ACEPTA

Empresas
a velocidad
digital

PO02

Declaración de Prácticas de Certificación

Firma Móvil

Enero 2017

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 Prácticas de Certificación Firma Móvil-PO02	1.0	Primera versión	13-01-2017
Declaración de Prácticas de Certificación Firma Móvil-PO02	5.0	Revisión anual	01-10-2017
Declaración de Prácticas de Certificación Firma Móvil-PO02	5.1	Posibilidad de realizar la operación de registro y Validación en base a Clave única del SRCeI	07-11-2017
Declaración de Prácticas de Certificación Firma Móvil-PO02	5.2	Ajustes Jurisprudencia	02-04-2018
Declaración de Prácticas de Certificación Firma Móvil-PO02	6.0	Revisión anual	01-10-2018
Declaración de Prácticas de Certificación Firma Móvil-PO02	7.0	Revisión anual	01-10-2019
Declaración de Prácticas de Certificación Firma Móvil-PO02	8.0	Revisión anual	01-10-2020

Declaración de Prácticas de Certificación Firma Móvil-PO02	9.0	Revisión anual	15-03-2022
Declaración de Prácticas de Certificación Firma Móvil-PO02	9.1	IAO2022, se incorpora: • Punto 2.1 Obligaciones: Subpunto 10, proceso de devoluciones y reembolsos. • Punto 2.1 Obligaciones: Subpunto 11, proceso soporte y asistencia. • Punto 2.1.2 Obligaciones de la Autoridad de Registro (AR) y la Autoridad Certificadora (AC): Se incorpora la no existencia de canales de distribución, SOVOS como adquiriente de ACEPTA y Aplicativos Identidad Digital y DEC5 como parte del porfolio de productos. • Punto 4 Requisitos Operacionales: Se corrige URL mencionada en "Sistema de directorios para los certificados de firma Electrónica"	12-10-2022
Declaración de Prácticas de Certificación Firma Móvil-PO02	10.0	Revisión anual	15-03-2023
Declaración de Prácticas de Certificación Firma Móvil-PO02	10.1	Ajuste puntos 1.4.3 y 1.5	03-07-2023
Declaración de Prácticas de Certificación Firma Móvil-PO02	11.0	Revisión anual	30-04-2024

CLASIFICACIÓN DEL DOCUMENTO

NIVEL DE CRITICIDAD: Baja **NIVEL DE CONFIDENCIALIDAD: Pública**
NOTA DE CONFIDENCIALIDAD: Información de Libre Acceso al Público. 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) • Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Reconstrucción • 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

En el siguiente documento se presenta la Declaración de "Prácticas de Certificación" (CPS, por su sigla en inglés Certification Practice Statement) de Acepta para los certificados de firma electrónica móvil. Estas son una descripción detallada de los procedimientos o prácticas que Acepta declara convenir en la prestación de sus servicios de certificación, cuando emite y gestiona certificados de firma electrónica móvil 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 móvil (Autoridad de Registro).

Es así como la presente Declaración de Prácticas de Certificación (CPS) detalla las normas y condiciones de los servicios de certificación de firma electrónica móvil que presta Acepta y que están relacionadas con la gestión del ciclo de vida de los certificados de firma electrónica, en particular lo relativo a la información utilizada en la emisión, la verificación de los certificados electrónicos y de su firma, las condiciones asociadas a la solicitud, emisión, uso, suspensión y la revocación de dichos certificados. También se describen las medidas de seguridad técnica y organizativa, los perfiles y los mecanismos de información que permiten verificar y administrar la vigencia de los certificados, así como la forma en que se asegura que el proceso de certificación es llevado a cabo en un ambiente seguro capaz de brindar total confianza a la comunidad que interactúa en torno a la firma electrónica móvil

1.1.1 Sobre las Prácticas de Certificación

Las prácticas de certificación aquí descritas establecen y configuran el ciclo de vida de los certificados de firma electrónica móvil que comercializa Acepta. Es decir, se trata de una declaración unilateral que hace Acepta por medio de la cual se obliga a desarrollar la actividad de certificación de firma electrónica móvil en la forma aquí declarada.

1.1.2 Alcance

El alcance de esta Declaración de Prácticas de Certificación (CPS) detalla las normas y condiciones de los servicios de certificación que presta Acepta para la emisión de sus certificados de firma electrónica móvil.

1.1.3 Referencias

La presente Declaración de Prácticas 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 de “Prácticas de Certificación de Acepta”, también acá referidas como “CPS”, está registrado con el número único internacional (OID) 1.3.6.1.4.1.6891.401.

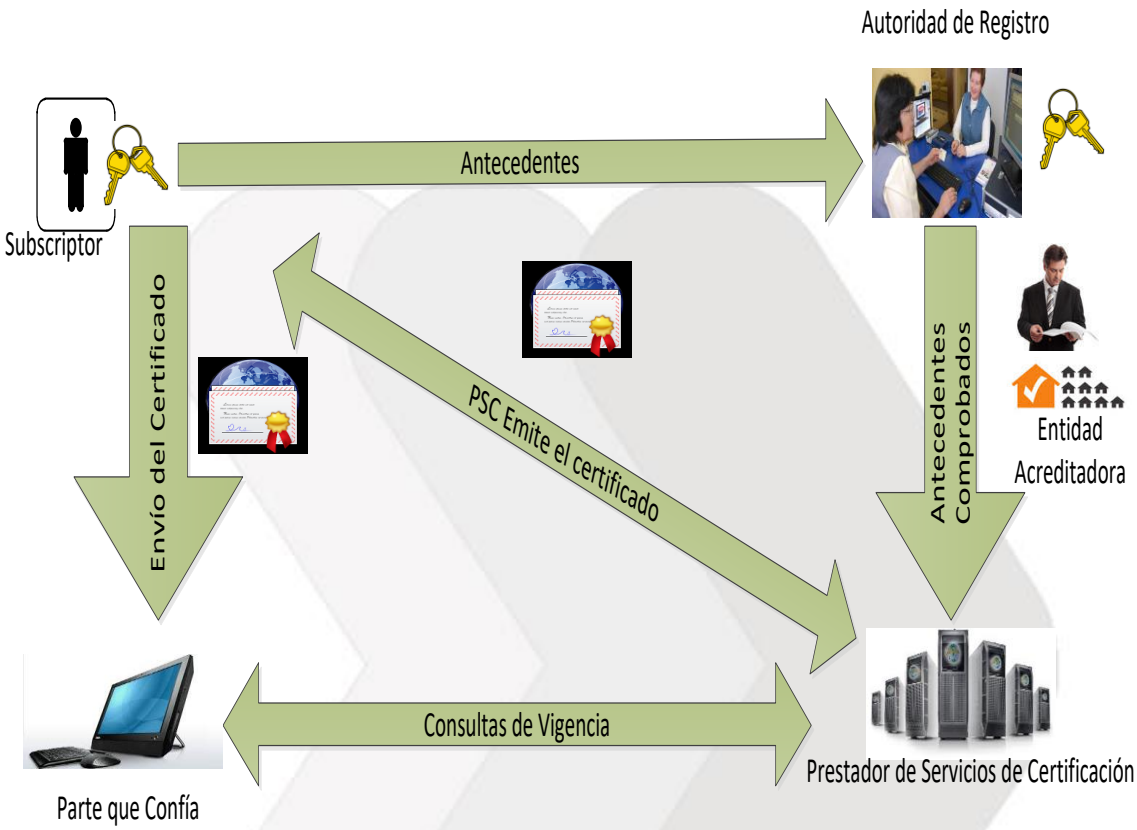
Acepta tiene asignado el identificador (OID) 1.3.6.1.4.1.6891, el cual está registrado en la Internet Assigned Number Authority (IANA). Este número identifica únicamente a Acepta en un contexto global.

Las políticas de las CPS y de cada tipo de certificado están registradas con un número único internacional, llamado Object Identifier (OID). La siguiente tabla resume todos los OID administrados por Acepta:

Descripción	OID
Prácticas de Certificación	1.3.6.1.4.1.6891.1
Políticas de certificados Clase 3	1.3.6.1.4.1.6891.2
Políticas de certificados de Firma Electrónica Avanzada	1.3.6.1.4.1.6891.3
Políticas de certificados de Sitio Web	1.3.6.1.4.1.6891.4
Extensión para indicar declaraciones del titular de un certificado X.509	1.3.6.1.4.1.6891.9
Extensión para certificados X.509 en la que se incluye el XML de un CAF.	1.3.6.1.4.1.6891.50.1
Identificador permanente administrado por Acepta para nombrar Servidores.	1.3.6.1.4.1.6891.100.1
Identificador permanente administrado por Acepta para nombrar Servicios.	1.3.6.1.4.1.6891.100.2
Políticas de certificados de Firma Electrónica Móvil	1.3.6.1.4.1.6891.400
Prácticas de certificados de Firma Electrónica Móvil	1.3.6.1.4.1.6891.401

1.3 Comunidad y Aplicabilidad

Los servicios de certificados de firma electrónica móvil de Acepta están insertos en una infraestructura en que se relacionan distintos sujetos. Básicamente: 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 móvil, 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 móvil. 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 móvil. 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 móvil, 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 Acepta.
- **Tercera parte que confía**: Es el receptor de un certificado de firma electrónica móvil. Normalmente, junto con el certificado este tercero recibe un documento electrónico que se encuentra suscrito con la firma electrónica móvil 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 móvil, permitiendo su inscripción en el registro de certificadores acreditados.

1.4. Aplicabilidad de los certificados

Los certificados de firma electrónica móvil emitidos por Acepta podrán ser utilizados por los suscriptores de conformidad con lo dispuesto en esta Declaración de Prácticas de Certificación y dando especial respeto a cualquier límite funcional que se incorpore en ellos, de conformidad con lo dispuesto en la Ley 19.799 y su reglamento.

1.4.1 Tipos y usos de los certificados

Acepta emite distintos tipos de certificados, definiendo para 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 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.

A continuación se muestra un resumen de los tipos de certificados emitidos por Acepta:

Tipo	Características generales	Usos típicos
Clase 3 Persona Natural	• Registro presencial. • Certificado para persona natural. • El medio de almacenamiento de la llave privada es elegido por el suscriptor del certificado. • Estas políticas de certificado han sido acreditadas por el SII y por Aduanas.	• e-mail firmado • e-mail cifrado • Autenticación del suscriptor en sitios Web, como el del SII. • Factura electrónica. • Operaciones aduaneras. • Otros en que las partes elijan libremente confiar en estos certificados.
FA Firma Electrónica Avanzada o Móvil	• Registro presencial. • Certificado para persona natural. • El medio de almacenamiento de la llave privada debe ser un dispositivo especializado que cumpla con la norma FIPS-140-2 nivel 2 o superior. • Estas políticas de certificado y la forma de cumplirlas han sido acreditadas por la Subsecretaría de Economía, Fomento y Reconstrucción.	• Todos los usos de los certificados Clase 3. • Firma electrónica de instrumentos públicos. • Firma electrónica de documentos privados con el mismo valor probatorio de un instrumento público.
Sitio Web	• Verificación de la propiedad de un dominio. • Certificado para un dominio.	• Sitios Web con conexión segura a través de SSL o HTTPS.

Tabla 1: Tipos de certificados

1.4.2 Limitaciones de Uso y Prohibiciones

Los Certificados de firma electrónica móvil emitidos por Acepta se utilizarán únicamente conforme a los usos y finalidades que tengan establecida en este documento y en las correspondientes Políticas de Certificación, y de acuerdo a la normativa chilena vigente y a los convenios internacionales ratificados por el Estado Chileno. 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

Este capítulo contiene especificaciones detalladas de los formatos y contenido de los certificados emitidos bajo la arquitectura señalada por estas CPS (campos, básicos y extensiones).

Composición del certificado raíz de Acepta

Campo	Descripción	Ejemplo
Versión	Versión del certificado, que deberá ser versión 3	V3
Nº de Serie	Número que identifica unívocamente al certificado dentro de los emitidos por Acepta	**00**
Algoritmo de Firma	Algoritmo utilizado por el PSC para firmar el certificado	SHA256 With RSAEncryption
Nombre del Emisor	Nombre distintivo (DN) del emisor, en el formato del estándar X.500. Deben incluirse los siguientes tipos: CN =Tipo de certificado E = e-mail del Prestador de Servicios de Certificación emisora Número de serie = Número identificador del Emisor C = País	C = CL Número de serie = 96919050-8 E = info@acepta.com CN = Acepta.com Autoridad Certificadora Raiz–G4
Periodo de Validez	Fecha de inicio y termino en que es válido el certificado. Para PSC = 10 años, para suscriptores = 1 año, para servidores = 2 años. Codificado en formato YYMMDDHHMMSSZ	Fecha inicio = 040201000000Z Fecha termino = 130201000000Z
Nombre del suscriptor	Nombre distintivo (DN) del suscriptor del certificado, en el formato del estándar X.500. Deben incluirse los siguientes tipos: CN = Nombre distintivo del suscriptor T = Profesión E = dirección de correo del suscriptor C = País	C = CL Número de serie = 96919050-8 E = info@acepta.com CN = Acepta.com Autoridad Certificadora Raiz–G4
Clave pública	Clave pública del suscriptor del certificado	3081 8702 8181 00B2 59D2 D6E6 27A7 68C9 4BE3 6164 C2D9 FC79 D97A AB92 5314 0E5B F177 5119 7731 D6F7 540D 2509 E7B9 FFEE 0A70 A6E2 6D56 E92D 2EDD 7F85 ABA8 5600 B690 89F3 5F6B DBF3 C298 E058 4253 5D9F 064E 6B03 91CB 7D30 6E0A 2D20 C4DF B4E7 B49A 9640 BDEA 26C1 0AD6 9C3F 0500 7CE2 513C EE44 CFE0 1998 E62B 6C36 37D3 FC03 9107 9B26 EE36 D502 0111

Tabla 2: Composición del certificado Raíz de Acepta

Tipo	Nombre	Descripción	OID	Valor
RES	KeyUsage	Esta extensión define el propósito para el cual deben ser usadas las claves correspondientes al certificado. El certificado debe ser utilizado sólo para los propósitos definidos por esta extensión.	2.5.29.15	Firma de certificados, Firma CRL sin conexión, Firma CRL(06)
RES	BasicConstrains	Permite diferenciar entre un certificado de PSC y uno de suscriptor final.	2.5.29.19	Tipo de asunto=CA Restricción de longitud de ruta=Ninguno
RES	AuthorityKeyIdentifier	Medio para identificar la llave pública de Acepta El campo KeyId es idéntico al valor de la extensión SubjectKeyIdentifier		Id. de clave = 85 f9 cd e2 9f b2 57 fc 58 b3 d2 e6 a2 3e a7 2b 56 42 3d e1
RES	SubjectKeyIdentifier	Identificador único de la llave pública del PSC, conteniendo el hash de 160bit de la llave pública		85 f9 cd e2 9f b2 57 fc 58 b3 d2 e6 a2 3e a7 2b 56 42 3d e1
RES	CertificatePolicy	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Ver sección 4.2.1.4		[1]Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.6891.1002.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: https://acg4.acepta.com/CPS-Aceptacom [1,2]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario Calificador: Referencia de aviso:Organización=Acepta.com S.A. Número de aviso=1 Texto de aviso=La utilización de este certificado está sujeta a las políticas de certificado (CP) y prácticas de certificación (CPS) establecidas por Acepta, y disponibles en www.acepta.com.
INF	IssuerAltName	Identificador alternativo del emisor, corresponde al RUT de Acepta, en formato análogo a SubjectAltName		Otro nombre: 1.3.6.1.4.1.8321.2=04 0c 39 36 2e 39 31 39 2e 30 35 30 2d 38
INF	SubjectAltName	Permite definir términos que identifican al suscriptor del certificado, adicionalmente a lo establecido en el campo estándar Subject. Se podrán registrar los siguientes campos adicionales: OtherName: Para certificados de identidad de individuos, aquí se registra el RUT, en la siguiente estructura: Type-id = 1.3.6.1.4.1.8321.1 Value =’xx.xxx.xx-v’		Otro nombre: 1.3.6.1.4.1.8321.2=04 0c 39 36 2e 39 31 39 2e 30 35 30 2d 38

Tabla 3: Extensiones del certificado raíz de Acepta

1.5 Detalle de los contactos y administración de la PSC

Cualquier consulta puede ser realizada al siguiente contacto:

- **Nombre**: Acepta.com S.p.A.
- **Dirección**: Enrique Foster Sur N°20 piso 5, Las Condes, Santiago de Chile
- **Portal de Clientes**: https://acepta.portalbeaware.com/login
    - Cree su cuenta con su Nombre, apellido, RUT y mail
    - Recibirá mail de confirmación
    - Una vez confirmado el mail, recibirá su clave
    - Ingrese su caso ingresando con su mail y clave registradas
- **Número telefónico**: (+56-2) 24968100
- **Autoservicio de asistencia**: https://asistencia.acepta.com/

1.6 Definiciones y Acrónimos

A efectos del documento de Prácticas 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 móvil.
- **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 móvil..
- **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 móvil:** 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 móvil 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 Móvil
- 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 de firma electrónica móvil, se obliga a realizar las siguientes actividades en la prestación de sus servicios:

1. Contar con reglas sobre prácticas de certificación que sean objetivas y no discriminatorias y comunicadas a los usuarios de manera sencilla y en idioma castellano.
2. Contar con un registro fidedigno de los antecedentes proporcionados por los solicitantes de los certificados de firma electrónica móvil al momento de comprobarse fehacientemente su identidad.
3. Comprobar fehacientemente la identidad del solicitante de los certificados de firma electrónica móvil.
4. Mantener un registro de acceso público de certificados, en el que quede constancia de los emitidos y los que queden sin efecto, sea por revocación o suspensión de los mismos.
5. Tratar los datos personales recolectados con ocasión de la actividad de certificación dando cumplimiento a lo dispuesto en la Ley 19.628 sobre protección de la vida privada, o su equivalente en el país donde se realice la función.
6. En el caso de cesar voluntariamente en su actividad, comunicarlo previamente a los titulares de los certificados de firma electrónica emitidos y, en caso de no existir oposición de los titulares, transferir los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, deja sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia.
7. Publicar en el home del sitio web de Acepta las resoluciones de la Entidad Acreditadora que la afecten.
8. Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Entidad Acreditadora, con una antelación no inferior a un mes cuando vayan a cesar su actividad, y comunicarle el destino que dará a los datos de los certificados, especificando, de ser el caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto.
9. Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento concursal de liquidación o que se encuentre en cesación de pagos.
10. Cumplir con las demás obligaciones legales, especialmente las establecidas en la ley N° 19.799, su reglamento, y las leyes Nº 19.496, sobre Protección de los Derechos de los Consumidores, y Nº 19.628, sobre Protección de la Vida Privada.
    En particular, referente a la Protección de los Derechos de los Consumidores (devoluciones y/o reembolsos) estas solicitudes pueden ser canalizadas a través del sitio de ACEPTA, bajo el link https://asistencia.acepta.com/; ya sea reportando la incidencia o seleccionando la opción de contacto. Para procesar su solicitud se solicitarán los datos de contacto del usuario, así como la boleta del depósito; procediendo con ello a gestionar la devolución solicitada, a través del área de operaciones.

11. Proveer en el sitio web de ACEPTA de opciones de soporte para la comunidad asociada al proceso de firma, lo cual se refleja a través del link https://asistencia.acepta.com/; ya sea reportando la incidencia o seleccionando la opción de contacto.
12. Ejecutar la actividad de certificación de conformidad a lo dispuesto en esta Declaración de Prácticas de Certificación (CPS).
13. Emitir los certificados de firma electrónica móvil con mecanismos tecnológicos y criptográficos que garanticen que el proceso de certificación es realizado adecuadamente y que cumplen con los requisitos establecidos por la Entidad Acreditadora.
14. Revocar los certificados de firma electrónica móvil en los cuales se vea comprometida la confianza respecto a la veracidad de su contenido.

2.1.1 Obligaciones de la AC Raíz (ACR)

El certificado raíz de Acepta permite firmar certificados de distintas comunidades. Es así como Acepta, a partir de su certificado raíz, genera la jerarquía de confianza para distintas comunidades, cada una de ellas encargadas de emitir certificados específicos de firma. Así es como a partir de la ACR, Acepta genera un conjunto de AC intermedias, cada una de las cuales posee su propia vigencia. La tabla siguiente da a conocer dicha jerarquía de confianza:

Tipo	**Bits de la llave privada**	**Años de operación**
Raíz de Acepta	RSA 2.048	10.
Clase 3 Persona Natural	RSA 2.048	10.
FA Firma Electrónica Avanzada y Móvil	RSA 2.048	10.
Sitio Web	RSA 2.048	10.

Los certificados de las autoridades certificadoras intermedias y el certificado raíz de Acepta tienen una fecha de vigencia de 10 años contados desde la fecha de generación de la raíz de Acepta. En el caso que el certificado de Acepta sea vulnerado durante su vigencia, Acepta procederá a su revocación inmediata conforme a lo indicado en la Sección 5.7 de estas CPS. Cuando se reemplazan estos certificados, se generan nuevos certificados, pertenecientes a una estructura jerárquica completamente nueva, cumpliendo con todas las formalidades de generación de llaves definidas para cada nueva autoridad certificadora intermedia.

Las autoridades certificadoras intermedias reemplazadas dejan de firmar certificados nuevos desde el momento de su revocación.

Las claves de las autoridades certificadoras reemplazadas siguen generando listas de revocación y respondiendo a consultas OCSP por un plazo de 10 años de disponibilidad adicional, por lo que todos los certificados firmados por estas autoridades certificadoras podrán cumplir su período de vigencia antes de que expire el certificado de alguna autoridad certificadora presente en su cadena de certificación.

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

Acepta para el desarrollo de la actividad de certificación de firma electrónica móvil desarrolla actividades que son propias de una autoridad certificadora de firma electrónica y otras que son propias de las autoridades de registro. Así, realiza actividades tales como: aprobar o rechazar solicitudes de certificados de firma electrónica móvil; emitir y publicar los certificados de firma electrónica móvil emitidos; proveer su llave pública de manera segura a terceros, de modo que ellos puedan verificar la validez de los certificados que Acepta ha emitido (modelo de confianza), así como informar la revocación de dicha llave; proveer información del estado de los certificados emitidos así como de la lista de revocación; proveer la infraestructura necesaria para proveer los servicios de Firma electrónica móvil, procedimientos, seguridad física y personal adecuado para llevar a cabo las funciones asociadas a la certificación; y, en general cumplir las obligaciones legales, reglamentarias y las que emanan de estas CPS.

Las actividades que desarrolla ACEPTA en su calidad de autoridad certificadora las ejecuta personalmente y no son delegables bajo ninguna circunstancia. Por su parte, las actividades que desarrolla en su calidad de autoridad de registro, las realiza en forma personal o representada.

ACEPTA para su proceso de emisión no posee canales de distribución, ejecuta sus tareas sin delegación bajo ninguna circunstancia. Los productos de ACEPTA además de ser comercializados a través de su nombre propio de empresa, podrán ser distribuidos a través de las páginas web de SOVOS, empresa que adquirió a ACEPTA durante el año 2021. Es de nuestro interés informar que, como parte de ampliar el porfolio de productos asociados a los procesos de firma electrónica, ACEPTA y/o SOVOS podrán distribuir los productos asociados a las aplicaciones de “Identidad Digital”, así como de su repositorio documental denominado *DEC5*, el cual permite a los titulares, hacer uso de las firmas electrónicas avanzadas, para la firma electrónica de documentos que estén almacenados en esta plataforma de gestión documental.

Obligaciones de la Autoridad de Registro (AR):

- Comprobar fehacientemente la identidad de los solicitantes de los certificados de firma electrónica móvil, de conformidad a lo dispuesto en estas CPS.
- Entregar a la Autoridad Certificadora (AC) los antecedentes exigidos por estas CPS que sirvieron de base para comprobar fehacientemente la identidad de los solicitantes de los certificados de firma electrónica móvil.
- Custodiar los antecedentes que sirvieron de base para comprobar fehacientemente la identidad de los solicitantes de los certificados de firma electrónica móvil mientras la AC no tome el control de éstos.
- Mantener los controles de seguridad física, de procedimiento y personales definidos para el desarrollo de la actividad de registro, de acuerdo a lo establecido en estas CPS y en la documentación de seguridad de Acepta.
- Contar con la infraestructura requerida para prestar el servicio de certificación, conforme al nivel de calidad comprometido.

Obligaciones de la Autoridad Certificadora (AC):

- Hacer públicas las políticas y prácticas de certificación a que están sujetos los certificados de firma electrónica móvil.
- Custodiar los datos de creación de firma con los cuales Acepta suscribe los certificados de firma electrónica móvil que comercializa de conformidad con las normas técnicas fijadas por la Entidad Acreditadora.
- Contar con la infraestructura requerida para prestar el servicio de certificación, conforme al nivel de calidad comprometido y los requisitos y obligaciones que impone la ley.
- Generar y firmar los certificados de firma electrónica móvil a partir de la información que le proporciona la Autoridad de Registro (AR).
- Entregar en la forma establecida en estas CPS los certificados de firma electrónica móvil a los titulares.
- Procesar y reportar los requerimientos de revocación y suspensión de los certificados de firma electrónica móvil.
- Proveer el estado de revocación de certificados a las partes interesadas.
- Mantener un registro de acceso público de los certificados de firma electrónica móvil, en el que quedará constancia de los emitidos y los que han quedado sin efecto.

Para asegurar el cumplimiento de las obligaciones señaladas precedentemente, Acepta ha definido:

- Prácticas de Certificación de firma electrónica móvil.
- Controles respecto a la generación de llaves, que aseguran que ellas son generadas en una infraestructura segura (con múltiples sitios), con roles definidos y con un doble control (operadores de registro y validación).
- Algoritmos reconocidos por la industria para la generación de claves.
- Un largo de llave de al menos 2048 bits.
- Procedimientos para generación de llave de la AC ante expiración de la misma, sin que ello implique interrupción de los servicios.
- Procedimientos para el respaldo, almacenamiento y recuperación de las llaves de la AC sólo por personal autorizado y en base al quórum que se ha definido para esta acción.
- Un canal seguro para la distribución de la llave pública de la AC que permita verificar a los terceros interesados, los certificados que Acepta a firmado.
- Que los certificados de firma estén asociados sólo al propósito para el cual han sido definido (Campo CN en Nombre de Emisor).
- Que la llave privada no puede ser usada de manera posterior a su fecha de expiración.
- Que existe un procedimiento para el control del ciclo de vida de los elementos criptográficos.
- Que la llave privada del cliente debe ser almacenada en un dispositivo que no comprometa su seguridad.
- Que la entrega de los datos de creación de firma al titular no debe comprometer su seguridad.

2.1.3 Obligaciones del Solicitante

Los solicitantes de certificados de firma electrónica móvil se encuentran obligados a:

- Conocer y aceptar estas CPS.
- Conocer y aceptar el propósito y alcance de los certificados de firma electrónica que le vaya a emitir Acepta.
- Brindar a la Autoridad de Registro (AR) declaraciones exactas y completas respecto a su identidad personal y otras circunstancias objeto de certificación por parte de Acepta.
- Notificar a Acepta cualquier cambio en las declaraciones, respecto a su identidad personal u otras circunstancias objeto de certificación y que hayan sido proporcionadas a la Autoridad de Registro al momento de la comprobación fehaciente de la identidad.
- Custodiar adecuadamente los datos de creación de firma del certificado de firma electrónica móvil que Acepta le emita, así como cualquier otro mecanismo de seguridad de funcionamiento del sistema de firma electrónica.
- Suscribir el contrato de prestación de servicios de certificación digital.
- Abonar la tarifa o precio establecido para el servicio solicitado.

2.1.4 Obligaciones del Suscriptor de la Llave

Las obligaciones del suscriptor del certificado de firma móvil se resumen en:

- Proteger y utilizar el certificado emitido para los fines con que ha sido solicitado; custodiando de manera adecuada dicho certificado, ya que este corresponde a su identidad en el mundo digital, por ende, al igual que una Cédula de Identidad, el certificado emitido debe ser protegido de un uso no apropiado dado una pérdida, robo o hurto, informando de manera oportuna a Acepta en caso de presentarse algún inconveniente de seguridad del mismo.
- Solicitar la revocación del certificado en caso de cumplirse condiciones tales como la pérdida del certificado o su dispositivo, la pérdida de la clave de acceso, la cesación del cargo en caso de ser certificados que se han asociado a un cargo específico, a solicitud del suscriptor del certificado, ante la no renovación del certificado o ante la necesidad de revocación de dicho certificado por parte de Acepta.
- No revelar la clave privada ni el código de activación del certificado, la que es de exclusiva responsabilidad del suscriptor.
- Verificar y asegurar que la información contenida en el certificado es fidedigna e informar a Acepta ante cualquier información incorrecta o inexacta detectada en dicho certificado o cambio que se haya generado respecto a la información originalmente entregada para la emisión de dicho certificado.
- Cualquiera otra obligación que derive de la Ley, el Reglamento, este documento o del certificado digital.

2.1.5 Obligaciones los Usuarios

Los usuarios de los certificados de firma electrónica móvil emitidos por Acepta se obligan a aceptar las siguientes condiciones:

- Comprobar en Acepta que el certificado en el que se pretende confiar se encuentra vigente (no ha sido revocado o suspendido o terminada su vigencia).
- Conocer y aceptar el propósito y alcance del certificado de firma electrónica en que se pretende confiar.

2.1.6 Confianza en las Firmas y certificados

Las partes que confíen en las firmas emitidas por Acepta deberán considerar:

- Que la operación que se pretende avalar con la firma, está en el ámbito de esta última, no sólo en el uso de la misma, sino en lo que determinan las normas legales y reglamentarias asociadas a la PSC y los distintos tipos de certificados emitidos.
- Que la parte que desea confiar ha tomado los resguardos de verificar la autenticidad de la firma en base a la llave pública de Acepta
- Que la parte que desea confiar ha asegurado la validación de caducidad o revocación de la firma en cuestión en base a los servicios provisto por Acepta.
- Que las partes que confían en los certificados han de:
    - Acotar la fiabilidad de los certificados emitidos, a los usos que se han definido para los mismos, en conformidad con lo definido en las extensiones de los certificados y la Política de Certificación pertinente.
    - Verificar la validez de los certificados en el momento de realizar o verificar cualquier operación basada en los mismos.
    - Asumir su responsabilidad en la correcta verificación de las firmas digitales.
    - Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados en que confía.
    - Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

2.1.7 Obligaciones de los Repositorios

El repositorio público de Acepta permite realizar distintas operaciones dependiendo del tipo de certificado con el que se esté trabajando. En este repositorio se llevará un registro actualizado de los certificados vigentes y revocados, estando dichas alternativas explicadas en el documento de políticas de cada tipo de certificado. En el caso de los certificados de firma móvil, se contará con el acceso público a las prácticas y políticas del PSC, asociado a este tipo de certificado, así como del estado de un certificado en particular, ya sea por medio de una consulta al servicio en línea OCSP o a través de la lista de revocación publicada por Acepta en su sitio web.

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 móvil ocasione y, en ningún caso será responsable del uso incorrecto, indebido o fraudulento de los certificados de firma electrónica móvil 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 móvil ocasione, debiendo demostrar que actuó con la debida diligencia.

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 Acepta. Por lo anterior, no otorga garantía alguna en relación al 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, Acepta 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 móvil.

Lo anterior se entenderá de conformidad a lo señalado en el Artículo 14 de la Ley 19.799.

2.2.1 Responsabilidad Pecuniaria

Las responsabilidades que afectan la operación de Acepta se encuentran establecidas y limitadas a lo señalado en el artículo 14 de la Ley 19.799 799 para Chile.

En todo caso, la responsabilidad de Acepta 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 correspondiente a UF5.000 (cinco mil unidades de fomento), monto asegurado de conformidad con lo dispuesto en el artículo 14 de la Ley 19.799 y el artículo 12 del Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Reconstrucción.

La actividad de certificación de firma electrónica móvil se encuentra limitadas al ciclo de vida del certificado, esto es:

1. Solicitud del solicitante. Proveer todas las condiciones necesarias para que el solicitante de un certificado de firma electrónica móvil pueda requerir y proporcionar toda la información necesaria para la emisión del mismo.

2. Registro del solicitante. Una vez que el prestador de servicios de certificación recibe la solicitud debe proceder a la aprobación de la misma, y para ello deberá comprobar los antecedentes que le han sido declarados, debiendo comprobar en la forma señalada en esta CPS y, especialmente la identidad del solicitante y que los datos de creación de firma son entregados realmente a quien solicitó el certificado de firma electrónica.

3. Firma y emisión del certificado. Una vez que se ha efectuado el registro del solicitante y se ha verificado la exactitud de los datos proporcionados, el prestador de servicios de certificación procede a emitir el certificado de firma electrónica, firmado por medio de la firma electrónica de la cual es titular.

4. Publicación y archivo. Una vez que el certificado de firma electrónica ha sido emitido y firmado por el prestador de servicios de certificación, hacerlo constar en el registro de acceso público a que se refiere el artículo 12 de la Ley 19.799.

5. Revocación y suspensión. Hacer cesar la vigencia del certificado, de manera temporal o definitiva, según sea el caso en la forma descrita en esta CPS.

2.2.2 Fuerza Mayor

Acepta no será responsable por daños, pérdidas o perjuicios que provengan de incumplimientos en el desarrollo de la actividad de certificación de firma electrónica móvil y que sean atribuibles a circunstancias constitutivas de caso fortuito o fuerza mayor.

Las obligaciones de Acepta afectadas por el caso fortuito o la fuerza mayor se suspenderán por el período de tiempo que dure el hecho que lo motivó.

Para los efectos de estas CPS, se entenderá por caso fortuito o fuerza mayor lo dispuesto en el artículo 45 del Código Civil, lo que incluye guerras, desastres naturales, paros, huelgas o suspensión de laborales del personal de Acepta o de sus contratistas o subcontratistas, sin que esta enumeración sea taxativa.

2.2.3 Responsabilidad de la AC y AR

Aplica el régimen de responsabilidad establecido en 2.2, no siendo pertinente diferenciar entre la responsabilidad de la AR y la AC en virtud de la Ley 19.799 (Chile).

2.3 Ley Aplicable y Resolución de Conflictos

2.3.1 Ley Aplicable

Estas CPS y las Prácticas de Certificación específicas para cada tipo de certificado se regirán e interpretarán de conformidad con la ley chilena.

2.3.2 Resolución de Conflictos.

Cualquier diferencia, dificultad, problema o controversia que pueda surgir entre Acepta y los suscriptores o signatarios que suscriban él (los) respectivo(s) contrato(s) de certificación o con los terceros interesados que adhieran a las CPS de Acepta con motivo de la validez, eficacia, interpretación, nulidad, cumplimiento o incumplimiento de estas CPS o de la actividad de certificación de firma electrónica móvil será resuelta definitivamente por un árbitro mixto, quien tramitará como árbitro arbitrador pero que fallará conforme a derecho. El fallo del árbitro será en única y definitiva instancia, sin que, en contra de sus resoluciones y fallo, ya sean de substanciación o de medidas precautorias o bien el fallo definitivo, proceda ningún recurso. El arbitraje se llevará a cabo en la ciudad de Santiago. El árbitro estará solamente obligado a constituir legalmente el arbitraje, a oír a las Partes en conjunto o separadamente, según él lo decida, a recibir las pruebas que se presenten y a dictar su sentencia oportunamente. Las resoluciones se notificarán por carta certificada dirigidas a las Partes o a sus representantes designados en esta escritura o en el respectivo proceso, a las direcciones que ellos señalen en tales instrumentos, salvo la primera notificación del proceso y la de la sentencia definitiva que deberán notificarse en conformidad a las reglas establecidas para dichas resoluciones en el Título Sexto, del Libro Primero, del Código de Procedimiento Civil. El árbitro designado podrá actuar cuantas veces fuere requerido, por asuntos diferentes, promovidos por cualquiera de las Partes, y en caso de ausencia o impedimento acreditada a juicio del sustituto, éste podrá intervenir de inmediato, en carácter de subrogante, en el estado en que el asunto se encuentre, sin otro requisito que aceptar el cargo. El respectivo proceso podrá continuarse incluso en una copia autorizada de los autos que cualquiera de las Partes presentare ante el sustituto. La evidencia de haberse ausentado del país el

árbitro en ejercicio por más de treinta días sin haber regresado, o de impedimento de otra naturaleza acreditado ante el sustituto por medios idóneos y que dure más de treinta días será considerado como ausencia del árbitro.

El árbitro, en Chile, deberá ser designado de común acuerdo por las Partes, dentro del plazo máximo de 15 días hábiles. A falta de acuerdo respecto de la persona que actuará en el cargo, el árbitro deberá tener el carácter de mixto y su designación será efectuada, a solicitud escrita de cualquiera de las Partes por la Justicia Ordinaria, debiendo recaer la designación en una persona que haya sido Ministro o Abogado Integrante de la Excelentísima Corte Suprema de Justicia, o bien, Profesor de las cátedras de Derecho Civil o Comercial de las Facultades de Derecho de las Universidades de Chile, Católica de Santiago o Católica de Valparaíso, excluidos quienes hubieren asesorado o prestado servicios a cualquier título a alguna de las partes en el bienio inmediatamente anterior.

2.4 Publicación y Repositorios

Acepta mantiene publicadas en su sitio web https://sovos.com/es/politicas-y-practicas/, esta Declaración de Prácticas de Certificación (CPS).

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

Acepta y sus PSC acreditadas se obligan a mantener dicha información disponible para su acceso público, así como publicar la información consistentemente con las prácticas de confidencialidad estipuladas en este documento, así como de las leyes vigentes.

La disponibilidad de los servicios señalados no podrá ser inferior a un 99,5 % al año, excluyendo de este compromiso, los tiempos de mantención programados o casos de fuerza mayor indicados en 2.2.2.

La información de validación del estado de los certificados de firma electrónica móvil (vigente, revocado o suspendido) se mantiene permanentemente actualizada.

Las listas de revocación de todos los tipos de certificados son actualizadas cada 24 horas.

El registro de acceso público de certificados funciona bajo las siguientes normas:

a. La información relativa a los certificados de firma electrónica móvil es publicada, a través de sistemas automatizados, en el mismo momento en que éstos son emitidos.
b. La información relativa a la revocación de los certificados de firma electrónica móvil es publicada dentro de un plazo que no puede exceder de 6 horas laborales (entre 9:00 y 18:00 horas), contada desde la solicitud de revocación realizada de conformidad con el procedimiento indicado en 4.9.3 de estas CPS.

La información relativa a la suspensión de los certificados de firma electrónica móvil es publicada, a través de sistemas automatizados, en el mismo momento en que ésta es solicitada de conformidad con el procedimiento indicado en 4.9.6 de estas CPS.

2.5 Privacidad y Protección de los Datos Personales

Las Políticas de Privacidad de Acepta se encuentran publicadas en el sitio web de Acepta https://sovos.com/es/politicas-y-practicas/.

2.5.1 Tipos de Información a Proteger

De manera complementaria a lo dispuesto en las Políticas de Privacidad de Acepta, la empresa protege especialmente la siguiente información:

- Información propia de la operación de Acepta y de sus llaves
  - Las claves privadas de las entidades que componen a Acepta.
  - Toda información relativa a las operaciones que lleve a cabo Acepta.
  - Toda información relativa a los controles de seguridad y procedimientos de auditoría.
  - Planes de continuidad de negocio y de emergencia.
  - Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
  - Toda la información clasificada como “CONFIDENCIAL”.
- Información propia del suscriptor capturada durante el registro
  - Toda la información de carácter personal proporcionada a Acepta durante el proceso de registro de los suscriptores de certificados.

2.5.2 Tipos de Información que puede ser entregada

Acepta considera como información de acceso público y, consecuentemente se encuentra disponible al público en https://sovos.com/es/politicas-y-practicas/ o en las oficinas de la empresa:

- La Declaración de Prácticas de Certificación de Acepta.
- Toda aquella información que y no teniendo un estatuto de protección especial establecido en la ley sea por Acepta clasificada como "PÚBLICA".
- La contenida en los certificados de firma electrónica avanzada, en cumplimiento de lo dispuesto en la Ley 19.799 (Chile).
- La contenida en el registro de acceso público de certificados de firma electrónica avanzada, en cumplimiento de lo dispuesto en la Ley 19.799.

Y en https://asistencia.acepta.com/firma-avanzada.html se encuentra:

- La lista de certificados revocados (CRL).
- La contenida en los certificados de firma avanzada

Pese a la calificación de la información como de acceso público, Acepta se reserva el derecho de imponer medidas y controles de seguridad adecuados y proporcionales con el fin de asegurarla autenticidad e integridad de los documentos, así como de imponer medidas tecnológicas anti copia y de impresión para aquellos que se encuentren soportados electrónicamente.

2.5.3 Información del Certificado

Los certificados de firma electrónica móvil 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.

Campo	Descripción	Ejemplo
Versión	Versión del certificado, que deberá ser versión 3	v3
Nº de Serie	Número que identifica unívocamente al certificado dentro de los emitidos por Acepta	**0090 0001**
Algoritmo de Firma	Algoritmo utilizado por el PSC para firmar el certificado	SHA256 WithRSAEncryption
Nombre del Emisor	Nombre distintivo (DN) del emisor, en el formato del estándar X.500. Deben incluirse los siguientes tipos: CN =Tipo de certificado E = e-mail del Prestador de Servicios de Certificación Número de serie = Número identificador del certificado, se utiliza el RUT de Acepta. C = País	CN = Acepta Autoridad Certificadora Firma Electrónica Móvil E = info@acepta.com SN = 96919050-8 C = CL
Periodo de Validez	Fecha de inicio y termino en que es válido el certificado. Para PSC = 10 años, Para suscriptores = 1 a 3 años, Codificado en formato YYMMDDHHMMSSZ	Fecha inicio = 040914140522Z Fecha termino = 050914140522Z
Nombre del suscriptor	Nombre distintivo (DN) del suscriptor del certificado, en el formato del estándar X.500. Deben incluirse los siguientes tipos: CN = Nombre distintivo del suscriptor T = Profesión E = dirección de correo del suscriptor Número de serie = Número identificador del certificado. Se utiliza el RUT del suscriptor del certificado. C = País	CN = Nombre Apellido1 Apellido2 T = Profesión E = persona@sitio.com SN = 99999999-9 C = CL
Clave pública	Clave pública del suscriptor del certificado	3081 8902 8181 009D ECC1 62F4 FE2D 73DD BE6D 53C3 E578 7F98 38AE ED42 B03D A804 F4D5 CA86 9563 2757 D556 7A4F 0C94 DBBA 8F4E 80B0 C334 6B01 B85D 1872 635F 40C3 F294 24E9 FD92 C97A D3B4 798E 680C 7F92 5889 4786 41DC 1AB0 80D4 CCDE 1280 9334 90F1 A1BE 9E96 72AF AA28 3BEA 2DCC 13BC 685C 7782 E869 A7C4 98B6 9094 43FF 574F 3025 5A2C 8880 3F02 0301 0001

2.5.4 Entrega de Información sobre la Revocación o Suspensión del Certificado

La información relativa a la revocación o suspensión de certificados se proporciona vía CRL por parte de Acepta. Esta información también se encuentra disponible en el servidor de validación OCSP de Acepta.

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

Acepta sólo podrá comunicar informaciones calificadas como confidenciales o que contengan datos de carácter personal en aquellos casos en los que así se le requiera por la autoridad pública competente y bajo los procedimientos que se han previstos legalmente por el Poder Judicial de la República de Chile, o de sus tribunales competentes.

Las obligaciones, prohibiciones y responsabilidades de custodia de información sujeta a secreto, reserva o confidencialidad de acuerdo con la ley y estas CPS no regirán si media alguna disposición legal o resolución judicial que obligue a entregar al conocimiento de los Tribunales de Justicia, organismos, instituciones o entidades facultadas por la ley para solicitarlos y que actúen dentro del ámbito de sus atribuciones.

Sin perjuicio de lo cual, Acepta le informará al titular al correo electrónico contenido en el certificado de firma electrónica móvil la existencia del requerimiento de información, de modo que el titular pueda ejercer sus derechos ante la autoridad competente.

2.5.6 Entrega de Información a Petición del Titular

Acepta entregará la información del titular del certificado que mantiene en sus registros previo ejercicio del derecho de acceso por éste, en la forma establecida en las Políticas de Privacidad de Acepta.

En virtud de lo dispuesto en la Ley 19.799 (Chile), Acepta mantendrá a disposición de cualquier interesado, a través del registro de acceso público de los certificados emitidos, el nombre, RUT, correo electrónico y cualquier otra circunstancia que haya sido objeto de la certificación de la firma electrónica móvil.

2.6 Derechos de Propiedad Intelectual e Industrial

La prestación de los servicios de certificación de firma electrónica móvil en ningún caso otorga a los participes de la comunidad descritos en 1.3 de estas CPS derecho de propiedad intelectual o industrial alguno. Así, Acepta retiene todos sus derechos de propiedad intelectual e industrial sobre las obras creadas, desarrolladas o modificadas. Ningún derecho de propiedad intelectual o industrial preexistente o que se adquiera o licencie a o por Acepta, se entenderá conferido a los miembros de la comunidad antes citada.

Salvo acuerdo previo, específico y por escrito en contrario celebrado con algún miembro de la comunidad descrita en 1.3 de estas CPS, ninguno de ellos puede publicar o usar logotipos, marcas, marcas registradas, incluso marcas de servicio y patentes, nombres, redacciones, imágenes, símbolos o palabras de Acepta.

Los documentos definidos cómo públicos pueden ser reproducidos respetando las restricciones indicadas en cada documento:

- Políticas de privacidad
- Políticas de certificados
- Prácticas de certificación

3 Identificación y Autenticación

La identificación de los solicitantes y titulares de certificados de firma electrónica móvil se realiza de acuerdo con las normas y procedimientos contenidas en esta sección de las CPS, con independencia de que la actividad de registro sea realiza directamente por Acepta o por un mandatario.

3.1 Registro Inicial

3.1.1 Registro de Nombres

De conformidad con la Ley 19.799 (Chile), los certificados de firma electrónica móvil deberán contener como menciones mínimas: El nombre del solicitante, su rol único nacional (RUN) y una dirección de correo electrónico.

El nombre corresponderá al nombre completo del solicitante en los términos consignados en su cédula de identidad (nombres y apellidos). Este deberá ser registrado por Acepta, personalmente o a través de mandatario, en los términos definidos en el estándar X.509 y será incluido en el certificado en el campo Common Name (CN).

El rol único nacional del solicitante (RUN) en Chile, corresponderá a aquel que se encuentre consignado en la cédula de identidad del solicitante.

La dirección de correo electrónico será aquel que declare el solicitante al momento de realizarse la comprobación fehaciente de su identidad.

Acepta sólo incorporará en los certificados de firma electrónica móvil el nombre y el RUN consignado en la cédula de identidad en Chile. Asimismo, incorporará la dirección de correo electrónico que haya sido declarada en la solicitud del certificado y no resolverá disputa alguna relativa a la titularidad de los nombres, números de RUN en Chile, ni dominios de las direcciones de correo electrónico.

3.1.2 Verificación General

Todas las menciones incorporadas en los certificados de firma electrónica móvil son comprobadas por Acepta, de manera de asegurar que el nombre y RUN en Chile, incluido en éstos se encuentre efectivamente agregado en idénticos términos a los consignados en la cédula de identidad del solicitante. Respecto a la dirección de correo electrónico o cualquier otra mención certificable, Acepta se asegurará que se adicione en idénticos términos consignados en la solicitud del certificado o en la documentación acreditativa de la respectiva mención.

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

La revocación es el mecanismo a través del cual Acepta deja sin efecto de manera permanente un certificado de firma electrónica móvil emitido por él, cesando permanentemente los efectos jurídicos del certificado conforme a los usos que le son propios impidiendo el uso legítimo del mismo.

Tendrá lugar cuando Acepta constate alguna de las siguientes circunstancias:

a) 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).
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.

4 Requisitos Operacionales

En este capítulo se describen los requisitos operativos de Acepta, dentro de su prestación de servicios asociados a su PSC, la cual cuenta con los siguientes componentes de sistema:

- **Interfaces:** Acepta, para su emisión de certificados, establece una relación entre la AC la AR y el titular. Esta relación se inicia en la captura de los datos relevantes para la emisión del certificado de firma desde el solicitante, los cuales son comprobados por la Autoridad de Registro. De ser aprobada esta solicitud, ella se envía a través de un canal seguro a la Autoridad de Certificación, de manera que el titular pueda realizar la generación de su par de llaves así como solicitar la generación de su certificado de firma electrónica, elementos a ser almacenados y controlados por el titular en su dispositivo criptográfico.

  La comunicación entre la AR y la AC, con posterioridad a la generación de las llaves, sólo ocurre en el registro de las revocaciones y suspensiones, las que son ingresadas por el operador de validación y cuyo efecto es el modificar la CRL y el servicio OCSP.

- **Sistema de directorios para los certificados de firma Electrónica**: En caso de requerir información asociada a la emisión de certificados, los interesados pueden acceder, a través de un servidor web, al repositorio que contiene los certificados de firma Electrónica mediante la siguiente URL:
  - https://asistencia.acepta.com/buscar-certificado.html

  Y para poder recuperar la lista de revocación se cuenta además con el siguiente enlace:

  - https://asistencia.acepta.com/firma-avanzada.html (Rótulo ***Revocación de la Firma Avanzada*** sub ítem ***Ver listados de revocación (CRL)***)

- **Procesos de Auditoría:** La auditoría sobre la PSC de Acepta, se realizará al menos una vez al año, para garantizar el funcionamiento y seguridad, de acuerdo a las disposiciones contenidas en la Declaración de Prácticas de Certificación de esta PSC.

- **Bases de datos**: La información relevante incluida en la Base de Datos de la PSC de Acepta, que está asociada al proceso de emisión de certificados incluye:
  - Solicitudes de Certificado y su estado
  - Certificados emitidos y su estado

- **Privacidad:** Acepta mantiene un compromiso respecto al uso de los datos personales, el cual asegura la confidencialidad de los datos personales de los titulares que se faciliten, remítase a https://legal.acepta.com/corporativo/politicas_privacidad.pdf, ya sea mediante el o los formulario(s) establecido(s) para esos efectos o bien los que sean recogidos por el hecho mismo de navegar por la Web. Acepta únicamente recolectará aquellos datos que han sido entregados voluntariamente por los usuarios, los que serán usados o tratados únicamente para los fines para los cuales dichos datos fueron proporcionados.

- **Entrenamiento del personal:** Como parte de sus actividades, Acepta realiza cursos de capacitación, los cuales en contenido, duración y fechas estimadas se encuentran descritos en el plan de capacitación anual de su PSC. Este plan incluye labores de reentrenamiento de existir cambios tecnológicos, en las políticas o prácticas de certificación o cualquier documento que se considere relevante de ser informado.

De igual forma, Acepta para estos requisitos, considera un plan de auditoría que verifica que su modelo incluye:

- **Seguridad y dispositivos de seguridad**: El hardware criptográfico utilizado por la PSC de Acepta cuenta con la certificación FIPS 140-2 Nivel 3.

- **Restricciones de personal**: Acepta filtra adecuadamente los candidatos para el empleo, los contratistas y sus usuarios especialmente en las tareas sensibles y se asegura de que estos sean aptos para los roles que están siendo considerados, de tal forma de disminuir los riesgos de hurto, fraude o mal uso de las instalaciones. Para esto, la Gerencia de Recursos Humanos utiliza procedimientos de requerimiento y comprobación de antecedentes, entregando a cada empleado, al momento del contrato, del Reglamento Interno el cual en uno de sus capítulos indica deberes, obligaciones y sanciones en caso de incumplimiento de las obligaciones del cargo. Todo trabajador de la PSC Acepta, firma un acuerdo de confidencialidad.

- **Procedimientos de recuperación de desastres**: El Plan de Continuidad de Negocio y Gestión de Contingencias de Acepta, tiene por objetivo el proveer un conjunto de políticas y procedimientos, tanto para prevenir como para enfrentar una situación de emergencia en los sistemas de información, así como también, de mantener la continuidad de las operaciones y asegurar la capacidad de responder eficazmente ante un desastre y otras situaciones de emergencia. Este plan contempla un conjunto de escenarios de contingencia, así como una frecuencia de revisión de dicho Plan.

- **Procedimiento de respaldo**: Los respaldos de servidores centrales de la PSC de Acepta, son realizados haciendo uso de medios magnéticos que aseguran la permanencia de la información a lo menos en 5 años. Los respaldos se realizan diariamente, incluyendo un respaldo incremental de los datos administrados por los sistemas de información, así como un respaldo total semanal. Los respaldos mensuales, son mantenidos como históricos.

Finalmente, Acepta considera los siguientes requerimientos de seguridad:

- **Seguridad física de las instalaciones:** Acepta concibe la seguridad física como parte de una política global, que garantiza la protección de los activos del negocio, mitigando el riesgo asociado a las amenazas y vulnerabilidades, de aquellos activos que pueden protegerse físicamente. Estos recursos incluyen el personal, el sitio donde ellos laboran, los datos, equipos y los medios con los cuales los empleados interactúan, en general los activos asociados al

mantenimiento y procesamiento de la información. Acepta desarrolla sus operaciones en 3 lugares físicos, siendo ellos su Casa Matriz, Sitio Principal y el Sitio Secundario.

- **Seguridad del Personal:** Acepta, con el objeto de favorecer un uso adecuado de la información y de los sistemas que la apoyan, cuenta con políticas de seguridad de la información vinculadas al recurso humano. Esas políticas, en la medida que se refieran a obligaciones o prohibiciones que afecten al personal de Acepta, deberán encontrarse alineadas, entre otras, con las normas laborales vigentes, en especial, con los contratos de trabajo y el reglamento interno de orden, higiene y seguridad.

- **Seguridad del módulo criptográfico**: 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.

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 los siguientes puntos, se procede a describir y detallar el proceso antes mencionado. Las especificaciones contenidas en estos puntos lo son sin perjuicio de las estipulaciones previstas en cada una de las distintas Políticas de Certificación para los distintos tipos de certificados emitidos por Acepta.

4.2 Solicitud de Certificado

Para solicitar un certificado de firma electrónica móvil el solicitante debe comparecer personalmente ante la Autoridad de Registro de Acepta y junto con completar el formulario de solicitud debe:

- Presentar su cédula de identidad vigente, a los efectos de que Acepta compruebe:
  a. El RUN en Chile
  b. Nombres y apellidos. Se hace presente que en el registro y por razones de compatibilidad con el estándar X.509v3, las letras acentuadas son reemplazadas por letras sin acento y las “ñ” son reemplazadas por “n”.
- Indicar una dirección de correo electrónico.

En caso que el solicitante desea que el certificado cuente con una mención especial, de las que son susceptibles de certificación, deberá presentar la documentación acreditativa de dicha circunstancia.

Si el registro presencial es hecho por un operador de registro de Acepta, se almacena la siguiente documentación:

- 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 en Chile
- 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 en Chile
- Nombres
- Fecha de nacimiento
- Firma
- Fotocopia de cédula de identidad

4.2.1 Verificación General

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

En el caso de que el registro presencial sea realizado por un operador de registro de Acepta, este puede reunirse con el solicitante en una de las oficinas de registro de Acepta y también es posible acordar un registro presencial en dependencias del solicitante. Acepta se reserva el derecho a definir la cobertura disponible para este efecto. En la información capturada por el operador de registro se incluye el RUN en Chile, fecha de nacimiento, e-mail, foto, firma manuscrita, impresión dactilar y datos de contacto del suscriptor del certificado.

En caso que el solicitante desee realizar una solicitud para la emisión de un certificado de firma electrónica móvil vía web, Acepta proveerá de un link, en el que deberá completar un formulario on line denominado solicitud de contrato de suscripción, el cual debe imprimir y llevar ante un Notario. Dicho documento contempla los datos básicos del solicitante, su impresión dactilar y la firma manuscrita de él y la del notario, siendo este último quien certificará que el Nombre y RUN en Chile de la persona solicitante, coincidan con lo indicado en el formulario de solicitud.

Luego de firmar el documento, es el mismo notario quien lo envía por carta certificada a Acepta; carta que incluye:

- Formulario de suscripción, impresión dactilar, firma manuscrita del solicitante y la firma del notario.
- Fotocopia de cédula de identidad del solicitante

Si el registro presencial es hecho por el Registro Civil, entonces se utilizan los mismos procedimientos de verificación de identidad utilizados por este organismo para la emisión de cédulas de identidad y pasaporte. El Registro Civil le comunica a Acepta los datos de la identidad del solicitante a través de un canal seguro y utilizando mensajes firmados electrónicamente. En la información enviada por el Registro Civil se incluye el RUN en Chile, nombre, fecha de nacimiento, e-mail, foto, digitalización de la firma manuscrita, impresión dactilar y datos de contacto del suscriptor del certificado. El Registro Civil además entrega en un documento el PIN de activación, el cual es generado por sistema.

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.

Acepta no implementa procedimientos de control a las actividades del Registro Civil, ya que se trata de la máxima Autoridad en Chile en verificación de identidad.

4.2.2 Labores de AC y AR

A la Autoridad de Registro propia o designada por Acepta para esta labor, le corresponde la comprobación de la identidad del solicitante, la verificación de la documentación por él presentada y la constatación de que el solicitante ha firmado el contrato de suscripción. Una vez completa la solicitud, la Autoridad de Registro remitirá esta solicitud al operador de validación de Acepta.

Este proceso de validación consiste en la centralización de las solicitudes con la información proporcionada por el suscriptor de una firma electrónica en el proceso de registro presencial de la identidad. Para cumplir esta función, el operador de validación, ubicará el registro a validar y sólo si los datos se encuentran correctos, al compararlo con la imagen del documento de identidad presentado, procederá a aceptar dicha solicitud. En caso contrario, o exista alguna inconsistencia en la solicitud, ella puede quedar en un estado pendiente o ser rechazada definitivamente. Así la validación aplicada se resume en:

1. Cuando el registro presencial fue hecho por un operador de registro:
   - Verifica que la información del nombre y RUN en Chile asociados a la solicitud correspondan con las copias electrónicas de la Cédula Nacional de Identidad.
   - Verifica que el nombre, RUN en Chile, 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 Cédula Nacional de Identidad.
2. 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.

3. 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.

El objetivo de esta segunda validación es contar con un quórum de dos operadores distintos en la aprobación de una solicitud.

Una vez aprobada la solicitud, se procederá a enviar un mensaje electrónico al suscriptor, a fin de que proceda a emitir su certificado de firma.

4.3 Emisión de Certificados

Acepta sólo emite certificados de firma electrónica móvil cuando ha sido comprobada fehacientemente la identidad del solicitante en la forma señalada en esta Declaración de Prácticas de Certificación.

4.4 Aceptación de Certificados

Los procedimientos mediante los cuales el suscriptor de cada tipo de certificado acepta el certificado emitido, están indicados en las políticas de cada tipo de certificado.

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.

4.5 Uso del par de claves y del certificado

El suscriptor sólo puede utilizar los datos de creación de firma y el certificado de firma electrónica móvil para los usos autorizados en este instrumento y de acuerdo con lo establecido en los campos “Key Usage” y “Extended Key Usage” del certificado.

Tras la expiración o revocación del certificado, el suscriptor debe cesar en el uso de los datos de creación de firma.

Todo uso del certificado fuera del ámbito o uso autorizado indicado en éste, es de exclusiva responsabilidad del titular y representan usos ilegítimos.

4.6 Renovación de certificados.

Acepta permite solicitudes de renovación de certificados, clasificándose ellas en:

a. **Rutinarias**: Durante el período de vigencia, el suscriptor podrá siempre solicitar otro certificado, sin necesidad de repetir el registro presencial. El suscriptor podrá enviar un e-mail firmado electrónicamente solicitando un nuevo certificado o conectarse a una página Web usando su Password de activación, lo que asegura la identidad puesto que ésta fue comprobada cuando se realizó el primer registro presencial

En ambos casos, el suscriptor recibirá un e-mail de Acepta comunicándole un nuevo número de solicitud. Con este número de solicitud y su Password de activación el Suscriptor podrá crear un nuevo certificado.

b. **Producto de una revocación:** La política de identificación y autenticación para la renovación de un certificado después de una revocación y sin compromiso de la clave será la misma que para el registro inicial, o bien se empleará algún método electrónico que garantice de manera fiable e inequívoca la identidad del solicitante y la autenticidad de la solicitud.

4.7 Renovación de claves

La renovación de claves implica necesariamente la emisión de un nuevo certificado de firma electrónica móvil. Las claves no son recuperables.

4.8 Modificación de certificados.

No aplica.

4.9 Suspensión y Revocación de Certificado

Las alternativas disponibles para suspender o revocar cada tipo de certificado están disponibles en las políticas de certificación correspondientes.

4.9.1 Circunstancias de Revocación

Aplica lo dispuesto en 3.4.

4.9.2 Solicitud de Revocación

Aplica lo dispuesto en 3.4.

4.9.3 Procedimiento de Revocación

La revocación se realiza en forma presencial en oficinas de Acepta, entregando los antecedentes que comprueben la identidad del suscriptor, mencionando los motivos de la revocación.

En el caso de no ser presencial, el cliente debe enviar un correo indicando la solicitud de revocación, señalando los motivos y una copia de cédula de identidad por ambos lados con su firma manuscrita ante notario.

4.9.4 Motivos de Suspensión

La suspensión implica invalidar un certificado durante el tiempo que permanece suspendido. La suspensión únicamente se puede efectuar ante:

- Una solicitud de revocación de un certificado en que no ha sido posible verificar de inmediato la identidad del solicitante.
- Cuando Acepta tiene convencimiento que se ha podido comprometer la clave privada asociada al certificado de un usuario.
- Cuando una autoridad judicial lo establezca.
- Una solicitud del propio suscriptor del certificado.

4.9.5 Solicitud de Suspensión

La solicitud de suspensión de un certificado se puede instar tanto por el suscriptor del certificado, por Acepta como AC o, en caso excepcionales, a través de una orden judicial.

4.9.6 Procedimiento de Suspensión

Para solicitar la suspensión de un certificado, el titular o un tercero deberán enviar un e-mail a la casilla admin-suspensiones@acepta.com, indicando el 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 enviará al suscriptor un e-mail de confirmación de lectura cuando se haya recibido la solicitud y un segundo e-mail avisando cuando se haya procesado la solicitud. El plazo transcurrido entre la recepción de la solicitud y su procesamiento no podrá ser superior a 6 horas, considerando lunes a viernes de 9:00 a 18:00 horas.

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.

Las solicitudes de suspensión no tendrán costo para el usuario.

4.9.7 Límite de Suspensión

La suspensión de un certificado es un estado temporal de 72 horas corridas, salvo que la resolución judicial que lo dictamine imponga un plazo superior o inferior, después del cual el certificado puede ser revocado permanentemente o puede recuperar su estado de vigente.

4.9.8 Listado de Certificados Revocados

Acepta publicará una nueva CRL en su repositorio en intervalos de 24 horas, aunque no se hayan producido modificaciones en la misma (cambios de estado de certificados) durante dicho periodo.

4.10 Servicios de comprobación de estado de certificados.

Acepta cuenta con dos servicios para la comprobación de los certificados, el primero es la CRL o lista de revocación, la que se actualiza tal como se indica en 4.9.8; la segunda es el servicio OCSP, el cual entrega el estado actual de un certificado.

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 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 configuración1+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 se 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 gasFM-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.

5.2.1 Seguridad Física Data Center

Los sistemas de Acepta, como Entidad de Certificación, se encuentran alojados en un Sitio Principal y uno secundario. Ambos sitios cuentan con niveles de protección y solidez de la construcción adecuado y con vigilancia durante las 24 horas al día, los 7 días a la semana.

Ambos sitios cuentan con diversos perímetros de seguridad, diferentes requerimientos de seguridad y autorizaciones. Entre los equipos que protegen los perímetros de seguridad se encuentran sistemas de control de acceso físico, sistemas de video vigilancia y de grabación, de detección de intrusiones entre otros.

Los sitios además cuentan con un sistema central de vigilancia mediante circuito cerrado de televisión, distribuidas en lugares estratégicos del piso, las que permanentemente están grabando las actividades y registrando los accesos de personas a lugares que requieren acceso restringido. El centro de control es monitoreado por guardias de seguridad las 24 horas del día, todos los días de la semana, lo que permite llevar un registro y control total de acceso.

Se ha reforzado el control del ingreso a áreas de alta seguridad, como es el área de servidores, a través de la instalación de puertas reforzadas que permanecen constantemente cerradas y que sólo pueden ser abiertas por personas previamente autorizadas por la Gerencia del CGSI, bajo la estrecha supervisión de Guardias de Seguridad.

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.

5.2.2 Sistema de Energía Eléctrica

El suministro eléctrico para el sitio principal está garantizado con un grupo electrógeno dimensionado para proporcionar energía eléctrica a todas las instalaciones del sitio, ante fallas de los proveedores de energía. Todo el sistema de suministro eléctrico está reforzado por una serie de UPS's instaladas en cascada, tiempo más que suficiente para activar el generador y asegurar la continuidad del servicio. También se cuenta con tableros eléctricos redundantes de modo de asegurar el funcionamiento antes fallas de la distribución de los equipos.

Respecto a los sitios principal y secundario, sus instalaciones disponen de sistemas de alimentación ininterrumpida con una potencia suficiente para mantener autónomamente la red eléctrica durante los períodos de apagado controlado del sistema y para proteger a los equipos frente a fluctuaciones eléctricas que los pudieran dañar. Ambos sitios cuentan con todos los resguardos necesarios para mantener una continuidad de energía suficiente y su operación por largos periodos de tiempo.

5.2.3 Sistema de Control Ambiental

Ambos sitios cuentan con un suministro continuo de climatización (aire acondicionado, humedad, polvo en suspensión) en modalidad 24x7x365, garantizando el buen funcionamiento de los equipos. Las especificaciones son:

- Temperatura: 21°C+/-3°C.
- Humedad relativa: 45%+/-10%.
- Polvo en suspensión: 75 Microgramos por m3, como máximo.

Para cumplir esta función los sitios cuentan con equipos de climatización precisa que detectan y controlan la humedad relativa del ambiente, lo que permite mantener ambientes óptimos de temperatura y humedad, en las distintas salas. Ambos cuentan además con un sistema redundante de climatización dimensionado para asegurar una temperatura estable y continua a las salas de equipamiento y a las áreas de operación. En caso de fallas del sistema de aire acondicionado, éste cuenta con un sistema de respaldo que garantiza la continuidad del servicio.

5.2.4 Sistema de Extinción y Control de Incendios

Dado los riesgos de incendio a que pueden estar sujetos los sitios, es que tanto el sitio principal como el secundario cuentan con el suministro e instalación de un sistema de protección contraincendios sobre la base de detección temprana que se realiza bajo vía un sistema de aspiración de partículas del ambiente y de extinción automática con FM-200, aprobación UL, e instalado bajo norma NFPA.

5.2.5 Telecomunicaciones

Tomando en cuenta la importancia que tiene la infraestructura de comunicaciones para el negocio de Acepta, es que se ha diseñado en ambos sitios una plataforma robusta, segura y escalable, utilizando como base para ello los servicios WAN, estos servicios provistos por los principales carriers del país, nos aseguran, redes confiables y con tecnología de última generación.

El objetivo principal de este diseño es cumplir con los niveles de servicio comprometidos por Acepta, por lo que se contempla respaldos en todos los puntos críticos. Adicionalmente, cabe destacar que las redes de transporte del carrier están diseñadas para entregar una alta disponibilidad, con una arquitectura redundante interna, lo cual permite garantizar el servicio de conectividad sobre su red.

5.2.6 Seguridad Lógica Data Center

Ambos sitios cuentan los siguientes aspectos de seguridad lógica:

- Múltiple tecnología de firewall
- Sistema de detección de intrusos
- Sistemas de análisis de seguridad activos

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: A cargo de
  - La instalación y configuración de sistemas operativos, de productos de software y del mantenimiento y actualización de los productos y programas instalados. Cuentan con capacidad para configurar y mantener los sistemas, pero sin acceso a los datos.
  - Activar los servicios de CRL, OCSP.
  - Establecer y documentar los procedimientos de monitorización de los sistemas y de los servicios que prestan.
  - Son responsables de la correcta ejecución de la Política de Copias, y en particular, de mantener la información suficiente que permita restaurar eficientemente cualquiera de los sistemas.
  - Debe mantener el inventario de servidores y equipamiento que compone el núcleo de la plataforma de certificación.
- Administrador de Seguridad
  - Debe cumplir y hacer cumplir las políticas de seguridad de Acepta, y debe encargarse de cualquier aspecto relativo a la seguridad de la AC de Acepta, desde seguridad física hasta la seguridad de las aplicaciones, pasando por seguridad de la red. Esta función estará soportada a través de una oficina de seguridad técnica, además del oficial de seguridad.
- Operador de Registro
  - Responsable de realizar el registro presencial ante la solicitud de un certificado de firma, preocupándose de la verificación de identidad del solicitante y la tramitación del certificado.
- Operador de Validación
  - Tiene por función validar el correcto ingreso de una solicitud de certificado, validando la identidad ingresada versus la imagen de los documentos que respaldan dicha identidad. También verificará el pago de la solicitud antes de aprobar la misma.
  - Adicionalmente se encarga de gestionar las suspensiones, revocaciones y renovaciones de certificados.
- Responsable de formación, soporte y comunicación
  - Se encarga del mantenimiento de contenidos de la web de Acepta.

- Se encarga de definir el plan de formación para usuarios finales, para agentes de Call Center y para personal implicado directamente en la operación y administración de la plataforma de certificación de la AC de Acepta.
- Debe revisar mensualmente los ficheros de incidencias y respuestas de Call Center, y revisar los registros de los agentes de Call Center.
- El Responsable de formación, soporte y comunicación contará con la colaboración de las áreas de RRHH, Marketing o Post venta de estimarse necesario.

- Responsable de Seguridad
  - Se asigna esta tarea al Comité de Seguridad de la Información de Acepta, asumiendo la responsabilidad general en cuanto a la actualización e implantación de las políticas y procedimientos de seguridad que han sido aprobadas.
  - Gestionará que los sitios donde se encuentran los sistemas de Acepta, cumplan con gestionar los sistemas de protección perimetral y la correcta gestión de los sistemas de detección de intrusiones (IDS) y de las herramientas asociadas a éstos.
  - Es el responsable de resolver o hacer que se resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, y otras tareas relacionadas.
  - Es responsable de autorizar movimientos de material fuera de las instalaciones de la AC.
  - Debe encargarse de efectuar la selección y determinar la contratación de terceros especialistas que puedan colaborar en la mejora de la seguridad de la AC de Acepta.
- Auditor
  - Encargado de realizar auditorías internas. En definitiva, debe comprobar todos los aspectos recogidos en la política de seguridad, políticas de copias, prácticas de certificación, políticas de certificación, etc. tanto en el núcleo de sistemas de la AC de Acepta y su personal como en los puntos de Registro. Para esta labor se hará uso de Auditores internos como también la contratación de una auditoría externa anual.
- Responsable de Documentación
  - Se encargará de mantener el repositorio de documentación y los archivos de documentación en papel.
  - Controlará que cada área lleve a cabo la actualización de documentos cuando se requiera.
  - Se encargará de mantener actualizado el fichero de índice de documentos y será el único habilitado para almacenar, borrar o modificar documentos en el repositorio de documentación.

5.4 Controles de seguridad del personal

5.4.1 Requerimientos de antecedentes y experiencia

Acepta requiere que todo el personal asociado a la AC cuente con una calificación y experiencia acorde a la prestación de servicios de certificación, de acuerdo a la Ley 19.799 (Chile), sobre documentos electrónicos firma electrónica y certificación de dicha firma.

5.4.2 Comprobación de antecedentes

Mediante CV y entrevistas realizadas al momento de la vinculación.

5.4.3 Requerimientos de formación y reentrenamiento

Como parte de las recomendaciones en que Acepta ha trabajado, se considera para el personal asociado a la AC, cursos de capacitación, los cuales en contenido, duración y fechas estimadas se encuentran descritos en el plan de capacitación anual de Acepta para la AC. Este plan incluirá labores de reentrenamiento de existir cambios tecnológicos, en las políticas o prácticas de certificación o cualquier documento que se considere relevante de ser informado.

5.4.4 Frecuencia de rotación de tareas

No aplica.

5.4.5 Sanciones

Acepta informa y entrega a cada empleado el Reglamento Interno de Orden, Higiene y Seguridad de la empresa, en el cual se establecen las obligaciones de los trabajadores y las sanciones aplicables en caso de incumplimiento de las mismas, atendidas las responsabilidades o funciones de éstos.

5.4.6 Requerimientos de contratación

Todo trabajador de la AC asume obligaciones de confidencialidad, las que están descritas en su contrato de trabajo.

5.4.7 Documentación entregada al personal

El personal de la AC tendrá a su disposición el siguiente material:

- Declaración de Prácticas de Certificación
- Políticas de certificación
- Política de privacidad
- Política de Seguridad de la Información
- Organigrama y funciones del personal

Adicionalmente, se facilitará el acceso a la documentación técnica necesaria para llevar a cabo sus funciones.

5.4.8 Control de cumplimiento

De acuerdo al Plan de seguridad se mide el control de cumplimiento de las actividades programadas de manera anual.

5.4.9 Finalización de contratos

El oficial de seguridad con el apoyo del área de sistemas y RRHH, procederá a:

- Suprimir los privilegios de acceso del individuo a las instalaciones de la organización
- Suprimir los privilegios de acceso del individuo a los Sistemas de Información de la organización
- Supresión de acceso a toda información, a excepción de la considerada PÚBLICA
- Informar al resto de la organización claramente de la marcha de individuo y de su pérdida de privilegios.
- Informar a los proveedores y entidades externas a Acepta la marcha de individuo y de que ya no representa a la AC de Acepta.
- Verificar la devolución del material proporcionado por la Acepta. Por ejemplo:
    - Equipo computacional

- Llaves mobiliario oficinas
- Teléfono móvil
- etc.

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 en los servidores.
- Inicio y detención de la AC.
- 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 suscriptores 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

Acepta implementa una infraestructura y sistema de certificación de tal modo que permita monitorear continuamente las operaciones realizadas; y poder detectar cualquier situación errónea, así como cualquier intento de uso o ingreso no-autorizado al sistema. Dicho monitoreo se realiza continuamente por personal autorizado.

Adicionalmente, se cuenta con una serie de herramientas de prevención y detección de posibles intentos de penetración indebida a los sistemas de certificación y datos o funciones del back-end del sistema. Dichos registros son revisados al menos mensualmente.

5.5.3 Periodo de Retención para el log de auditoría

Todos los registros correspondientes al registro de eventos con el fin de auditoría se mantienen de tal forma que se permita una adecuada consulta y revisión de tales registros por personal autorizado. Por tanto, varios de dichos registros se mantienen on-line, realizándose respaldos increméntales diariamente, así como respaldos completos con una base mensual.

Cada mes se obtiene un respaldo completo el cual es custodiado de manera segura. Para ello, Acepta cuenta con servicios de custodia electrónica de documentos, los cuales se retienen por un período no inferior a 10 años.

5.5.4 Protección del log de auditoría

Toda la información pertinente a auditorías de seguridad se mantiene de manera segura y no es accesible por cualquier persona o proceso computacional, salvo por aquellos estrictamente autorizados.

5.5.5 Procedimientos de respaldo del log de auditoría

Los respaldos de la información de auditoría se realizan acorde a un detallado programa de respaldos aplicable por igual al resto de los datos generados en las operaciones del PSC. Dicho programa contempla respaldos incrementales diarios y respaldos completos una vez al mes.

En los respaldos completos se almacenan los datos en soporte físico y además en dependencias externas al PSC, así como en custodia electrónica en Custodium.com.

5.5.6 Evaluaciones de vulnerabilidad

Con el propósito de mantener un ambiente seguro y confiable, Acepta y sus PSC acreditadas tienen un accionar sistemático y pro-activo respecto a la detección y evaluación de posibles vulnerabilidades que puedan atentar contra dicha seguridad.

Para ello, se mantienen aplicaciones específicas de monitoreo permanente de las operaciones del sistema. Además, se efectúa una adecuada capacitación de todo el personal, sobre sus responsabilidades y conductas respecto a la conservación de un ambiente seguro.

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:

- Registros de auditoría especificados en el punto 5.5 de esta Declaración de Prácticas de Certificación.
- Soportes de backup de los servidores que componen la infraestructura de la AC de Acepta.
- Documentación relativa al ciclo de vida de los certificados, entre la que se encuentra:
  - Contrato de certificación
  - Copia de la documentación de identificación aportada por el solicitante del certificado
  - Identidad del operador de registro y validación que participaron en la emisión del certificado
  - Fecha de solicitud y verificación de identidad del suscriptor
- Acuerdos de confidencialidad
- Contratos suscritos por Acepta en su función de AC
- Autorizaciones de acceso a los Sistemas de Información

5.6.2 Requerimientos para "marca de tiempo" de registros

Todos los registros de auditoría contienen la fecha y hora del servidor de la PSC, para la ocurrencia del evento pertinente.

5.6.3 Sistema de colección de archivos

Los documentos electrónicos aludidos se mantienen en custodia electrónica cerrada para su conservación segura. Cada archivo estará firmado digitalmente por su emisor.

5.6.4 Procedimientos para obtener y verificar información de archivos

La consulta de los documentos electrónicos dejados en custodia electrónica en Acepta, se hace mediante el uso de certificados digitales debidamente autorizados, para garantizar la confidencialidad de la información y autorización requerida.

La verificación de la autenticidad de los documentos electrónicos está dada por la verificación de la firma digital del emisor.

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.

Los certificados firmados por la entidad comprometida, en el periodo comprendido entre el compromiso de la clave y la revocación del certificado correspondiente, serán a su vez revocados, informando a sus suscriptores el hecho y el procediendo para emitir nuevos certificados.

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

En caso de sospecha de haber sido alterados uno de estos recursos, de responsabilidad de Acepta, se detendrá el funcionamiento de los servicios de Acepta hasta el restablecimiento de un entorno seguro, con la incorporación de nuevos componentes. De forma paralela se realizará una auditoría para identificar la causa de la alteración y asegurar la no repetición de la misma.

En el caso de verse afectados certificados emitidos, se notificará del hecho a los suscriptores de los mismos y se procederá a emitir los nuevos certificados.

5.8.2 La clave pública de una entidad se revoca

En el caso de la revocación del certificado de una entidad de Acepta, se generará y publicará la correspondiente lista de revocación y se detendrá el funcionamiento de la entidad, hasta que se proceda a la generación, certificación y puesta en marcha de una nueva entidad con la misma denominación que la eliminada y con un nuevo par de claves.

Las entidades dependientes de la entidad renovada serán informadas del hecho y se solicitará que realicen su re certificación con la nueva instancia de la entidad.

5.8.3 La clave de una entidad se compromete

En el caso de compromiso de la clave de una entidad perteneciente a Acepta, se procederá a su revocación inmediata (como se indica en 5.8.2) y se informará del hecho al resto de entidades dependientes.

Los certificados firmados por entidad comprometida, en el periodo comprendido entre el compromiso de la clave y la revocación del certificado correspondiente, serán a su vez revocados, informando a sus suscriptores y procediendo a emitir ellos.

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

En caso de desastre natural que afecte a las instalaciones del sito principal de Acepta y sus servicios, se procederá a activar el Plan de Continuidad del Servicio y recuperación de desastres.

5.9 Cese de la actividad del PSC

En el evento que Acepta vaya a descontinuar sus operaciones como prestador de servicios de certificación de firma electrónica móvil, deberá comunicar tal situación a los titulares de los certificados por ella emitidos en la siguiente forma:

a) Si el cese es voluntario, con una antelación de a lo menos dos meses y señalando al titular que de no existir objeción a la transferencia de los certificados a otro prestador de servicios de certificación, dentro del plazo de 15 días hábiles contados desde la fecha de la comunicación, se entenderá que el usuario ha consentido en la transferencia de los mismos. En este caso, si el prestador es acreditado, se traspasará los certificados, necesariamente, a un certificador acreditado.

b) Si el cese no es voluntario, la cancelación de la acreditación se comunicará inmediatamente a los titulares. En caso que el prestador de servicios de certificación esté en situación de traspasar los certificados a otro prestador acreditado, se informará tal situación en la forma y plazo señalado en la letra a).

Si el titular del certificado se opone a la transferencia, el certificado quedará sin efecto sin más trámite, que deberá estar acreditado si aquel lo fuera, o a una empresa especializada en la custodia de datos electrónicos, por el tiempo faltante para completar los 6 años desde la emisión de cada certificado. Esta situación deberá verse reflejada en el registro público de prestadores acreditados de servicios de certificación, el que deberá contener el número de la resolución que concede la acreditación, el nombre o razón social del certificador, la dirección social, el nombre de su Representante Legal, el número de su teléfono, su sitio de dominio electrónico y correo electrónico así como la compañía de seguros con que ha contratado la póliza de seguros.

En caso que el cese en la prestación del servicio sea por voluntad del Acepta, deberá solicitar a la Entidad Acreditadora, con al menos un mes de anticipación, la cancelación de su inscripción en el registro público mencionado en párrafo anterior, comunicándole el destino que dará a los datos de los certificados, especificando, en su caso, los que va a transferir y a quién, cuando proceda. El cese de la actividad será registrado como nota de cancelación de la inscripción de la acreditación por la Entidad Acreditadora en el registro público mencionado.

En cualquiera de estos casos, las relaciones entre la PSC y los usuarios seguirán rigiéndose por lo señalado en estas CPS mientras no se ponga en conocimiento de los usuarios un nuevo documento por escrito que venga a sustituir este documento.

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 suscriptor 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 suscriptores, 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

- **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 de suscriptores:** Las claves del suscriptor son generadas por él mismo siendo él quien almacenadas dichas claves en el dispositivo criptográfico (HSM). El proceso de generación de llaves es realizado por el propio suscriptor, quien determina los datos de generación de firma que empleará. Para esta generación se utilizará el número de solicitud proporcionado por Acepta al suscriptor, vía correo electrónico; además de un pin que es ingresado por el propio suscriptor al momento de realizar el registro. Las claves generadas se almacenan en el dispositivo HSM externo, el cual es custodiado y cumple con el estándar mencionado en el punto 6.2.6 de estas prácticas de certificación, así como también con el largo de llave especificado en el punto 6.2.5 del mismo documento. El certificado queda almacenado bajo una OCS virtual proporcionada por el hardware criptográfico, para cada uno de los suscriptores y sólo serán accesibles al suscriptor dueño de la clave.

6.2.2 Entrega de la clave privada a la entidad

No aplica.

6.2.3 Entrega de la clave pública al emisor del certificado

La clave pública es generada por el suscriptor y es entregada a la AC de Acepta mediante el envío de una solicitud de generación de certificado en un formato apropiado (El formato mencionado corresponde al CSR: Certificate Signing Request, formato que sigue la especificación PKCS#10 y que es firmado digitalmente con la clave privada del suscriptor). El certificado solicitado es generado a partir de este requerimiento y firmado digitalmente por la PSC.

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 de ACEPTA, particularmente en el link https://asistencia.acepta.com/firma-avanzada.html.

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 AC, 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

Las claves de las autoridades de certificación AC raíz, así como las diferentes AC intermedias en cada una de las dos jerarquías están creadas con el algoritmo RSA

Los parámetros de generación de claves siguen las recomendaciones FIPS 140-2 Nivel 3.

6.2.7 Comprobación de la calidad de los parámetros

El identificador de algoritmo (AlgorithmIdentifier) que emplea Acepta para firmar los certificados es SHA-2 (algoritmo de hash) con RSA (algoritmo de firma) que corresponde al identificador para "Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc." Aquellos certificados firmados con SHA-1 seguirán vigentes hasta su vencimiento o revocación.

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

Los usos de la clave para cada tipo de certificado emitido por Acepta, vienen definidos por la Política de Certificación que corresponda, siendo el propósito de este par de llaves el identificar al suscriptor y permitirle firmar electrónicamente documentos electrónicos, así como cifrar dichos documentos.

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.

6.3 Protección de la llave privada

Respecto a la protección de las llaves se tiene que:

- **Módulos criptográficos**: El HSM "Hardware Security Module" (Módulo de Seguridad Hardware), es un dispositivo hardware de seguridad criptográfica que genera y protege claves privadas. Los nuevos HSM de Acepta cumplan el criterio FIPS 140-2 Nivel 3 o equivalente.
- **Control multipersona de la llave privada**: Las claves privadas utilizadas por las autoridades de certificación de Acepta y sus jerarquías se encuentran bajo control multipersona, es decir, es necesario un mínimo de 3 personas de un total de 8 para modificar el ambiente criptográfico.
- **Depósito de la llave privada**: La clave privada está cifrada y queda contenida en el repositorio asociado a dispositivo HSM.
- **Copia de respaldo de la llave privada**: Existe un procedimiento de recuperación de claves de los módulos criptográficos HSM de la AC (raíz o intermedias) que se puede aplicar en caso de contingencia. El procedimiento de recuperación de claves de módulos criptográficos corresponde al contexto de procesos certificados que posee el dispositivo HSM.
- **Introducción de la clave privada en el módulo criptográfico**: Las claves privadas se crean en el módulo criptográfico HSM en el momento de la creación de cada una de las entidades de Acepta que hacen uso de dichos módulos.
- **Método de activación de la clave privada**: Las claves privadas de las autoridades de certificación de Acepta y que componen su jerarquías, se activan mediante la inicialización del software de AC y la activación del hardware criptográfico que contiene las claves.
- **Método de desactivación de la clave privada**: Un Administrador puede proceder a la desactivación de la clave privada de las AC de Acepta, mediante la detención del software de la AC.
- **Método de destrucción de la clave privada**: Existe un procedimiento de destrucción de claves de la AC. Los dispositivos criptográficos que contienen las claves privadas creadas por los suscriptores, poseen un procedimiento de destrucción de claves.

6.4 Otros aspectos de gestión del par de claves

- **Archivo de la clave pública**: Los certificados generados por la AC, son almacenados durante el periodo de tiempo mínimo de 10 años.
- **Periodos de utilización de las claves pública y privada**: Corresponde al periodo de vigencia de cada uno de los certificados.

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

Acepta, en lo referente al dominio de la AC, hace uso de procedimientos de pruebas y paso a producción de cualquier cambio que afecta al software de la CA. Estos cambios están regulados por un procedimiento de control de cambio administrado por el área de desarrollo de Acepta. Asimismo, la aplicación del procedimiento para el almacenamiento seguro del hardware criptográfico y los materiales de activación se materializa después de la ceremonia de generación de claves.

6.8 Controles de seguridad de red

Acepta limita el acceso de sus redes al personal debidamente autorizado. En particular:

- Se implementan controles para proteger la red interna de acceso por terceras partes
- Los datos sensibles son cifrados al momento ser intercambiado a través de redes no seguras. Se garantiza que los componentes locales de red están ubicados en entornos seguros

6.9 Controles de seguridad de los módulos criptográficos

Acepta utiliza módulos criptográficos con hardware y software disponibles comercialmente, los cuales son desarrollados por terceros.

Los módulos criptográficos utilizados cuentan con un nivel de certificación de seguridad suficiente para la funcionalidad y seguridad que se exige.

7 Administración de las CPS

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

7.1 Procedimientos para Modificar las CPS

Las prácticas 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, significativo en el contenido de estas prácticas será comunicado al público y suscriptores mediante su publicación en el sitio Web de Acepta en https://sovos.com/es/politicas-y-practicas/.

7.3 Procedimientos de aprobación de las CPS

Estas CPS 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 CPS, 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.