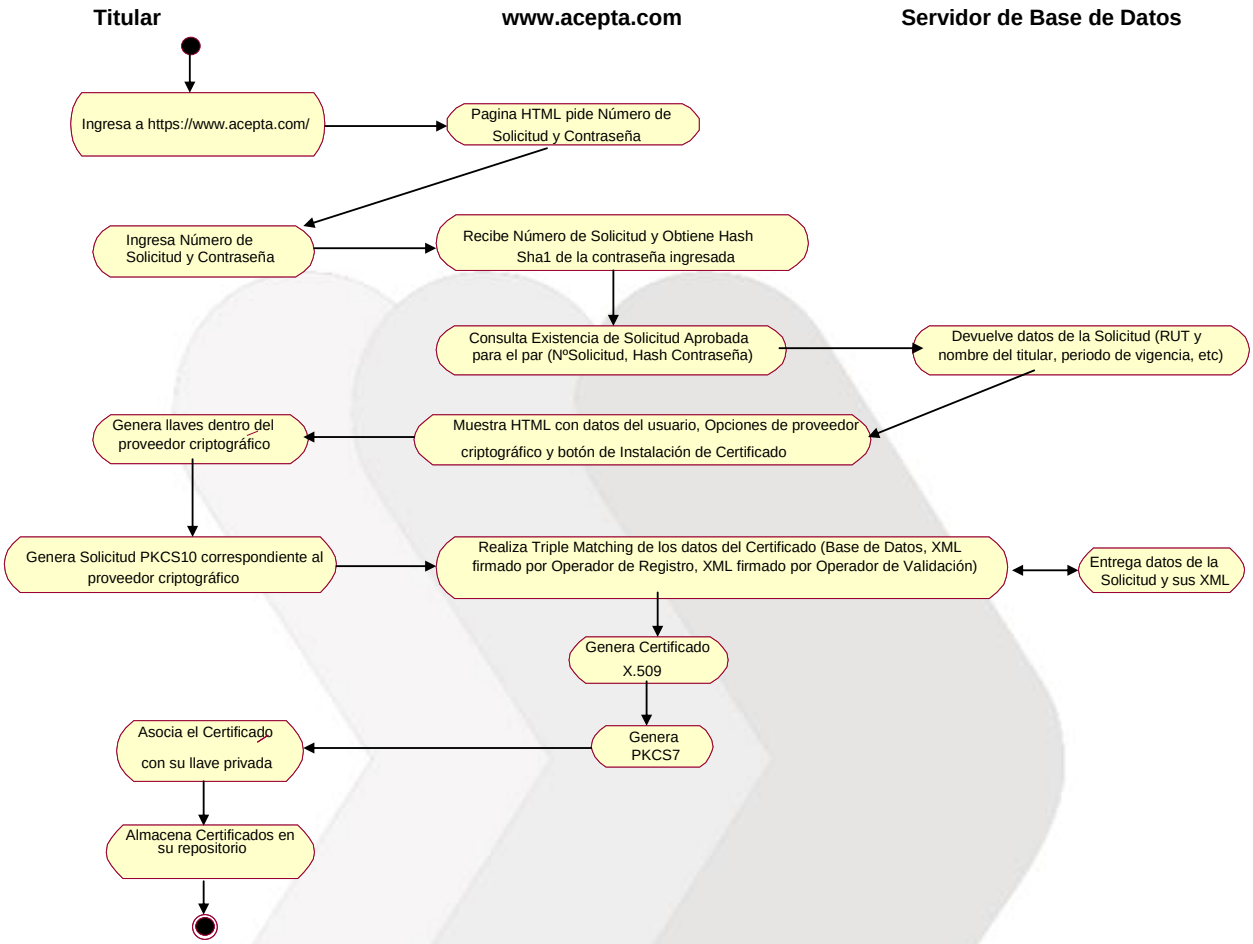
c. Cuando la solicitud de registro fue realizado por el solicitante y la identidad verificada ante un notario:

- Verifica que los datos recibidos, desde el notario, estén completos y no tengan problemas de formato.

Si las validaciones anteriores son exitosas, entonces el operador aprueba la solicitud, con lo que se envía automáticamente un e-mail al suscriptor con el Número de la solicitud y notificando que ésta ha sido aprobada. Esta etapa además sirve como forma de verificación de la casilla de e-mail declarada por el solicitante, ya que sin este número de solicitud no se podrá emitir el certificado.

4.3 Emisión de Certificados

El proceso seguido para la emisión, recuperación e instalación de un certificado de firma avanzada es descrito a continuación:



Una vez que el suscriptor ha recibido por e-mail la notificación de que su solicitud de certificado ha sido aprobada, éste debe conectarse a una página web de emisión de certificados ubicada en:

www.acepta.com → Autoservicio → Instalar Certificado

Luego, el suscriptor deberá proporcionar la clave de activación (definida en el registro presencia) y el número de solicitud (recibido por e-mail).

Todos los datos digitados por el usuario son enviados de manera segura (cifrada) al sitio de Acepta a través de Internet, en donde se realiza la validación necesaria para comprobar que dichos datos correspondan efectivamente a una solicitud previamente requerida, y que hasta ese momento se encuentra en estado pendiente y aprobada. Esto garantiza que el certificado será instalado sólo en el equipo del suscriptor que corresponde a la solicitud, y cuyos antecedentes de registro se encuentran en Acepta.

Siguiendo con el proceso, Acepta le envía al usuario una página con los antecedentes del certificado requerido y se los presenta al usuario para su confirmación.

Si el usuario reconoce, se genera el par de llaves pública y privada, lo que es realizado íntegramente en el equipo computacional del suscriptor, dentro del dispositivo de almacenamiento de llaves privadas.

La clave pública generada es enviada de manera segura al sitio de Acepta. La información correspondiente de la llave pública, se transmite usando el formato estándar PKCS#10.

En los servidores de Acepta se prepara un certificado en formato X.509v3 se envía a servidores de firma. Los servidores de firma son administrados con los más altos niveles de seguridad y no tienen acceso a Internet.

Antes de firmar el certificado X.509v3, en los servidores de firma se realiza un “Triple matching", el cual valida los siguientes elementos:

- Que los datos del certificado que se generará coincidan con los datos de la base de datos que apoyan los procesos de Acepta. Esto se hace indirectamente al usar los datos de la base de datos de Acepta para preparar el archivo X.509v3 y tomar sólo la clave pública del archivo PKCS#10.
- Que los datos del certificado que se generará coincidan con una solicitud de registro firmada con la firma electrónica avanzada de un operador de registro autorizado por Acepta.
- Que los datos del certificado que se generará coincidan con una autorización firmada con la firma electrónica avanzada de un operador de validación central autorizado por Acepta.

La lista de Operadores de Registro y Operadores de Validación autorizados por Acepta se encuentra firmada por la AC intermedia de Acepta y es generada con los mismos estándares de seguridad con los que se generan los certificados de las Autoridades Certificadoras intermedias de Acepta.

Si estas 3 verificaciones resultan exitosas, se firma el certificado X.509v3 y es enviado como respuesta al browser del usuario.

Posteriormente dicho certificado es instalado en el dispositivo de almacenamiento de llave privada de Acepta.

4.4 Aceptación de Certificados

La aceptación de los certificados por parte de los firmantes se produce en el momento de la firma del contrato de suscripción asociado a cada Política de Certificación. La aceptación del contrato implica el conocimiento y aceptación por parte del suscriptor de la Política de Certificación asociada.

El contrato de suscripción es un documento que debe ser firmado por el suscriptor, y cuyo fin es vincular a la persona a certificar con la acción de la solicitud, con el conocimiento de las normas de uso y con la veracidad de los datos presentados.

4.5 Uso del par de claves y del certificado

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

4.6 Renovación de certificados.

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

4.7 Renovación de claves

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

4.8 Modificación de certificados.

No aplica.

4.9 Suspensión y Revocación de Certificado

Los certificados de firma electrónica avanzada podrán ser revocados principalmente bajo las siguientes circunstancias:

a) Solicitud del titular del certificado.
b) Fallecimiento del titular.
c) Resolución judicial ejecutoriada.
d) Que el titular haya proporcionado al momento de solicitar el certificado información inexacta o incompleta.
e) Que el titular no custodie adecuadamente los mecanismos de seguridad de funcionamiento del sistema de certificación provistos por Acepta.
f) Si el titular no actualiza los datos proporcionados a Acepta al momento de solicitar el certificado.

Frente a cualquiera de estas circunstancias, un operador de validación de Acepta podrá ingresar a una aplicación especial y firmar electrónicamente la autorización de revocación.

Esta aplicación alimenta la base de datos de Acepta con la que se generan las listas de revocación (CRL) y respuestas a consultas en línea, ya sea a través del sitio web o de OCSP.

Respecto a la suspensión, su efecto será el invalidar un certificado durante el tiempo que permanece suspendido. Pudiendo ser solicitada por el suscriptor del certificado, por Acepta como AC o en caso excepcionales a través de una orden judicial

La solicitud de suspensión será administrada a través de un mail a Acepta, indicando el tipo de certificado y número de serie del certificado que desea suspender. La casilla de e-mail usada para este envío debe coincidir con la casilla del certificado. Acepta confirmará la recepción de este correo e informará al suscriptor cuando la solicitud haya sido procesada. Las solicitudes de suspensión no tendrán costo para el usuario.

Para aquellos casos que se encuentren fuera del horario indicado, la PSC de Acepta, a través de su página web provee un formulario que permite suspender temporalmente el certificado, por un plazo máximo de 72 horas, pasado este periodo el certificado quedará automáticamente vigente a menos que se repita el proceso de suspensión temporal. De confirmarse por parte del usuario esta solicitud, se procederá a suspender el certificado inmediatamente de recibida esta confirmación.

Para un mayor detalle respecto a revocación y/o suspensión de certificados, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

4.9.1 Circunstancias de Revocación

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

4.9.2 Solicitud de Revocación

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

4.9.3 Procedimiento de Revocación

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

4.9.4 Motivos de Suspensión

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

4.9.5 Solicitud de Suspensión

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

4.9.6 Procedimiento de Suspensión

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

4.9.7 Límite de Suspensión

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

4.9.8 Listado de Certificados Revocados

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

4.10 Servicios de comprobación de estado de certificados.

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

4.11 Finalización de la suscripción.

La suscripción finaliza con el término de vigencia de un certificado o la revocación del mismo.

4.12 Depósito y recuperación de claves.

Acepta no genera las claves de sus suscriptores, y por lo tanto no tiene la posibilidad de almacenar ni recuperar sus claves.

Acepta mantiene los certificados emitidos, los cuales contienen sólo la llave pública del titular. Estos certificados pueden ser descargados por la comunidad para los fines que estime conveniente.

5 Controles de Personas, Físicos y de Procedimientos

5.1 General

En este capítulo se describen los controles físicos, de procedimientos y de personal que utiliza la AC en los procesos de identificación, emisión, revocación, auditoría y almacenamiento de sus certificados.

5.2 Data Center

Los sistemas e infraestructura del Servicio de Emisión de Certificados, se encuentra alojado en un Sitio Principal y uno secundario. Las características generales del recinto Principal comprenden una Zonificación en Alta Criticidad (Sitio de Producción) y una Zona de Media Criticidad (recintos de Operaciones y Cintoteca).

- Zona Alta Criticidad: Sitio de Producción:
  - El espacio físico blindado en su perímetro desprotegido de muros estructurales del edificio.
  - Sistema de esclusas mediante puerta corta fuego y blindada opaca y vidriada blindada.
  - Acceso restringido.
  - Sistema de video vigilancia.
  - Piso falso de 30cm de altura con cámara plena para distribución de aire para climatización de todos los equipos de la sala.
  - Acceso por rutas físicas redundantes para fibras ópticas carriers.
  - Equipos de Climatización precisa redundantes en configuración 1+1.
  - Equipos de energía ininterrumpida UPS redundantes en configuración 1+1 . La iluminación de la sala se encuentra respaldada por el sistema UPS y el grupo electrógeno.
  - Sistema autónomo de detección y extinción de incendios en base a gas FM-200.
  - Soporte generación autónoma de energía de emergencia mediante Grupo Electrógeno de operación continua. Todos los equipos están respaldados.

- Zona Criticidad Media: Operaciones:
  - Espacio cerrado de oficinas dotado de puestos de trabajo para personal operación y administración.
  - Acceso restringido mediante tarjeta magnética u botonera con clave.
  - Sistema de Video Vigilancia.
  - Iluminación y puestos de trabajo respaldados por el grupo electrógeno.

- Zona Criticidad Media: Cintoteca:
  - El espacio físico blindado en su perímetro desprotegido de muros estructurales del edificio, alejado del Sitio de Producción.
  - Puerta de acceso corta fuego y de seguridad.
  - Acceso restringido mediante cerradura de seguridad.
  - Sistema autónomo de detección y extinción de incendios en base a gas FM-200.
  - Iluminación respaldada con grupo electrógeno.

Respecto al sitio secundario sus principales características son:

- Acceso restringido y controlado.
- Climatización full redundante calculada de acuerdo a la carga térmica de la sala.
- Alimentación del sistema eléctrico independiente de otros consumos propios del lugar en que se encuentra ubicado el sitio secundario.

- Sistema de respaldados con UPS redundante y grupo electrógeno.
- Sistema de detección temprana de incendio y extinción vía agente limpio FM-200
- Sistema de detección de sobre temperatura para monitorear permanentemente el funcionamiento del sistema de Aire Acondicionado.
- Sistema de detección de intrusos
- Acceso por rutas físicas redundantes para fibras ópticas carriers
- Acceso a través de una puerta cortafuego de características para resistencia al fuego F-60.
- Sistemas de Circuito Cerrado de Televisión.

Los controles definidos en ambos sitios, para proteger los elementos que forman parte de la solución de Acepta, se basan en procedimientos y estándares de seguridad física para las instalaciones informáticas. Estos a su vez se encuentran elaborados según la norma ISO 27001, para la cual ambos sitios se encuentran certificados.

5.2.1 Seguridad Física Data Center
De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.2.2 Sistema de Energía Eléctrica
De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.2.3 Sistema de Control Ambiental
De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.2.4 Sistema de Extinción y Control de Incendios
De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.2.5 Telecomunicaciones
De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.2.6 Seguridad Lógica Data Center
De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.3 Controles de procedimientos
Los sistemas de información y los servicios de Acepta se operan de forma segura, siguiendo procedimientos preestablecidos.

5.3.1 Papeles de confianza
Los roles definidos para el control y gestión del sistema son:

- Administrador de Sistemas
- Administrador de Seguridad
- Operador de Registro
- Operador de Validación
- Responsable de formación, soporte y comunicación
- Responsable de Seguridad
- Auditor

- Responsable de Documentación

Para un mayor detalle remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.4 Controles de seguridad del personal

5.4.1 Requerimientos de antecedentes y experiencia

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.4.2 Comprobación de antecedentes

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.4.3 Requerimientos de formación y reentrenamiento

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.4.4 Frecuencia de rotación de tareas

No aplica.

5.4.5 Sanciones

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.4.6 Requerimientos de contratación

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.4.7 Documentación entregada al personal

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.4.8 Control de cumplimiento

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.4.9 Finalización de contratos

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.5 Procedimientos de auditoría de seguridad

5.5.1 Tipos de eventos registrados

Los tipos de eventos registrados dependen de las políticas señaladas para cada tipo de certificado. En particular para certificados avanzados se registra:

- Intentos exitosos o fracasados de cambiar los parámetros de seguridad del sistema operativo.
  - Inicio y detención de la CA.
  - Intentos exitosos o fracasados de inicio y fin de sesión de administradores.
  - Intentos exitosos o fracasados de crear, modificar o borrar cuentas del sistema.
  - Intentos exitosos o fracasados de crear, modificar o borrar usuarios del sistema autorizados.
  - Intentos exitosos o fracasados de solicitar, generar, firmar, emitir o revocar claves y certificados.
  - Intentos exitosos o fracasados de generar, firmar o emitir una CRL.

- Intentos exitosos o fracasados de crear, modificar o borrar información de los titulares de certificados.
- Intentos exitosos o fracasados de acceso a los sitios principal y secundario por parte de personal autorizado o no.
- Backup, archivo y restauración.
- Cambios en la configuración del sistema.
- Actualizaciones de software y hardware.
- Mantenimiento del sistema.

5.5.2 Frecuencia de procesamiento del log

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.5.3 Periodo de Retención para el log de auditoría

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.5.4 Protección del log de auditoría

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.5.5 Procedimientos de respaldo del log de auditoría

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.5.6 Evaluaciones de vulnerabilidad

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.6 Políticas para archivo de registros

5.6.1 Documentos archivados

Con el fin de mantener un adecuado respaldo de la información involucrada en el proceso de certificación, así como para brindar seguridad y garantía a todas las partes involucradas, se almacenaran en un medio seguro una serie de documentos relevantes al proceso de certificación. Ellos son:

- Los registros de auditoría especificados en el punto 5.5 de esta Declaración de Prácticas de Certificación.
- Los soportes de backup de los servidores que componen la infraestructura de la AC de Acepta.
- Documentación relativa al ciclo de vida de los certificados
- Acuerdos de confidencialidad
- Contratos suscritos por la Acepta en su función de CA
- Autorizaciones de acceso a los Sistemas de Información

5.6.2 Requerimientos para “marca de tiempo” de registros

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.6.3 Sistema de colección de archivos

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.6.4 Procedimientos para obtener y verificar información de archivos

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.7. Compromiso de clave de una entidad

En el caso de compromiso de la clave de una entidad perteneciente a la PSC de Acepta, se procederá a su revocación inmediata y se informará del hecho al resto de entidades dependientes

Para un mayor detalle remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.8 Recuperación en caso de compromiso de una clave o de desastre

5.8.1 Alteración de los recursos hardware, software y/o datos

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.8.2 La clave pública de una entidad se revoca

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.8.3 La clave de una entidad se compromete

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.8.4 Instalación de seguridad después de un desastre natural u otro tipo de desastre

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

5.9 Cese de la actividad del PSC

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

6 Controles de Seguridad Técnica

6.1 General

En este punto Acepta describe las medidas de seguridad que ha tomado para proteger tanto las llaves generadas, como los datos de activación de dichas llaves (Clave creada por el usuario al momento de la solicitud), a fin de que dicha información sea sólo accesible a las personas autorizadas. También se describe los aspectos técnicos relacionados con la generación de llaves, la identificación de los usuarios, el registro de certificados, su revocación, auditoria y almacenamiento.

6.2 Instalación y Generación de Pares de Llaves

6.2.1 Generación del par de claves

Los pares de claves para todos los componentes internos de Acepta, se generan en módulos de hardware criptográficos con certificación FIPS 140-2 Nivel 3.

- **Certificados Propios de la PSC:** Los pares de claves para todos los componentes internos de Acepta, se generan en módulos de hardware criptográficos con certificación FIPS 140-2 Nivel 3.
    - AC raíz: La máquina donde reside la AC raíz dispone de un dispositivo criptográfico (HSM) para la generación de claves de la AC raíz.
    - AC intermedias: La máquina donde residen las AC intermedias dispone de un dispositivo criptográfico (HSM) para la generación de claves de las distintas AC intermedias.
- **Certificados subscriptores**: Las claves de los certificados de subscriptores pueden ser generadas empleando:
    - Dispositivo de software criptográfico en posesión del suscriptor.
    - Dispositivo criptográfico (HSM) en Acepta con control exclusivo del suscriptor

6.2.2 Entrega de la clave privada a la entidad

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

6.2.3 Entrega de la clave pública al emisor del certificado

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

6.2.4 Entrega de la clave pública de la AC a los usuarios

Las claves públicas de todas las AC pertenecientes a la jerarquía de confianza de Acepta se pueden descargar del sitio web http://www.acepta.com.

Adicionalmente, en el caso de certificados de firma electrónica avanzada, se puede descargar desde el sitio web de la entidad acreditadora de Chile en www.entidadacreditadora.gob.cl, donde se encuentran los certificados intermedios de todos los Prestadores de Servicios de Certificación Acreditados.

6.2.5 Tamaño de las claves

Las claves de la AC raíz y las autoridades de certificación que se encuentran en la misma jerarquía son claves RSA de 2048 bits de longitud.

El tamaño de las claves para cada tipo de certificado emitido por la CA, se establece en la Política de Certificación que le es de aplicación. En todo caso, su tamaño nunca será inferior a 2048 bits para los certificados emitidos con la nueva versión de la AC. Todos aquellos certificados que fueron emitidos con

un largo de clave de 1024 bits, continuarán en operación durante su periodo de vigencia o hasta su revocación.

6.2.6 Parámetros de generación de la clave pública

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

6.2.7 Comprobación de la calidad de los parámetros

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

6.2.8 Hardware/software de generación de claves

Las claves son generadas, según el caso, de la siguiente forma:

- CA: En el propio dispositivo HSM.
- Entidad final (suscriptor): En los propios dispositivos o sistemas que las soportan.

6.2.9 Fines del uso de la clave

Todos los certificados emitidos por Acepta contienen la extensión KEY USAGE definidas por el estándar X.509 v3 para la definición y limitación de fines.

Las claves definidas por la presente política se utilizarán para usos descritos en el punto de este documento, 1.4.1 Tipos y usos de los certificado.

6.3 Protección de la llave privada

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

6.4 Otros aspectos de gestión del par de claves

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

6.5 Datos de activación

Los datos de activación de las Autoridades de Certificación de Acepta, se generan y almacenan en smart cards criptográficas en posesión de personal autorizado. Sólo este personal conoce las contraseñas para tener acceso a datos de activación.

En relación al dato de activación (PIN) de firma, se requiere a los operadores autorizados de los certificados, memoricen estos y además mantengan su confidencialidad.

6.6 Controles de seguridad informática

Actualmente, Acepta cuenta con un plan de seguridad de la información, el cual contempla distintos controles de seguridad, desde un plan de recuperación de desastres hasta los respectivos controles de acceso. Mayor detalle de estos controles son parte del Plan de Seguridad de Acepta.

6.7 Controles de Seguridad Técnica

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

6.8 Controles de seguridad de red

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

6.9 Controles de seguridad de los módulos criptográficos

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de Acepta.

7 Administración de las CP

Este capítulo establece los procedimientos aplicables respecto a las modificaciones del presente documento.

7.1 Procedimientos para Modificar las CP

Las políticas de certificación contenidas en este documento, son administradas y mantenidas rigurosamente por personal especializado y en posiciones de confianza en la compañía.

7.2 Publicación y notificación

Cualquier cambio en el contenido de estas políticas será comunicado al público y usuarios mediante su publicación en el sitio Web de Acepta en www.acepta.com.

7.3 Procedimientos de aprobación de las CP

Estas CP y las subsecuentes versiones futuras de éste documento están sujetas a la aprobación del Comité de seguridad de Acepta.

8 REVISIÓN Y APROBACIÓN DEL DOCUMENTO

8.1 Revisión

Este documento es revisado anualmente a fin de verificar su validez y eficacia, o en un plazo menor en caso de producirse cambios significativos que ameriten su revisión de acuerdo al marco regulatorio, comercial, legal o técnico.

8.2 Control de cambio

Cada vez que se requiera efectuar una modificación a estas CP, esta debe ser incorporada al documento y reflejada en un historial de cambios. Para ello, se debe ingresar una nueva entrada en el historial de cambios de la portada de este documento conforme se detalla a continuación:

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha

Con esto se logrará mantener una traza respecto a las actualizaciones que ha sufrido este documento. La nueva versión del documento será almacenada en el sistema documental de Acepta, con su respectivo control de versión, posterior a su aprobación.

Además, en caso de existir cambio en la referencia a documentación externa se debe modificar el siguiente cuadro, incorporando este cambio:

REFERENCIAS

Documentos Internos	
Título	**Nombre del archivo**
Documentos Externos	

8.3 Aprobación

Este documento así como sus modificaciones deben ser aprobados por el dueño del documento y en comité de seguridad, a fin de que sea incorporado como la nueva versión vigente al sistema de gestión documental y para posteriormente proceder a su difusión con los empleados y partes externas pertinentes.