PO02
Prácticas de Certificación
CPS

Documento Público

Acepta.com S.A.

Versión 1.0 - Septiembre 2004

Contacto: Roberto Opazo Gazmuri
Gerente General de Acepta.com
roberto@opazo.cl

Paseo Bulnes 241, piso 5, Santiago, Chile.
Fono: (56 2) 496 8100 Fax: (56 2) 496 8130
www.acepta.com
info@acepta.com

PROPIEDAD INTELECTUAL

El presente documento es propiedad intelectual de Acepta.com.

Se autoriza su lectura, publicación y reproducción total, por cualquier medio, en forma pública o privada, sin necesidad de autorización previa.

Su reproducción parcial se encuentra estrictamente prohibida, a menos que exista una autorización previa y escrita, firmada por representantes legales de Acepta.com cuya firma conjunta sea suficiente para actuar en representación de la empresa.

El único fin para el cual podrá copiarse en forma parcial este documento, sin contar con autorización previa, será cuando se esté citando el documento.

En particular, de deja expresa constancia de que Acepta.com no autoriza la copia de segmentos de este documento para incluirlos en otros documentos que no citen la fuente de la información.

RESUMEN EJECUTIVO

En el siguiente documento se presentan las “Prácticas de Certificación” (CPS, por su sigla en inglés Certification Practice Statement) de Acepta.com. Estas son una descripción detallada de los procedimientos o prácticas que Acepta.com declara convenir en la prestación de sus servicios de certificación, cuando emite y gestiona certificados digitales en su rol de Prestador de Servicios de Certificación (PSC). Además, se incluyen las normas a seguir por las Autoridades de Registro (AR).

Acepta.com emite distintos tipos de certificados, y cada usuario que requiera uno puede elegir el que mas se acomode a sus propias necesidades.

En estas CPS no se muestran los tipos de certificados emitidos por Acepta.com, se trata de un conjunto de prácticas comunes a todos los certificados emitidos. Cada tipo de certificado emitido cuenta con un documento de políticas de certificación propio, el cual explica los elementos que deben conocerse para decidir cuando usarlos y cuando confiar en cada tipo de certificado.

También se describen los procedimientos e infraestructura de Acepta.com que permiten asegurar que el proceso de certificación es llevado a cabo en un ambiente y de una manera segura, que puede dar total confianza a los usuarios de la calidad de los certificados digitales y servicios anexos proporcionados por Acepta.com.

ÍNDICE

1.- INTRODUCCIÓN

En este capítulo se introducen y describen las Prácticas de Certificación (CPS) de Acepta.com. Se muestra un resumen del proceso de certificación, entidades involucradas, y uso de certificados. Por último, se detallan contactos donde obtener información o ayuda adicional.

1.1.- Resumen

Las políticas y prácticas de certificación (CP y CPS), así como las políticas de privacidad, contienen la información más importante que una comunidad de usuarios debe conocer para definir el nivel de confianza que le asigna a cada tipo de certificados. Estos documentos se hacen públicos, para que cualquier usuario tenga acceso a esta información relevante.

Adicionalmente, existen otros documentos importantes para la operación de una empresa que presta servicios de certificación, entre ellos están la evaluación de riesgos, las políticas de seguridad, las políticas del personal, el plan de continuidad operacional y otros que apoyan el correcto funcionamiento de todas las funcionalidades anunciadas en los documentos públicos de la empresa. Estos documentos no son públicos porque su difusión puede comprometer el nivel de seguridad del servicio prestado. Sin embargo, estos documentos existen y son auditados por organismos independientes, especializados y que sean de confianza para toda la comunidad de usuarios.

Acepta.com ha pasado por varios procesos de acreditación realizados por los siguientes organismos independientes de acreditación: Servicios de Impuestos Internos, Servicio Nacional de Aduanas y Ministerio de Economía de Chile. Estas entidades han tenido acceso a todos los documentos de la empresa, han podido revisar los procedimientos seguidos, han entrevistado y evaluado al personal, resolviendo acreditar a Acepta.com.

Las acreditaciones mencionadas son una declaración pública, orientada a que la comunidad de usuarios pueda tener confianza, en que tanto las políticas como las prácticas de certificación coincidan con lo que Acepta.com realmente hace y además, indica que estas políticas y prácticas son suficientemente exigentes como para confiar en los certificados de Acepta.com.

La diferencia entre políticas y prácticas de certificación consiste en que las políticas (CP) son específicas para cada tipo de certificado y muestran información general con respecto a “QUE” es lo que el PSC hace para emitir este tipo particular de certificados. En cambio, las prácticas (CPS) contienen información más precisa sobre “COMO” el PCS realiza ciertas funciones. Las prácticas son comunes para todos los tipos de certificados emitidos.

Las CP no detallan COMO o con que MECANISMOS se cumplen los requisitos establecidos. De esta forma, es posible definir CP que sean compatibles entre distintos PCS que cumplen con estos requisitos usando MECANISMOS diferentes, como ocurre con la firma electrónica avanzada, regulada por la Ley 19.799 de la República de Chile.

Los MECANISMOS y detalles operacionales utilizados para cumplir con cada política señalada en las CP de cada tipo de certificados son explicados en los manuales operacionales del PCS. Estos documentos y los elementos de software y hardware de apoyo correspondientes también son auditados por los organismos acreditadores.

Para poder comparar CP y CPS es necesario que exista algún punto de referencia común que guíe la evaluación. Es por eso que Acepta.com, en su deseo de promover la transparencia y calidad de los certificados que emite, ha adoptado criterios internacionalmente reconocidos en la definición, estructura y presentación de estas prácticas de certificación. Específicamente, es consistente con las recomendaciones surgidas en la Internet Engineering Task Force (IETF)[1] expresadas en el documento denominado "Marco estructural para políticas y prácticas de certificación"[2], las cuales han sido internacionalmente apreciadas por organismos como el Departamento de Defensa de U.S.A y otras agencias federales[3], comisiones de la Comunidad Europea como la Iniciativa para la Estandarización de Firmas Digitales (EESSI)[4], gobierno de Canadá, grupos de trabajo de la APEC[5] como el Electronic Authentication Task Group y variadas autoridades certificadoras internacionales como Entrust, PSCE y Camerfirma de España, IDSafe, BelSIgn, Digital Signature Trust (DST) y NetTrust.

[1] Comunidad internacional compuesta por gran cantidad de ingenieros, diseñadores, vendedores y expertos que investigan y promueven las distintas tendencias, estándares e investigaciones relacionadas con Internet. Entre los estándares que han surgido desde la IETF destacan:

[2] Referenciado como el documento RFC 2527.

[3] Modelo recomendado por el Federal PKI Steering Committee, grupo de expertos trabajando en definir un modelo para agencias federalesen U.S.A.

[4] European Electronic Signature Standardization Initiative (EESSI).

[5] Asia Pacific Economic Cooperation (APEC). Grupo que incluye las mayores economías de la región de Asia y el Pacífico, contando actualmente con 21 países miembros. En el Electronic Authentication Task Group han identificado el modelo propuesto en el documento RFC2527 como estándar para las CPS.

Tales prácticas son las que se prosigue en detallar, y están disponibles en el Sitio WEB de Acepta.com (www.acepta.com) para conocimiento público.

1.1.1.- Estructura de este documento

Una de las características de un buen sistema de certificación es que provee de un ambiente seguro y confiable durante todos los procesos en que se generan y administran certificados digitales. Esto implica que se establezca un sistema con software, hardware, políticas y procedimientos seguros, con disponibilidad y confianza en su diseño y funcionamiento.

Un sistema de certificación de firma electrónica de confianza debe cumplir con los siguientes requisitos:

FIGURA Nº 1 – SISTEMA DE CONFIANZA

Cada uno de esto a establecer cómo los servicios de Acepta.com y sus autoridades de registro operan bajo un sistema e infraestructura de confianza. Cada componente se detalla según el siguiente esquema:

- **Usuarios Informados:** Un sistema confiable debe proporcionar a los usuarios información de tipo y calidad tales que le permitan estar correctamente informado sobre los servicios de certificación ofrecidos. Esto es abordado en los Capítulos Nº1 "*Introducción*", Nº7 "*Formatos de certificados y listas de revocación*" y Nº8 "*Mantención de las CPS*".

- **Ambiente de Operación Seguro:** Se deben efectuar las operaciones de certificación bajo un ambiente seguro y confiable, que establezca todos los resguardos necesarios para proteger la información, recursos y servicios ofrecidos, de manera que se proporcionen certificados de firma electrónica. Esto es abordado en los Capítulos Nº 5 "*Controles de seguridad físicos, de procedimientos y de personal*" y Nº6 "*Controles de seguridad técnicos*".
- **Responsabilidad bien definida:** Un aspecto importante de la confianza es que todas las partes involucradas tengan suficiente claridad respecto a las obligaciones y responsabilidades de cada cual, y así poder anticipar de manera segura las consecuencias y efectos respecto al uso de los certificados digitales bajo cualquier circunstancia. Esto es abordado en el Capítulo Nº 2 "*Consideraciones generales*".
- **Operaciones bien efectuadas:** Un Prestador de Servicios de Certificación debe llevar de manera adecuada dichas operaciones, e informar respecto a todos los procedimientos aplicables. Esto es abordado en el Capítulo 4 "*Requerimientos operacionales*".
- **Autentificación correcta de Identidad:** Un aspecto esencial para establecer la confianza en los certificados emitidos, es que se tomen las medidas adecuadas para acreditar fielmente la identidad de los suscriptores de los certificados. Dichas medidas son abordadas en Capítulo Nº 3 "*Identificación y autentificación*".

Todos estos tópicos son abordados en estas CPS consistentemente con lo estipulado en las guías de la IETF (RFC 2527), diseñadas para guiar en la correcta definición de CP y CPS.

1.1.2.- Llaves públicas y privadas, y certificados digitales

Los certificados digitales son documentos electrónicos que establecen que cierto dato denominado "llave pública" le pertenece exclusivamente a una entidad en particular (individuo, servidor, etc.). Además, dicha llave pública esta ligada de manera única con otro dato, denominado "llave privada", la cual la conoce y mantiene exclusiva y privadamente la entidad dueña del par de llaves. Es decir, dada una llave pública existe una única llave privada correspondiente y viceversa. Además, conociendo sólo la llave pública no es posible derivar y conocer la llave privada asociada.

Por otro lado, estas llaves tienen la particularidad que, mediante el uso de técnicas matemáticas (criptográficas), se puede cifrar[6] información usando para ello cualquiera de las llaves; pero luego sólo se puede recuperar o descifrar la información usando la otra llave correspondiente. Adicionalmente, dado el mecanismo matemático utilizado para generar el par de llaves, se garantiza que dos entidades distintas no generen el mismo par de llaves, por lo tanto, se asegura que la llave privada es única o que su probabilidad de repetición es tan baja que se puede considerar única.

El uso de llaves públicas y privadas permite variadas aplicaciones, como por ejemplo:

Supóngase que dos personas deseasen intercambiar información confidencial; digamos, Andrea y Bernardo.

- **Firma Electrónica**: Si Andrea envía a Bernardo un mensaje cifrado usando su propia llave privada, Bernardo lo puede recuperar usando la llave pública de Andrea, la cual es conocida. Bernardo esta seguro que el mensaje venía de Andrea, pues solo él lo pudo cifrar usando su llave privada. Esto garantiza la autenticidad del autor y que el mensaje no ha sido modificado. A esto se le llama firma electrónica y en la práctica se combina con técnicas denominadas hashing para evitar que las firmas sean tan grandes como los mensajes firmados.
- **Cifrado**: Si Andrea enviase a Bernardo un mensaje cifrado usando la llave pública de Bernardo, esta segura de que sólo Bernardo puede recuperar o leer el mensaje original, pues sólo él tiene la otra llave necesaria para descifrar (la llave privada de Bernardo). Esto garantiza confidencialidad.

En los ejemplos mencionados, un aspecto fundamental es poder garantizar que la llave pública de Bernardo que tiene Andrea sea la que le corresponde a Bernardo realmente, y no sea de un impostor (lo mismo para el caso de Bernardo). Esta garantía es la que brindan los certificados de firma electrónica emitidos por Prestadores de Servicios de Certificación (PSC) como Acepta.com.

Para garantizar que una llave pública le pertenece a cierta persona o entidad, un PSC emite un certificado digital en el cual aparecen una serie de datos de la entidad, como el nombre que la identifica, su llave pública, el periodo de validez de dicho certificado, mas otros datos como el e-mail, restricciones de uso, etc. La

[6] Cifrar es el mecanismo por el cual se transforma un texto en otro texto totalmente ininteligible. Para ello se utiliza cierta información secreta o “llave”, la cual se requerirá posteriormente para descifrar o recuperar el texto a su estado original.

autenticidad de estos datos es asegurada pues el PSC anexa en el mismo certificado su propia "firma digital", tal como se describió en el punto 4 anterior.

La firma correspondiente, luego se puede verificar usando la llave pública del Prestador de Servicios de Certificación, de manera que si alguno de los datos del certificado es alterado en lo más mínimo, la firma se invalida automáticamente.

Garantizadas la autenticidad, integridad y confidencialidad para la transmisión de información firmada digitalmente, se sientan las bases para la no-repudiabilidad, que quiere decir que el autor de un mensaje así firmado no puede negar ni su autoría ni el contenido del propio mensaje.

En resumen, podría decirse que el certificado digital es una especie de "pasaporte electrónico", que luego puede utilizar la entidad para identificarse (por ejemplo, en el contexto de una transacción electrónica, envió de e-mail, etc).

Así, los certificados digitales permiten efectuar comunicaciones electrónicas seguras, proporcionando medios de autenticidad, confidencialidad, no-repudiación e integridad sobre la información transmitida.[7]

Para el formato de los certificados digitales, existe un estándar internacional ampliamente reconocido; denominado "X.509"[8], estándar que Acepta.com ha adoptado en la emisión de sus certificados digitales. Este estándar establece en detalle la estructura de información que contendrán los certificados, y su formato. El uso de un estándar permite que un certificado sea reconocido y compatible con distintas aplicaciones de software y en variados ambientes. Adicionalmente, tales formatos podrán modificarse o adecuarse a la luz de nuevos avances tecnológicos o nuevos estándares.

1.1.3.- Políticas de certificados

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

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

[7] Mas detalles sobre estos conceptos en el Glosario de Términos

[8] Específicamente corresponde al estándar ISO/IEC 9594-8

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

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 titular del certificado. • Estas políticas de certificado han sido acreditadas por el SII y por Aduanas.	• e-mail firmado • e-mail cifrado • Autenticación del usuario 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	• 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 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 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.
Firma de Código	• Constitución legal de la empresa. • Calidad de representante legal del solicitante. • Certificado de vigencia.	• Firmar plugins y otros tipos de programas.
CAF	• Código de autorización de folios firmado por el SII en formato PEM.	• Timbrar electrónicamente Documentos Tributarios Electrónicos.
Cifrado, Grupo o Sistema	• Se evalúa caso a caso y depende del criterio del operador de validación.	• Duran 10 años. • Son útiles para recibir información cifrada. • La información puede cifrarse para todo el grupo de personas que tiene una copia de la llave privada del certificado. • Útiles para interconectar sistemas.

Tabla 1: Tipos de certificados

1.2.- Identificación

El presente documento se denomina “Prácticas de Certificación de Acepta.com”, las que internamente se citan como CPS y están registradas con el número único internacional (OID) 1.3.6.1.4.1.6891.1.

Acepta.com tiene 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.com en un contexto global.

Este documento se encuentra disponible, en forma pública, en www.acepta.com.

Las políticas de las CPS y de cada tipo de certificado están registradas con un número único internacional, llamado Object Indentifier (OID).

La siguiente tabla resume todos los OID administrados por Acepta.com:

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
Políticas de certificados de Grupos y Sistemas	1.3.6.1.4.1.6891.5
Extensión para indicar declaraciones del titular de un certificado X.509	1.3.6.1.4.1.6891.9
Políticas de certificados de Firma de Código	1.3.6.1.4.1.6891.14
Políticas de certificados de CAF	1.3.6.1.4.1.6891.15
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.com para nombrar Servidores.	1.3.6.1.4.1.6891.100.1
Identificador permanente administrado por Acepta.com para nombrar Servicios.	1.3.6.1.4.1.6891.100.2

1.3.- Comunidad de usuarios y aplicabilidad de los certificados

Los servicios de certificados de firma electrónica o clave pública de Acepta.com están insertos en una infraestructura en que se relacionan distintas entidades. Básicamente existen 5 tipos: Autoridad Certificadora o Prestador de Servicios de Certificación (PSC), Autoridades de Registro (AR), titulares, terceras partes que confían en los certificados y entidades acreditadoras.

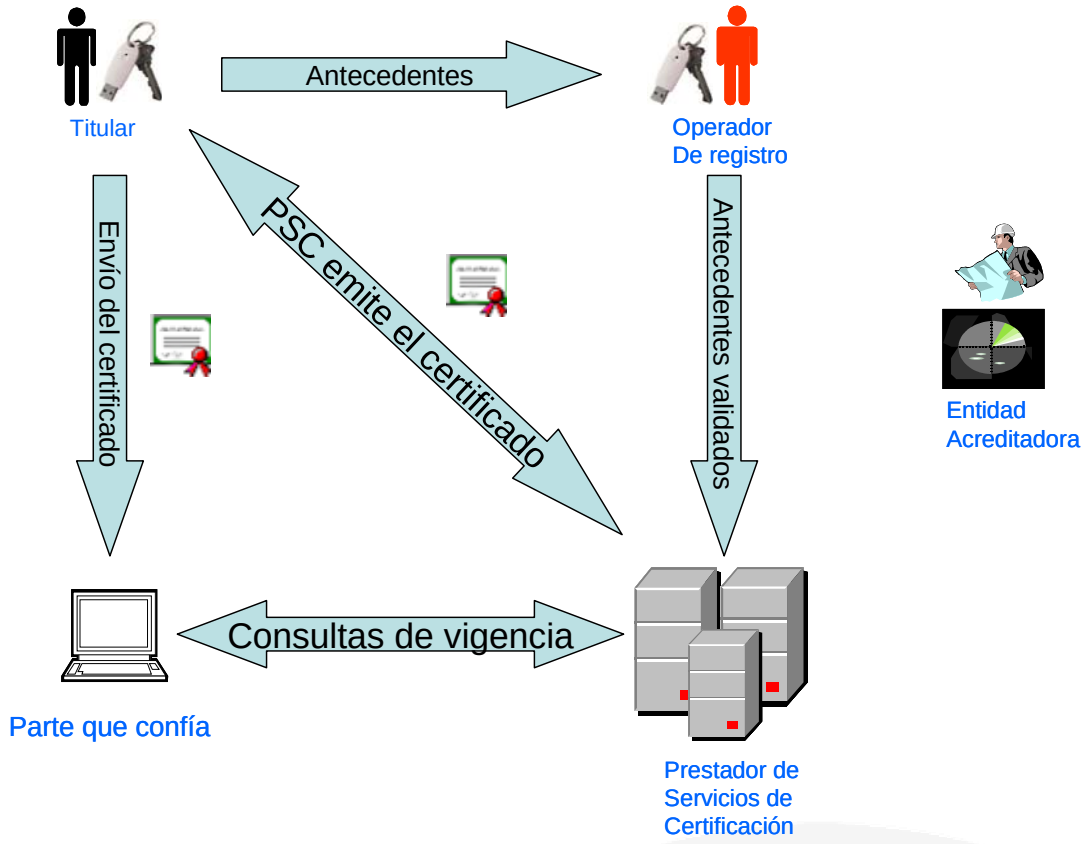

Ilustración 1: Comunidad de usuarios

- **Titulares, usuarios o suscriptores**: Son las personas o entidades que administran la clave privada que le corresponde a la clave pública informada en los certificados de clave pública o certificados de firma electrónica. Antes de obtener el certificado y después de solicitarlo son llamados **solicitantes**.

  Los suscriptores, pueden ser individuos, empresas, sistemas y otro tipo de titulares que se defina en las políticas del certificado correspondiente. Solicitan la emisión de certificados digitales, eligiendo el tipo según sus propias necesidades.

- **Autoridad de registro**: La recepción y procesamiento de las solicitudes de certificados es realizada por una o más "Autoridades de Registro" (AR). Estas efectúan la verificación de los antecedentes y de la identidad de los suscriptores que solicitan certificados. Estas AR son parte de Acepta.com u organismos independientes, pero que establecen y llevan a cabo sus operaciones sobre la base de una acreditación con Acepta.com. En las políticas de cada tipo de certificado se indica cuales son las AR que pueden realizar el registro inicial en cada caso. Esto garantiza que se ofrezca un nivel de servicio consistente con las políticas y prácticas requeridas por Acepta.com.

Cabe señalar que un PSC puede por si mismo realizar el papel de AR, vale decir, recibir directamente las solicitudes de certificados. Por otro lado, para aquellos tipos de certificados que no requieran la presencia personal del suscriptor, las solicitudes y presentación de antecedentes puede realizarse en línea a través del Web.

- **Prestador de Servicios de Certificación o Autoridad Certificadora**: Es la organización que opera y controla el funcionamiento de los procesos de registro, emisión y verificación del estado de certificados. Normalmente es Acepta.com.

  Adicionalmente, Acepta.com puede acreditar a una o más "Autoridades Certificadoras" (PSC), para que emitan certificados, bajo las mismas políticas y procedimientos de Acepta.com. Para ello, Acepta.com emite un certificado del tipo de "Prestador de Servicios de Certificación", con el cual el PSC acreditado puede emitir los certificados digitales a los suscriptores finales.

- **Tercera parte que confía**: Es el receptor de un certificado de firma electrónica o clave pública. Normalmente, junto con el certificado se recibe un documento y su firma electrónica. La parte que confía debe contar con mecanismos que le permitan validar si se trata de un certificado auténtico y si este certificado se encuentra vigente.

- **Entidad Acreditadora**: En algunos tipos de certificados, la comunidad de usuarios requiere de un organismo independiente y de confianza que acredite que las políticas y prácticas del PSC son coherentes con las necesidades de un tipo de certificados en particular y que el PSC cumple cabalmente con dichas políticas y prácticas. Por ejemplo, para los certificados de firma electrónica avanzada la entidad acreditadora es el Ministerio de Economía; para los certificados válidos en el ámbito tributario la entidad acreditadora es el Servicio de Impuestos Internos y para los certificados de sitio Web Acepta.com trabaja sin una entidad acreditadora.

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

1.4.- Contactos

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

Acepta.com
Paseo Bulnes 241, 5º Piso. Santiago Centro – Chile
Teléfono: +56 (2) 688 64 99
Fax: +56 (2) 672 90 87
Código Postal: 6520420
E.-mail: info@acepta.com
Web: http://www.acepta.com

Le recomendamos utilizar los formularios de consulta disponibles en nuestro sitio web. Lamentablemente la proliferación del spam (correo electrónico masivo no solicitado, normalmente comercial) hace que los e-mails enviados a info@acepta.com corran el riesgo de ser confundidos con spam.

2.- CONSIDERACIONES GENERALES

En este capítulo se expresan una serie de tópicos legales y generales, como obligaciones, responsabilidades, tarifas, etc., relevantes para todas las partes interesadas directa o indirectamente con los certificados digitales emitidos por **Acepta.com** o por alguna de sus Autoridades de Registro o Certificadoras acreditadas.

2.1.- Obligaciones

2.1.1.- Obligaciones de Acepta.com

Acepta.com, en su calidad de Prestador de Servicios de Certificación se obliga a realizar las siguientes actividades con todos los tipos de certificados emitidos:

- Registro fidedigno de los antecedentes proporcionados por los suscriptores
- Mantención de un registro electrónico actualizado con la lista de los certificados revocados y/o suspendidos, el cual puede ser consultado públicamente
- Ejecutar todas sus actividades de certificación acorde a las normas estipuladas en éstas CPS y CP pertinente a cada tipo de certificado.
- Expedir o emitir los certificados con mecanismos tecnológicos y criptográficos que garanticen que el proceso de certificación es realizado adecuadamente.
- Revocar unilateralmente los certificados, en los cuales se vea comprometida la confianza respecto a la veracidad de su contenido, y notificar a las partes correspondientes acorde a las normas estipuladas en estas CPS.
- Mantener los resguardos tecnológicos para evitar cualquier falsificación y adulteración de las llaves privadas mantenidas por Acepta.com.

Las obligaciones específicas, pertinentes a cada clase de certificado emitido se detallan en las “Políticas de Certificado” correspondiente, y disponible públicamente en www.acepta.com.

2.1.2.- Obligaciones de autoridades de registro o certificadoras acreditadas

Cada AR o PSC acreditado por Acepta.com deberá cumplir las normas y ser consistente con lo establecido en este documento (CPS), en todas sus actividades. Específicamente, se obliga a:

- Acreditar fidedignamente la identidad de aquellas entidades que soliciten certificados, acorde a los requerimientos estipulados en las políticas de certificados correspondientes.

- Proporcionar antecedentes e información fidedigna al momento de enviar los antecedentes a Acepta.com para su validación y posterior emisión del certificado.
- Mantener bajo adecuadas medidas de seguridad su llave privada, para evitar cualquier compromiso.
- Ser consistente con las normas estipuladas en éstas CPS.

2.1.3.- Obligaciones de los suscriptores

Los suscriptores que soliciten certificados a Acepta.com, se obligan a cumplir con los siguientes requerimientos comunes:

- Conocer las normas estipuladas en las CPS y CP (pertinente a cada tipo de certificado) de Acepta.com, y aceptar lo que allí se estipule en formas previas a la instalación y eventual aceptación de un certificado digital emitido por Acepta.com o alguno de sus PSC acreditadas.
- Conocer y aceptar el propósito y alcance de un certificado obtenido en Acepta.com o en algún Prestador de Servicios de Certificación acreditado, acorde a lo estipulado en las Políticas de Certificados definidas por Acepta.com.
- Proporcionar antecedentes fidedignos requeridos por Acepta.com, las autoridades de registro o certificadoras acreditadas, necesarios para su validación posterior y eventual emisión de los certificados correspondientes.
- Notificación a Acepta.com (o la Autoridad de Registro, o Prestador de Servicios de Certificación acreditada correspondiente) de cualquier modificación de sus antecedentes, que como consecuencia pudiese invalidar uno o más certificados para tal suscriptor.

2.1.4.- Obligaciones de usuarios de certificados

Los usuarios de certificados emitidos por Acepta.com, o cualquier entidad que deposite su confianza en dichos certificados, ya sea en el contexto de una transacción electrónica, transmisión de información, etc., se obligan a aceptar las siguientes condiciones:

- Comprobar previamente en el sitio Web de Acepta.com (o del Prestador de Servicios de Certificación acreditada correspondiente) que el certificado en el que se pretende confiar no ha caducado, o ha sido revocado o suspendido.
- Tener en conocimiento y aceptar el propósito y alcance de un certificado emitido por Acepta.com o por alguna Prestador de Servicios de Certificación

acreditada, acorde a lo estipulado en este documento, y a las políticas de certificados definidas por Acepta.com.[9].

2.1.5.- Obligaciones del repositorio

El repositorio público de Acepta.com permite realizar distintas operaciones dependiendo del tipo de certificado con el que se esté trabajando. Estas alternativas son explicadas en el documento de políticas de cada tipo de certificado.

2.2.- Responsabilidad

Acepta.com no será responsable de cualquier perjuicio que derive de una utilización negligente o no acorde con las políticas establecidas en estas CPS por parte de los suscriptores o terceras partes interesadas.

Los servicios de certificación de Acepta.com no han sido diseñados, autorizados o destinados para su aplicación en transacciones relacionadas con actividades que requieran funcionamiento a prueba de errores, como es el caso de instalaciones nucleares, sistemas de navegación o tráfico aéreo, sistemas de comunicación o de control de armamento, sistemas de equipos médicos o de todo otro sistema digital en que un error pueda conducir a la muerte, a las lesiones de personas, o a daños ambientales. Acepta.com no será responsable en caso de producirse daños por el uso de sus servicios de certificación en ámbitos como los indicados en esta cláusula.

Acepta.com declara que las responsabilidades por ella asumidas en estas CPS y en los contratos o acuerdos de suscripción que a ellas se remitan serán aseguradas y reaseguradas conforme a las prácticas que habitualmente se aplican para los seguros de responsabilidad civil, y en concordancia con lo estipulado por la legislación que exista o llegare a existir. La cobertura señalada no podrá ser invocada directamente por el suscriptor o signatario titular de los certificados digitales, a menos que este sea la parte perjudicada. Los límites de responsabilidad a aplicar en cada tipo de certificado se señalan en las políticas de certificación correspondientes.

2.3.- Responsabilidades financieras

2.3.1.- Indemnizaciones

Las indemnizaciones cubiertas por Acepta.com dependen del tipo de certificado, y están detalladas en las Políticas de Certificado (CP) correspondientes.

[9] Ver sección 1.3 sobre aplicabilidad

2.3.2.- Relaciones comerciales

Acepta.com declara que no es el aval o representante de los suscriptores o terceras partes que utilicen los certificados emitidos por Acepta.com.

Tampoco los suscriptores ni terceras partes tienen autorización para imputar a Acepta.com cualquier obligación o responsabilidad, fuera de las estipuladas en estas CPS.

Acepta.com tiene instalados sus servidores en el Telefónica Internet Center (TIC).

El Servicio de Registro Civil e Identificación de Chile brinda el servicio de verificación de identidad para certificados de firma electrónica simple y avanzada emitidos por Acepta.com.

2.4.- Interpretación y legislación aplicable

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

En particular, declara dar estricto cumplimiento a la Ley Nº 19.496, sobre Protección de los Derechos de los Consumidores y Nº 19.628, sobre Protección de la Vida Privada.

Todas y cualquier controversia que se suscite entre Acepta.com y los suscriptores o signatarios que suscriban él (los) respectivo(s) contrato(s) de certificación o los terceros interesados o usuarios que adhieran a las CPS y reconozcan por ende la validez de sus certificados digitales, con motivo de la interpretación, aplicación, ejecución, vigencia, cumplimiento, incumplimiento o terminación de los servicios prestados por Acepta.com y del contenido de las presentes CPS, serán resueltas por un árbitro arbitrador, sin forma de juicio y sin ulterior recurso, renunciando desde ya a todos los recursos legales, incluso el de casación en la forma.

El Arbitro será nombrado por las partes de común acuerdo y, en caso de no haberlo dentro de quince días de la solicitud escrita de cualquiera de ellas, será designado por la Justicia Ordinaria, debiendo en tal caso 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 los que hubieren prestado sus servicios a cualquier titulo a alguna de las partes.

2.5.- Tarifas

Las tarifas cobradas por Acepta.com dependen del tipo de certificado, y están detalladas en las Políticas de Certificado (CP) correspondiente.

2.6.- Publicaciones

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

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

Acepta.com 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.

Sin perjuicio de lo anterior, Acepta.com se exime de toda obligación y responsabilidad cuando por razones de fuerza mayor o caso fortuito, como terremotos, actos terroristas, cortes de energía eléctrica, falla en proveedores de acceso a Internet, actos de Estado y otros, no sea posible consultar el estado de algún certificado.

La información de certificados emitidos queda disponible en el repositorio público en el mismo momento en el que se emite cada certificado.

La información de revocación o suspensión, es ingresada a la base de datos de Acepta.com usando aplicaciones operadas por funcionarios que validan la información. El tiempo transcurrido desde que se solicita revocar o suspender un certificado hasta que se actualiza la base datos no puede exceder 6 horas laborales, en un horario de 9:00 AM a 19:00 PM de lunes a domingo.

La información de validación en línea de certificados está directamente conectada con la base de datos de revocaciones y suspensiones, por lo que queda actualizada en cuanto se ingresan las solicitudes al sistema.

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

2.7.- Conformidad con auditorias

Con el fin de dar transparencia a los usuarios e interesados en los cerificados emitidos por Acepta.com, y garantizar la calidad de los certificados y de las

prácticas seguidas en el proceso de certificación, es que Acepta.com adhiere a la certificación y realización de auditorias externas e independientes a sus prácticas internas. Tales auditorias serán realizadas por organismos competentes definidos para cada tipo de certificado.

Actualmente, las prácticas de certificación de Acepta.com son acreditadas por los siguientes organismos:

Política Base del Certificado	Entidad Acreditadora
Clase 3	Servicio de Impuestos Internos de Chile
Clase 3	Servicio Nacional de Aduanas de Chile
Firma Electrónica Avanzada	Subsecretaría de Economía, Fomento y Reconstrucción de Chile

En todos estos casos, se ha puesto ha disposición del órgano acreditador los antecedentes legales de la empresa, entrevistas con el personal, visitas de inspección, las políticas de privacidad, la política de seguridad, el documento de valoración de riesgos de la empresa, el plan de continuidad del negocio, el plan de recuperación de desastres, el plan de seguridad de sistemas, el plan de administración de llaves, las políticas de certificados, las prácticas de certificación, el modelo operacional, el manual de operaciones, las políticas generales de contratación del personal, las políticas del oficial de seguridad y otros documentos solicitados especialmente por cada órgano acreditador.

2.8.- Confidencialidad

Acepta.com, adhiere y efectúa sus operaciones en conformidad con lo establecido por la Nº 19.628, sobre Protección de la Vida Privada.

Las políticas de privacidad de Acepta.com se encuentran publicadas en www.acepta.com.

2.9.- Derechos de propiedad intelectual

Todos los documentos y programas utilizados por Acepta.com en la Prestación de Servicios de Certificación son propiedad intelectual de Acepta.com.

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

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

4.- REQUERIMIENTOS OPERACIONALES

En este capítulo se describen los requisitos operativos pertinentes a las etapas de certificación, desde el registro inicial hasta su aceptación y emisión. Además, se describe el mecanismo de revocaciones y/o suspensiones, así como los procedimientos de auditoría y

4.1.- Solicitud de certificados

La forma en que debe ser solicitado cada tipo de certificado está indicada en las políticas del tipo de certificado.

4.2.- Emisión de certificados

Los métodos usados para emitir cada tipo de certificado están indicados en las políticas del tipo de certificados.

4.3.- Aceptación de certificados

Los procedimientos mediante el titular de cada tipo de certificado acepta el certificado emitido están indicados en las políticas de cada tipo de certificado.

4.4.- Suspensión y revocación de certificados

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

4.5.- Procedimientos de auditoria de seguridad

4.5.1.- Tipos de eventos registrados

Los tipos de eventos registrados dependen de las políticas señaladas para cada tipo de certificado.

4.5.2.- Frecuencia de procesamiento del log

Acepta.com 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 cuentan 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 semanalmente.

4.5.3.- 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 semanal.

Cada mes se obtiene un respaldo completo el cual es custodiado de manera segura. Para ello, Acepta.com cuenta con los servicios de Custodium.com, el cual brinda custodia electrónica segura de documentos, los cuales se retienen por un período de al menos 10 años.

4.5.4.- 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.

Para proteger los documentos de auditoría se utilizan los servicios de custodia electrónica de Custodium.com, en el cual se almacenan los documentos encriptados. Además, el acceso está restringido sólo a personas autorizadas, las cuales deben autentificarse mediante su correspondiente certificado de firma electrónica.

4.5.5.- 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 increméntales diarios, semanales 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.

4.5.6.- Evaluaciones de vulnerabilidad

Con el propósito de mantener un ambiente seguro y confiable, Acepta.com 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.

Por otro lado, Acepta.com mantiene un programa formal de “Evaluación de vulnerabilidades”, en que se realizan pruebas y ataques a sistemas especialmente diseñados para pruebas (sistemas “bastión”), con el fin de detectar posibles vulnerabilidades. Este programa contempla el accionar de

agentes externos, en el contexto de colaboraciones, en la cual se acuerda efectuar ciertos ataques o pruebas específicas bajo un ambiente controlado.

4.6.- Políticas para archivo de registros

4.6.1.- 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. El detalle de los documentos archivados está explícito en las Políticas de Certificado (CP) asociadas a cada clase de certificado emitido. Estas CP están disponibles en www.acepta.com.

4.6.2.- Requerimientos para "time-stamping" de registros

Todos los registros de auditoría contienen la fecha y hora de ocurrencia del evento pertinente.

4.6.3.- Sistema de colección de archivos

Los documentos electrónicos aludidos en la sección 4.8.1 se deberán mantener en custodia electrónica cerrada para su conservación segura. Cada archivo estará firmado digitalmente por su emisor.

4.6.4.- Procedimientos para obtener y verificar información de archivos

La consulta de los documentos electrónicos dejados en custodia electrónica en Custodium.com deberá hacerse 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 estará dada por la verificación de la firma digital del emisor.

4.7.- Procedimientos para cambios de las claves

La forma en que son cambiadas las llaves de los titulares de certificados se señalan en las políticas de cada tipo de certificado.

Los certificados de las autoridades certificadoras intermedias y el certificado raíz de Acepta.com son cambiados una vez cada 7 años, medidos con respecto a la fecha de generación de la raíz de Acepta.com. Cuando se reemplazan estos certificados, se crean certificados nuevos, pertenecientes a una estructura jerárquica completamente nueva, cumpliendo con todas las formalidades de generación de llaves definidas para cada tipo de Autoridad Certificadora.

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

Las claves de las autoridades certificadoras reemplazadas siguen generando listas de revocación y respondiendo a consultas OCSP hasta cumplir 10 años de operación, 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.

4.8.- Planes de contingencia y recuperación

4.8.1.- Corrupción de recursos computacionales

En la eventualidad de producirse alguna contingencia que corrompa algunos de los recursos computacionales que afecten el normal funcionamiento de los servicios de certificación, se deberá proceder como sigue:

En primer lugar, se deben restaurar los recursos computacionales alterados para dar inicio a la etapa de recuperación.

1.- Llave privada no comprometida y en respaldo seguro

Si la llave privada de Acepta.com todavía se mantiene de manera segura y no existe riesgo de compromiso o revelación, se deberá re-establecer las operaciones de la manera más rápida posible, utilizando los medios de respaldo disponibles, dando prioridad a las funcionalidades de revocación y suspensión de certificados.

Para recuperar las llaves privadas de Acepta.com cuando no existen copias legibles de archivos de respaldo, el Administrador de Operaciones del sitio de Acepta.com deberá notificar de una manera segura (out-the-band) a 2 de los directores de la empresa, respecto a la necesidad de recuperar la llave privada. Dichos directores son las únicas personas autorizadas para recuperar el respaldo de la llave privada raíz de Acepta.com, la cual se mantiene en custodia segura en sendas placas de aluminio.

Tales directores se deberán dirigir a los correspondientes lugares de custodia y recuperar las placas de aluminio en donde están impresas las llaves privadas. Una vez en el sitio de Acepta.com, se procede a realizar la “ceremonia de recuperación de llaves”.

En primer lugar, el Administrador de Operaciones procede a reiniciar los equipos y activar el módulo criptográfico de recuperación de llaves. Este módulo se encarga de recibir la secuencia completa de la llave, verificarla y posteriormente activar la llave para que quede operativa.

Luego, sólo los directores se reúnen privadamente en el site de Acepta.com, junto con las placas de aluminio con las llaves, y proceden a digitar la inscripción

estampada en la placa de aluminio directamente en el módulo criptográfico de recuperación de llaves.

Una vez digitada y verificada la llave privada raíz de Acepta.com, el módulo procede a activarla y a generar el resto de las llaves correspondientes a los distintos tipos de certificados emitidos por Acepta.com, según la jerarquía explicada en la sección 1.1.5 ("Infraestructura de certificados digitales de clave pública").

Si no es factible re-establecer las funcionalidades de revocación en un periodo inferior a 48 horas, se deberá regenerar las llaves públicas y privadas de Acepta.com y de todos los suscriptores vigentes. En este caso se procederá a notificar en primer lugar por e-mail a todas las entidades involucradas respecto a la necesidad de una re-emisión de certificados.

2.- Regeneración de la llave privada de Acepta.com

En el caso de que Acepta.com y sus PSC acreditados, el par de llaves es generado en forma segura en una habitación especial usando un dispositivo físicos de respaldo, tal como se describe en la sección 6.1.2.

4.8.2.- Revocación de llaves públicas

Si se declara como comprometida las llave privada de Acepta.com, se deberán revocar todos los certificados vigentes y re-emitirlos con una nueva llave.

Todos los usuarios deberán ser comunicados por e-mail.

Además, se deberá pagar un inserto en un medio de difusión masivo comunicando la situación.

4.8.3.- Instalaciones de seguridad frente a desastres naturales

Acepta.com y sus PSC acreditados mantienen ubicaciones externas para mantener toda la información y recursos de respaldo suficientes que permitan re-establecer las operaciones normales de certificación en un periodo no inferior a 48 hrs., en la eventualidad de un desastre natural.

4.9.- Término de las actividades de Acepta.com como PSC

En el evento que Acepta.com vaya a descontinuar sus operaciones como Prestador de Servicios de Certificación, procederá a notificar por escrito y con la debida antelación a todas las partes involucradas con sus servicios de certificación: suscriptores, autoridades de registro y certificadoras acreditadas.

El procedimiento a seguir para el término de actividades, así como las medidas a tomar para el archivo de los registros y documentación necesaria, estará en conformidad con la ley aplicable de la República de Chile.

Algunos tipos de certificados, como el de firma electrónica avanzada, definen medidas adicionales en sus políticas de certificación.

5.- CONTROLES DE PROCEDIMIENTO, PERSONAL Y FÍSICOS

En este capítulo se detallan los controles y procedimientos establecidos para garantizar una operación de los servicios de certificación bajo un ambiente seguro, desde el punto de vista de la seguridad de las dependencias físicas, y las conductas y capacidad del personal. También se mencionan las capacidades de recuperación frente a desastres.

5.1.- Controles Físicos

Los servidores de Acpepta.com utilizados para brindar servicios de certificación, se encuentra físicamente ubicados en el Telefónica Internet Center (TIC), el cual cuenta con la certificación internacional de seguridad de TruSecure.

El TIC cuenta con instalaciones óptimas de seguridad y ha sido acreditado considerando aspectos físicos, lógicos y de políticas internas.

Desde el punto de vista físico, este cuenta con infraestructura de alta calidad en cuanto a:

- Ubicación del Site y calidad de la construcción arquitectónica.
- Controles de acceso físico.
- Energía eléctrica y aire acondicionado.
- Protección contra inundaciones.
- Sistemas de detección y extinción automática de incendios.
- Medios de almacenamiento.
- Dispositivos de eliminación de desechos.

5.2.- Controles del personal

Los controles del personal de Acepta.com están detallados en el documento denominado “Manual de Operaciones del Prestador de Servicios de Certificación”, el cual es por naturaleza confidencial, pero ha sido puesto a disposición de los órganos acreditadores de Acepta.com.

En este manual se detallan varios aspectos relevantes para brindar un servicio de calidad, entre otros:

- Los roles de usuarios requeridos para brindar los servicios de certificación.
- Los procedimientos de evaluación del personal.
- Los procedimientos de capacitación del personal.

6.- CONTROLES DE SEGURIDAD TÉCNICA

En este capítulo se describen una serie de controles de carácter técnico que permiten mantener un ambiente de operación seguro, tanto en la generación y administración de los certificados y llaves asociadas a la autoridad certificadora raíz de Acepta.com, así como sus Autoridades Certificadoras Intermedias. Los controles de seguridad técnicos asociados a las llaves de cada tipo de certificado emitido por las autoridades certificadoras intermedias son explicados en las políticas de certificados de cada tipo de certificados.

Todo el proceso de generación, respaldo y recuperación de las llaves criptográficas de la AC Raíz de Acepta.com y sus AC Intermedias se encuentra descrito en un documento confidencial llamado “Manual de Operaciones de Acepta.com”. Este documento y su cumplimiento por parte de Acepta.com ha sido auditado por los organismos acreditadores de Acepta.com.

6.1.- Entrega de la llave pública de Acepta.com a usuarios

La llave pública de Acepta.com es proporcionada a los usuarios durante el proceso de instalación de los certificados, el cual instala automáticamente el certificado raíz de Acepta.com y el certificado de la AC Intermedia de Firma Electrónica Avanza.

Las partes que confían pueden descargar el certificado Raíz de Acepta.com y todos los certificados de AC intermedias desde www.acepta.com.

Algunas políticas de certificados de Acepta.com pueden indicar otras formas de obtención de los certificados de AC Intermedia correspondiente.

Los usuarios que deseen realizar una inspección visual para validar la llave pública del certificado Raíz de Acepta.com deben comparar los siguientes datos con la Raíz que hayan instalado:

```
30 82 01 08 02 82 01 01 00 c1 18 43 f3 7c b3 d3 c3 46 b4 5a a8 a6 c7 18 39 4d f4 b3
fb f8 4d c7 27 43 e8 03 22 ba 80 e2 57 c9 57 91 64 72 c0 d5 50 d2 e4 82 66 48 a9 9c
e4 12 bc f0 3b 6b 8e 29 00 d1 a5 ec ef a0 04 01 24 cf 72 fb a1 d4 af b2 41 16 7d 30
53 df 06 ec 45 91 6c 8b 4e 85 c7 91 6a b9 89 ad 96 d1 81 b2 04 88 24 6b dc dd 70 29
9d 2a bf 29 8e 80 2e 3e 0c 4c 7d 5a 3b df 02 95 7a 62 62 8e 30 c6 d6 2a 38 a9 47 37
47 2f 48 94 2d 55 da 7e bc e1 44 80 fa 06 70 d1 89 b1 ed ce 04 4c 87 e8 cb 95 31 21
5c d0 8a 4b e6 a9 0f 2b bb f5 c0 f5 0e 6b c6 6f 40 02 d3 b9 ea 04 cc bc fe ba b2 e5
3f c3 02 05 91 a3 54 39 b9 d6 16 fd ac ec d1 5f 1d 33 89 de b3 73 06 09 d8 1d 3c 18
5f 02 92 d4 d4 19 76 c3 8f ca 4e f8 8a 08 e6 54 f4 e1 05 a7 12 b5 36 d3 1f dd 54 67
f8 46 71 50 78 21 c5 94 b5 bd c7 d6 6b 02 01 03.
```

6.2.- Tamaño de las claves y duración de las AC

La siguiente tabla lista las autoridades certificadoras de la jerarquía de confianza de Acepta.com y el período de vigencia de su certificado:

Tipo	Bits de la llave privada	Años de vigencia
Raíz de Acepta.com	2.048	10
Clase 3 Persona Natural	2.048	Expira 5 minutos antes que la Raíz de Acepta.com.
FA Firma Electrónica Avanzada	2048	Expira 5 minutos antes que la Raíz de Acepta.com.
Sitio Web	2.048	Expira 5 minutos antes que la Raíz de Acepta.com.
Firma de Código	2.048	Expira 5 minutos antes que la Raíz de Acepta.com.
CAF	2.048	Expira 5 minutos antes que la Raíz de Acepta.com.
Cifrado, Grupo o Sistema	2.048	Expira 5 minutos antes que la Raíz de Acepta.com.

7.- PERFILES DE CERTIFICADOS Y DEL REGISTRO DE ACCESO PÚBLICO

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

7.1.- Composición del certificado raíz de Acepta.com

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.com	00
Algoritmo de Firma	Algoritmo utilizado por el PSC para firmar el certificado	SHA-1 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 de el 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. Firma Electrónica Avanzada Test CA
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 titular	Nombre distintivo (DN) del titular 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. Firma Electrónica Avanzada Test CA
Clave pública	Clave pública del titular 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.com

Tipo	Nombre	Descripción	OID	Valor
RES	KeyUsage	Esta extensión define el propósito para el	2.5.29.15	Firma de certificados,

		cual deben ser usadas las claves correspondientes al certificado. El certificado debe ser utilizado sólo para los propósitos definidos por esta extensión.		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.com 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 de el 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	Ver sección 7.1.6		[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.6891.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://www.acepta.com/CPS/ [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 esta sujeta a las políticas de certificado (CP) y prácticas de certificación (CPS) establecidas por Acepta.com, y disponibles públicamente en

				www.acepta.com.
INF	IssuerAltName	Identificador alternativo del emisor, corresponde al RUT de Acepta.com, 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 sujeto o titular 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 deAcepta.com

7.2.- Composición de las listas de revocación

El certificado raíz de Acepta.com y sus AC Intermedias no puede ser revocado. Existen otros mecanismos definidos en estas PCS para abordar problemas de compromiso de la llave privada de la Raíz de Acepta.com o alguna AC Intermedia.

Las estructuras de las listas de revocación de los certificados firmados por las AC Intermedias de Acepta.com se encuentran detalladas en las respectivas políticas de certificación.

8.- ESPECIFICACIONES DE ADMINISTRACIÓN DE LA POLÍTICA DE CERTIFICACIÓN

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

8.1.- Procedimientos para cambios en 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.

8.2.- Publicación y notificación

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

8.3.- Procedimientos de aprobación de las CPS

Estas CPS y las subsecuentes versiones futuras de éste documento están sujetas a la aprobación del directorio de Acepta.com.