ACEPTA

Empresas
a velocidad
digital

Plan de Privacidad

Septiembre 2016

RESPONSABLES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Certificación y seguridad	-Gerente de certificación y seguridad.	Gerente General Comité de Seguridad

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
Plan de Privacidad	1.0	Primera versión	08-09-2016
Plan de Privacidad	4.0	Revisión Anual	01-10-2016
Plan de Privacidad	5.0	Revisión Anual	01-10-2017

CLASIFICACIÓN DEL DOCUMENTO

NIVEL DE CRITICIDAD: Baja **NIVEL DE CONFIDENCIALIDAD:** Pública
NOTA DE CONFIDENCIALIDAD: Se encuentra disponible ante su solicitud.

CONTROL DE DIFUSIÓN

AUTOR/ES: Gerencia de Certificación y Seguridad
DISTRIBUCIÓN: • Ministerio de Economía. • Personal de Acepta. • Sitio Web

REFERENCIAS

Documentos Internos	
Título	**Nombre del archivo**
Política de Privacidad	Política de Privacidad.doc
Documentos Externos	
Ley N° 19.628 (Chile) Ley N° 29733 (Perú) MARCO DE PRIVACIDAD DEL FORO DE COOPERACIÓN ECONÓMICA ASIA PACÍFICO (APEC)	

ÍNDICE

1.- TÉRMINOS GENERALES

ACEPTA fue fundada a principios del año 2000, con la misión de crear un sistema de claves públicas para que Chile aproveche el estado del arte a nivel internacional, pero aplicado según las necesidades y normativas legales propias de Chile.

En el año 2001, el Servicio de Impuestos Internos de Chile acreditó a ACEPTA como el primer Prestador de Servicios de Certificación autorizado para emitir certificados de firma electrónica reconocidos en el ámbito tributario. Las políticas acreditadas son las de los Certificados Clase 3 para Persona Natural. Posteriormente, las mismas políticas fueron acreditadas por el Servicio Nacional de Aduanas, el año 2002, permitiendo usar estos certificados en el ámbito aduanero.

ACEPTA ha trabajado en Chile en desarrollar aplicaciones en donde el uso de certificados de firma electrónica aporte valor al sector público y privado. El desarrollo de la factura electrónica es el principal resultado de este trabajo, mercado en el que ACEPTA participó en Alianza con Telefónica Empresas y logró un 45% de participación, aventajando por más del doble a su seguidor más cercano.

Otras aplicaciones implementadas son las del sistema de evaluación de impacto ambiental de CONAMA y las declaraciones juradas de SOFOFA. En ambos casos se aprovecha el Plug-In CA4Web para firmar electrónicamente documentos visualizados en un browser.

ACEPTA ha modificado en Chile sus políticas de los certificados Clase 3, agregándoles requerimientos adicionales impuestos por la Ley 19.799 para aumentar su nivel de seguridad y permitir la generación de firma electrónica avanzada. Estas nuevas políticas de certificación son fiscalizadas anualmente durante el proceso de acreditación por parte del Ministerio de Economía.

ACEPTA en la actualidad se encuentra trabajando a fin de cumplir con las regulaciones y leyes de Perú a fin de poder prestar los mismos servicios de Entidad de Certificación y de Registro, ambos servicios bajo la supervisión e inspección de la entidad reguladora de ese país que es INDECOPI.

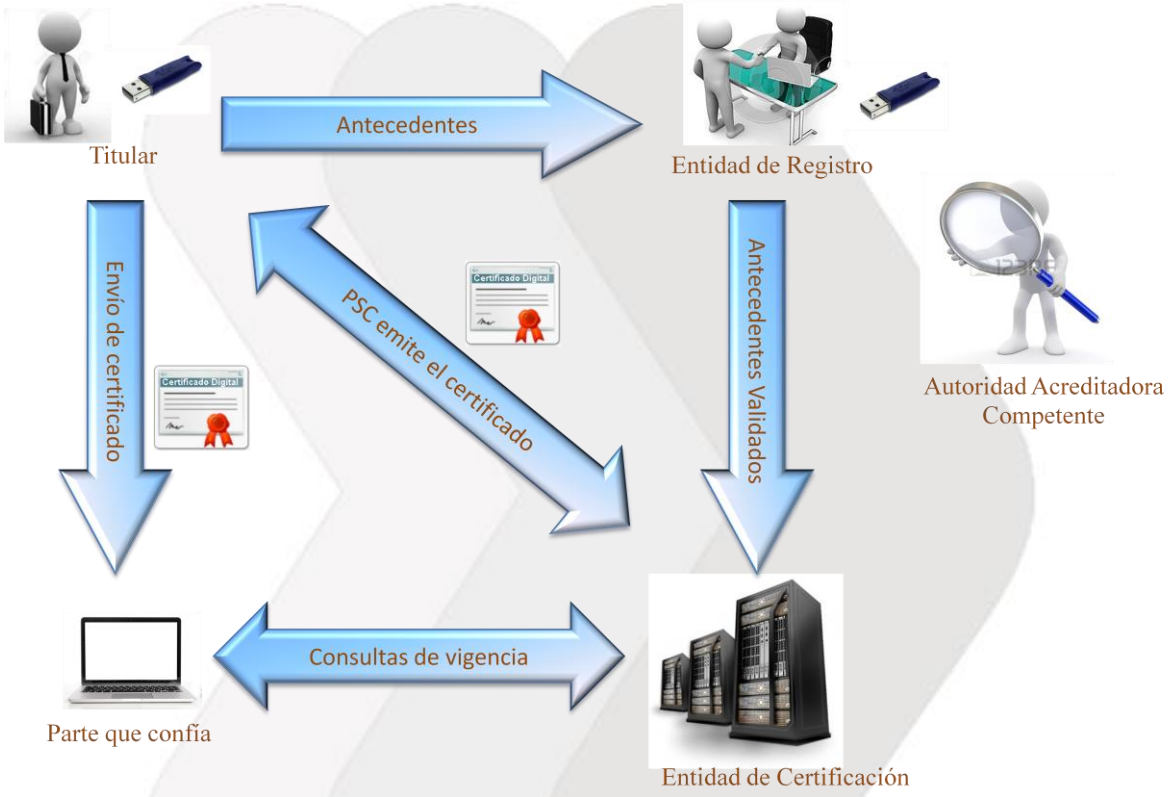
1.1.- Definiciones y Acrónimos

El alcance de las definiciones del documento de Políticas de Certificación, se entenderá como:

- **Autoridad de Certificación (AC):** Es aquella entidad que en conformidad con la legislación vigente de firma electrónica, emite certificados electrónicos en Chile
- **Autoridad de Registro (AR):** Es aquella entidad designada por Acepta que realiza la verificación de identidad de los solicitantes de certificados en Chile
- **Entidad de Certificación (EC):** Es aquella entidad que en conformidad con la legislación vigente de firma digital, emite certificados electrónicos en Perú
- **Entidad de Registro (ER):** Es aquella entidad designada por Acepta, que realiza la verificación de identidad de los solicitantes de certificados en Perú
- **Firma electrónica avanzada (FEA):** En Chile es aquella firma electrónica que permite establecer la identidad personal del suscriptor respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al suscriptor, como a los datos a que se refiere, y por haber sido creada por medios que mantiene bajo su exclusivo control.
- **Firma digital (FD):** En Perú, es la firma electrónica que usa técnica criptográfica asimétrica. Las firmas digitales son generadas a partir de certificados que son:
    - Emitidos por EC controlada por AAC
    - Incorporados la IOFE por acuerdos cruzados
    - Por reconocimiento mutuo de la AAC
    - Por EC extranjeras incorporadas a la IOFE
- **AAC**: Autoridad Administrativa Competente, encargada de aprobar las políticas de certificación, verificación y valor agregado, prácticas de certificación y planes de privacidad. Responsable de acreditar las ER, acreditar los prestadores de SVA, registrar a los prestadores de servicios de certificación digital, supervisar a los PSCD, cancelar acreditaciones, publicar los PSCD acreditados, aprobar estándares, suscribir acuerdos de reconocimiento mutuo con AAE (Autoridades Administrativas Extranjeras), Autorizar la certificación cruzada con EC Extranjeras, fomentar el uso de la IOFE. Para el caso de Perú esta labor la desempeña INDECOPI.
- **IOFE:** En Perú corresponde a la Infraestructura Oficial de Firma Electrónica

2.- PARTICIPANTES

Los servicios de certificados de firma electrónica o clave pública de Acepta están insertos en una infraestructura en que se relacionan distintas entidades. Básicamente existen 5 tipos: Prestador de Servicios de Certificación (PSC), Entidad de Registro (ER), Suscriptor, terceras partes que confían en los certificados y Entidad acreditadora. La siguiente figura muestra dicha relación:



2.1.- Comunidad de usuarios

- Solicitante: Son las personas que concurren a Acepta a solicitar un certificado de firma electrónica avanzada, completan el formulario de solicitud y proveen todos los antecedentes que exige la ley y sus prácticas de certificación, para comprobar fehacientemente su identidad.
- Titulares: Son las personas titulares de los datos de creación de firma a quienes le corresponde o está asociada la clave pública informada en los certificados de firma electrónica avanzada. Los suscriptores son personas naturales, sin perjuicio que puedan concurrir en la suscripción documental en nombre propio o en la representación de alguna persona jurídica.

- Entidad de registro: La recepción y procesamiento de las solicitudes de certificados es realizada por la "Entidad de Registro" (ER) de Acepta, sea que lo haga directamente o a través de un mandatario especialmente designado para tal objeto. La Entidad de Registro debe realizar la comprobación fehaciente de la identidad de los solicitantes de certificados de firma electrónica avanzada. En caso que sea un tercero el que actúe, en calidad de mandatario de Acepta, como Entidad de Registro, la actividad deberá desarrollarla dando pleno cumplimiento al contrato de mandato y a esta Declaración de Prácticas de Certificación.
- Prestador de Servicios de Certificación ("PSC"): Es la entidad prestadora de los servicios de certificación de firma electrónica avanzada (EC), de conformidad a la ley, en particular, a lo previsto en la Ley 19.799 para Chile y Ley 27269, para el caso de Perú, sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma, que en este caso es Acepta.
- Tercera parte que confía: Es el receptor de un certificado de firma electrónica avanzada. Normalmente, junto con el certificado este tercero recibe un documento electrónico que se encuentra suscrito con la firma electrónica avanzada del suscriptor. La parte que confía debe contar con mecanismos que le permitan validar si se trata de un certificado auténtico y si este certificado se encontraba vigente en el momento en que se produjo la suscripción documental.
- Autoridad Acreditadora Competente: Para el caso de Chile, corresponde a la Subsecretaría de Economía, de conformidad con lo dispuesto en la Ley 19.799. En el caso de Perú, el DS 0019 -2002 designa al Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) como la Autoridad Acreditadora Competente conforme al Art 15 de ley 27269

3.- ALCANCE

La política de privacidad de ACEPTA es de cumplimiento obligatorio para su personal, que participa en operaciones críticas de los servicios descritos en sus prácticas de certificación

4.- INFORMACIÓN RECOLECTADA Y PROTEGIDA

Como parte de las operaciones de registro y en su calidad de ER (Entidad de registro) de la EC (Entidad de Certificación) de ACEPTA, es que su ER recolecta la información de los suscriptores y titulares asociada a:

- Datos de identificación personal, impresión dactilar, poderes de representación (si corresponde); incluyendo la fotografía que aparece en su documento de identidad
- Contrato de solicitud de servicios que realizan los suscriptores

5.- TRATAMIENTO DE DATOS PERSONALES

ACEPTA, considera como información pública aquella información personal que esté públicamente disponible o es conseguida legalmente desde:

- Registros gubernamentales que se encuentran disponibles al público;
- Reportes periodísticos; o
- Información requerida por ley para hacerse disponible al público.
- La contenida en la Declaración de Prácticas de Certificación de Acepta.
- La contenida en las diferentes Políticas de Certificación de Acepta.
- Los certificados emitidos así como las informaciones que ellos contienen.
- La lista de certificados revocados (CRL).
- Toda aquella información que sea calificada como "PÚBLICA".

Para este tipo de información no se necesitará autorización del usuario para su publicación.

ACEPTA entiende por información privada la siguiente:

- En conformidad con la Norma Marco sobre privacidad del APEC, aquella información relativa a un individuo identificado o identificable, que permita construir el perfil las actividades del usuario

Acepta adhiere Acepta, adhiere y efectúa sus operaciones en conformidad con lo establecido por la Ley Nº 19.628, sobre Protección de la Vida Privada (Chile), así como la Ley N° 29.733 (Perú) sobre Protección de Datos Personales.

ACEPTA solicitará el consentimiento del individuo identificado para el tratamiento y almacenamiento de estos datos de manera voluntaria. Lo anterior se encontrará tanto en el contrato de suscripción, sus prácticas de certificación y su política de privacidad. Adicionalmente Acepta no podrá divulgar a terceros (a menos que sea legalmente solicitado por un tribunal competente):

- Las claves privadas de las entidades que componen a Acepta.
- Toda información relativa a las operaciones que lleve a cabo Acepta.
- Toda información relativa a los controles de seguridad y procedimientos de auditoría.
- Toda la información de carácter personal proporcionada a Acepta durante el proceso de registro de los suscriptores de certificados.
- Planes de continuidad de negocio y de emergencia.

- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Toda la información clasificada como “CONFIDENCIAL”.

Cualquier violación a estas clausulas será sancionada por ACEPTA.

6.- FLUJO TRANSFRONTERIZO DE DATOS PERSONALES

Los contratos de los suscriptores contendrán cláusulas que soliciten el consentimiento del suscriptor y titular de transferir los datos personales contenidos en el certificado digital a los países donde se encuentren instalada ACEPTA.

7.- IMPLEMENTACIÓN DE LOS PRINCIPIOS DE PRIVACIDAD

Este capítulo adopta lo establecido en el Marco de la APEC, en lo que respecta a la Norma Marco sobre Privacidad, respecto a principios a ser seguidos durante funciones que involucren la recolección, procesamiento, posesión, uso, transferencia o revelación de información personal de carácter privado.

7.1.- Medidas preventivas

ACEPTA mantiene un sistema de seguridad de la información, el cual permite mitigar los riesgos a lo que se ven enfrentados los activos de información en las dimensiones de Disponibilidad, Integridad, Disponibilidad, Trazabilidad y Confidencialidad. Para ello ACEPTA cuenta con:

- Una política de seguridad de la información
- Un análisis de riesgo periódico
- Un plan de acción que permiten mitigar las brechas de seguridad
- Controles de seguridad física, de procedimientos y humanos
- Políticas y prácticas de certificación de acuerdo a RFC3647 (*Internet X.509 Public Key Infrastructure Certificate*)
- Comité de seguridad de la información
- Oficial de seguridad de la información
- Procedimientos para recuperación de desastres
- Una gestión documental y de registros
- Auditorías de seguridad de la información de manera periódica

7.2.- Información

Remítase a punto 4 de este documento

7.3.- Limitaciones de recolección

La información que es capturada por ACEPTA es sólo aquella relevante para el propósito para el cual se recolecta. Detalle de la información recolectada se puede ver en las prácticas de certificación de ACEPTA; siendo principalmente:

- Datos de identificación personal, impresión dactilar, poderes de representación (si corresponde); incluyendo la fotografía que aparece en su documento de identidad
- Contrato de solicitud de servicios que realizan los suscriptores

Esta recolección es bajo el consentimiento del individuo al cual pertenece, lo que es ratificado en su contrato de suscripción.

7.4.- Uso de información personal

ACEPTA usa la información recolectada sólo para el propósito para el cual fue capturada y bajo el consentimiento del individuo al cual pertenece, lo que es ratificado en su contrato de suscripción. Esta información es recolectada en virtud de un servicio o producto solicitado y que es definida en las prácticas de certificación del producto o servicio particular. Si esta recolección fue realizada por mandato, ACEPTA debe contar con la evidencia de dicha solicitud.

7.5.- Elección

Cuando sea posible ACEPTA entregará procedimientos y elementos que permitan al solicitante tomar una decisión informada respecto a entregar o no la información solicitada, ello a través de medios tales como:

- Su política de privacidad, políticas y prácticas de certificación publicada en la página web
- En los mismos contratos de suscripción

Lo anterior no es necesario en caso de tratarse de información públicamente disponible

7.6.- Integridad de información personal

Acepta realiza un análisis anual de riesgos, planes de acción que mitiguen los mismos, así como auditorías de seguridad (ISO 27001:2013), de manera tal que la información capturada permanezca completa, exacta y actualizada cuando sea necesario y posible.

7.7.- Salvaguardas de seguridad

ACEPTA mantiene un plan de seguridad de la información, basado en su análisis anual de riesgo, bajo la norma ISO 27001:2013 y los controles definidos en la norma ISO 27002, a fin de evitar la pérdida, acceso indebido, destrucción, uso, modificación o revelación no autorizada de la información privada que ha recolectado

7.8.- Acceso y corrección

Los individuos que han entregado información a Acepta, deberán verificar y asegurar que la información contenida en el certificado es fidedigna; informando a Acepta ante cualquier información incorrecta o inexacta detectada en dicho certificado, o cambio que se haya generado respecto a la información originalmente entregada para la emisión de dicho certificado.

7.9.- Responsabilidad

El Oficial de Cumplimiento de ACEPTA, en conjunto con el Comité de Seguridad aprobarán, asignarán los recursos y gestionará la implementación de los controles definidos, velando por el cumplimiento de las políticas de privacidad, así como de su revisión periódica, actualización, difusión, concientización y capacitación al personal y terceros para su adecuado cumplimiento.

8.- CONFORMIDAD

Este documento ha sido aprobado por ACEPTA y su comité de seguridad de la información, y cualquier incumplimiento por parte de los empleados, contratistas y terceros mencionados en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.