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
Plan de Privacidad	5.1	Ajuste Oficial de Seguridad y Privacidad	06-04-2018
Plan de Privacidad	5.2	Ajustes nomenclatura y aplicabilidad para el caso de Chile	05-06-2018
Plan de Privacidad	6.0	Revisión Anual	01-10-2018
Plan de Privacidad	7.0	Revisión Anual	01-10-2019
Plan de Privacidad	7.1	Ajustes multi-país	26-11-2019
Plan de Privacidad	7.2	Ajuste capítulo 6, para mayor claridad en Perú	04-12-2019
Plan de Privacidad	8.0	Revisión Anual	01-10-2020

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. • INDECOPI • DIAN • SUNAT • Personal de Acepta. • Sitio Web

Documentos Internos	
Título	**Nombre del archivo**
Política de Privacidad	Política de Privacidad.doc
Documentos Externos	
Ley N° 19.628 (Chile) Ley N° 29733 (Perú) Ley N° 1581 (Colombia) 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. Adicional a lo antes mencionado, ACEPTA ha acreditado en los últimos años, adicional a Chile, su operación en los procesos de Emisión y Validación de Documentos tributarios tanto en Perú (SUNAT) como Colombia (DIAN). Aún cuando estos sistemas no manejan información personal de carácter confidencial, ambos países adhieren a las política y plan de privacidad de ACEPTA, en lo que respecta a otros sistemas que sí manejan este tipo de datos.

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 ha logrado cumplir con las regulaciones y leyes de Perú, pudiendo 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.

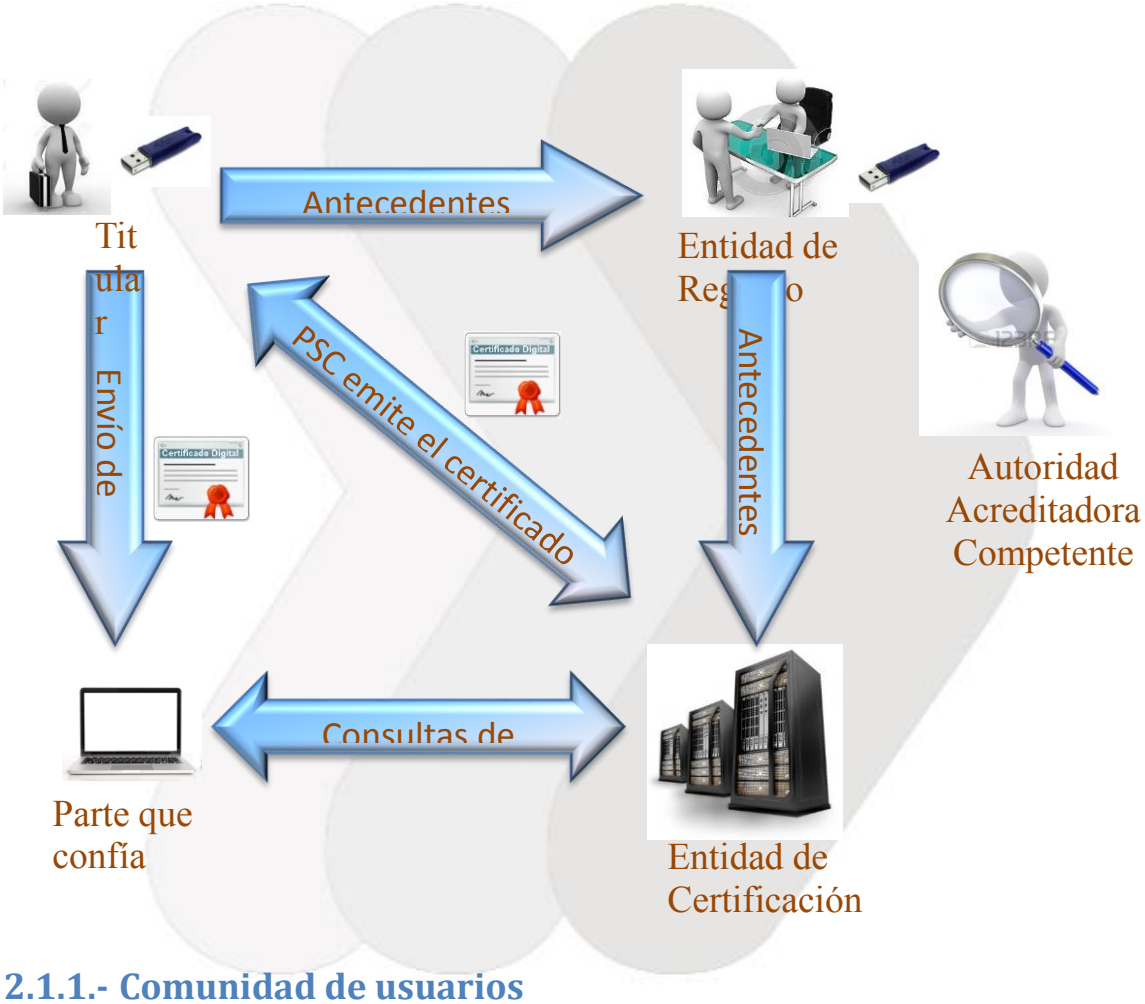
1.1.- Definiciones y Acrónimos

- **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
- **DIAN:** Dirección de Impuestos y Aduanas Nacionales de Colombia
- **SUNAT:** Superintendencia Nacional de Aduanas y de Administración Tributaria de Perú
- **SII.** Servicios de Impuestos Internos de Chile

2.- PARTICIPANTES

2.1.- Servicio de Emisión de Certificados

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:



2.1.1.- Comunidad de usuarios

- **Solicitante**: Son las personas que concurren a ACEPTA a solicitar un certificado de firma (Electrónica avanzada en Chile, Digital en Perú), 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 en Chile, Digital en Perú). 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 (o la "Autoridad de Registro" (AR) en Chile), 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 Chile, Digital en Perú). En caso de 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 (EC) de firma (Electrónica avanzada en Chile, Digital en Perú), de conformidad a la ley y 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 en Chile, Digital en Perú). Normalmente, junto con el certificado este tercero recibe un documento electrónico que se encuentra suscrito con la firma electrónica 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

2.2.- Servicio de Emisión y Validación de documentos tributarios

Los servicios de emisión y/o validación de documentos tributarios electrónicos, son otro de los servicios que provee ACEPTA a su comunidad, a fin de facilitar el flujo de los comprobantes electrónicos asociados al comercio electrónico. ACEPTA, para poder prestar estos servicios, es regulado por distintas entidades que son propias de cada país (SII: Servicio de Impuestos Internos de Chile, DIAN: Dirección de Impuestos y Aduanas Nacionales de Colombia y SUNAT: Superintendencia Nacional de Aduanas y de Administración Tributaria en Perú). Estas entidades Reguladores proveen la autorización de operación a los proveedores de servicios que cumplen adecuadamente el marco regulatorio

de cada país. Adicional a estos participantes de la comunidad, se encuentran las empresas emisoras de documentos tributarios y los receptores (o tercera parte que confía), de dichos documentos. Todos estos actores basan su confianza en la correcta operación del proveedor de servicios y las inspecciones que realizan los reguladores y/o certificaciones que posee dicho proveedor ante terceros independientes. Mayor detalle de los actores de este servicio se pueden encontrar en 2.2.1 de este mismo documento.

Cabe destacar que este servicio no realiza recolección de información personal confidencial, sino que sólo hace uso de ella, a través de certificados digitales usados para firmar los documentos Tributario-Electrónicos, así como los sobres de intercambio que consolidan los primeros. Es por esta razón que ACEPTA ha implantado un Sistema de Gestión de la Seguridad de la Información para proteger la confidencialidad de esta información.

2.2.1.- Comunidad de usuarios

- **El Subscriptor del servicio (Cliente):** Corresponde a empresas que tienen como necesidad la adquisición de Servicios de Emisión y/o Validación de Documentos Tributarios Electrónicos.
- **Las Terceras partes que confían:** Corresponde a los adquirientes o usuarios que reciben las salidas de los Servicios de Emisión y/o Validación de Documentos Tributarios Electrónicos.
- **El Proveedor del Servicio (ACEPTA):** Su necesidad es proveer los Servicios para la Emisión y/o Validación de Documentos Tributarios Electrónicos, con el uso de la tecnología, así como de su personal especializado que participa en el alcance de cada servicio.
- **Los inversionistas de ACEPTA:** Para entregarles la información relevante asociada a los servicios, que les permitan tomar decisiones estratégicas en las reuniones de directorio.
- **La Entidad reguladora:** En Perú corresponde a SUNAT, siendo su necesidad contar con PSE y OSE acreditados en los servicios por ellos inspeccionados. En Colombia corresponde a DIAN, siendo su necesidad el contar con Proveedores Tecnológicos autorizados de los servicios por ellos inspeccionados y que cumplan con la normatividad vigente.
- **Tribunales:** Para la entrega de información en virtud de un procedimiento judicial y/o administrativo.
- **Empleados:** Personal de las empresas ACEPTA, que realiza labores para la entrega de Servicios de Emisión y/o Validación de Documentos Tributarios Electrónicos, siendo su necesidad contar con herramientas y entrenamientos necesarios para cumplir su labor.

3.- ALCANCE

El plan de privacidad de ACEPTA es de cumplimiento obligatorio para su personal, que participa en operaciones críticas de los servicios que gestionan información personal de carácter confidencial.

4.- INFORMACIÓN RECOLECTADA Y PROTEGIDA

Como parte de las operaciones de registro y en su calidad de ER (Entidad de registro ER en Perú o Autoridad de Registro AR en Chile) pertenecientes a la EC de ACEPTA (Entidad de Certificación EC en Perú o Autoridad de Certificación AC en Chile), 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

Para el caso de emisión de Documentos tributarios y/o Validación de estos, no se recolecta información personal de carácter confidencial, sino que sólo hace uso de ella, a través de certificados digitales usados para firmar los documentos Tributario-Electrónicos, así como los sobres de intercambio que consolidan los primeros. Es por esta razón que ACEPTA ha implantado un Sistema de Gestión de la Seguridad de la Información para proteger la confidencialidad de esta información.

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 de las actividades del usuario.

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 y la Ley de protección de datos personales de privacidad, la cual se rige por el marco establecido por la Ley 1581 de 2012 (Colombia).

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 de certificado digital 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 cláusulas será sancionada por ACEPTA.

6.- FLUJO TRANSFRONTERIZO DE DATOS PERSONALES

Los contratos de los suscriptores, de ser necesario, 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. En la actualidad ACEPTA no realiza flujo transfronterizo de datos personales para ninguno de los servicios prestados en los diversos países, a excepción de Perú, en la cual se utilizan hosting ubicados en Chile para el proceso de firma digital.

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 y de Privacidad
- 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 emisión de certificados de firma 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.

Para los servicios asociados a emisión y/o validación de documentos tributarios, no se realiza recolección de información personal confidencial, sino que sólo hace uso de ella, a través de certificados digitales usados para firmar los documentos Tributario-Electrónicos, o los sobres de intercambio que consolidan los primeros. Es por esta razón que ACEPTA ha implantado un Sistema de Gestión de la Seguridad de la Información para proteger la confidencialidad de esta información.

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.

Para los servicios asociados a emisión y/o validación de documentos tributarios, el uso de los certificados digitales es sólo para firmar los documentos Tributario-Electrónicos, o los sobres de intercambio que consolidan los primeros, siendo estos certificados protegidos por el Sistema de Gestión de la Seguridad de la Información de ACEPTA.

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 de certificados de firma, 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

Para los certificados digitales, en que los individuos que han entregado información a ACEPTA, ellos 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 Seguridad y de Privacidad 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.