firmaschile

POLÍTICA DE CERTIFICACIÓN

FIRMA ELECTRÓNICA

CP (Certification Policy)

14-Octubre-2022
Versión 1.0

Tabla de Contenido

1. Definiciones y Acrónimos

1.1 Definiciones

Para efectos del documento de Políticas de Certificación, las expresiones que se indican a continuación tienen el alcance y/o significado que se expresa en cada caso:

- **Prestador de Servicios de Certificación:** Es aquella entidad que en conformidad con la legislación vigente emite certificados de firma electrónica.
- **Autoridad de Registro:** Es firmaschile personalmente o representada a través de un mandatario o a través de medios informáticos automatizados, para la comprobación de la identidad de los solicitantes de certificados.
- **Autoridad Acreditadora:** Es la entidad que asegura que los Prestadores de Servicios de Certificación operan de acuerdo con la normativa vigente aplicable y los acreditan e incluyen en un listado público de PSC acreditadas
- **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 emudhra y pertenece a la jerarquía que emudhra 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.
- **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 firmaschile, respecto a aquellas prácticas, a nivel de sistemas y de personal, que dan seguridad y confianza a los certificados y servicios provistos por firmaschile.
- **emudhra:** firmaschile es la representante en Chile de la PSC emudhra
- **Entidad Acreditadora:** Es la entidad que asegura que los Prestadores de Servicios de Certificación operan de acuerdo con la normativa vigente aplicable y los acreditan e incluyen en un listado público de PSC acreditadas
- **Firma electrónica:** 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 (esto último en caso de firmas digitales o avanzadas)
- **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 firmaschile.
- **Online Certificate Status Protocol:** Protocolo informático que permite la comprobación del estado de un certificado en el momento en que éste es utilizado.
- **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 firmaschile 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 losdocumentos 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. 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 losdocumentos durante el proceso de Firma electrónica.
- **Solicitante:** Persona que solicita la emisión de un certificado de firma electrónica, dando cumplimiento a las exigencias establecidas en la Ley y en la Declaración de Prácticasde 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 firmaschile.
- **Terceras partes que confían:** Aquellas personas que voluntariamente depositan su confianza enun certificado de firmaschile, 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.

1.2 Acrónimos

- AA: Autoridad Acreditadora
- AC: Autoridad Certificadora
- ACR: Autoridad Certificadora Raíz
- AFIS: Automated Fingerprint Identification System
- AR: Autoridad de Registro
- CA: Certification Authority
- CP: Certificate Policy
- CP: Políticas de Certificado de Firma Electrónica
- CPS: Certification Practice Statement
- CRL: Certificate Revocation List
- EA: Entidad Acreditadora
- EC: Entidad de Certificación
- ER: Autoridad de Registro
- 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
- 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. Introducción

Este documento presenta la Política de Certificación (CP, por su sigla en inglés Certification Policy) de firmaschile para los certificados de firma electrónica. Esta es una descripción de los procedimientos que firmaschile 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 en la comprobación de la identidad de los solicitantes de certificados de firma electrónica, Autoridad de Registro (AR / RA).

La Política de Certificación referida en este documento se utilizará para la emisión de certificados de firma electrónica, generados por firmaschile. Mediante los certificados emitidos por firmaschile se generarán firmas electrónicas reconocidas por las terceras partes.

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

3. Sobre las Políticas de Certificación

Las políticas de certificación aquí descritas establecen el ciclo de vida de los servicios que provee firmaschile, 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 firmaschile.

3.1 Alcance

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

3.2 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.

3.3 Visión general del sistema

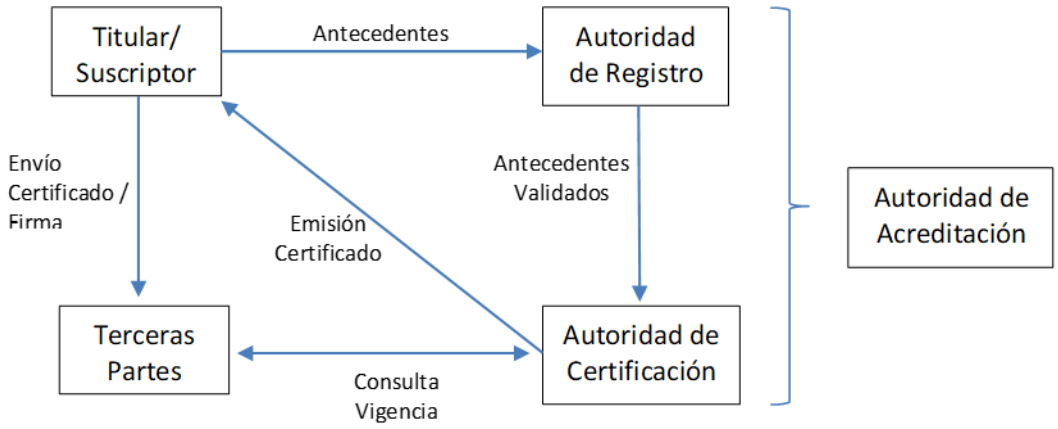
Los servicios de certificados de firma electrónica, o clave pública de firmaschile, están insertos en una infraestructura en que se relacionan distintas entidades.

3.3.1 Comunidad y Aplicabilidad

Los servicios de certificados de firma electrónica operan en una infraestructura que relaciona cinco entidades, como se muestra a continuación:

- Entidad Certificadora (EC) o Prestador de Servicios de Certificación (PSC) o Certification Authority (CA),
- Autoridad de Registro (AR) o Register Authority (RA),
- Titulares,
- Terceras partes que confían en los certificados y
- Autoridad de Acreditación (AA) o Entidad Acreditadora (EA)

La siguiente figura muestra dicha relación:



En la figura la Autoridad de Registro es firmaschile y la Autoridad de Certificación es EMUDHRA. firmaschile es la representante en Chile de la empresa EMUDHRA.

Las prácticas y políticas de la AR de firmaschile son publicadas en la página web de la empresa www.firmaschile.cl. Cabe destacar que la AR de firmaschile tiene un convenio establecido con la CA de la empresa EMUDHRA. Las políticas y prácticasde esta última empresa también se publican en la página web de firmaschile para su consulta.

3.3.2 Comunidad de usuarios

- **Solicitante:** Son las personas que concurren a firmaschile a solicitar un certificado de firma electrónica, completan el formulario de solicitud y proveen todos los antecedentes que exige la ley, la CPS y la CP para comprobar 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. Los suscriptores son personas naturales.

- **Autoridad de registro**: La recepción y procesamiento de las solicitudes de certificados es realizada por la Autoridad de Registro (ER / RA) de firmaschile, sea que lo haga directamente o a través de un mandatario especialmente designado para tal objeto. La Autoridad de Registro debe realizar la comprobación de la identidad de los solicitantes de certificados de firma electrónica.

- **Prestador de Servicios de Certificación (PSC)**: Es la entidad prestadora de los servicios de certificación de firma electrónica, 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, que en este caso es firmaschile.

- **Tercera parte que confía**: Es el receptor de un certificado de firma electrónica. Normalmente, junto con el certificado este tercero recibe un documento electrónico que se encuentra suscrito con la firma electrónica 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:** El Servicio de Impuestos Internos en su Resolución Exenta N° 09 del 15 de febrero de 2001 establece normas que regulan el uso de la firma electrónica simple para el ámbito tributario, actuando como Entidad Acreditadora para estos fines e inscribiendo a las PSC en su lista de entidades acreditadas para efectos tributarios.

Los usuarios que utilicen los certificados emitidos por firmaschile, antes de solicitar dichos certificados, deben conocer y manifestar su conformidad con lo establecido en la CPS de firmaschile y en la CP correspondiente al tipo de certificado.

3.3.3 Aplicabilidad de los certificados

Los Certificados emitidos por firmaschile se utilizarán únicamente conforme a la función y finalidad que tengan establecidos en la presente Política de Certificación (CP) y en la Declaración de Políticas de Certificación (CPS).

La aplicabilidad de los certificados de Firma Electrónica es la siguiente:

Firma digital, No repudio, Uso Tributario

3.3.4 Tipos y usos de los certificados

firmaschile emite certificados de firma electrónica, definiendo 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 certificados de firma electrónica de persona natural son emitidos por firmaschile para soportar las siguientes necesidades de seguridad:

1. **Autentificación:** proporciona suficientes garantías respecto a la identidad del suscriptor del certificado, al haberse validado que la cédula de identidad, su vigencia,

su no bloqueo y que el suscriptor es una persona viva a través de una entidad o bureau especialista y que posee información tanto pública como del Servicio de Registro Civil e Identificación, para proveer un servicio confiable y seguro de verificación de identidad e imponer que el almacenamiento de la llave privada sea en un medio válido que soporte una firma electrónica.

2. **Integridad de mensajes:** los mensajes firmados con certificado de firma electrónica permiten validar si el contenido de mensaje ha sido alterado en el tiempo transcurrido desde su generación.

3. **Firmas electrónicas:** las firmas electrónicas producidas con certificados de firma electrónica ofrecen los medios de respaldo para demostrar fehacientemente, incluso ante Tribunales, la autenticidad de un mensaje o documento electrónico.

3.3.5 Limitaciones de Usos y Prohibiciones

Los Certificados de firma electrónica emitidos por firmaschile se utilizarán únicamente conformea los usos y finalidades que tengan establecida en este documento y en las correspondientes Prácticas de Certificación, y de acuerdo con la normativa chilena vigente y a los convenios internacionales ratificados por Chile. 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 firmaschile, los que solo serán válidos en la forma suministrada por firmaschile.

4. Contenido de los Certificados

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de firmaschile.

5. Requerimientos Generales

5.1 Obligaciones

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

5.2 Obligaciones de la AC Raíz (ACR)

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

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de

Certificación (CPS) de EMUHDRA.

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

Cada AR y AC deberá cumplir las normas y ser consistente con lo establecido en el documento Declaración de Prácticas de Certificación.

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

5.4 Obligaciones del Solicitante

Los solicitantes de certificados a firmaschile, 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 firmaschile.

5.5 Obligaciones del Suscriptor de la llave

Los suscriptores de certificados a firmaschile, 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 firmaschile.

5.6 Obligaciones los Usuarios

Los usuarios de certificados emitidos por firmaschile, 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 firmaschile.

5.7 Confianza en las Firmas y Certificados

Las partes que consideren confiar en las firmas y certificados emitidos por firmaschile 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 firmaschile.

5.8 Obligaciones de los Repositorios

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de firmaschile.

6. Responsabilidad del PSC

firmaschile solo será responsable de los daños y perjuicios que en el ejercicio de la actividad de certificaciónde firma electrónica ocasione y, en ningún caso será responsable del uso incorrecto, indebido ofraudulento de los certificados de firma electrónica emitidos, ni de cualquier daño indirecto o imprevisto que resulte de su uso.
Se deja expresa constancia que, atendida la complejidad de los sistemas informáticos y el riesgo tecnológico que los mismos conllevan, no es posible garantizar que los sistemas operen libres de errores o inconsistencias, no obstante, el cuidado y la diligencia empleada por firmaschile. Por lo anterior, no otorga garantía alguna en relación con el posible compromiso en el futuro del sistema de claves asimétricas o cualquier otro riesgo no predecible de naturaleza similar. En todo caso, a fin propender a mitigar esta clase de riegos, firmaschile aplicará los procedimientos previstos en sus planes de contingencia.

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.

La responsabilidad de firmaschile cualquiera sea la naturaleza de la acción o reclamo y salvo que medie dolo o culpa grave atribuible a ésta, quedará limitada como máximo al monto pagado por el certificado.

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

6.1 Responsabilidad Pecuniaria

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de firmaschile.

6.2 Fuerza Mayor

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de firmaschile.

6.3 Responsabilidad de la AC y AR

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de firmaschile.

6.4 Ley Aplicable y Resolución de Conflictos

firmaschile declara efectuar sus actividades en conformidad con los principios generales de la legislación chilena y dando cumplimiento a todas y cada una de las leyes aplicables a las actividades desarrolladas por firmaschile.

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

7. Publicación y Repositorios

firmaschile publica en su sitio web en www.firmaschile.cl, las prácticas de certificación por ella utilizadas, así como las políticas de certificado (CP) pertinentes a cada tipo de certificado emitido.

La información respecto al estado de vigencia y validez de los certificados emitidos por firmaschile, se encuentra disponible en el sitio web de firmaschile www.firmaschile.cl..

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

7.1 Privacidad y Protección de los Datos Personales

Las Políticas de Privacidad de firmaschile se encuentran publicadas en el sitio web de firmaschile www.firmaschile.cl.

8.1.1 Tipos de Información a Proteger

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de firmaschile.

8.1.2 Tipos de Información que puede ser entregada

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de firmaschile.

8.1.3 Información del Certificado

Los certificados de firma electrónica emitidos por firmaschile están en conformidad con el formato X.509 v3 definido en ITU-T X.509 v3.

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

8.1.4 Entrega de Información sobre la Revocación del Certificado

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de firmaschile.

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

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de firmaschile.

8.1.6 Entrega de Información a Petición del Titular

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de firmaschile.

8.1.7 Entidades de certificación afiliadas a la AC

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de firmaschile.

9. Identificación y Autenticación

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

9.1 Registro

9.1.1 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.

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

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

9.1.2 Registro Inicial

El solicitante deberá completar el formulario de solicitud del Certificado que está a su disposición en la dirección de Internet www.firmaschile.cl, indicar la vigencia del certificado, los datos del solicitante, además deberá aceptar las condiciones e ingresar los datos para la facturación.

Con el envío del formulario, el Solicitante proporciona a firmaschile toda la información y documentación que requerida para registrarlo como Suscriptor e incluirla en el Certificado, de acuerdo con los requisitos establecidos en esta CP.

Si los datos son correctos el solicitante podrá continuar con el proceso, en caso contrario se le indicará los pasos a seguir.

Con la aceptación de la solicitud que se despliega en pantalla el solicitante deberá realizar el pago correspondiente al tipo de Certificado, mediante el botón de pago que se despliega en la misma pantalla.

El envío de los datos solicitados en este formulario y el abono de las tasas de registro supondrá su consentimiento para ser registrado como suscriptor de un certificado de firmaschile. La solicitud de este certificado no implicará en ningún caso su obtención si no se llegan a cumplir por parte del solicitante los requisitos establecidos en la CPS y en las CP de Certificados Firma Electrónica Simple.

La solicitud de un certificado de firma electrónica para fines tributarios es un acto personal y en tal sentido se reconoce que la usurpación de nombre es un delito que se sanciona penalmente por ejercicio ilegal de nombre y/o por estafa y otros engaños. Asimismo, declara que acepta las políticas de certificación de firmaschile y de uso de estos certificados por el Servicio de Impuestos Internos.

9.1.3 Autenticación de la Identidad del Suscriptor

Para acreditar las circunstancias que garantizará el Certificado en la fase definitiva se requerirá la presentación de la siguiente información

- Número de la cédula de identidad chilena vigente del suscriptor
- Número de serie o de documento de la cédula de identidad

9.1.4 Aceptación y Rechazo de la Solicitud

Una vez recibida la solicitud y la información, la AR debe proceder al proceso de verificación de la información proporcionada, previo la aceptación de ésta.

En concreto, la AR confirmará:

a) La información entregada por el solicitante y que figurará en el Certificado.
b) Que se haya entregado la documentación requerida y que ésta se ajuste a lo solicitado.
c) La comprobación de la cédula a través de la serie, vigencia, bloqueo, y eventualmente otras preguntas personales, se realiza mediante consulta a un bureau de información.
d) Cualquier otra información que se incluye en el Certificado, a no ser que en éste se indique expresamente la ausencia de la verificación correspondiente.

9.1.5 Aceptación de la Solicitud

De no haber circunstancias que de alguna manera afecten a la seguridad del servicio de certificación y siempre que la identidad del solicitante sea válida, la AR procederá a la aprobación de la solicitud.

9.1.6 Rechazo de la Solicitud

Si la AR decidiese rechazar la solicitud del Certificado, comunicará a través de la página web la decisión, con la indicación de los motivos que lo provocaron y procederá a la devolución del importe pagado.

En caso de que los defectos encontrados sean subsanables, el solicitante tendrá la posibilidad de solicitar nuevamente el certificado, iniciando un nuevo ciclo de solicitud y subsanando los defectos causantes del rechazo.

9.1.7 Emisión de Certificados

Realizada la validación de pago y datos personales entregados, se le informa al Solicitante por e-mail el ID y Password necesarios para generar y descargar el certificado en un computador vía web.

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

9.1.8 Reemisión de la Llave

No aplica

9.1.9 Reemisión de la Llave luego de una Revocación

No aplica

9.1 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 firmaschile 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 de que el certificado esté emitido para un cargo de dicha empresa).
- Por oficio de firmaschile ante sospecha fundada de compromiso en la clave privada de un suscriptor.
- Presencial con una identificación similar a la primera solicitud de certificado.
- Por medio electrónico, en que el titular debe enviar a firmaschile un e-mail firmado con firma electrónica, siendo la casilla de destino revocaciones@firmaschile.cl.

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

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

9.2 Reemisión de certificados

Las solicitudes de reemisión no aplican ya que una renovación de certificado significa la emisión de un nuevo certificado, siguiendo los mismos requerimientos de la primera emisión.

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

10. Derechos de Propiedad Intelectual e Industrial

De acuerdo con lo especificado en la Declaración de Prácticas de Certificación (CPS) de firmaschile.

11. Detalle de los contactos y administración de la CA

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

- **Nombre**: firmaschile
- **Dirección de e-mail**: contacto@firmaschile.cl
- **Número telefónico**: +562 2306 6170