POLÍTICAS PARA CERTIFICADOS (CP) DE SERVIDOR SEGURO

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.

1 INTRODUCCIÓN

En este documento se definen y detallan las políticas de certificado aplicables a los certificados de servidor seguro, emitidos por **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 Políticas de certificados

Una política de certificado está definida, según el estándar internacional "ISO/IEC 9594-8/ITU-T Recomendación X.509", como "un conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad en particular y/o clase de aplicación con requerimientos de seguridad comunes".

Una explicación detallada de las prácticas que Acepta.com emplea para emitir y gestionar certificados, y que implementa y soporta los requerimientos de estas políticas de certificado, se encuentra en el documento "Prácticas de Certificación (CPS) de Acepta.com".

Estas políticas de certificado o CP, en conjunto con las CPS, son los únicos instrumentos que establecen las reglas aplicables para la solicitud, validación, aceptación, entrega, emisión, y revocación de los certificados, así como las restricciones y aplicaciones en las cuales se deben utilizar dichos certificados de servidor seguro.

Tales políticas 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

La estructura de este documento es análoga a la de las CPS de Acepta.com, detallándose los aspectos pertinentes a los certificados de servidor.

1.2 Identificación

El presente documento se denomina "Políticas de certificado de servidor seguro de Acepta.com", las que internamente se citan como CP.

1.3 Comunidad y Utilización de los certificados

Los certificados digitales de servidor seguro son emitidos para soportar las siguientes necesidades de seguridad:

- **Autentificación:** proporciona garantías respecto a la identidad del servidor,
- **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 a firmado digitalmente dicha transacción.
- **Privacidad:** permitiendo una conexión segura e intercambio confidencial de información con el servidor

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

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. Pertinentes a los certificados de servidor seguro, y 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 cumplir los requerimientos detallados en las CPS de Acepta.com. Específicamente, al emitir certificados de servidor seguro se obliga a lo siguiente:

- Resguardar una copia electrónica de la solicitud de revocación cuando se solicite, el la cual se especificará la fecha y hora en que se recibió dicha solicitud
- Resguardo de un registro electrónico 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 CP y CPS.
- 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 éstas CP
- Mantener los resguardos tecnológicos para evitar cualquier falsificación y adulteración de las llaves privadas mantenidas por **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 las CPS de Acepta.com.

2.1.3 Obligaciones de los suscriptores

Los suscriptores que soliciten certificados de servidor seguro a **Acepta.com**, se obligan a cumplir con los siguientes requerimientos:

- Conocer las normas estipuladas en las CPS y CP 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 este documento, y a las prácticas de certificación definidas por Acepta.com.
- Cancelar las tarifas establecidas para la emisión de un certificado de servidor
- Protección y confidencialidad de su llave privada asociada a la llave pública. Dicha llave es confidencial, generada exclusivamente en el equipo o servidor asociado al certificado. En caso de su pérdida o cualquier circunstancia que comprometa la confidencialidad de dicha llave, se deberá acudir a las oficinas de **Acepta.com** o notificar a través de los servicios ofrecidos port Acepta.com en www.acepta.com de tal circunstancia. La administración de la llave privada es de exclusiva competencia de la organización responsable y legítimamente propietaria del certificado de servidor.
- 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, se obligan a cumplir lo s requerimientos comunes estipulados en las CPS.

2.1.5 Obligaciones respecto a publicación de información de certificados y revocaciones

Corresponden a los requerimientos comunes establecidos en las CPS, sección 2.1.5.

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

2.2.1 Responsabilidades asumidas

Junto con las responsabilidades comunes especificadas en las CPS, Acepta.com es responsable de proporcionar los siguientes mecanismos de prueba, necesarios para dilucidar responsabilidades en caso de cualquier conflicto o perjuicio que se derive por la utilización de los certificados digitales de servidor seguro:

- Si un usuario solicita revocar o suspender un certificado, queda un registro con la fecha y hora en que se realizó la notificación, ya sea por vía electrónica o comprobante impreso si se solicitó personalmente por una persona autorizada. También queda registrada la fecha y hora a partir de la cual el certificado será publicado como inválido, no pudiendo superar ésta última a 12 horas desde la notificación. La fecha de revocación efectiva es comunicada al contacto técnico y administrativo responsables por el servidor vía e-mail firmado digitalmente.
- Si un usuario consulta por el estado de un certificado, y éste es reportado por Acepta.com - a través de una respuesta firmada digitalmente - erróneamente como válido, siendo que fue revocado previamente, fácilmente se puede determinar la responsabilidad de Acepta.com, contrastando dicha

respuesta con el comprobante emitido por Acepta.com en el que se estipula a partir de que momento el certificado debiera haber sido reportado como revocado.

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 CP y las CPS por parte de los suscriptores o terceras partes interesadas.

2.3 Responsabilidades financieras

2.3.1 Indemnizaciones

Tanto respecto de los suscriptores que contraten los servicios de certificación digital y que acepten las presentes CP y CPS, como respecto de los terceros que adhieran a ella, Acepta.com declara que:

En la eventualidad de haberse consultado por el estado de un certificado de clase 3 de persona, por medio de los servicios de consulta electrónica vía el protocolo OCSP que Acepta.com proporciona, y que habiéndose obtenido una respuesta electrónica firmada digitalmente por Acepta.com respecto al estado de tal certificado, se establece que Acepta.com se hace responsable por la validez de dicha respuesta, y delimita su responsabilidad hasta 5000 US$ como monto máximo o de tope, con total independencia del número de firmas digitales y de transacciones para las cuales sea utilizado dicho certificado.

Las responsabilidades limitadas en la forma señalada, rigen y se aplica para toda clase de daños y perjuicios, cualquiera sea su clase y naturaleza. Estos se aplican tanto para el suscriptor o signatario titular del mismo y del tercero o receptor confiado que acepte su valor y adhiera a estas CP.

2.4 Normas respecto a aplicabilidad de estas CP

Los estatutos legales que rigen la aplicabilidad de las Políticas de Certificado establecidas por Acepta.com están estipuladas en las CPS.

2.5 Tarifas

2.5.1 Tarifas para emisión de certificados

Las tarifas anuales por concepto de la emisión de certificados están disponibles en el sitio Web en www.acepta.com .

2.6 Publicaciones

Acepta.com publica en su sitio Web en www.acepta.com, las políticas de certificado aplicables a los certificados de servidor seguro, así como las Prácticas de Certificación (CPS), 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.

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 de servidor seguro, previamente a la emisión propiamente tal.

3.1 Registro inicial

3.1.1 Tipos, interpretación y unicidad de nombres

En los certificados se incluirá el nombre distintivo especificado en el requerimiento de firma de certificado proporcionado por la entidad legítimamente dueña del servidor, en un formato consistente con las especificaciones para certificados X.509v3.

3.1.2 Método para probar posesión de la llave privada

La llave privada asociada a un certificado digital de servidor emitido por **Acepta.com** o alguna de sus AC acreditadas es siempre generada exclusivamente en el propio servidor, a través de la herramienta administrativa correspondiente.

3.1.3 Autentificación de identidades de servidores

Para autentificar la identidad del servidor se valida que el nombre de dominio esté inscrito y que los contactos administrativos y técnicos correspondan a las personas y entidad que solicita el certificado. Además se valida que dicha entidad esté legalmente constituida, consultando bases de datos públicas y requiriendo los antecedentes necesarios que acrediten tal situación.

3.2 Renovación de Certificados

Los certificados tendrán un período de vigencia de 1 año. 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**.

Al vencimiento del certificado se podrá solicitar una renovación del mismo por un período adicional , en cuyo caso deberá así solicitarlo mediante e-mail dirigido al administrador del sitio de **Acepta.com** (e-mail: admin@acepta.com) con una antelación mínima de 30 días a la fecha de su caducidad, o llenando el formulario que al efecto se contenga en el sitio web de Acepta.com.

En el evento que hayan transcurrido más de cuatro (4) años desde la emisión del primer certificado, esto es, la emisión de un certificado y tres renovaciones posteriores, no se dará curso a una nueva solicitud de renovación y el suscriptor o signatario deberá solicitar un nuevo certificado.

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.

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.

Los procedimientos aplicables para la revocación o suspensión de certificados se detallan en el punto 4.5.

4 REQUERIMIENTOS OPERACIONALES

En este capítulo se describen los requisitos operativos pertinentes a las etapas de certificación, conducentes a la obtención de un certificado de servidor seguro. 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 solicitar certificados de servidor seguro

La información que se debe proporcionar al solicitar un certificado de servidor seguro, así como el mecanismo de entrega de dichos antecedentes son los siguientes:

SOLICITUD DE CERTIFICADO DE SERVIDOR SEGURO	
INFORMACIÓN REQUERIDA	***RECEPCIÓN DE ANTECEDENTES***
Archivo de texto con requerimiento de firma de certificado (CSR), generado en el propio servidor por la herramienta administrativa correspondiente. Dicho archivo debe estar en el formato PKCS#10 y contener la siguiente información: Nombre de dominio del servidor Nombre de la organización a la que pertenece el servidor Rol Único Tributario (RUT) si corresponde Unidad organizacional dentro de la entidad que corresponde al servidor (opcional) Ciudad de residencia de la organización (opcional) Estado o provincia de residencia de la organización(opcional) País Antecedentes de contacto. Se deberá proporcionar el R.U.T.,nombre, teléfono, y e-mail de un contacto técnico, y contacto administrativo. Clave de acceso o PIN. Esta clave será requerida posteriormente si se solicita la revocación del certificado. Tipo de servidor, con el cual se generó el CSR Antecedentes legalizados que acrediten que la organización existe y está legalmente constituida. Información de cómo se efectuará el pago.	Se copia el contenido del CSR, antecedentes de contacto, y clave de acceso en un formulario disponible para tales efectos en el sitio Web www.acepta.com , y se envía a Acepta.com. Dicho formulario electrónico es enviado a través de una conexión segura, resguardando la privacidad de la información proporcionada. Se envía por correo o entregar directamente los antecedentes legalizados a las oficinas de Acepta.com..

Tabla Nº 1 – Solicitud de certificado de servidor seguro

4.2 Validación y aprobación de certificados

Luego que los antecedentes son remitidos a **Acepta.com**, se procede a su validación necesaria para verificar la consistencia de dichos antecedentes en relación con petición de firma de certificado correspondiente (CSR). También se valida que el nombre de dominio seleccionado corresponda a un nombre legítimamente inscrito por la organización. Para ello, un operador calificado obtiene y revisa las peticiones pendientes, corroborando la siguiente información:

- Verifica que la información del nombre de dominio esté inscrito a nombre de la organización estipulada en el CSR. Para ello, se consulta a la autoridad de dominio que corresponda.
- Verifica que el nombre de la organización del CSR corresponda a los antecedentes legalizados que acreditan la existencia de la organización
- Verifica que el contacto administrativo corresponda al definido en la inscripción de dominio, según conste en al autoridad de dominio correspondiente

Si las validaciones anteriores son exitosas, entonces el operador aprueba inicialmente la solicitud, con lo que se envía automáticamente una notificación a la dirección de e-mail de los contactos administrativo y técnico. Adicionalmente, se podrá realizar consultas a bases de datos públicas para corroborar la identidad de la organización, como el S.I.I. y Dicom para el caso de organizaciones constituidas en Chile, y otras fuentes de información similares para organizaciones extranjeras.

4.3 Emisión e instalación

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

1.- Una vez aprobada la petición de certificado proporcionada por la organización, se emite el certificado y se envía por e-mail a la dirección de correo electrónico establecidas para el contacto técnico y administrativo, junto con las instrucciones para su activación. Adicionalmente, se podrá recuperar dicho certificado a través de los servicios disponibles en el sitio Web de Acepta.com en www.acepta.com.

Dicho certificado se entrega en un formato adecuado para el tipo de servidor, el cual fue definido en el momento de generar la solicitud.

2.- Se revisa el contenido del certificado y se notifica su conformidad a Acepta.com a través de formulario establecido para tales efectos en www.acepta.com. En caso de ser aceptado el certificado, se procede automáticamente a activar el certificado quedando como válido y disponible para ser consultado en www.acepta.com .

En el formulario mencionado se podrá declarar y notificar de cualquier disconformidad que se tuviese con relación al certificado emitido.

3.- Se instala el certificado en el servidor mediante la herramienta administrativa correspondiente

4.4 Proceso de suspensión y revocación de certificados

Un certificado digital emitido por **Acepta.com** o una de sus Autoridades Certificadoras acreditadas, podrá ser revocado previamente al 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.

4.5 Causales y procedimientos para revocar o suspender certificados

Un certificado de servidor seguro deberá ser revocado si concurre alguna de las siguientes circunstancias:

- Compromiso de la llave privada del servidor
- Modificación posterior de los antecedentes de la organización suscriptora del certificado
- Falsificación de los antecedentes de la organización suscriptora del certificado

Se podrá solicitar que un certificado sea suspendido sólo como medida precautoria frente a un posible compromiso de la llave privada.

Para solicitar la revocación, se deberá llenar un formulario establecido para tales efectos en www.acepta.com , en donde se requerirá ingresar el PIN o clave de acceso proporcionada en el

momento de solicitar el certificado. Al recibir dicha solicitud, automáticamente se procede a revocar el certificado correspondiente, por lo que dicha información estará disponible para consultas on-line en **Acepta.com**. Se notifica por e-mail firmado digitalmente al contacto administrativo y técnico de la fecha y hora a partir de la cual se hace efectiva la revocación.

Adicionalmente, se publicará una lista de revocación con los certificados revocados, con una frecuencia de 12 horas.

En caso de perdida del PIN necesario para efectuar la revocación, el contacto administrativo deberá comunicarse con las oficinas de **Acepta.com**.

4.5.1 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) .

La información respecto a la revocación o suspensión de un certificado de servidor seguro 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 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 servidor asociado.

Para brindar un adecuado servicio de información sobre las revocaciones y suspensiones, **Acepta.com** y las AC acreditadas soportarán 3 medios para distribuir dicha información, las cuales se detallan a continuación:

4.5.1.1 LISTAS DE REVOCACIÓN (CRL)

Acepta.com y las AC acreditadas mantendrán listas de revocación o CRL con la información de los certificados de servidor 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.

4.5.1.2 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.

4.5.1.3 CONSULTA MEDIANTE EL WEB

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

4.5.2 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.

4.6 Procedimientos de auditoria de seguridad

Los mecanismos de auditoria son los mismos para cada tipo de certificado, y están estipuladas en las CPS.

4.7 Políticas para archivo de registros

4.7.1 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 los siguientes documentos:

DOCUMENTOS ARCHIVADOS				
Documento	***Descripción***	***Retención***	***Protección***	***Respaldo***
Solicitud de certificado	Se almacenará copia digital de todos los antecedentes proporcionados al solicitar el certificado.	Por un año posterior a vencimiento del certificado	Copia digital se almacenará cifrada en custodia electrónica en Custodium.com	De forma incremental diariamente, y luego se realizará un respaldo semanal y uno completo una vez al mes.
Notificación de aceptación del certificado	Se almacenará una copia digital cifrada de la notificación de aceptación del certificado realizada en el proceso de instalación	Por un año posterior a vencimiento del certificado		
Solicitud de Revocación o Suspensión	Se almacenará una copia digital cifrada de la solicitud de revocación o suspensión de certificados.	Por un año posterior a vencimiento del certificado		

TABLA Nº1 – DOCUMENTOS ARCHIVADOS

5 CONTROLES DE SEGURIDAD FÍSICOS, DE PROCEDIMIENTOS Y DE PERSONAL

Los controles y procedimientos establecidos para garantizar una operación de los servicios de certificación bajo un ambiente seguro, desde el punto de vista de la seguridad de las dependencias físicas, las conductas y capacidad del personal, así como las capacidades de recuperación frente a desastres, está establecido en las CPS de Acepta.com. Dichos controles se aplican por igual para la emisión de todos los tipos de certificados.

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 de servidor seguro y llaves asociadas.

6.1 Generación e instalación del par de llaves

6.1.1 Generación de llaves de los suscriptores de certificados

El par de llaves pública y privada asociadas al servidor son generadas en el propio servidor por la herramienta administrativa correspondiente.

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

Al momento de emitir el certificado, se proporciona adicionalmente el certificado raíz de **Acepta.com**, y el Certificado Raíz de Servidor de **Acepta.com**.

6.1.3 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 certificados de servidor son de un tamaño de 1024 bits.

6.1.4 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 según los mecanismos descritos en las CPS.

6.3 Otros aspectos de gestión de claves

6.3.1 Archivo de llaves publicas

Las llaves públicas de los suscriptores 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

En el momento de solicitar un certificado de servidor seguro, se requiere que se proporcione una clave de activación o PIN, el cual será requerido posteriormente cuando se solicite la revocación del certificado. Este dato es generado por la propia persona que ingresa la solicitud.

6.4.2 Protección de datos de activación

El PIN mencionado anteriormente debe mantenerse con la adecuada confidencialidad, por personal debidamente autorizado de la organización que solicita el certificado de servidor seguro.

6.5 Controles de seguridad computacionales

Acepta.com implementa una serie de controles que le permiten un adecuado resguardo de sus recursos computacionales, lo que está descrito en las CPS de **Acepta.com**.

7 FORMATOS DE CERTIFICADOS Y LISTA DE REVOCACIÓN

Este capítulo contiene especificaciones detalladas de los formatos y contenido de los certificados de servidor seguro (campos, básicos y extensiones). Además se especifica el formato de las listas de revocación (CRL).

7.1 Composición básica de los certificados

En esta sección se detalla la composición y formato de los certificados emitidos por **Acepta.com** y sus AC acreditadas. Dichos certificados están en conformidad con el estándar internacional ITU-T X.509v3.

FORMATO DE CERTIFICADOS DE CLASE 3 DE PERSONA		
CAMPO	***DESCRIPCIÓN***	***EJEMPLO***
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	0234865AF87AC87CCB2
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 certificado raíz de servidor E = info-servidor@acepta.com
Periodo de Validez	Fecha de inicio y termino en que es válido el certificado. Para AC = 10 años, para servidores = 1 año. Codificado en formato YYMMDDHHMMSSZ	Fecha inicio = 29/11/2001 Fecha termino = 29/01/2002
Nombre del titular	Nombre distintivo (DN) del titular del certificado, en el formato del estándar X..500. Deben incluirse los siguientes tipos: C = País O = Nombre de la organización OU = Unidad organizacional (opcional) L = Localidad o ciudad (opcional) S = Estado o provincia (opcional) CN = Nombre de dominio del servidor	C = Chile O = Custodium.com S.A. L = Santiago S = Región Metropolitana OU = Tecnología CN = www.custodium.com
Clave pública	Clave pública del titular del certificado	3081 8902 8181 00C0 476C 477B E5D3 7598 AB7F 6C84 5B80 08F2 9376 3954 2260 3B43 53A9 2885 D308 C57D 5441 D066 86EF 4AE5 15D8 0730 FFFC 43B0 5DF4 EC5F 1817 69F2 4B26 DB57 4C2C 8C4C 7BED 418C E92D 46AF BF0E A39F 45E1 5FA7 AC3C CA5C B4A7 A18D 763F 39E5 8100 549F A9B0 E0C8 93A7 B085 5ADF 5339 C853 A8E1 B17C 9DD6 F0EF 67CD E399 EF51 50FD 4B02 0301 0001

TABLA Nº2 – COMPOSICIÓN BÁSICA DE CERTIFICADOS SEGÚN ESTÁNDAR X509V3

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 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 los certificados de clase 3 de persona. 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).

EXTENSIONES SEGÚN ESTÁNDAR X.509V3				
Tipo	***Nombre***	***Descripción***	***OID***	***Valor***
RES	KeyUsage	Esta extensión define el propósito para el cual deben ser usadas las claves correspondientes al certificado. El certificado debe ser utilizado sólo para los propósitos definidos por esta extensión.	2.5.29.15	Digital Signature , Non-Repudiation , Key Encipherment(E0)
RES	ExtendedKeyUsage	Esta extensión define una serie de propósitos respecto al uso del certificado, adicionalmente a las definidas en KeyUsage. El certificado debe ser utilizado sólo para los propósitos definidos por esta extensión.	2.5.29.37	Server Authentication(1.3.6.1.5.5.7.3.1) Client Authentication(1.3.6.1.5.5.7.3.2)
RES	AuthorityKeyIdentifier	Medio para identificar la llave pública de Acepta.com El campo KeyId es idéntico al valor de la extensión SubjectKeyIdentifier		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	CertificatePolicy	Ver sección 7.1.6		
INF	SubjectAltName	Extensión opcional que permite definir términos que identifican únicamente a la organización titular del certificado, adicionalmente a lo establecido en el campo estándar Subject. Se podrán registrar los siguientes campos adicionales: OtherName: Se registra el RUT de la organización (si correspondiese), en la siguiente estructura: Type-id = 1.3.6.1.5.5.7.8.2 Value =’xx.xxx.xx-v’ El campo Value es un IA5String		Other Name: 1.3.6.1.4.1.6891.7= 040C 3132 2E35 3233 2E39 3132 2D39
INF	CrlDistributionPoint	En este campo se establece la localización del CRL correspondiente para consultar sobre revocaciones de certificado de servidor. Contiene la sgte. estructura: DistribuitonPoint: Un URL para identificar el CRL	2.5.29.31	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.acepta.com/ClaseServidor.crl

TABLA Nº3 – 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. En este caso, corresponde al protocolo OCSP, con OID=13.6.1.48.1 AccessLocation: Ubicación del servicio de consulta OCSP	13.6.1.5.5.7.1.1	[1]Authority Info Access Access Method=On-line Certificate Status Protocol(1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.acepta.com/

TABLA Nº4 – 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**	**VALOR**
INF	Netscape-base-url	Define un URL base para ser usado por Netscape-url-revocation.	2.16.840.1.113730.1.2	https://www.acepta.com/servicios/
INF	NetscapeComments	Descripción del servidor		
INF	Netscape-revocation-url	Es una URL relativa que especifica la ubicación de un servicio de consulta por revocaciones de certificados.	2.16.840.1.113730.1.3	check_rev_ns.asp

TABLA Nº5 – 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 Nº6 – OBJETOS IDENTIFICADORES DE ALGORITMOS

7.1.4 Nombres

Ver sección 3.1

7.1.5 Restricciones para los nombres

Para los nombres asociados a correo electrónico, se deberá utilizar el formato según RFC822.

7.1.6 Objeto identificador de las políticas de certificados

Estas políticas de certificado son identificadas mediante un número único, denominado Object Identifier (OID), según el estándar X.509. Dicho número es incluido en el certificado para hacer referencia a éstas políticas.

Para obtener identificadores únicos, **Acepta.com** ha registrado un número que la identifica como empresa, en la Internet Assigned Number Authority (IANA), organización internacional que administra un conjunto de estos números para Internet, y asegura que sean únicos.

El OID para **Acepta.com** es el 1.3.6.1.4.1.6891.

El OID de las políticas de certificado de servidor seguro es el 1.3.6.1.4.1.6891.5

7.1.7 Calificadores de política de certificados, sintaxis y semántica

En dicha extensión, se representa la siguiente información:

PolicyIdentifier: identificador de la política de certificados correspondiente al tipo de certificado asociado.

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. Esta notificación contiene el siguiente texto:

  "La utilización de éste certificado está sujeta a las políticas de certificado (CP) y prácticas de certificación (CPS) establecidas por Acepta.com, y disponibles públicamente en www.acepta.com."

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 Nº7 – EXTENSIONES SOPORTADAS PARA LA LISTA DE REVOCACIÓN

8 MANTENCION DE ESTAS CP

8.1 Procedimientos para cambios en las CP

Las políticas de certificado de clase 3 de persona 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 CP 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 CP

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