PRÁCTICAS DE CERTIFICACIÓN (CPS)
Versión 1.0

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

TABLA DE CONTENIDO

ÍNDICE DE TABLAS Y FIGURAS

AGRADECIMIENTOS

Se reconoce la participación en la creación, desarrollo y revisión de este documento al Sr. Roberto Opazo Gazmuri, Director y Gerente General de **Acepta.com**, y al Sr. Juan Carlos Pérez Aguayo, Gerente de Tecnología de **Acepta.com**.

Adicionalmente, se reconoce su valiosos aporte en sus comentarios y revisión de este documento a las siguientes personas:

RESUMEN EJECUTIVO

En el siguiente documento se presentan las "Prácticas de Certificación" (CPS) de **Acepta.com**. Estas son una descripción detallada de las normas 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 Autoridad Certificadora (AC). Además, se incluyen las normas a seguir por las Autoridades de Registro (AR) y Autoridades Certificadoras que efectúen sus labores debidamente acreditadas.

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 se muestran los tipos de certificados emitidos por **Acepta.com**, y el proceso que se debe seguir para obtener uno. Cada certificado es emitido por un cierto periodo, durante el cual puede eventualmente ser cancelado o invalidado por el suscriptor. Para ello, también se explican los distintos mecanismos que pueden ser utilizados por cualquier usuario para consultar por la validez de un certificado.

Por otro lado, en este documento también se especifican claramente las obligaciones y responsabilidades que son adquiridas en el momento de solicitar y obtener un certificado digital, para claridad y conocimiento de todos los usuarios.

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**.

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

1.1.1 Sobre las Prácticas de Certificación

En este documento se presentan las "Prácticas de Certificación" (CPS)[1] de **Acepta.com**. Estas son una descripción detallada de las normas o prácticas que **Acepta.com** declara convenir en la prestación de sus servicios de certificación, cuando emite y gestiona certificados electrónicos o digitales en su rol de Autoridad Certificadora (AC). Además, se incluyen las normas a seguir por las Autoridades de Registro (AR) y Autoridades Certificadoras que efectúen sus labores debidamente acreditadas por **Acepta.com**.

Al emitir un certificado digital, una Autoridad Certificadora establece cierto nivel de seguridad a todos los agentes que depositarán su confianza en la validez de dicho certificado, como instrumento que da garantías sobre la identidad del titular del mismo. En ese sentido, establece que se han tomado las medidas y procedimientos adecuados para constituir la correspondencia entre dicho certificado y una cierta entidad en particular (individuo, servidor, etc.)

Un mecanismo para evaluar la calidad y grado de confianza que se puede depositar en un certificado digital, es a través de la revisión de las prácticas usadas por la autoridad certificadora para emitir dicho certificado, es decir, las CPS. Asimismo, también es relevante poder distinguir que práctica es mejor que otra, así como el grado de reconocimiento que dichas practicas puedan tener en distintas comunidades y ambientes.

Por otro lado, para poder comparar 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)[2] expresadas en el documento denominado "Marco estructural para políticas y prácticas de certificación"[3], las cuales han sido internacionalmente apreciadas por organismos como el Departamento de Defensa de U.S.A y otras agencias federales[4], comisiones de la Comunidad Europea como la Iniciativa para la

[1] CPS, por su sigla en Inglés de Certification Practices Statement en Ingles

[2] 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:

[3] Referenciado como el documento RFC2527.

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

Estandarización de Firmas Digitales (EESSI)[5], gobierno de Canadá, grupos de trabajo de la APEC[6] como el Electronic Authentication Task Group y variadas autoridades certificadoras internacionales como Entrust, ACE y Camerfirma de España, IDSafe, BelSIgn, Digital Signature Trust (DST) y NetTrust.

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

1.1.2 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 identidades digitales de confianza puede visualizarse como compuesto por una serie de requerimientos:

FIGURA Nº 1 – SISTEMA DE CONFIANZA

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

[6] 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.

Cada uno de éstos componentes es abordado en estas CPS para establecer cómo los servicios de **Acepta.com**, sus autoridades de registro y certificadoras acreditadas 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 identidad confiables. 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:** Una autoridad certificadora 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 que son abordados en estas CPS son detallados consistentemente con lo estipulado en las guías de la IETF (RFC2527) mencionadas anteriormente.

1.1.3 Llaves públicas y privadas, y certificados digitales

Los certificados digitales básicamente 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 publica 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[7] información usando para ello cualquiera de las llaves; pero luego sólo se puede recuperar o descifrarla información usando el otro par de llave correspondiente.

[7] 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.

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. Esto permite que por medio de ésta llave privada se establezca un medio seguro para la autentificación de la identidad de la entidades, de una manera electrónica.

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

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

1.- Si Bernardo envía a Carolina un mensaje cifrado usando su propia llave privada, Carolina lo puede recuperar usando la llave pública de Bernardo, la cual es conocida. Carolina esta segura que el mensaje venía de Bernardo, pues solo él lo pudo cifrar usando su llave privada. Esto garantiza la autenticidad.

2.- Asimismo, si Bernardo enviase a Carolina un mensaje cifrado usando la llave pública de Carolina, esta seguro que sólo Carolina puede recuperar o leer el mensaje, pues solo ella tiene el otro par de la llave necesario para descifrar (la llave privada de Carolina). Esto garantiza confidencialidad.

3.- Por otro lado, existe una técnica matemática que permite que, a partir de un conjunto de datos, generar otro conjunto denominado "hash", que es un aespecie de "resumen" de los datos, con la particularidad que si alguno de los datos originales es modificado, el hash automáticamente cambia de valor en gran medida.

Esta técnica garantiza que no es posible que a partir de 2 conjuntos de datos diferentes, por ejemplo, 2 documentos distintos, generar el mismo hash. Necesariamente los hash deben ser distintos.

Si el usuario receptor de un mensaje, recibe también el hash, puede verificar si el mensaje ha sido modificado, generando él mismo el hash y comparándolo con el que recibe. Si son distintos, quiere decir que el mensaje ha sido modificado y no corresponde al original. Esto garantiza la integridad de la información enviada.

4.- Si se genera el hash de cierto documento, y luego se cifra dicho hash y se envía de manera confidencial a otra persona, usando la técnica descrita en el punto 1 anterior, se obtiene lo que se denomina "firma digital". Es decir, esta no es mas que el hash cifrado con la llave privada del autor del mensaje o documento. Al usar la llave privada se garantiza la autenticidad, tal como se describió en el punto 2 anterior.

En los ejemplos mencionados, un aspecto fundamental es poder garantizar que la llave publica de Carolina que tiene Bernardo sea la que le corresponde a Carolina realmente, y no de una impostora (lo mismo para el caso de Carolina). Esta garantía es la que brindan los certificados digitales de identidad emitidos por Autoridades Certificadoras (AC) como **Acepta.com**.

Para garantizar que una llave pública le pertenece a cierta entidad, una AC 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 autenticidad de estos datos es asegurada pues la AC anexa en el mismo certificado su propia "firma digital", tal como se describión el el punto 4 anterior.

La firma correspondiente luego se puede verificar usando la llave pública de la Autoridad Certificadora, de manera que si alguno de los datos del certificado es alterado en lo mas mínimo, la firma se invalida automáticamente (pues el hash no correspondera).

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.[8]

Para el formato de los certificados digitales, existe un estándar internacional ampliamente reconocido; denominado "X.509"[9], 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.

1.1.4 Políticas de certificados

Acepta.com emite distintas 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** define 6 políticas de certificados, una para cada tipo de certificado.[10]

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

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

[10] Mas detalles en la sección 1.3

A continuación se muestra un resumen de los tipos de certificados emitidos por **Acepta.com** :[11]

DESCRIPCIÓN DE TIPOS DE CERTIFICADOS			
Tipo	***Política de certificado***	***Características generales***	***Usos típicos***[12]
Clase 2 de persona	Política de certificado para clase 2 de persona . Documento disponible en www.acepta.com	No requiere presencia personal del suscriptor para acreditar su identidad. La autentificación de la identidad es realizada utilizando la información proporcionada por algún medio externo, el cual acredita la identidad del suscriptor. Por ejemplo, un banco o institución financiera que acredita la identidad de sus clientes.	Correo electrónico seguro Transacciones comerciales de bajo riesgo con monto máximo limitado Autentificación en sitio Web
Clase 3 de persona	Política de certificado para clase 3 de persona. Documento disponible en www.acepta.com	Requiere presencia personal para autentificar la identidad Se registra foto, huella digital y firma holográfica de la persona	Comercio electrónico Servicios de suscripción Correo electrónico seguro Autentificación en sitio Web
Para autoridades acreditadas	Política de certificado para AC acreditada. Documento disponible en www.acepta.com	Requiere presencia personal de representante legal Contrato formal con la AC	Emisión y firma de certificados de usuarios finales
Para servidor de empresas	Política de certificado para servidor seguro. Documento disponible en www.acepta.com	Confirmación externa de identidad de empresa asociada al servidor Validación de identidad del servidor con autoridades de registro de nombres de dominio	Autentificación de servidor Comercio electrónico
Para notarización electrónica	Política de certificado para notarización. Documento disponible en www.acepta.com	Distintos agentes que firman documentos, cada uno identificado por su correspondiente certificado digital	Firma de documentos Acuerdo de contratos on-line
Para firma de programas de software	Política de certificado para firma de código. Documento disponible en www.acepta.com	Requiere revisión y validación del s oftware por parte de la AC	Distribución segura de programas de software

TABLA Nº1 – TIPOS DE CERTIFICADOS

[11] Para mas detalles, ver sección 1.3.5 y capítulo 7

[12] No significa un recomendación de uso exhaustiva por parte de **Acepta.com**, sólo ejemplos ilustrativos

1.1.5 Infraestructura de certificados digitales de clave pública

Los servicios de certificados digitales de **Acepta.com** están insertos en una infraestructura en que se relacionan distintas entidades. Básicamente existen 4 tipos: Autoridades Certificadoras (AC), Autoridades de Registro (AR), suscriptores y usuarios. Los suscriptores son los que solicitan certificados digitales para acreditar su propia identidad, y los usuarios o "terceras partes confiables" son aquellas entidades que en determinado momento reciben certificados digitales y deben decidir si depositan su confianza en ellos. Un esquema general de dicha infraestructura puede visualizarse a continuación:

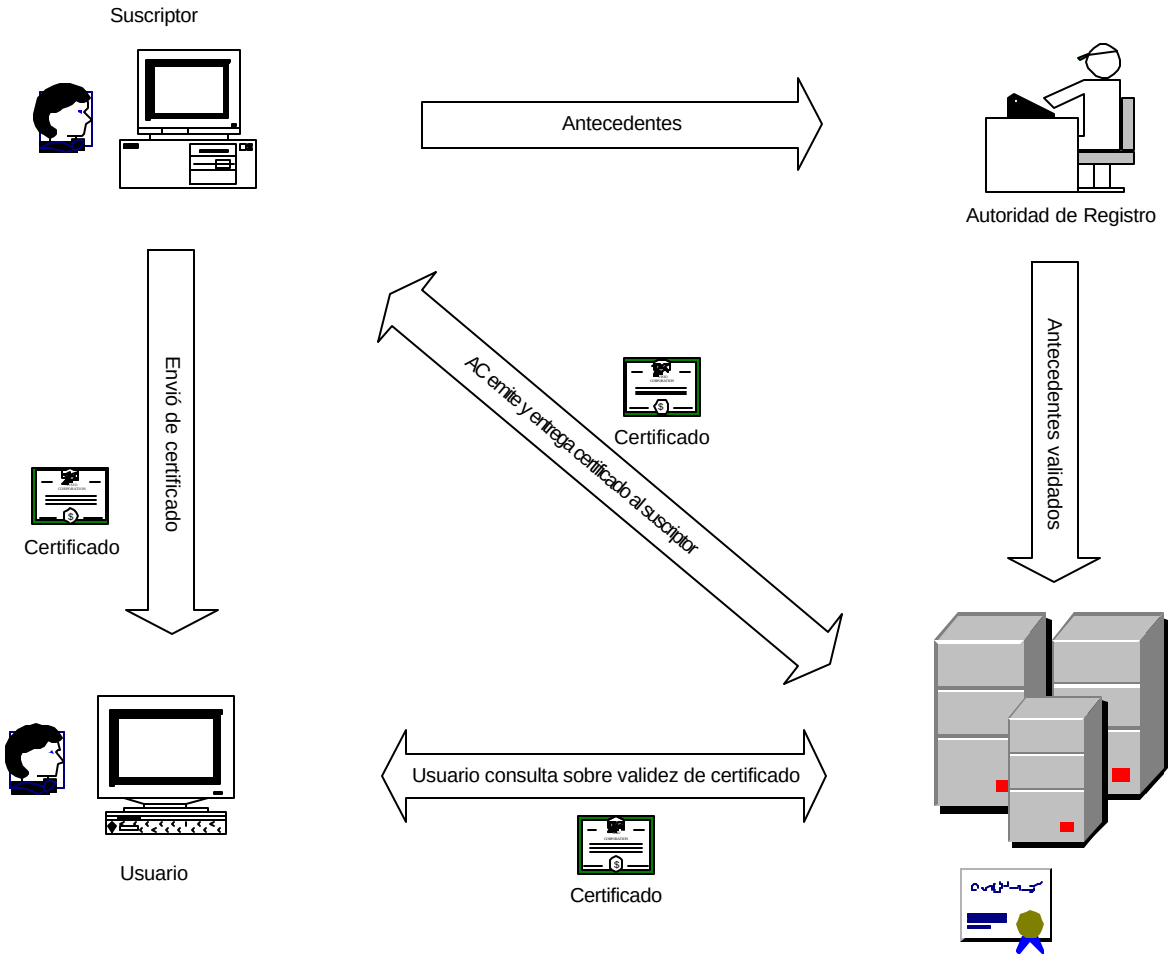


FIGURA Nº2 – INFRAESTRUCTURA DE CLAVE PÚBLICA

Los suscriptores– que pueden ser individuos o empresas – solicitan la emisión de certificados digitales, eligiendo el tipo según sus propias necesidades.

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 organismos independientes, pero que establecen y llevan a cabo sus operaciones sobre la base de una acreditación con **Acepta.com**. Esto garantiza que se ofrezca un nivel de servicio consistente con las políticas y prácticas requeridas por **Acepta.com**.

Cabe señalar que una AC puede por si misma 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.

Adicionalmente, **Acepta.com** puede de igual forma acreditar a una o más "Autoridades Certificadoras" (AC), para que emitan certificados, bajo las mismas políticas y procedimientos de **Acepta.com**. Para ello, **Acepta.com** emite un certificado del tipo de "autoridad certificadora", con el cual la AC acreditada puede emitir los certificados digitales a los suscriptores finales.

Por otro lado, **Acepta.com** establece una jerarquía de autoridades certificadoras propias, emitiendo cada una un cierto tipo de certificado. La relación entre estos tipos de AC, así como con las AC acreditadas, puede observarse en la siguiente figura:

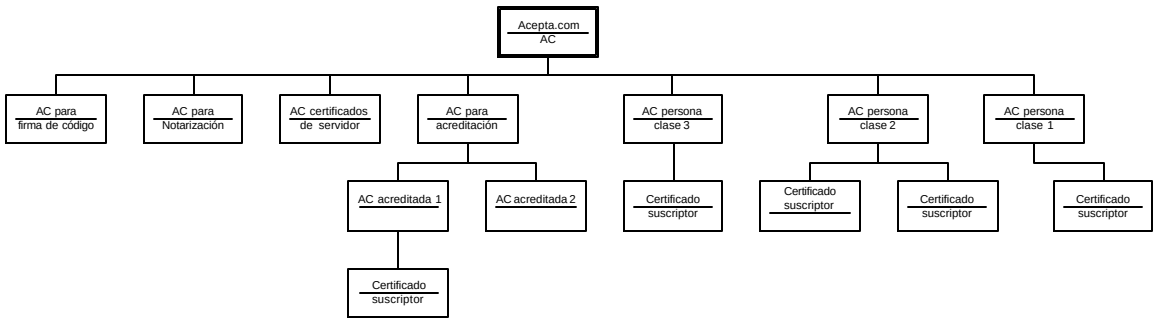


FIGURA Nº3 – JERARQUÍA DE AUTORIDADES CERTIFICADORAS

Cada AC en la jerarquía tiene su propio certificado digital que la acredita como AC, y el cual es emitido por la AC inmediatamente en el nivel superior en la jerarquía. Esto es salvo para el caso de la AC raíz de **Acepta.com**, quien emite su propio certificado. La relación jerárquica mostrada en la figura establece dicha dependencia entre emisor y suscriptor de certificados de AC.

Los suscriptores finales obtienen su certificado digital desde la AC situada en los niveles inferiores de la jerarquía mostrada.

Cada autoridad certificadora en la jerarquía anterior mantiene procedimientos en conformidad con éstas CPS, asegurando un servicio de calidad uniforme, que se acomoda a una vasta comunidad de

usuarios posiblemente dispersos geográficamente, y que pueden depositar equivalentes niveles de confianza en los servicios de certificación ofrecidos.

1.1.6 Servicios de información de Acepta.com

Uno de los servicios proporcionados por **Acepta.com** para todas las partes que intervienen durante la utilización de un certificado digital emitido por ésta, es el servicio de consulta sobre el estado de un certificado. Un certificado digital puede quedar invalidado si por alguna causal la información contenida en el certificado ya no refleja fielmente la identidad del suscriptor o tenedor del mismo, lo que requiere la emisión de un nuevo certificado. En tal caso, se hace necesario la notificación respecto a tal situación de invalidez.

Para ello, **Acepta.com** mantiene la información del estado de los certificados en un lugar en donde se pueda acceder públicamente y de manera expedita. Esto se muestra en la figura Nº 6:

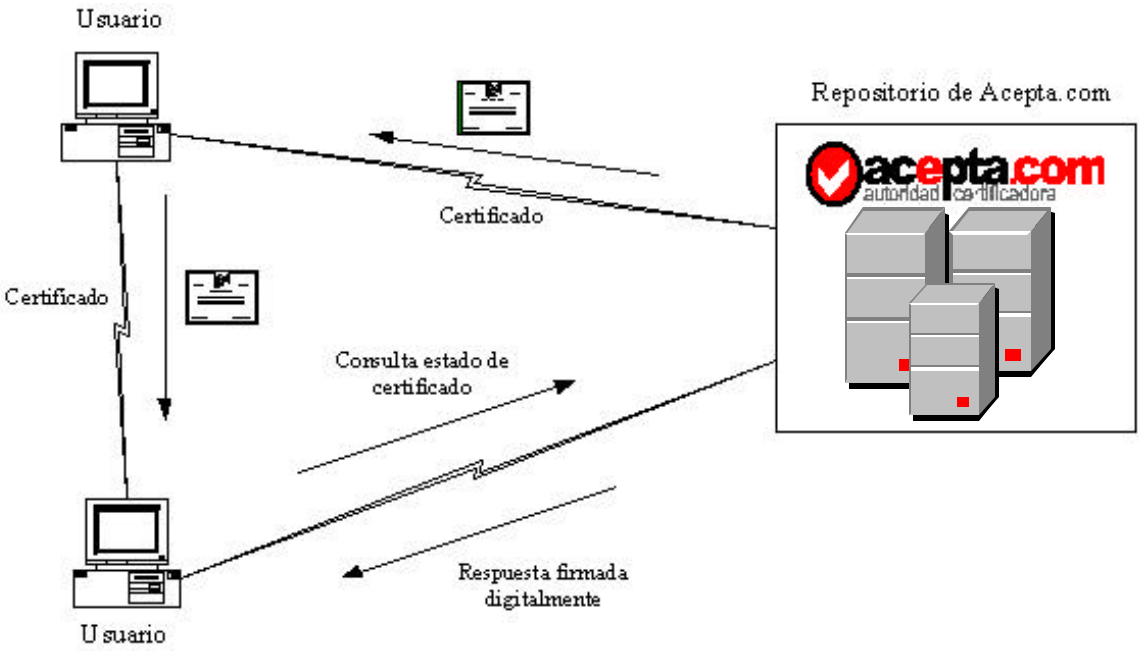


FIGURA Nº6 – CONSULTA DEL ESTADO DE CERTIFICADOS

Los suscriptores pueden comunicar una causal que requiera marcar su certificado como inválido. Dicha acción de invalidar o cancelar un certificado es lo que se denomina “revocar un certificado”. También es factible “suspender” un certificado, siendo la diferencia que en el último caso es una “cancelación temporal”, pudiéndose reestablecer posteriormente la validez del certificado. En el caso de una revocación, el certificado queda invalidado permanentemente.

Los procedimientos aplicables para notificar sobre un requerimiento de revocación (o suspensión) y hacer públicamente asequible dicha información, están estipulados en las CP correspondientes al tipo de certificado.[13]

Respecto a los usuarios que reciben certificados emitidos por **Acepta.com**, denominados "terceras partes confiables"[14], en determinado momento deciden si pueden depositar su confianza en tal certificado. Antes de hacer eso, se recomienda que se revise el sitio Web de **Acepta.com** (www.acepta.com) para confirmar que el certificado es válido y no esta revocado, o suspendido.

Básicamente un usuario tiene 4 mecanismos de consulta disponibles para obtener la información de estado de un certificado[15]:

- **Consulta a través de una página Web**, en donde se puede buscar el certificado por e-mail, nombre o RUT del suscriptor (certificados de persona), nombre del servidor (certificados de servidor), y así como por el Nº de serie del certificado.
- **Consulta a través del directorio LDAP**[16]. Un directorio es análogo a un "directorio telefónico". LDAP es el formato mas ampliamente utilizado para consultar un directorio, estando herramientas de consulta incorporadas en la mayoría de los sistemas operativos, como por ejemplo, en la libreta de direcciones de Microsoft Outlook.
- **Consulta on-line automática vía el protocolo OCSP**[17]. Este es un mecanismo que permite la consulta en línea y que proporciona todas las respuestas respecto al estado de un certificado firmadas digitalmente, lo que ofrece considerables garantías de confiabilidad.
- **Consulta del CRL.**[18] Este es un archivo que está firmado digitalmente por la autoridad Certificadora y que contiene una lista con los certificados revocados en un periodo de tiempo determinado.

1.2 Identificación

El presente documento se denomina "Prácticas de Certificación de **Acepta.com**", las que internamente se citan como CPS.

1.3 Comunidad de usuarios y aplicabilidad de los certificados

Acepta.com efectúa sus operaciones en el contexto de una infraestructura de servicios de certificados digitales, tal como se describió en la sección 1.1.5. En tal sentido, **Acepta.com** puede

---

[13] Más información sobre revocaciones en la sección 4.4

[14] Es decir, aquellas entidades que necesitan depositar su confianza en un certificado, en el transcurso de alguna transacción electrónica o transmisión o recibo de información, para validar la autenticidad del dueño del certificado, integridad de mensajes, etc.

[15] Para mayores detalles sobre los mecanismos de consulta, véase la sección 4.4.2

[16] Corresponde a las siglas en Inglés de Lighteened Directory Access Protocol (LDAP), un lenguaje estandar para formular consultas y recibir respuestas desde un directorio.

[17] Corresponde a las siglas en Inglés de On-line Certificate Status Protocol (OCSP),

[18] Corresponde a las siglas en Inglés de Certificates Revocation List (CRL)),

efectuar tanto las operaciones de registro inicial como la emisión y administración de los certificados propiamente tales.

Las autoridades de registro y autoridades certificadoras que pueden operar bajo la infraestructura de **Acepta.com** deben acreditarse previamente. Dicha acreditación establece las políticas y procedimientos a los cuales dichas autoridades deben ceñirse en la prestación de sus servicios, y básicamente requieren estar en conformidad con estas CPS. No obstante, **Acepta.com** se reserva el derecho de establecer restricciones y políticas adicionales para otorgar una acreditación. Información adicional en la sección 4.1.

Respecto a la utilización de los certificados emitidos bajo la infraestructura de **Acepta.com**, éstos son proporcionados para soportar las siguientes necesidades de seguridad fundamentales:

- Autentificación: proporciona garantías respecto a la identidad del suscriptor ,
- Integridad de mensajes: asegura que el contenido de un mensaje no ha sido alterado en el tiempo transcurrido entre su envió y su recepción efectiva,
- Firmas digitales: asistir a cualquier usuario que necesita confiar en un certificado digital respecto a que un suscriptor deniegue que ha autorizado cualquier transacción en particular, sí el suscriptor ha firmado digitalmente dicha transacción.
- Privacidad: garantizando que los mensajes transmitidos sean solo observados por el remitente correspondiente.

Acepta.com define un conjunto de políticas de certificados, las cuales son normas que regulan la aplicabilidad de los certificados, y establecen las restricciones aplicables, según se ha descrito en sección 1.1.4. Existe una política definida para cada tipo de certificado, y las cuales pueden ser consultadas públicamente en el sitio Web de **Acepta.com** en www.acepta.com .

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

2 CONSIDERACIONES GENERALES

En este capítulo se expresan una serie de tópicos legales y generales, como obligaciones, responsabilidades, tarifas, etc., relevantes para a 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 como autoridad certificadora

Acepta.com, en su calidad de Autoridad Certificadora se obliga a realizar las siguientes actividades:

- 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 (ver Cap. 3.3)
- 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 AC acreditada 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 estas normas
- 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 forma previa a la instalación y eventual aceptación de un certificado digital emitido por **Acepta.com** o alguna de sus AC acreditadas.
- Conocer y aceptar el propósito y alcance de un certificado obtenido en **Acepta.com** o en alguna Autoridad Certificadora acreditada, acorde a lo estipulado en las Políticas de Certificados definidas por **Acepta.com**.[19]
- 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.
- Protección y confidencialidad de su llave privada asociada a la llave pública. Dicha llave es personalísima y confidencial, conocida solo por el suscriptor y tenedor del certificado. En caso de su pérdida o cualquier circunstancia que comprometa la confidencialidad de dicha llave, deberá acudir personalmente a las oficinas de **Acepta.com** o enviar un correo electrónico firmado digitalmente notificando de tal circunstancia. La administración de la llave privada es de exclusiva responsabilidad del tenedor o suscriptor del certificado.
- Notificación a **Acepta.com** (o la Autoridad de Registro, o Autoridad Certificadora 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 de la Autoridad Certificadora acreditada correspondiente) que el certificado en el que se pretende confiar no ha caducado, o ha sido revocado o suspendido.
- La utilización de un certificado en cualquier transacción electrónica implica que se aceptan las condiciones, restricciones y normas estipuladas en este documento.
- Tener en conocimiento y aceptar el propósito y alcance de un certificado emitido por **Acepta.com** o por alguna Autoridad Certificadora acreditada, acorde a lo estipulado en este documento, y a las políticas de certificados definidas por **Acepta.com**.[20].

[19] Ver sección 1.3 sobre aplicabilidad

[20] Ver sección 1.3 sobre aplicabilidad

2.1.5 Obligaciones respecto a publicación de información de certificados y revocaciones

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**. (o en el sitio de la AC acreditada correspondiente)

Acepta.com y sus AC acreditadas se obligan a mantener dicha información disponible para su acceso publico, así como publicar la información consistentemente con las prácticas de confidencialidad estipuladas en este documento así como de las leyes vigentes[21].

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, etc. no sea posible consultar el estado de algún certificado.

2.2 Responsabilidades de Acepta.com como autoridad certificadora y de sus Autoridades acreditadas

2.2.1 Responsabilidades asumidas

Acepta.com será responsable de tomar todas las medidas adecuadas que aseguren una correcta ejecución del proceso de emisión de un certificado. Lo anterior implica que debe acreditar fielmente la identidad del suscriptor, que en el momento de emitirse el certificado este cumplía con los requisitos establecidos en estas CPS y CP pertinentes a cada tipo de certificado, y la efectiva vigencia entre la correspondencia entre la información del suscriptor y la llave pública acreditada en el certificado.

Por otro lado, **Acepta.com** se hace responsable de la información que emita relativa al estado de los certificados, información que **Acepta.com** proporciona firmada digitalmente.

Al respecto, los servicios de certificación de **Acepta.com** están diseñados y construidos en forma que pueda proporcionar fácilmente todos los mecanismos de prueba suficientes para dilucidar responsabilidades en caso de cualquier conflicto o perjuicio que se derive por la utilización de los certificados digitales emitidos por ésta.

Tales mecanismos de prueba específicos a cada clase de certificado son detallados en las Políticas de Certificado pertinentes, y públicamente disponibles en www.acepta.com .

Por último, **Acepta.com** será responsable de los daños o perjuicios que, sólo como consecuencia de su actividad directa dolosa y negligencia o culpa grave, ocasione a los suscriptores o signatarios que contraten sus servicios y a los terceros interesados que adhieran a las presentes prácticas, todo ello en conformidad a la ley.

[21] Ver sección 2.8 sobre solicitudes de confidencialidad

2.2.2 Exclusiones de 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.

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.

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

2.3.3 Publicación de Procedimientos Administrativos

La publicación de información administrativa, como reportes financieros, etc., será acorde a las exigencias que la Ley Chilena establezca para tales efectos.

2.4 Normas respecto a aplicabilidad de este CPS

2.4.1 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**.

Específicamente, referente a la confidencialidad de la información, declara dar estricto cumplimiento a la Ley Nº19.628 sobre protección de datos personales.

2.4.2 Reglas de interpretación

Cada cláusula de estas CPS. es válida en si misma y no invalidará el resto. La cláusula inválida o incompleta podrá ser sustituida por otra equivalente y válida por acuerdo de las partes.

Las normas contenidas en las secciones 2.1, 2.2 y 2.3 (obligaciones y responsabilidades), 2.7 (conformidad con auditorias), y 2.8 (información confidencial) permanecerán en vigor aún después de la pérdida de vigencia de éstas CPS.

Las notificaciones a **Acepta.com** podrán realizarse mediante mensajes de correo electrónico firmados digitalmente, de acuerdo con las prescripciones de estas CPS, o por escrito.

Las comunicaciones electrónicas serán efectivas tras la recepción por parte del emisor del correspondiente acuse de recibo firmado digitalmente, dentro de los cinco (5) días siguientes al envío.

Las comunicaciones escritas deben ser enviadas por servicio certificado con acuse de recibo o equivalente, a la siguiente dirección: **Acepta.com**, Paseo Bulnes 241, 5º piso, Santiago, Chile.

Estas reglas serán igualmente de aplicación a las autoridades de registro o certificadoras acreditadas, si bien las notificaciones se realizarán a las direcciones que las mismas aporten a sus suscriptores.

2.4.3 Arbitraje

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

2.5.1 Tarifas para emisión de certificados

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

2.5.2 Tarifas para acceso a información de certificados

El acceso a la información de certificados (vigencia, revocaciones, etc.), consistentemente con las políticas de confidencialidad establecidas en estas CPS (ver sección 2.8) es gratuito, y esta disponible en el sitio Web de **Acepta.com**

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.

En caso de modificarse dicho documento, se le notificara a los usuarios por e-mail, en la dirección por ellos establecida durante los procesos de certificación. [22]

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 practicas seguidas en el proceso de certificación, es que **Acepta.com** adhiere a la certificación y realización de auditorias externas e independientes a las practicas y operaciones de **Acepta.com**. Tales auditorias serán realizadas por organismos competentes, específicamente por el Dpto. de Ciencias de la Computación de la Universidad de Chile, institución de reconocido prestigio en el ámbito nacional e internacional, además de ser un órgano de garantizada autonomía e independencia con respecto a **Acepta.com**.

En un compromiso de transparencia, los resultados de dichas auditorías podrán ser comunicados públicamente, por mecanismos que en su momento se determinen.

[22] Mas detalles en la sección 8 de estas CPS

2.8 Confidencialidad

Acepta.com, adhiere y efectúa sus operaciones en conformidad con lo establecido por la Ley 19.628 de Chile, sobre protección de datos personales.

2.9 Derechos de propiedad intelectual

Acepta.com se reserva la propiedad intelectual y patrimonial de las prácticas de certificación o CPS, el software de administración e instalación de certificados *Acepta.exe?* , y el software de administración de autoridad de registro *Acepta.reg?* . Queda por ende prohibida toda reproducción, comunicación, distribución, archivo o transmisión de cualquier tipo y por cualquier medio, mecánico, electrónico, fotográfico o magnético, total o parcial de las mismas sin previa y expresa autorización escrita de **Acepta.com**.

3 IDENTIFICACION Y AUTENTIFICACIÓN

En este capítulo se presentan las prácticas y especificaciones seguidas por **Acepta.com** y sus AR o AC acreditadas, para autentificar fielmente la identidad de las entidades a las cuales se le emitirá un certificado, previamente a la emisión propiamente tal.

3.1 Registro inicial

3.1.1 Tipos, interpretación y unicidad de nombres

Acepta.com revisará y validará la información solicitada a los suscriptores, a fin de otorgar una correcta y unívoca identificación de las entidades involucradas. En tal sentido, tal como se menciono en la sección 2.1.3 (Obligaciones del suscriptor), es requisito fundamental que los antecedentes entregados por los suscriptores sean fidedignos.

Las reglas aplicables para el tratamiento de nombres están estipuladas en las Políticas de Certificados pertinentes al tipo de certificado en particular, las cuales están disponibles en www.acepta.com .

3.1.2 Método para probar posesión de la llave privada

La llave privada asociada a un certificado digital emitido por **Acepta.com** o alguna de sus AC acreditadas es siempre generada exclusivamente en el equipo computacional del suscriptor del certificado.

El detalle de los mecanismos de generación de la llave privada para los suscriptores están estipuladas en las Políticas de Certificado (CP) pertinentes al tipo de certificado en particular, las cuales están disponibles en www.acepta.com .

3.1.3 Autentificación de identidades

El mecanismo específico utilizado para autentificar las identidades de los suscriptores de certificados, depende de la clase de certificado, por lo que dicho mecanismo está expresado en las Políticas de Certificado (CP) pertinente, disponible en www.acepta.com .

3.2 Renovación de Certificados

Todos los tipos de certificados tendrán un período de vigencia que será indicado en el contrato y en el mismo certificado emitido. Dichos certificados caducarán automáticamente al finalizar dicho período y de pleno derecho ocasionando la invalidez del certificado, el cese permanente de su operatividad y el término de la prestación de los servicios de certificación por **Acepta.com**.

La opción de renovación de certificados se establece para los casos en que un certificado vaya a caducar y el suscriptor o signatario quiera utilizar un certificado de las mismas características que el usado válidamente hasta esa fecha. Será responsabilidad del suscriptor, el informar a **Acepta.com** si algunos de los datos registrados o contenidos en el certificado anterior han cambiado.

Los procedimientos específicos para solicitar y efectuar la renovación están estipulados en las Políticas de Certificados pertinentes al tipo de certificado en particular, las cuales están disponibles en www.acepta.com.

3.3 Re-emisión de llaves después de una revocación

La revocación del certificado digital tiene como consecuencia principal la terminación inmediata del período operativo del certificado, el que legalmente pasa a ser "inválido".

La revocación del certificado digital acarrea como consecuencia, además, que no puedan crearse o generarse válidamente firmas digitales.

Todas las notificaciones electrónicas comunicando la revocación o suspensión de un certificado serán a través de e-mail firmado digitalmente por **Acepta.com**.

Los procedimientos específicos para solicitar y efectuar la renovación están estipulados en las Políticas de Certificados pertinentes al tipo de certificado en particular, las cuales están disponibles en www.acepta.com.

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 registros de datos aplicables.

4.1 Requerimientos para autoridades de registro o certificadoras bajo la jerarquía de Acepta.com

4.1.1 Procedimiento de acreditación

Acepta.com, puede aprobar, bajo su exclusiva discrecionalidad, la operación de varias autoridades de registro (AR) y autoridades certificadoras (AC), las cuales efectuarán sus actividades en un esquema de acreditación respecto a los requerimientos establecidos por **Acepta.com** sobre la prestación de sus servicios. Dicha acreditación establece que éstas entidades operan en conformidad con políticas y procedimientos establecidos por **Acepta.com**, estipulados en éstas CPS. Esto garantiza una uniformidad en la calidad de los servicios de certificación ofrecidos.

Cada entidad que desee operar subordinada a los servicios de **Acepta.com**, deberá completar una solicitud previa.

La solicitud anterior deberá ser enviada mediante correo postal certificado a la siguiente dirección::

Acepta.com
Servicios de Acreditación
Avda. General Bulnes 241 Piso 5
Código Postal: 6520420
Santiago
Región Metropolitana, CHILE

4.1.2 Solicitud de acreditación

La información que debe contener la solicitud de acreditación está especificada en el documento "Políticas de Acreditación para Autoridades Externas", disponible en el sitio Web de **Acepta.com** (www.acepta.com)

4.1.3 Aprobación para inicio de actividades de autoridad acreditada

Luego de la apropiada revisión e investigación de los antecedentes presentados, **Acepta.com**, bajo su exclusiva discreción y sin expresión de causa, podrá aprobar o rechazar la solicitud presentada.

Sin perjuicio de lo anterior, **Acepta.com** se reserva el derecho de realizar cualquier investigación o auditoria futura para garantizar que la autoridad acreditada realiza sus operaciones de una manera consistente con los requerimientos establecidos en éstas CPS.

El procedimiento aplicable para notificar y aprobar el inicio de las actividades de la entidad acreditada, está especificado en el documento "Políticas de Acreditación", disponible en el sitio Web de **Acepta.com** (www.acepta.com)

4.1.4 Validación, aceptación y emisión de certificados de autoridades acreditadas

En el caso de autoridades certificadoras acreditadas, corroborado la fiabilidad y consistencia de los procedimientos e infraestructura de certificación, se procederá a emitir los certificados de autoridad certificadora o de registro correspondientes.

Acepta.com se reserva el derecho de llevar a cabo investigaciones tendientes a corroborar la fiabilidad y capacidad idónea de las autoridades que soliciten acreditación para llevar a cabo sus servicios consistentemente con estas CPS. Para ello, dichas entidades deberán proporcionar los antecedentes que se les soliciten, como manuales, documentos de procedimientos, etc., relacionados con los servicios de certificación.

4.2 Requerimientos para certificación otras entidades

El detalle de los requerimientos aplicables para este tipo de certificados están estipulados en las políticas de certificados para servidores seguros, disponibles públicamente en el sitio Web de **Acepta.com**, en la dirección www.acepta.com .

4.3 Proceso de suspensión y revocación de certificados

Un certificado digital emitido por **Acepta.com** o una de sus AC acreditadas, podrá ser revocado antes del término del periodo de validez del certificado, cuando concurren algunas circunstancias que generan que la información contenida en el certificado sea inválida. Un certificado revocado queda invalidado permanentemente para su uso. Por otro lado, pueden haber circunstancias menos drásticas que ameriten la necesidad de suspender temporalmente la validez del certificado, el cual puede volver a su estado de vigencia en algún momento posterior.

4.3.1 Causales y procedimientos para revocar o suspender certificados

Un certificado deberá ser revocado si concurre alguna de las siguientes circunstancias, lo cual se aplica por igual para todos los tipos de certificados emitidos:

- Compromiso de la llave privada correspondiente asociada al certificado.
- Modificación posterior de los antecedentes de la entidad suscriptora o titular del certificado
- Falsificación de los antecedentes de la entidad suscriptora o titular del certificado

El detalle de los requerimientos aplicables está establecido en las Políticas de Certificados, disponible en el sitio Web www.acepta.com .

4.3.2 Procedimientos de publicación de información de revocaciones

La información pertinente a los certificados digitales suspendidos o revocados será publicada en el sitio Web de **Acepta.com** (www.acepta.com) o en el de la AC acreditada que corresponda.

La información respecto a la revocación o suspensión de un certificado quedará disponible en el sitio Web de **Acepta.com** inmediatamente después de completado el proceso de la solicitud de revocación. Es decir, una vez que se le confirme al usuario sobre la recepción conforme de la

solicitud de revocación, ésta información ya estará disponible en el sitio Web para consulta de cualquier parte que requiera confiar en el certificado del suscriptor.

Para brindar un adecuado servicio de información sobre las revocaciones y suspensiones, **Acepta.com** y las AC acreditadas soportarán variados medios para distribuir dicha información. Entre los mecanismos utilizados se cuenta pero no se limita a:

4.3.2.1 LISTAS DE REVOCACIÓN (CRL)

Acepta.com y las AC acreditadas mantendrán listas de revocación o CRL con la información de los certificados revocados o suspendidos. Estas listas están en un formato compatible con el estándar X.509.

En cada certificado emitido, en la extensión apropiada se incluirá la información de la ubicación de la lista de revocación para su consulta. (ver sección 7.1.2 sobre extensiones)

4.3.2.2 CHEQUEO DE REVOCACIÓN ON-LINE (OCSP)

Acepta.com soporta la consulta "on-line" sobre el estado de los certificados por ella emitidos, a través del protocolo OCSP (On-line Certificate Status Protocol). Este es un protocolo estándar ampliamente reconocido. Información adicional y ayuda respecto a como realizar consultas utilizando dicho protocolo se encuentra disponible en el sitio Web de **Acepta.com** en www.acepta.com.

El detalle de los mecanismos de consulta aplicables a cada clase de certificado está establecido en las Políticas de Certificados, disponible en el sitio Web www.acepta.com .

4.3.2.3 CONSULTA MEDIANTE EL WEB

También se podrán consultar el estado de los certificados on-line mediante el uso del Web en www.acepta.com .

4.3.3 Frecuencia de la actualización de la información de revocación

Las listas de revocación (CRL) serán actualizadas con una frecuencia de 12 horas entre cada publicación.

4.4 Procedimientos de auditoria de seguridad

4.4.1 Tipos de eventos registrados

Con el fin de mantener un ambiente seguro y controlado, se registrará la ocurrencia de una serie de eventos; registrándose para cada uno información relativa al tipo de evento y el tiempo en que el evento ocurrió. Dependiendo del tipo de evento, se puede registrar información adicional, como la creación de archivos, envío de mensajes o notificaciones, operador que genera el evento, etc.

A continuación se muestra una lista de los eventos que se registran como mínimo, sin excluir la posibilidad de registrar información o eventos adicionales:

AUDITORIA DE EVENTOS	
Eventos Auditados	***Observaciones***
Firma de contrato	Se registra una copia en papel del contrato firmado por el suscriptor. Además, se genera una copia digital la cual se envía a custodia electrónica.
Envío antecedentes desde AR a AC	Cuando la AR envía los antecedentes del suscriptor a la AC, mediante un canal seguro, se registra la fecha y hora de envío, y operador que genera el envío.
Recepción solicitud de certificado por parte de la AC	Se registra fecha y hora de recepción de los antecedentes desde una AR..
Aprobación o rechazo de solicitud de certificado por parte de la AC	Se registra fecha , hora y operador que autoriza o rechaza la solicitud.
Requerimiento para recuperar e instalar certificado	Generado al instalar el certificado en el equipo del suscriptor del mismo y enviado a la AC. Se registra la fecha, hora, y Nº de solicitud correspondiente.
Notificación de aceptación de certificado	Notificación enviada por el suscriptor a Acepta.com, comunicando que acepta el certificado provisorio, con lo cual pasa a ser un certificado válido. Se registra fecha y hora, Nº de solicitud asociado.
Solicitud de Revocación o Suspensión	Se registra fecha y hora cuando el suscriptor comunica y solicita la necesidad de revocar o suspender el certificado.
Revocación o suspensión de certificado	Se registra la fecha y hora en que el certificado pasa a estar efectivamente revocado o suspendido.
Solicitud de renovación de vigencia de certificado suspendido	Se registra la fecha y hora en que se solicita la renovación.
Activación de certificado suspendido	Se registra fecha y hora a partir de la cual el certificado retoma su validez, así como el operador que autoriza su renovación.
Respuesta sobre estado de certificado	Cuando se solicita información respecto al estado de un certificado, se registra la fecha y hora, así como la respuesta entregada.
Generación de CRL	Se registra la fecha y hora en que se actualiza una lista de revocación.
Login y Logouts de operadores	Se mantendrá un registro con el inicio y término de las sesiones.
Cambios en la configuración de los servidores	Se deberán registrar los cambios hechos a las configuraciones; la fecha y hora, así como el personal que autoriza y realiza los cambios.

TABLA Nº9 – AUDITORIA DE EVENTOS

4.4.2 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.

4.4.3 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 en dependencias externas (off-site) a **Acepta.com**. 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.

4.4.4 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 identidad digital.

4.4.5 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 de la AC. 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 a la AC, así como en custodia electrónica en Custodium.com.

4.4.6 Sistema de colección de auditoria

Los respaldos e información de auditoria se mantendrán en custodia electrónica por un periodo de al menos 10 años.

4.4.7 Notificación de eventos

En los eventos de auditoría que tienen directa relación y son activados por los suscriptores de certificados, como la firma de contrato, aceptación de certificado, solicitud de revocación, etc., el suscriptor es notificado del registro del evento en el momento de ocurrencia del mismo.

4.4.8 Evaluaciones de vulnerabilidad

Con el propósito de mantener un ambiente seguro y confiable, **Acepta.com** y sus AC 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 de manera sistemática y controlada 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 recompensadas, en la cual se acuerda efectuar ciertos ataques o pruebas especificas bajo un ambiente controlado.

4.5 Políticas para archivo de registros

4.5.1 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.

4.5.2 Requerimientos para "time-stamping" de registros

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

4.5.3 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.

4.5.4 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.

4.6 Procedimientos para cambios de las claves

Para cambiar su clave el suscriptor de un certificado deberá solicitar una revocación del mismo (en caso de que el certificado todavía sea válido) y volver a solicitar un nuevo certificado.

4.7 Planes de contingencia y recuperación

4.7.1 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.

4.7.1.1 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 sus 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**, el Administrador de Operaciones del sitio de **Acepta.com** deberá notificar de una manera segura (out-the-band) a 3 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.

4.7.1.2 REGENERACIÓN DE LA LLAVE PRIVADA DE ACEPTA.COM

En el caso de **Acepta.com** y sus AC acreditadas, el par de llaves es generada seguramente en una habitación especial usando un dispositivos físicos de respaldo, tal como se describe en la sección 6.1.2.

4.7.2 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.

4.7.3 Compromiso de llaves de entidades

Ver sección 4.3 .

4.7.4 Instalaciones de seguridad frente a desastres naturales

Acepta.com y sus AC acreditadas 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.

4.8 Término de las actividades de Acepta.com como autoridad certificadora

En el evento que **Acepta.com** vaya a discontinuar sus operaciones como Autoridad Certificadora, 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 necesarias, estará en conformidad con la ley aplicable de la República de Chile..

5 CONTROLES DE SEGURIDAD FISICOS, DE PROCEDIMIENTOS Y DE PERSONAL

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 las 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

5.1.1 Ubicación y construcción del sitio de operación de servidores (site)

Los servidores de **Acepta.com** están ubicados en un recinto físico (o site) con un ambiente protegido, de manera de prevenir y detectar cualquier acceso no autorizado, extravío de información sensible o corrupción de recurso de cualquier índole.

El site está construido con material resistente al fuego, con un acceso principal con puertas blindadas, en una habitación que se mantiene permanentemente cerrada con cerrojos, pudiendo ingresar solo personal autorizado. Interiormente mantiene ductos de ventilación para mantener una temperatura ambiente adecuada.

5.1.2 Accesos físicos

Los accesos para entrar al site tienen 3 niveles de seguridad: para cada uno hay que tener una llave distinta, la cual sólo la mantiene personal autorizado.

Una vez al día, se revisan todos los accesos para asegurar que mantienen un nivel de seguridad aceptable. Además, se revisa que el equipamiento, tanto para los servidores y dispositivos criptográficos están funcionando apropiadamente.

5.1.3 Condiciones de electricidad y aire

Las condiciones de electricidad y aire son las adecuadas para asegurar un ambiente que permita una operación segura. Además, el piso de la habitación del site está cubierto con un material antiestático.

Se mantienen UPS conectadas a los servidores para asegurar un suministro continuo de energía eléctrica. Además se mantiene un sistema automático de alarma y extinción de incendios.

5.1.4 Exposición al agua

El site está ubicado en un 5º piso, aislado de exposición a aguas lluvias o inundaciones. Además, está en una dependencia independiente del sistema de circulación de agua, para prevenir cualquier exposición o derrame.

5.1.5 Prevención y protección de incendios

Se cuenta con dispositivos de detección y extinción de incendios para amortiguar cualquier emergencia posible.

5.1.6 Medios de almacenamiento de información

Toda la información crítica es respaldada sobre una base diaria. Adicionalmente se realiza un respaldo semanal y cada mes se realiza un respaldo completo, almacenándose los datos en un medio magnético en dependencias externas.

Adicionalmente, se dispone de los servicios de custodia electrónica segura que están disponibles en Custodium.com, en donde se almacenan respaldos electrónicos de información crítica.

5.1.7 Disposición de desechos

Acepta.com mantiene cuidadosos procedimientos y mecanismos de revisión previa a la destrucción de información que pueda ser sensitiva, lo cual es administrado y controlado por personal autorizado.

5.1.8 Respaldos Off-site

Vea sección 5.1.6

5.2 Controles de procedimientos

5.2.1 Roles de confianza

Los servicios de **Acepta.com**, y autoridades certificadoras acreditadas son operados por personal cuidadosamente seleccionado y entrenado, para proporcionar un ambiente de operación segura y de confianza.

Todos los empleados que tengan acceso, control o directa relación con los módulos criptográficos que puedan afectar los procesos de emisión, uso, revocación o suspensión de certificados, incluyendo el proceso de respuestas on-line sobre el estado de certificado, estan definidos como personal que mantiene una “posición de confianza”.

Dichas posiciones de confianza deberán ser revalidadas cada 2 años, revisándose las calificaciones del personal para asegurar que pueden continuar en dichas posiciones.

5.2.2 Numero de personas requerido por tarea

Acepta.com mantiene una rigurosa política de segregación y control de las responsabilidades del personal bajo posiciones de confianza.

En ese sentido, no existe una única persona que pueda realizar las tareas mas sensitivas, como son los módulos de firma y manejo de llaves criptográficas; necesariamente se requiere la concurrencia de distintas personas, cada una en una posición de confianza distinta (por ejemplo, una controla el acceso físico y otra la operación lógica).

5.2.3 Identificación y autentificación para cada rol

Todo el personal se debe autentificar de manera segura usando claves y certificados digitales, para obtener permiso de ejecutar las funciones pertinentes a su propio rol.

5.3 Controles del personal

5.3.1 Calificaciones, experiencia y acreditación del personal

Todo el personal bajo posiciones de confianza debe mantener una conducta y antecedentes intachables, con adecuadas calificaciones y experiencia en las funciones que desempeñen.

El cumplimiento de los requerimientos para calificar como personal de confianza se establecen bajo un cuidadoso programa de selección e investigación de las capacidades, antecedentes y experiencia del personal. Dicho personal es continuamente entrenado y requiere pleno conocimiento y entendimiento de las políticas de seguridad y certificación que permiten mantener un ambiente seguro y confiable.

5.3.2 Procedimientos de selección

Todo el personal es cuidadosamente seleccionado y debe calificar previamente a iniciar su trabajo bajo **Acepta.com**. Solo se selecciona personal con adecuada experiencia y antecedentes académicos derivados de instituciones de reconocido prestigio a nivel nacional e internacional.

Además, es requisito mantener una adecuada conducta profesional y antecedentes financieros intachables.

Todo el personal deberá ceñirse además a las restricciones y normas adicionales especificadas en el reglamento interno de **Acepta.com.**

5.3.3 Requerimientos de aprendizaje

Todo el personal seleccionado para laborar en **Acepta.com** es entrenado adecuadamente previamente al inicio de sus operaciones normales. Este entrenamiento incluye charlas, material escrito y audiovisual, asi como una adecuada supervisión bajo profesionales expertos.

5.3.4 Frecuencias de capacitación

Vea sección 5.3.3.

5.3.5 Sanciones por actividades no autorizadas

Todo el personal de **Acepta.com** entiende que el servicio en sus funciones es contingente con el desempeño respecto a sus propias responsabilidades funcionales y de seguridad.

5.3.6 Requerimientos para contratación de personal

Ver sección 5.3.2.

5.3.7 Documentación proporcionada al personal

A cada persona se le proporciona suficiente documentación y acceso a material que le permita efectuar exitosamente las funciones que le son propias según su propio rol. Entre la documentación proporcionada está y no se limita a:

Manuales de instalación y utilización de herramientas de software

Libros sobre materias técnicas para consulta

Documentación relativa a las políticas de certificados y prácticas de certificación de **Acepta.com**

Normas de diseño y programación de software

CDs con material técnico de consulta

Acceso a Internet para obtener información adicional

6 CONTROLES DE SEGURIDAD TÉCNICOS

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.

6.1 Generación e instalación del par de llaves

6.1.1 Generación de llaves de los suscriptores de certificados

Estipulado en las Políticas de Certificado correspondientes a cada clase de certificado. Documento disponible en www.acepta.com .

6.1.2 Generación del par de llaves de Acepta.com o de las AC acreditadas

Para la generación de la llave privada, se realizan los siguientes pasos:

Para generar las llaves privadas de **Acepta.com**, el Administrador de Operaciones del sitio de **Acepta.com** deberá notificar de una manera segura (out-the-band) a los directores de la empresa, respecto a la necesidad de generación de la llave privada, para proceder con el "acto de creación de llave privada" de **Acepta.com**.

Para dar inicio a dicho acto, previamente el Administrador de Operaciones deberá preparar el software y hardware requeridos para el inicio del módulo criptográfico de generación de llaves, el cual se encargará de crear el par de llaves pública y privadas, así como todas las siguientes en la jerarquía de **Acepta.com** explicada en la sección 1.1.5 ("Infraestructura de certificados digitales de clave pública"). Para comenzar con el proceso de generación de llaves se requerirá digitar una clave de activación sólo conocida por los directores de la empresa.

Posteriormente los directores de **Acepta.com** se reúnen para proceder con el inicio del módulo criptográfico de generación en una habitación herméticamente cerrada en donde se encuentra el servidor con dicho módulo criptográfico, y alguno de los directores procede a digitar la clave de activación para que el módulo de creación de llaves se inicie. Acto seguido, luego que el módulo hubiese generado el par de llaves pública y privada de **Acepta.com**, éstas son mostradas en formato hexadecimal en la pantalla del servidor, para que los directores procedan a su respaldo. Esta consiste en una secuencia de 512 caracteres por cada llave.

Dicho respaldo consiste en el grabado de la secuencia de caracteres mostrados en la pantalla en sendas placas de aluminio, generándose 2 placas por secuencia (es decir, por llave). Dicho grabado es realizado en forma manual.

Dichas placas son guardadas en cajas metálicas con llave.

Luego de finalizado el grabado de las placas, el módulo criptográfico procede a activar dichas llaves y de manera de continuar con el proceso de inicialización de todos los servicios de firma y generación de certificados. Se mantiene una copia encriptada de las llaves privadas en los servidores de firma, para efectos de recuperación posterior. Dichas llaves son encriptadas con una contraseña definida en el "acto de generación de la llave", y conocida sólo por los directores de **Acepta.com**.

6.1.3 Entrega de llaves pública y privada a suscriptor

Estipulado en las Políticas de Certificado correspondientes a cada clase de certificado. Documento disponible en www.acepta.com .

6.1.4 Entrega de la llave publica de Acepta.com a usuarios

Estipulado en las Políticas de Certificado correspondientes a cada clase de certificado. Documento disponible en www.acepta.com .

6.1.5 Tamaño de las claves

Todos los pares de llaves para firma de certificados usados por **Acepta.com** y sus AC acreditadas son de un tamaño de 2048 bits. Las llaves de los suscriptores son de un tamaño de 1024 bits.

6.1.6 Parámetros de generación de llaves públicas de Acepta.com

La llaves pública de **Acepta.com** es creada de manera tal que la llave resultante tenga muy pocos unos (1) en la serie de bits obtenida. Esto permite que la verificación de dicho certificado sea mucho mas rápida y sin comprometer la seguridad. También los números p y q usados por el algoritmo RSA son generados de manera que el módulo de la diferencia entre ambos números sea grande, haciendo mas difícil la posibilidad de un ataque exitoso para descubrir la llave privada asociada a la llave pública.

6.1.7 Hardware/software para generación de llaves

Para la generación de las llaves de **Acepta.com** , y de las AC acreditadas, se utilizan módulos criptográficos , acorde a las recomendaciones del estándar FIPS140-1.

La generación de las claves de los usuarios o suscriptores es realizada por mecanismos que utilicen módulos criptográficos en conformidad con el estándar FIPS 140-1 nivel 1. El detalle está estipulado en las Políticas de Certificado correspondientes a cada clase de certificado. Documento disponible en www.acepta.com .

6.1.8 Propósitos para el uso de las llaves

Todos los certificados emitidos por **Acepta.com** o por alguna de sus AC acreditadas, incluyen la extensión KeyUsage, para establecer el propósito de uso de los certificados y las llaves asociadas. Opcionalmente se puede incluir en los certificados la extensión ExtendedKeyUsage para definir restricciones adicionales.

Para mas detalles ver sección 7.1.2.

6.2 Protección de las llaves privadas

La llave privada de **Acepta.com** se encuentra protegida internamente en los módulos criptográficos que la requieran. Además, como se utiliza un sistema de firma distribuido, no existe un único servidor que almacene la llave completa durante un proceso de firma de datos. Además, dicha llave es respaldada en sendas placas de aluminio, durante la “ceremonia de creación de llave privada” de **Acepta.com** descrita en el apartado 6.1.2.

6.2.1 Estándares para el módulo criptográfico

Acepta.com y sus autoridades certificadoras acreditadas sólo utilizan en todas sus operaciones módulos criptográficos que sigan la normativa requerida por el estándar FIPS 140-1.

Todos los pares de llaves de **Acepta.com** y sus AC acreditadas son generadas y mantenidas en dispositivos físicos. Nunca son almacenadas – aunque sea temporalmente – en texto plano.

6.2.2 Control múltiple de la llave privada

Las llaves privadas de **Acepta.com** y sus AC acreditadas están sujetas a un control multi-personal y de multi-servidor.

Cuando se genera la llave privada por primera vez, se divide en múltiples fragmentos que son distribuidos cifrados con una clave de activación, y almacenados en varios servidores distintos. Estos servidores ejercen en conjunto la funcionalidad de firma distribuida, operando en secuencia. Es decir, para proceder a firmar cualquier conjunto de datos, se le pasa el requerimiento a uno de estos servidores, los cuales van firmando consecutivamente los datos, hasta llegar al último servidor quien completa la firma. En ningún momento un servidor único mantuvo la llave privada de manera completa.

Cabe señalar que el fragmento de la llave se mantiene cifrada en cada servidor, y para proceder a activarla dentro de un proceso de firma, se requiere la clave de activación. En ningún momento la llave privada es revelada ni almacenada en texto plano bajo ningún medio. Además, dicha clave de activación es mantenida y manejada sólo por personal autorizado.

Por otro lado, dicha clave de activación se utiliza sólo para activar los módulos para utilizar la llave privada en un proceso de firma. Para activar los módulos que generan una nueva llave se utiliza una clave de activación distinta, la cual es sólo manejada por los directores de la compañía.

6.2.3 Respaldo y archivo de la llave privada

La llave privada de **Acepta.com** o de alguna de sus AC acreditadas, éstas se respaldan en placas de aluminio, dejadas en custodia segura, según como se detalla en la sección 6.1.2.

El respaldo de las llaves privadas de los suscriptores esta detallado en las Políticas de Certificado correspondientes a la clase de certificado, y lo que está disponible en www.acepta.com .

6.2.4 Métodos para activación de la llave privada de Acepta.com

La llave privada es activada utilizando las claves de activación mantenidas por personal autorizado, según se menciona en la sección 6.2.2.

6.2.5 Métodos para destrucción de la clave privada

En el eventual caso de necesidad de destrucción de la llave privada, se utilizara los comandos establecidos para tales efectos que tienen disponibles los módulos criptográficos..

6.3 Otros aspectos de gestión de claves

6.3.1 Archivo de llaves publicas

Las llaves públicas son archivadas según el formato estándar PKCS#7.

6.3.2 Periodos de uso de las llaves

El periodo de uso de las llaves es descrito en la sección 7.1

6.4 Datos de activación

6.4.1 Generación y activación de datos de activación

Para el caso de **Acepta.com** o una de sus AC acreditadas, los módulos criptográficos que manejan las llaves privadas, tanto para su generación como eventual recuperación posterior, son activados usando claves de activación, las cuales son administradas sólo por personal autorizado, según se describe en la sección 6.2.

Los procedimientos aplicables para el caso de certificado de entidades finales se detallan en las Políticas de Certificado correspondiente, disponibles en www.acepta.com .

6.4.2 Protección de datos de activación

Los datos de activación requeridos para el manejo de la llave privada de los suscriptores son definidos por éstos mismos, y mantenidos pajo su exclusivo control. Asimismo, para el caso de los datos de activación de **Acepta.com** o sus AC acreditadas, ésta información es mantenida sólo por personal autorizado que ocupa posiciones de confianza dentro de la compañía.

Para iniciar el proceso de generación de la llave privada de **Acepta.com**, se requiere una clave de activación la cual es sólo conocida por los directores de **Acepta.com**. Lo mismo sucede para recuperar la llave privada desde un respaldo físico (ver sección 6.2)

6.5 Controles de seguridad computacionales

6.5.1 Requerimientos técnicos específicos

Acepta.com utiliza sistemas computacionales que han sido configurados para garantizar un adecuado nivel de seguridad, confiabilidad y disponibilidad de los servicios.

Se utilizan mecanismos criptográficos para autentificar a todos los operadores y accesos a las distintas operaciones del sistema de certificación, además de los propios controles de seguridad ofrecidos por los sistemas operativos.

6.5.2 Niveles de seguridad computacional

Acepta.com utiliza plataformas mixtas con sistemas en Windows NT Server 4.0 y Linux Red Hat 6.2.

6.6 Controles técnicos de ciclo de vida

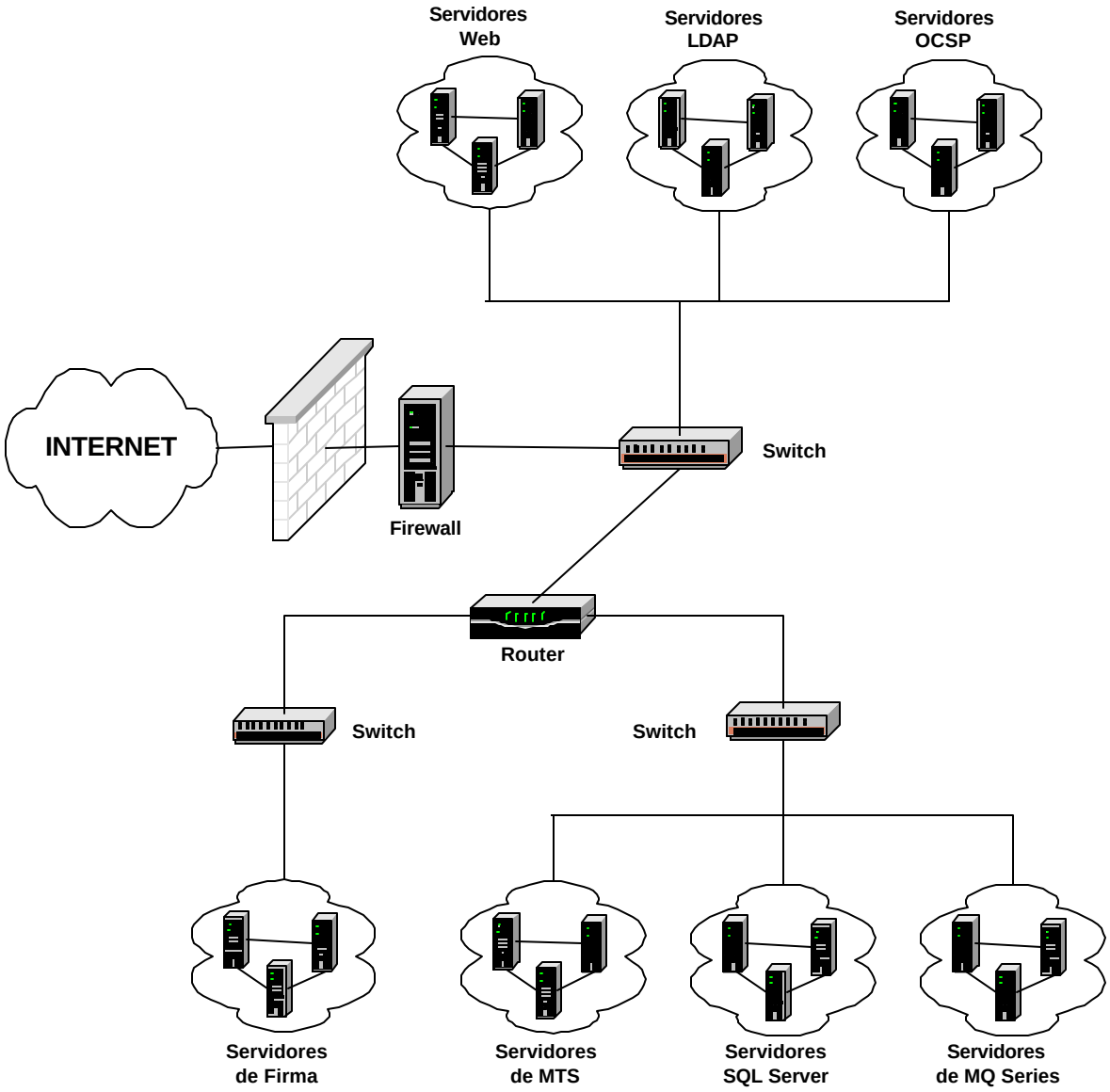
Con el fin de garantizar que los sistemas de software y hardware son diseñados, desarrollados, implementados y operados adecuadamente desde un punto de vista de la seguridad, **Acepta.com** efectúa una serie de controles técnicos en cada etapa del ciclo de vida de los sistemas.

Lo anterior es asegurado mediante auditorias periódicas realizadas por el Departamento de ciencias de la computación de la Universidad de Chile, prestigiosa institución académica a nivel nacional e internacional.

Estas auditorias contemplan una revisión y validación detallada del código, procedimientos y arquitectura de los sistemas de **Acepta.com**, en los que se consideran modelos estándar universalmente aceptados como metodología de evaluación de la seguridad de los sistemas, como son ISO/IEC 15408 o Common Criteria.

6.7 Controles de seguridad de redes

En la siguiente figura se muestra la arquitectura de red de **Acepta.com**:



La arquitectura de red de **Acepta.com** esta diseñada para amortiguar las posibles amenazas y ataques a los servicios de certificación.

Firewalls filtran y monitorean todos los paquetes de datos transmitidos y recibidos en la red. Además, están configurados de tal forma que todos los puertos que no estén en uso están deshabilitados. Asimismo. Sólo los servicios de red requeridos están habilitados.

Con adecuada frecuencia existe un monitoreo el tráfico en la red utilizando para ello herramientas de monitoreo automático. Entre dichas herramientas destacan:

Productos comerciales utilizados para Windows NT y UNIX

Herramientas de libre distribución disponibles para UNIX, incluyendo pero no limitados a:

TCPWrapper, para controlar el acceso a servicios de red

Nessus, nMap, para escanear y monitorear la red

7 FORMATOS DE CERTIFICADOS Y LISTA DE REVOCACIÓN

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). Además se especifica el formato de las listas de revocación (CRL).

7.1 Composición del certificado raíz de Acepta.com

Todos los certificados emitidos por **Acepta.com** están en conformidad con el estándar internacional ITU-T X.509, y recogen las recomendaciones de la PKIX.

El certificado raíz de **Acepta.com** como Autoridad Certificadora tiene la siguiente estructura:

FORMATO DEL CERTIFICADO RAÍZ DE ACEPTA.COM		
CAMPO	***DESCRIPCIÓN***	***VALOR***
Versión	Versión del certificado, que deberá ser versión 3	3
Nº de Serie	Nº que identifica unívocamente al certificado dentro de los emitidos por **Acepta.com**	00
Algoritmo de Firma	Algoritmo utilizado por la AC 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: C = País O = Nombre de la autoridad certificadora emisora OU = Nombre de la autoridad certificadora emisora del tipo de certificado CN =Tipo de certificado E = e-mail de la autoridad certificadora emisora	C = CL O = Acepta.com S.A. OU = Acepta.com autoridad certificadora CN = Acepta.com autoridad certificadora raíz E = caadmin@acepta.com
Periodo de Validez	Fecha de inicio y termino en que es válido el certificado. 10 años, codificado en formato YYMMDDHHMMSSZ	Fecha inicio = 05/01/2001 Fecha termino = 05/01/2011
Nombre del titular	Ídem a lo correspondiente al nombre del emisor.	C = CL O = Acepta.com S.A. OU = Acepta.com autoridad certificadora CN = Acepta.com autoridad certificadora raíz E = caadmin@acepta.com
Clave pública	Clave pública de **Acepta.com**	3082 0108 0282 0101 00C1 1843 F37C B3D3 C346 B45A A8A6 C718 394D F4B3 FBF8 4DC7 2743 E803 22BA 80E2 57C9 5791 6472 C0D5 50D2 E482 6648 A99C E412 BCF0 3B6B 8E29 00D1 A5EC EFA0 0401 24CF 72FB A1D4 AFB2 4116 7D30 53DF 06EC 4591 6C8B 4E85 C791 6AB9 89AD 96D1 81B2 0488 246B DCDD 7029 9D2A BF29 8E80 2E3E 0C4C 7D5A 3BDF 0295 7A62 628E 30C6 D62A 38A9 4737 472F 4894 2D55 DA7E BCE1 4480 FA06 70D1 89B1 EDCE 044C 87E8 CB95 3121 5CD0 8A4B E6A9 0F2B BBF5 C0F5 0E6B C66F 4002 D3B9 EA04 CCBC FEBA B2E5 3FC3 0205 91A3 5439 B9D6 16FD ACEC D15F 1D33 89DE B373 0609 D81D 3C18 5F02 92D4 D419 76C3 8FCA 4EF8 8A08 E654 F4E1 05A7 12B5 36D3 1FDD 5467 F846 7150

TABLA Nº10 – COMPOSICIÓN BÁSICA DE CERTIFICADOS SEGÚN ESTÁNDAR X509V3

El formato de los certificados asociados a las distintas clases de certificados se detalla en el documento con las Políticas de Certificado correspondiente, disponibles en www.acepta.com .

7.1.1 Números de versión(s)

Todos los certificados emitidos corresponden a la versión 3 del estándar X.509

7.1.2 Extensiones

Acepta.com y sus AC acreditadas emiten certificados los cuales contemplan un número de extensiones para mejorar la aplicabilidad, y uso de los certificados. Las extensiones se pueden clasificar en 2 tipos:

- *Extensiones de Restricciones*: Restringen o clarifican el uso de los certificados y las correspondientes claves. Pretenden establecer los limites de uso, políticas aplicables y restricciones adicionales.
- *Extensiones de Información*: Proporciona información adicional a los usuarios de los certificados, pero no limita en cualquier forma el uso de los certificados. Principalmente pretenden brindar información adicional respecto al contenido de los certificados o del sujeto o titular del mismo.

A su vez, éstas pueden ser extensiones estándar o extensiones privadas. Las primeras corresponden a aquellas definidas en el estándar X.509, y las segundas corresponden tanto a extensiones de uso privado definidas por **Acepta.com**, o a extensiones definidas por diferentes organismos y las cuales se soportan para efectos de compatibilidad. En ese sentido, se soportan un conjunto de extensiones privadas recomendadas por Microsoft, Netscape y las sugeridas por la IETF.

A continuación se detallan las extensiones incluidas en el certificado raíz de **Acepta.com** y sus AC acreditadas. Primero se detallan las extensiones estándar, luego las extensiones privadas. Para cada una, se muestra el número identificador asociada para la extensión (OID: Object Identifier). El OID es un número que permite identificar de manera única y global a través de Internet a cada extensión u objeto al que hace referencia. Además se muestra si es una extensión de carácter informativo (INF) o restrictivo (RES).

Las extensiones pertinentes a las distintas clases de certificados se detallan en el documento con las Políticas de Certificado correspondiente, disponibles en www.acepta.com .

EXTENSIONES SEGÚN ESTÁNDAR X.509V3				
Tipo	***Nombre***	***Descripción***	***OID***	***Valor***
RES	BasicConstrains	Establece que es un certificado de AC		Subject Type=CA Path Length Constraint=None
RES	AuthorityKeyIdentifier	Medio para identificar la llave pública de Acepta.com		KeyID=8B50 7988 00E1 6A80 FABE 673B E6AC 86E6 24A9 312A Certificate Issuer: Directory Address: C=CL O=Acepta.com S.A. OU=Acepta.com autoridad certificadora CN=Acepta.com autoridad certificadora raiz E=caadmin@acepta.com Certificate SerialNumber=00
RES	SubjectKeyIdentifier	Identificador único de la llave pública de la AC, conteniendo el hash de 160bit de la llave pública		8B50 7988 00E1 6A80 FABE 673B E6AC 86E6 24A9 312A
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 firma de certificados y firma de CRL (incluido off-line).	2.5.29.15	Certificate Signing , Off-line CRL Signing , CRL Signing(06)
RES	ExtendedKeyUsage	Esta extensión define una serie de propósitos respecto al uso del certificado, adicionalmente a las definidas en KeyUsage.	2.5.29.37	Code Signing(1.3.6.1.5.5.7.3.3) Server Authentication(1.3.6.1.5.5.7.3.1) Client Authentication(1.3.6.1.5.5.7.3.2) Secure Email(1.3.6.1.5.5.7.3.4)
RES	CertificatePolicy	Ver sección 7.1.6		
INF	CrlDistributionPoint	En este campo se establece la localización del CRL correspondiente para consultar sobre revocaciones. Contiene la sgte. estructura: DistribuitonPoint: Un URI para identificar el CRL	2.5.29.31	URL=http://crl.acepta.com/

TABLA Nº12 – EXTENSIONES DE CERTIFICADO SEGÚN ESTÁNDAR X509V3

EXTENSIONES SUGERIDAS POR IETF				
TIPO	***NOMBRE***	***DESCRIPCIÓN***	***OID***	***VALOR***
INF	AuthorityInfoAccessSyntax	En esta extensión se establece información de acceso a servicios de información de la autoridad certificadora. En este momento, establece el acceso para consultas de revocaciones on-line. Contiene la siguiente estructura: AccessMethod: OID identificando el método de acceso vía OCSP AccessLocation: Ubicación del servicio de consulta. vía OCSP	13.6.1.5.5.7.1.1	Access Method: On-line Certificate Status Protocol(1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.acepta.com/

TABLA Nº12 – EXTENSIONES DE CERTIFICADO SUGERIDAS POR EL IETF Y SU GRUPO DE TRABAJO PKIX

EXTENSIONES SOPORTADAS POR NETSCAPE CORPORATION EN SUS PRODUCTOS				
TIPO	**NOMBRE**	**DESCRIPCIÓN**	**OID**	**CRITICA?**
INF	NetscapeCAPoliciesUrl	URL a página Web donde encontrar información de las CPS de Acepta.com		http://www.acepta.com/CPS/
INF	Netscape-base-url	Define un URL base para ser usado por Netscape-url-revocation.	2.16.840.1.113730.1.2	http://www.acepta.com/
INF	Netscape-revocation-url	Es una URL relativa que especifica la ubicación de un servicio de consulta por revocaciones de certificados. Tiene el valor 'asp/check-rev.asp?'	2.16.840.1.113730.1.3	asp/check_rev.asp?

TABLA Nº13 – EXTENSIONES DE CERTIFICADO SUGERIDAS POR NETSCAPE CORPORATION

7.1.3 Objetos identificadores de algoritmos

Bajo la arquitectura definida por estas CPS, todos los certificados emitidos utilizan los siguientes algoritmos y sus correspondientes identificadores (OIDs):

NOMBRE	DESCRIPCIÓN	OID
SHA-1	Algoritmo de generación de hash	1 3 14 2 26 5
RSA	Algoritmo de cifrado de datos	1 3 14 3 2 1 1
RSAWithSHA-1	Algoritmo para firma de certificados. Se usa algoritmo Sha-1 como función hash, y algoritmo RSA para generar la firma.	1 3 14 3 2 15

TABLA Nº15 – OBJETOS IDENTIFICADORES DE ALGORITMOS

7.1.4 Nombres

Ver sección 3.1.

7.1.5 Restricciones para los nombres

Ver sección 3.1.

7.1.6 Objeto identificador de las políticas de certificados

Cada tipo de certificado tiene asociada una "política de certificado", que son las normas que rigen la utilización y aplicabilidad de ese certificado en particular, y las cuales pueden ser consultadas públicamente en www.acepta.com . Las CPS detallan como la AC implementa y soporta las políticas definidas.

Estas políticas se denotan por referencia en todos los certificados emitidos. Para ello, se utiliza la extensión estándar CertificatePolicy, la cual tiene el OID de 2.5.29.32.

Además, se utilizan calificadores, que son información adicional asociado a cada política. Se utilizan calificadores para denotar por referencias estas propias CPS, así como para hacer mención a una notificación al usuario. Estas se detallan en la sección 7.1.7.

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 identificador la identifica únicamente a **Acepta.com** en

un contexto global. Para cada tipo de certificado emitido, existe una política de certificado asociada, La lista de OIDs asociados a cada política es la mostrada en la sgte. página. Los documentos asociados a cada política se encuentran disponibles en www.acepta.com .

7.1.7 Calificadores de política de certificados, sintaxis y semántica

Para el caso del certificado raíz de **Acepta.com**, se representa la siguiente información:

PolicyIdentifier: identificador de la política de certificados correspondiente al tipo de certificado asociado. Esta corresponde a las CPS de **Acepta.com**.

PolicyQualifiers: Calificadores de la política. **Acepta.com** utiliza los siguientes calificadores:

- CPS Pointer: indica la ubicación de las Prácticas de Certificación (CPS) para ser consultada por los usuarios. Es un URL a un documento con las CPS, y es el siguiente www.acepta.com/CPS.
- UserNotice: Indica ubicación de información textual para ser presentada a los usuarios de certificados. El texto explícito se describe en las políticas de certificado correspondiente.

7.1.8 Semántica para el procesamiento de extensiones críticas

Para garantizar una adecuada interoperabilidad y procesamiento de los certificados por distintos sistemas de software, todas las extensiones son no-críticas.

7.2 Composición de la lista de revocación (CRL)

7.2.1 Número de versión(s)

Las listas de revocación manejadas por **Acepta.com** y sus AC acreditadas es la versión 2 según el estándar X.509.

7.2.2 Extensiones

Acepta.com y sus AC acreditadas usan las siguientes extensiones:

EXTENSIONES SOPORTADAS PARA LA LISTA DE REVOCACIÓN	
Nombre	***Descripción***
AuthorityKeyIdentifier	Identificador de la clave de la autoridad certificadora
CRLNumber	Número del CRL emitido

TABLA Nº17 – EXTENSIONES SOPORTADAS PARA LA LISTA DE REVOCACIÓN

8 MANTENCION DE ESTAS CPS

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 políticas 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**.