ACEPTA

Empresas
a velocidad
digital

PO01

Políticas de Registro

Enero de 2014

OID 1.3.6.1.4.4.6891.3

MANUEL
ENRIQUE
GODOY
RAMIREZ

Digitally signed by
MANUEL ENRIQUE
GODOY RAMIREZ
Date: 2025.02.14
10:35:42 -03'00'

RESPONSABLES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Certificación y Seguridad	- Gerente de Certificación y Seguridad - Oficina técnica. - Fiscalía	Gerente General

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
Declaración de Políticas de Registro y Verificación - PO01	1.0	Primera versión	23-01-2014
Declaración de Políticas de Registro y Verificación	1.1	Actualización proveedor de Data Center	04-03-2015
Declaración de Políticas de Registro y Verificación	2.0	Segunda versión	29-06-2016
Declaración de Políticas de Registro y Verificación	4.0	Revisión anual	01-10-2016
Declaración de Políticas de Registro y Verificación	4.1	Ajustes Perú	04-01-2017
Declaración de Políticas de Registro y Verificación	4.2	Ajuste a punto 3.4 (revocación por parte de la empresa)	29-05-2017
Declaración de Políticas de Registro y Verificación	5.0	Revisión anual	01-10-2017
Declaración de Políticas de Registro y Verificación	5.1	Posibilidad de realizar la operación de registro y validación en base a clave única del SRCeI	07-11-2017
Declaración de Políticas de Registro y Verificación	5.2	Ajustes asociados a Certificación 2018	06-04-2018
Declaración de Políticas de Registro y Verificación	5.3	Ajustes de nombres políticas certificación	11-04-2018
Declaración de Políticas de Registro y Verificación	5.4	Ajustes contacto, acrónicos y calificación asesores	24-04-2018

Declaración de Políticas de Registro y Verificación	5.5	Descripción de atención en terreno	04-06-2018
Declaración de Políticas de Registro y Verificación	6.0	Revisión anual	11-03-2019
Declaración de Políticas de Registro y Verificación	6.1	Ajustes a capítulo 9, producto de seguimiento 2019	15-04-2019
Declaración de Políticas de Registro y Verificación	6.2	Actualización producto de nuevas guías de acreditación INDECOPI	30-09-2019
Declaración de Políticas de Registro y Verificación	7.0	Revisión anual	01-10-2019
Declaración de Políticas de Registro y Verificación	8.0	Revisión anual	01-10-2020
Declaración de Políticas de Registro y Verificación	9.0	Revisión anual	15-03-2022
Declaración de Políticas de Registro y Verificación	10.0	Revisión anual	15-03-2023
Políticas de Registro y Verificación	10.1	Ajustes como parte del proceso de Renovación de acreditación	15-05-2023
Políticas de Registro	10.2	Ajuste nombre de documento como parte del proceso de Renovación de acreditación	09-06-2023
Políticas de Registro	11.0	Revisión anual	30-04-2024
Políticas de Registro	12.0	Revisión anual	14-02-2025

CLASIFICACIÓN DEL DOCUMENTO

NIVEL DE CRITICIDAD: Baja

NIVEL DE CONFIDENCIALIDAD: Pública

NOTA DE CONFIDENCIALIDAD: Se encuentra disponible ante su solicitud.

AUTOR/ES: Gerencia de Certificación y Seguridad
DISTRIBUCIÓN: • Sitio web • INDECOPI

REFERENCIAS

Documentos Internos	
Título	**Nombre del archivo**
Documentos Externos	
• Ley N° 27.269, Ley 29.733 (Perú) • SG-M-03 Manual de Seguridad • GG-P-01 Auditar gerencias • GG-P-05 Procedimiento de control de auditoría de sistemas de información	

ÍNDICE

1. Introducción

1.1 Presentación

Este documento presenta la Política de Registro (RP, por su sigla en inglés Registration Policy) de Acepta para los certificados de firma electrónica y firma digital. Estas son una descripción de los procedimientos que Acepta declara convenir en la prestación de sus servicios de certificación, cuando emite y gestiona certificados de firma electrónica y/o digital en su calidad de Prestador de Servicios de Certificación (PSC). Además, se incluyen las normas a seguir por quienes comprueban fehacientemente la identidad de los solicitantes de certificados de firma electrónica o digital (Autoridad de Registro).

La Política de Registro referida en este documento se utilizará para la emisión de certificados de firma electrónica y/o digital, generados por Acepta y que se emitirán sobre dispositivo seguro de creación de firma. Mediante los certificados emitidos por Acepta y los dispositivos seguros de creación de firma, que se indican en esta Política, se generarán firmas electrónicas y/o digital reconocidas por las terceras partes.

Cabe indicar que la presente Políticas de Registro se han generado siguiendo las especificaciones del documento RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" propuesto por Network Working Group para este tipo de documentos. Tales políticas son las que se prosigue en detallar, y están disponibles en el Sitio WEB de Acepta (https://sovos.com/es/politicas-y-practicas/) para conocimiento público.

Esta Política de Registro asume el manejo de conceptos básicos de Infraestructura de Clave Pública, certificado, firma electrónica y firma digital, en caso contrario se recomienda estudiar estos conceptos, previo a continuar con la lectura del presente documento.

1.1.1 Sobre las Políticas de Registro

Las políticas de registro aquí descritas establecen el ciclo de vida de los servicios que provee Acepta, que como antes se ha mencionado incluyen desde la gestión de la solicitud de certificado, la verificación y validación de la información proporcionada, pasando por la emisión, uso, administración de los certificados, su revocación y su re-emisión. Es decir son aquellas políticas que dan seguridad y confianza a los certificados y servicios provistos por Acepta.

1.1.2 Alcance

El alcance de las Políticas de Registro (RP) detalla las condiciones de los servicios de certificación que presta Acepta para la emisión de sus certificados de firma electrónica y/o digital.

1.1.3 Referencias

La presente Declaración de Políticas de Registro se ha generado siguiendo las especificaciones del documento RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" propuesto por Network Working Group para este tipo de documentos.

1.1.4 Visión general del sistema

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: Entidad Certificadora (EC) o Prestador de Servicios de Certificación (PSC), Entidades de Registro (ER), titulares, terceras partes que confían en los certificados y Autoridad Administrativa Competente (AAC).

1.2 Identificación

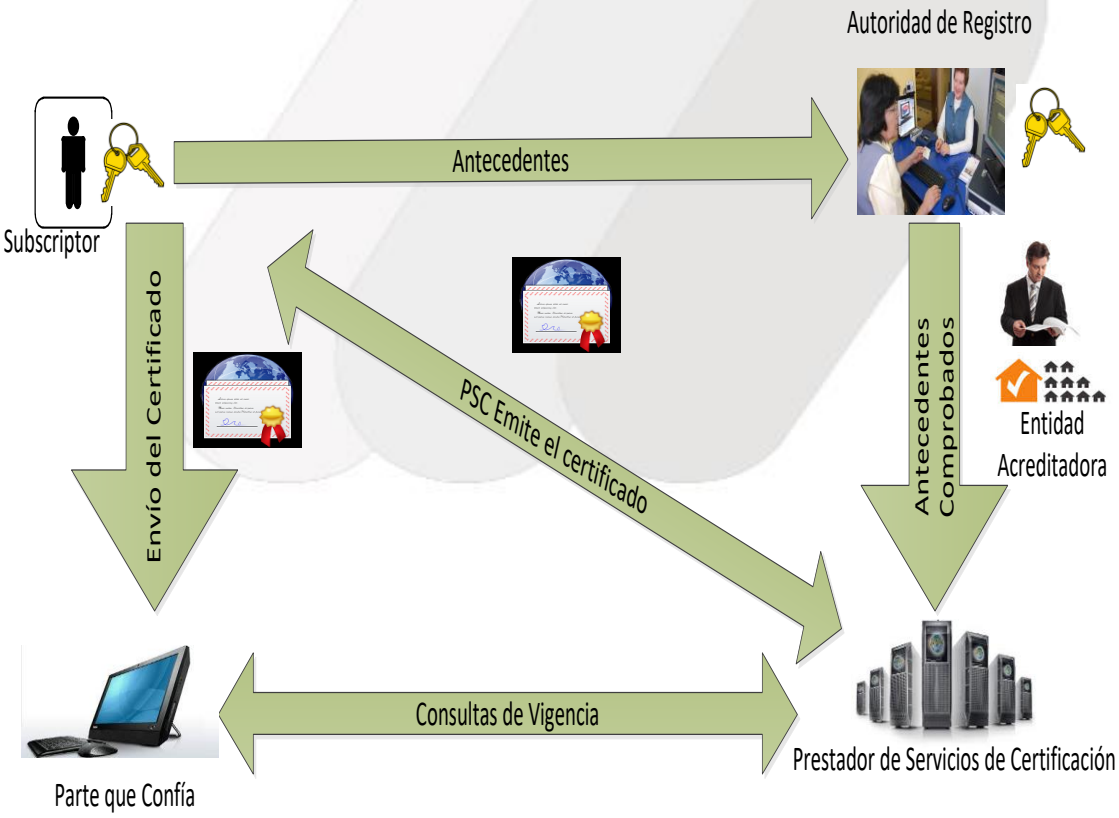
El presente documento se denomina "Políticas de Registro" para los certificados de Firma Electrónica y Firma Digital de Acepta, las que internamente se citan como RP y están registradas con el número único internacional (OID) 1.3.6.1.4.1.6891.3.

Acepta tiene asignado el identificador (OID) 1.3.6.1.4.1.6891, el cual está registrado en la Internet Assigned Number Authority (IANA). Este número identifica únicamente a Acepta en un contexto global.

En las RPS de Acepta, sección "1.2 Identificación", se presenta la lista completa de OIDs administrados por Acepta.

1.3 Comunidad y Aplicabilidad

Los servicios de certificados de firma electrónica y digital, 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), Autoridades de Registro (AR - ER en Perú), Suscriptor, terceras partes que confían en los certificados y Entidad acreditadora. La siguiente figura muestra dicha relación:



1.3.1 Comunidad de usuarios

- **Solicitante:** Son las personas que concurren a Acepta a solicitar un certificado de firma electrónica o digital, completan el formulario de solicitud y proveen todos los antecedentes que exige la ley y esta RP y su RPS, 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 o digital. 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.

- **Autoridad de registro**: La recepción y procesamiento de las solicitudes de certificados es realizada por la "Autoridades de Registro" (AR - ER en Perú) de Acepta, sea que lo haga directamente o a través de un mandatario especialmente designado para tal objeto. La Autoridad de Registro debe realizar la comprobación fehaciente de la identidad de los solicitantes de certificados de firma electrónica o digital. En caso que sea un tercero el que actúe, en calidad de mandatario de Acepta, como Autoridad 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 o digital, de conformidad a la ley, en particular, a lo previsto en la Ley 27.269, que en este caso es Acepta.

- **Tercera parte que confía**: Es el receptor de un certificado de firma electrónica o digital. Normalmente, junto con el certificado este tercero recibe un documento electrónico que se encuentra suscrito con la firma electrónica o digital 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.

- **Entidad Acreditadora:** La Subsecretaría de Economía, que de conformidad con lo dispuesto en la Ley 19.799 el Prestador de Servicios de Certificación de Firma Electrónica debe demostrarle que cuenta con las instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados de firma electrónica o digital, permitiendo su inscripción en el registro de certificadores acreditados.

Los usuarios que utilicen los certificados - emitidos directamente por Acepta 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 declarados por la EC de Acepta.

1.4 Aplicabilidad de los certificados

Los Certificados emitidos por Acepta se utilizarán únicamente conforme a la función y finalidad que tengan establecida en la presente Políticas de Registro, en las correspondientes Prácticas de Certificación y de conformidad con lo dispuesto en la Ley 27.269 y su reglamento.

1.4.1 Tipos y usos de los certificados

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

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

Los certificados de firma electrónica o digital de persona natural o jurídica, son emitidos por Acepta para soportar las siguientes necesidades de seguridad:

1. **Autentificación:** proporciona suficientes garantías respecto a la identidad del suscriptor del certificado, al requerirse la presencia del suscriptor junto con DNI y/o RUC, e imponer que el almacenamiento de la llave privada sea en un dispositivo especializado y acreditado según la norma internacional FIPS-140 nivel 2 para la firma digital, o en cualquier medio válido que soporte una firma electrónica.
2. **Integridad de mensajes:** los mensajes firmados con certificado de firma electrónica o digital permiten validar si el contenido de mensaje ha sido alterado en el tiempo transcurrido desde su generación.
3. **Firmas digitales:** las firmas digitales producidas con certificados de firma electrónica o digital, ofrecen los medios de respaldo para demostrar fehacientemente, incluso en tribunales, la autenticidad de un mensaje o documento electrónico.
4. **Privacidad:** Los certificados de firma electrónica o digital permiten cifrar mensajes de forma que al ser transmitidos sean visibles sólo por el remitente correspondiente. Sin embargo, Acepta recomienda usar otros certificados para estos fines, con una duración de al menos 10 años. La expiración o revocación de los certificados de firma electrónica o digital no provocan consecuencias con las firmas electrónicas o digitales generadas en forma previa al término de la vigencia del certificado, pero en el caso de mensajes cifrados, se genera un problema al expirar el certificado, ya que este se debe conservar durante todo el período de tiempo en el que se desee poder descifrar los mensajes protegidos (En el caso de Perú, la codificación no es permitida en esta clase de firmas)

1.4.2 Limitaciones de Usos y Prohibiciones

Los Certificados de firma electrónica o digital emitidos por Acepta se utilizarán únicamente conforme a los usos y finalidades que tengan establecida en este documento y en las correspondientes Prácticas de Certificación, y de acuerdo a la normativa peruana vigente y a los convenios internacionales ratificados por estos Estados. Cualquier uso diferente del autorizado por ley e indicado en estas prácticas está expresamente prohibido. En consecuencia, será responsabilidad del Suscriptor el uso no autorizado o indebido que éste haga del mismo

Asimismo, queda expresamente prohibido alterar en cualquier forma los certificados emitidos por Acepta, los que solo serán válidos en la forma suministrada por Acepta.

1.4.3 Contenido de los Certificados

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de la EC de Acepta.

1.5 Detalle de los contactos y administración de la CA

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

- **PERÚ:**
    - **Nombre**: ACEPTA PERU S.A.C.
    - **Dirección de e-mail**: contacto_cys@acepta.com
    - **Dirección**: Calle Amador Merino Reyna 465, Piso 6, Oficina 602, San Isidro, Lima, Perú
    - **Código Postal:** 15046
    - **Número telefónico**: (+511) 7307820

1.6 Definiciones y Acrónimos

A efectos del documento de Prácticas de Certificación, las expresiones que se pasan a indicar a continuación tendrán el alcance y/o significado que se pasa a indicar en cada caso:

- **Firma digital:** La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.
- **Titular de la firma digital:** El titular de la firma digital es la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos.
- **Obligaciones del titular de la firma digital:** El titular de la firma digital tiene la obligación de brindar a las entidades de certificación y a los terceros con quienes se relacione a través de la utilización de la firma digital, declaraciones o manifestaciones materiales exactas y completas.
- **Certificado digital:** El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.
- **Contenido del certificado digital:** Los certificados digitales emitidos por las entidades de certificación deben contener a l menos:
    1. Datos que identifiquen indubitablemente al titular.
    2. Datos que identifiquen a la Entidad de Certificación.
    3. La clave pública.
    4. La metodología para verificar la firma digital del titular impuesta a un mensaje de datos.
    5. Número de serie del certificado.
    6. Vigencia del certificado.
    7. Firma digital de la Entidad de Certificación.

- **Confidencialidad de la información:** La entidad de registro recabará los datos personales del solicitante de la firma digital directamente de éste y para los fines señalados en la presente ley. Asimismo la información relativa a las claves privadas y datos que no sean materia de certificación se mantiene bajo la reserva correspondiente. Sólo puede ser levantada por orden judicial o pedido expreso del titular de la firma digital.
- **Cancelación del certificado digital:** La cancelación del certificado digital puede darse:
    1 A solicitud del titular de la firma digital.
    2 Por revocatoria de la entidad certificante.
    3 Por expiración del plazo de vigencia.
    4 Por cese de operaciones de la Entidad de Certificación.
- **Revocación del certificado digital:** La Entidad de Certificación revocará el certificado digital en los siguientes casos:
    1 Se determine que la información contenida en el certificado digital es inexacta o ha sido modificada.
    2 Por muerte del titular de la firma digital.
    3 Por incumplimiento derivado de la relación contractual con la Entidad de Certificación.
- **Reconocimiento de certificados emitidos por entidades extranjeras:** Los Certificados de Firmas Digitales emitidos por entidades extranjeras tendrán la misma validez y eficacia jurídica reconocida en la presente ley, siempre y cuando tales certificados sean reconocidos por una entidad de certificación nacional que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, del procedimiento, así como la validez y la vigencia del certificado.
- **Entidad de Certificación:** La Entidad de Certificación cumple con la función de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado o aquellos que brinden seguridad al sistema de certificados en particular o del comercio electrónico en general. Las Entidades de Certificación podrán igualmente asumir las funciones de Entidades de Registro o Verificación.
- **Entidad de Registro o Verificación:** La Entidad de Registro o Verificación cumple con la función de levantamiento de datos y comprobación de la información de un solicitante de certificado digital; identificación y autenticación del titular de firma digital; aceptación y autorización de solicitudes de emisión de certificados digitales; aceptación y autorización de las solicitudes de cancelación de certificados digitales.
- **Depósito de los Certificados Digitales:** Cada Entidad de Certificación debe contar con un Registro disponible en forma permanente, que servirá para constatar la clave pública de determinado certificado y no podrá ser usado para fines distintos a los estipulados en la presente ley. El Registro contará con una sección referida a los certificados digitales que hayan sido emitidos y figurarán las circunstancias que afecten la cancelación o vigencia de los mismos, debiendo constar la fecha y hora de inicio y fecha y hora de finalización. A dicho Registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten.
- **Inscripción de Entidades de Certificación y de Registro o Verificación:** El Poder Ejecutivo, por Decreto Supremo, determinará la autoridad administrativa competente y señalará sus funciones y facultades. La autoridad competente se encargará del Registro de Entidades de

Certificación y Entidades de Registro o Verificación, las mismas que deberán cumplir con los estándares técnicos internacionales. Los datos que contendrá el referido Registro deben cumplir principalmente con la función de identificar a las Entidades de Certificación y Entidades de Registro o Verificación.

- **Reglamentación:** El Poder Ejecutivo reglamentará la presente Ley en un plazo de 60 (sesenta) días calendario, contados a partir de la vigencia de la Ley N° 27269.
- **Certificado raíz:** Certificado cuyo titular es Acepta y pertenece a la jerarquía que Acepta presenta como Prestador de Servicios de Certificación.
- **Clave:** Secuencia de símbolos.
- **Datos de creación de firma:** Son datos únicos que el titular utiliza para crear la Firma digital y que se encuentran inequívocamente unidos a la clave pública contenida en el certificado de firma digital.
- **Clave Pública:** Son los datos que se utilizan para verificar la Firma digital y que se encuentran inequívocamente unidos a los datos de creación de firma.
- **Declaración de Prácticas de Certificación:** Declaración de Acepta, respecto a aquellas prácticas, a nivel de sistemas y de personal, que en base a sus buenas prácticas dan seguridad y confianza a los certificados y servicios provistos pro Acepta.
- **Listas de Revocación de Certificados:** Registro de acceso público de certificados, en el que quedará constancia de los certificados que han perdido su vigencia por haber sido revocados.
- **Número de serie de Certificado:** Valor entero y único que está asociado inequívocamente con un certificado expedido por Acepta.
- **OCSP (Online Certificate Status Protocol):** Protocolo informático que permite la comprobación del estado de un certificado en el momento en que éste es utilizado.
- **Prestador de Servicios de Certificación (PSC):** Es aquella entidad que en conformidad con la legislación, emite certificados de firma digital.
- **Política de Certificación:** Es el 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. Es el documento que completa la Declaración de Prácticas de Certificación, estableciendo las condiciones de uso y los procedimientos seguidos por Acepta para emitir Certificados.
- **SHA-1: Secure Hash Algorithm** (algoritmo seguro de resumen –hash-). Desarrollado por el NIST- El algoritmo consiste en tomar mensajes de menos de 2^{64} bits y generar un resumen de 160 bits de longitud. La probabilidad de encontrar dos mensajes distintos que produzcan un mismo resumen es teóricamente nula. Por este motivo se usa para asegurar la Integridad de los documentos durante el proceso de Firma.
- **SHA-2: Secure Hash Algorithm** (algoritmo seguro de resumen –hash-). Desarrollado por el NIST- El algoritmo consiste en tomar mensajes de menos de 2^{64} bits y generar un resumen de 256 bits de longitud.
- **Solicitante:** Persona que solicita la emisión de un certificado de firma digital dando cumplimiento a las exigencias establecidas en la Ley y en esta Declaración de Prácticas de Certificación.
- **Terceras partes que confían:** Aquellas personas que voluntariamente depositan su confianza en un certificado de Acepta, comprobando la validez y vigencia del certificado según lo descrito en esta Declaración de Prácticas de Certificación y en las Políticas de Certificación asociadas a cada tipo de certificado.
- **X.509:** Estándar desarrollado por la UIT, que define el formato electrónico básico para certificados electrónicos.

Acrónimos

- AC: Autoridad Certificadora
- ACR: Autoridad Certificadora Raíz
- AFIS: Automated Fingerprint Identification System
- AR: Autoridad de Registro
- CA: Certification Authority
- CP: Certificate Policy
- CP-FA: Políticas de Certificado de Firma Electrónica y Digital
- CPS: Certification Practice Statement
- CRL: Certificate Revocation List
- DNI: Documento Nacional de Identificación
- ER: Entidad de Registro
- EC: Entidad de Certificación
- FIPS: Federal Information Processing Standard
- HSM: Hardware Security Module
- IANA: Internet Assigned Number Authority
- IETF: Internet Engineering Task Force
- ITU: international Telecommunication Union
- KEY USAGE: En este contexto es el uso que se da al Certificado
- NFPA: National Fire Protection Association
- NIST: Instituto Nacional de Estándares y Tecnología
- OCSP: On-line Certificate Status Protocol
- OID: Object Identifier
- PKCS#10: Certification Request Syntax Specification
- PSC: Prestador de Servicios de Certificación
- PIN: personal Identification Number
- PKI: Public Key Infrastructure
- RA: Registration Authority
- RSA: Algoritmo de Encriptación
- SII: Servicio de Impuestos Internos
- UIT: Unión Internacional de Telecomunicaciones
- X.500: Serie de estándares computacionales

2 Requerimientos Generales

2.1 Obligaciones

Acepta, en su calidad de Prestador de Servicios de Certificación se obliga ejecutar sus actividades de certificación acorde con las Prácticas de certificación asociadas a cada tipo de certificador. Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.1.1 Obligaciones de la AC Raíz (ACR)

El certificado raíz de Acepta, permite firmar aquellos certificados de las entidades que de él son subordinadas. Es así como el certificado raíz de Acepta es sobre el cual se basa el modelo de confianza de toda la jerarquía de entidades intermedias que ha emitido Acepta, ya que los certificados de estas entidades intermedias, en este caso Acepta ha generado para sí misma dichos certificados intermedios, son firmados por la raíz misma. Esta raíz es almacenada de manera offline cuando no está en uso.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de la EC de Acepta.

2.1.2 Obligaciones de la Autoridad de Registro (AR-ER) y la Autoridad Certificadora (AC-EC)

Cada AR (ER) y/o PSC (EC) acreditado deberá cumplir las normas y ser consistente con lo establecido en el documento de Prácticas de Certificación de cada tipo de certificado.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de la EC de Acepta y Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.1.3 Obligaciones del Solicitante

Los solicitantes de certificados a Acepta, se obligan a conocer las políticas y prácticas de certificación, entregar antecedentes fidedignos al momento de la solicitud, notificar cambios que en ellos ocurran y finalmente suscribir el contrato de servicios.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de la EC de Acepta y Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.1.4 Obligaciones del Suscriptor de la llave

Los suscriptores de certificados a Acepta, se obligan a conocer las políticas y prácticas de certificación, conocer el alcance del certificado, proporcionar antecedentes fidedignos, notificar cambios en dichos antecedentes y finalmente pagar la tarifa del servicio.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de la EC de Acepta y Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.1.5 Obligaciones los Usuarios

Los usuarios de certificados emitidos por Acepta, o cualquier entidad que deposite su confianza en dichos certificados deberá comprobar el estado de los certificados y conocer el propósito y alcance del certificado.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de la EC de Acepta y Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.1.6 Confianza en las Firmas y Certificados

Las partes que consideren confiar en las firmas y certificados emitidos por Acepta deberán tener conocimiento de las normas legales que sigue el Proveedor de Servicios de Certificación, deberán verificar la autenticidad de la firma, deberán asegurar el estado de esta firma, deberán acotar la confianza al uso definido para el certificado emitido, deberán verificar su validez y finalmente deberán tomar conocimiento de las consecuencias en que se incurre al aceptar y usar los certificados en que se confía.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de la EC de Acepta y Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.1.7 Obligaciones de los Repositorios

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación (CPS) de la EC de Acepta y Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.2. Responsabilidad del PSC

Acepta solo será responsable de los daños y perjuicios que en el ejercicio de la actividad de certificación de firma electrónica o digital ocasione y, en ningún caso será responsable del uso incorrecto, indebido o fraudulento de los certificados de firma electrónica o digital emitidos, ni de cualquier daño indirecto o imprevisto que resulte de su uso.

Acepta será responsable de los daños y perjuicios que en el ejercicio de su actividad de certificación de firma electrónica ocasione, debiendo demostrar que actuó con la debida diligencia.

Será responsabilidad de los usuarios adoptar las medidas de prevención usuales a la actividad computacional para evitar daños y perjuicios originados por el uso o incapacidad de uso de los certificados de firma electrónica.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación (CPS) de la EC de Acepta y Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.2.1 Responsabilidad Pecuniaria

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.2.2 Fuerza Mayor

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.2.3 Responsabilidad de la AC y AR

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.3 Ley Aplicable y Resolución de Conflictos

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

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.4 Publicación y Repositorios

Acepta publica en su sitio Web (https://sovos.com/es/politicas-y-practicas), las prácticas de certificación por ella utilizadas, así como las políticas de certificado (CP) pertinentes a cada tipo de certificado emitido, las cuales están a disposición de los usuarios sin cargo alguno.

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

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.5 Privacidad y Protección de los Datos Personales

Las Políticas de Privacidad de Acepta se encuentran publicadas en el sitio web de Acepta https://sovos.com/es/politicas-y-practicas/.

2.5.1 Tipos de Información a Proteger

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.5.2 Tipos de Información que puede ser entregada

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.5.3 Información del Certificado

Los certificados de firma electrónica o digital emitidos por Acepta están en conformidad con el formato X.509v3 definido en ITU-T X.509v3 y las recomendaciones de la IETF RFC-3280.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.5.4 Entrega de Información sobre la Revocación o Suspensión del Certificado

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.5.5 Entrega de Información en virtud de un Procedimiento Judicial y/o Administrativo

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.5.6 Entrega de Información a Petición del Titular

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.6 Derechos de Propiedad Intelectual e Industrial

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

2.7 Entidades de certificación afiliadas a la ER

La ER de Acepta sólo representa o tiene afiliación, para realizar las actividades de registro, con las EC indicadas en 2.1.2 de sus RPS. Para mayor detalle remítase a la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

3 Identificación y Autenticación

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

3.1 Registro Inicial

3.1.1 Registro de Nombres

Todos los suscriptores de contratos requieren un nombre distintivo como se menciona en el estándar X.500, el cual es registrado en un campo del certificado. Del mismo modo se registrará el DNI o RUC, en caso de emitirse el certificado a una persona natural o a una persona jurídica según corresponda.

Se considerará como válido, en el caso de los nombres, cualquiera que sea aceptado por RENIEC en Perú o en el Registro de personas Jurídicas.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

3.1.2 Verificación General

Acepta, como parte del proceso de emisión de certificados, procederá a verificar la identidad de la persona a la cual se asociará el certificado. Para esto el solicitante se presentará ante un operador de registro, o a quien Acepta determine para ejecutar esta función, quien estará encargado de verificar la identidad de este versus el Documento Nacional de Identidad (DNI) presentado. En caso de no estar disponible la verificación de identidad en línea con RENIEC – Para el caso del registro en Perú – la solicitud no podrá ser ingresada.

Respecto a la dirección de correo electrónico del suscriptor, Acepta informa que no garantiza que esta dirección de correo esté vinculada con el suscriptor del certificado, por lo que la confianza en que esta dirección recae sólo en la parte confiante. Acepta, garantiza que la dirección electrónica de correo contenida en el certificado, ha sido aportada por el suscriptor al momento de formalizar su solicitud.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

3.2 Reemisión de la Llave

No aplica

3.3 Reemisión de la Llave luego de una Revocación

No aplica

3.4 Requerimiento de Revocación

El proceso de solicitud de revocación viene definido por la Política de Certificación aplicable a cada tipo de certificado. La política de identificación para las solicitudes de revocación acepta los siguientes métodos de identificación:

- Solicitud del titular del certificado (en caso de emisión a persona natural) o solicitud del representante legal actual de la empresa o del titular del certificado a revocar (en caso que el certificado esté emitido para un cargo de dicha empresa).
- Por oficio de Acepta ante sospecha fundada de compromiso en la clave privada de un suscriptor.
- Presencial con una identificación similar a la primera solicitud de certificado (ver 3.1.2).
- Por medio electrónico, en que el titular debe enviar a Acepta un e-mail firmado con firma electrónica o digital, siendo la casilla de destino admin-revocaciones@acepta.com.
- Por carta certificada, en caso de revocar su certificado de firma electrónica y no desear continuar con el servicio, adjuntando además fotocopia de su Documento Nacional de Identidad (DNI).

La revocación tendrá lugar cuando Acepta constate alguna de las circunstancias especificadas en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

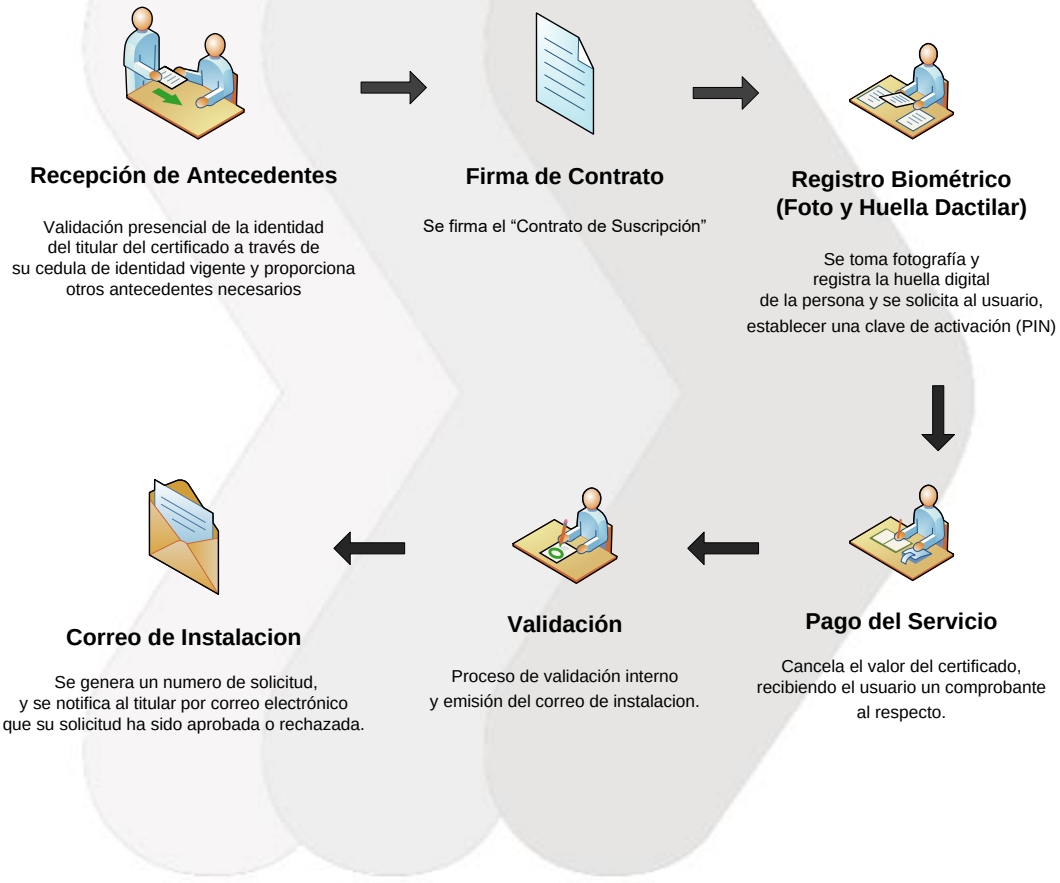
4 Requisitos Operacionales

Las especificaciones de este capítulo son complementadas en el documento de declaración de prácticas de certificación.

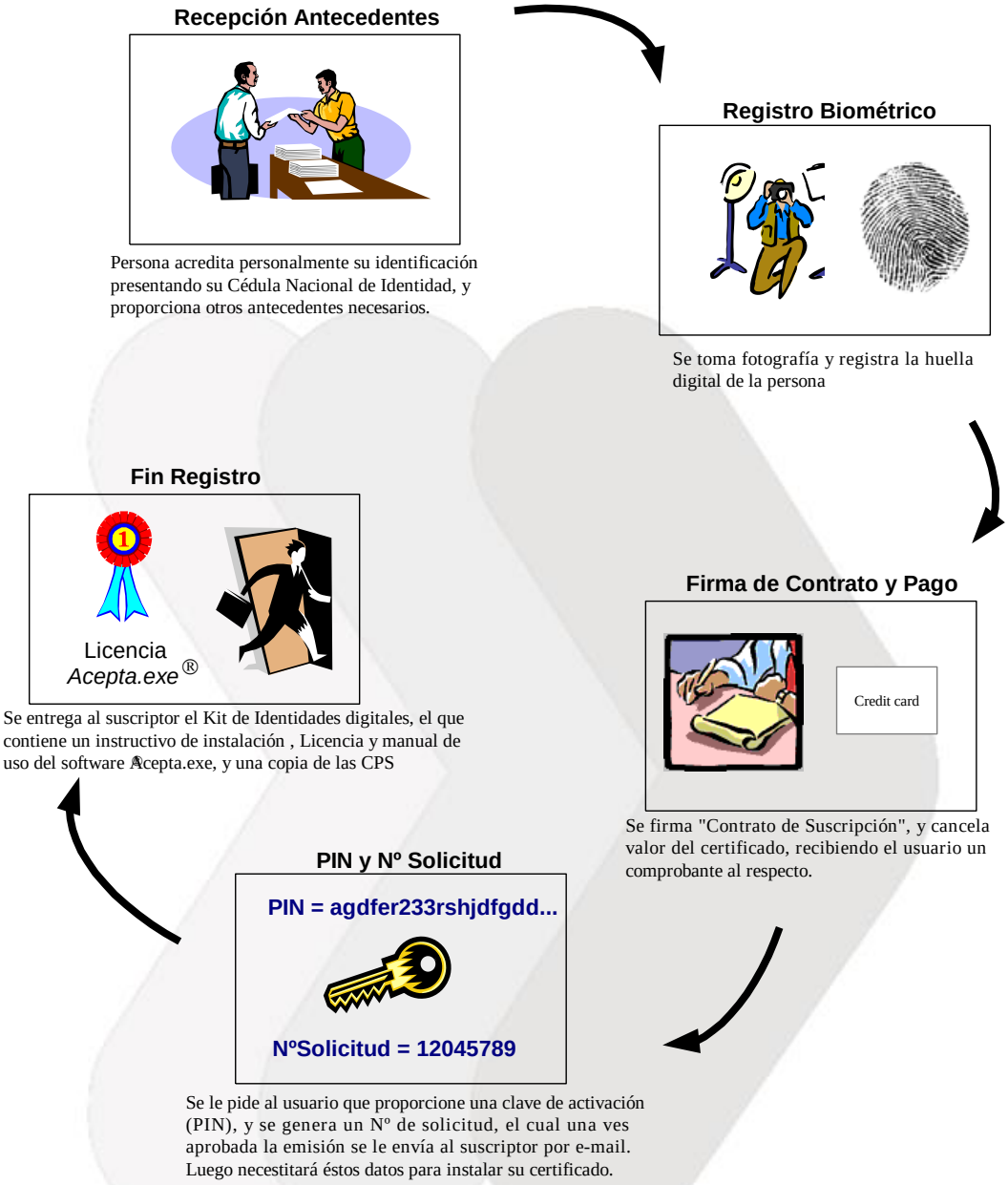
4.1 Manuales Operacionales

Para cumplir las labores de registro inicial, validación y emisión de certificados de firma, Acepta cuenta con manuales operacionales los cuales guían a los operadores de registro y validación en las labores asociadas a su rol. En estos documentos se describen los requisitos operativos pertinentes a las etapas de certificación, conducentes a la obtención de un certificado de persona de firma electrónica o digital. Además, se describe el mecanismo de revocaciones y/o suspensiones.

El siguiente diagrama muestra el proceso de registro



Un mayor detalle para este proceso, se presenta en la siguiente figura:



4.2 Solicitud de Certificado

4.2.1 Persona natural

4.2.1.1 Descripción de procedimiento

Para solicitar un certificado, tal como lo indican las CPS de la EC de Acepta, de firma electrónica y de firma digital; el solicitante debe comparecer personalmente ante la Entidad de Registro de Acepta o ser visitado por un puesto móvil de esta Entidad de Registro (ver "Atención en terreno). Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

ATENCIÓN EN TERRENO

ACEPTA a fin de masificar y prestar un mejor servicio a la ciudadanía, provee el servicio de atención en terreno (para el cual debe verse disponibilidad comunicándose con ACEPTA a través de los canales descritos en 1.5). Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

Verificación General

Las menciones exigidas por la Ley 29.733, según corresponda para los certificados de firma electrónica y de firma digital deben ser comprobados fehacientemente por Acepta. Adicionalmente para las solicitudes ingresadas y validadas por un notario, este último deberá corroborar lo antes mencionado, previo a su envío a Acepta.

En el caso de que el registro presencial sea realizado por un operador de registro de Acepta, este puede reunirse con el solicitante en una de las oficinas de registro de Acepta y también es posible acordar un registro presencial en dependencias del solicitante. Acepta se reserva el derecho a definir la cobertura disponible para este efecto. En la información capturada por el operador de registro se incluye el DNI en Perú, nombre, fecha de nacimiento, e-mail, foto, firma manuscrita, impresión dactilar y datos de contacto del suscriptor del certificado.

Acepta no implementa procedimientos de control a las actividades de RENIEC, máxima Autoridad en Perú en verificación de identidad.

Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.1.2 Verificación Presencial

Los certificados de firma digital que garantizan el no repudio, son emitidos por la ER y EC de Acepta, sólo si se ha realizado una verificación presencial de identidad positiva por parte de la ER. La ER de Acepta, puede además realizar la verificación presencial por medio de un Notario Público autorizado por la AAC. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.1.3 Verificación mediante consulta bases de datos nacionales

Acepta comprobará fehacientemente la identidad de los solicitantes de los certificados de firma electrónica y de firma digital. Para esta comprobación, en caso de ser ciudadanos peruanos los solicitantes, la verificación se realiza haciendo uso de las bases de datos del RENIEC, por medio de su sistema de verificación biométrica AFIS. De no estar disponible la verificación de identidad contra

RENIEC, no podrá cursarse la solicitud. En el caso de extranjeros, la verificación será realizada, haciendo uso de las bases de datos de migraciones.

4.2.1.4 Verificación de los datos de la solicitud

La ER de Acepta valida que los datos de la solicitud del certificado que es remitida a su EC, para la emisión del certificado, correspondan a los datos de la identidad validada, ello según 4.2.1.1, 4.2.1.2 y 4.2.1.3.

Luego que los antecedentes del suscriptor son remitidos a Acepta, se procede a su validación central, necesaria para verificar la consistencia de dichos antecedentes en relación con la solicitud de certificado correspondiente. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.1.5 No repudio de la solicitud

Acepta garantiza el no repudio de las solicitudes de los certificados solicitados, firmando dichas solicitudes con firma electrónica digital, tanto de su operador de registro, como del operador de validación de Acepta. La lista de Operadores de Registro y Operadores de Validación autorizados por la ER de Acepta se encuentra firmada por la EC intermedia de Acepta y es generada con los mismos estándares de seguridad con los que se generan los certificados de las Autoridades Certificadoras intermedias de Acepta. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.1.6 Aprobación o rechazo de la solicitud

Acepta rechazará solicitudes, si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE, al no cumplir las obligaciones indicadas en 2.1.3. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.1.7 No repudio de la invitación de generación de claves e instalación del certificado

La invitación para la generación de claves e instalación del certificado, asociado a la solicitud se realiza de acuerdo a lo indicado en el punto 6.2; de modo que sólo el suscriptor verificado tiene control sobre la generación del par de claves, incluyendo para el caso de la firma digital del exclusivo control del módulo criptográfico donde se almacenará su clave privadas. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.1.8 Contrato del suscriptor

El solicitante, al finalizar el proceso de registro de manera exitosa, tal como se indica en los puntos 4.2.1.1, 4.2.1.2 y 4.1.2.3, debe firmar el contrato de suscripción, el cual hace parte de la solicitud, y que es firmada digitalmente con un certificado de firma del operador de registro, de modo que ella no sea repudiable. Adicionalmente, este documento es almacenado de manera segura en la ER de Acepta. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.1.9 Tiempo de procesamiento

Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2 Persona jurídica

4.2.2.1 Descripción de procedimiento

Para solicitar un certificado, tal como lo indican las CPS de la EC de Acepta, de firma electrónica y de firma digital; el solicitante debe comparecer personalmente ante la Entidad de Registro de Acepta o ser visitado por un puesto móvil de esta Entidad de Registro (ver "Atención en terreno") Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

ATENCIÓN EN TERRENO

ACEPTA a fin de masificar y prestar un mejor servicio a la ciudadanía, provee el servicio de atención en terreno (para el cual debe verse disponibilidad comunicándose con ACEPTA a través de los canales descritos en 1.5). Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

Verificación General

Las menciones exigidas por la Ley 29.733, según corresponda para los certificados de firma electrónica y de firma digital deben ser comprobados fehacientemente por Acepta. Adicionalmente para las solicitudes ingresadas y validadas por un notario, este último deberá corroborar lo antes mencionado, previo a su envío a Acepta. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2.2 Acreditar la existencia de la persona jurídica

Acepta, durante el proceso de registro, solicitará al representante legal o una persona asignada por él que acredite la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2.3 Reconocimiento de nombres y marcas registradas

Acepta, durante el proceso de registro, solicitará la documentación o información necesaria para garantizar que un nombre o marca pertenece al solicitante o representado de un certificado digital. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2.4 Acreditar las facultades del solicitante

Acepta, durante el proceso de registro, solicitará al solicitante de los certificados deberá acreditar, mediante el documento legal respectivo, sus facultades como representante. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2.5 Verificación mediante consulta bases de datos nacionales

Acepta comprobará fehacientemente la identidad de los solicitantes de los certificados de firma electrónica y de firma digital. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2.6 Verificación de los datos de la solicitud

La ER de Acepta valida que los datos de la solicitud del certificado que es remitida a su EC, para la emisión del certificado, correspondan a los datos de la identidad validada, ello según 4.2.2.1, 4.2.2.2, 4.2.2.3 , 4.2.2.4 y 4.2.1.5. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2.7 Aprobación o rechazo de la solicitud

Acepta rechazará solicitudes, si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE, al no cumplir las obligaciones indicadas en 2.1.3. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2.8 Contrato del titular

El solicitante, al finalizar el proceso de registro de manera exitosa, tal como se indica en los puntos 4.2.2.1, 4.2.2.2, 4.2.2.3, 4.2.2.4 y 4.2.1.5, debe firmar el contrato de suscripción, el cual hace parte de la solicitud, y que es firmada digitalmente con un certificado de firma del operador de registro, de modo que ella no sea repudiable. Adicionalmente, este documento es almacenado de manera segura en la ER de Acepta. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2.9 No repudio de la solicitud

Acepta garantiza el no repudio de las solicitudes de los certificados solicitados, firmando dichas solicitudes con firma electrónica digital, tanto de su operador de registro, como del operador de validación de Acepta. La lista de Operadores de Registro y Operadores de Validación autorizados por la ER de Acepta se encuentra firmada por la EC intermedia de Acepta y es generada con los mismos estándares de seguridad con los que se generan los certificados de las Autoridades Certificadoras intermedias de Acepta.

Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2.10 Asignación de suscriptores

El representante autorizado, cuya identidad haya sido validada por Acepta, a través de la presentación de la documentación indicada en 4.2.2.4, designará a los suscriptores que recibirán certificados digitales en nombre de la persona jurídica, por medios no repudiables. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2.11 Verificación de la identidad de los suscriptores

Los certificados de firma digital que garantizan el no repudio, son emitidos por la ER y EC de Acepta, sólo si se ha realizado una verificación presencial de identidad positiva por parte de la ER. La ER de Acepta, puede además realizar la verificación presencial por medio de un Notario Público autorizado por la AAC. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2.12 Verificación de las facultades laborales de los suscriptores

En el caso que un certificado sea solicitado a Acepta para acreditar el ejercicio de un cargo en concreto, Acepta solicitará como prueba que evidencie el cargo, incluyendo las limitaciones y facultades de actuar como empleado de la persona jurídica correspondientes a dicho cargo, de un documento firmado por el

representante legal de la persona jurídica; así como el certificado que demuestre el nombramiento del cargo y poderes, para representar a la persona jurídica, del firmante de dicho documento. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2.13 Verificación de los datos de la solicitud

La ER de Acepta valida que los datos de la solicitud del certificado que es remitida a su EC, para la emisión del certificado, correspondan a los datos de la identidad validada, ello según 4.2.2.1, 4.2.2.2, 4.2.2.3 y 4.2.2.5. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2.14 información no verificada del suscriptor o titular

Acepta no incluye en sus certificados, información no verificada del suscriptor o el titular según sea el caso, siendo la única excepción la permitida por la IOFE, y que corresponde a la dirección de correo electrónico del suscriptor. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2.15 No repudio de la invitación de generación de claves e instalación del certificado

La invitación para la generación de claves e instalación del certificado, asociado a la solicitud se realiza de acurdo a lo indicado en el punto 6.2; de modo que sólo el suscriptor verificado tiene control sobre la generación del par de claves, incluyendo para el caso de la firma digital del exclusivo control del módulo criptográfico donde se almacenará su clave privadas. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2.16 Conformidad del titular

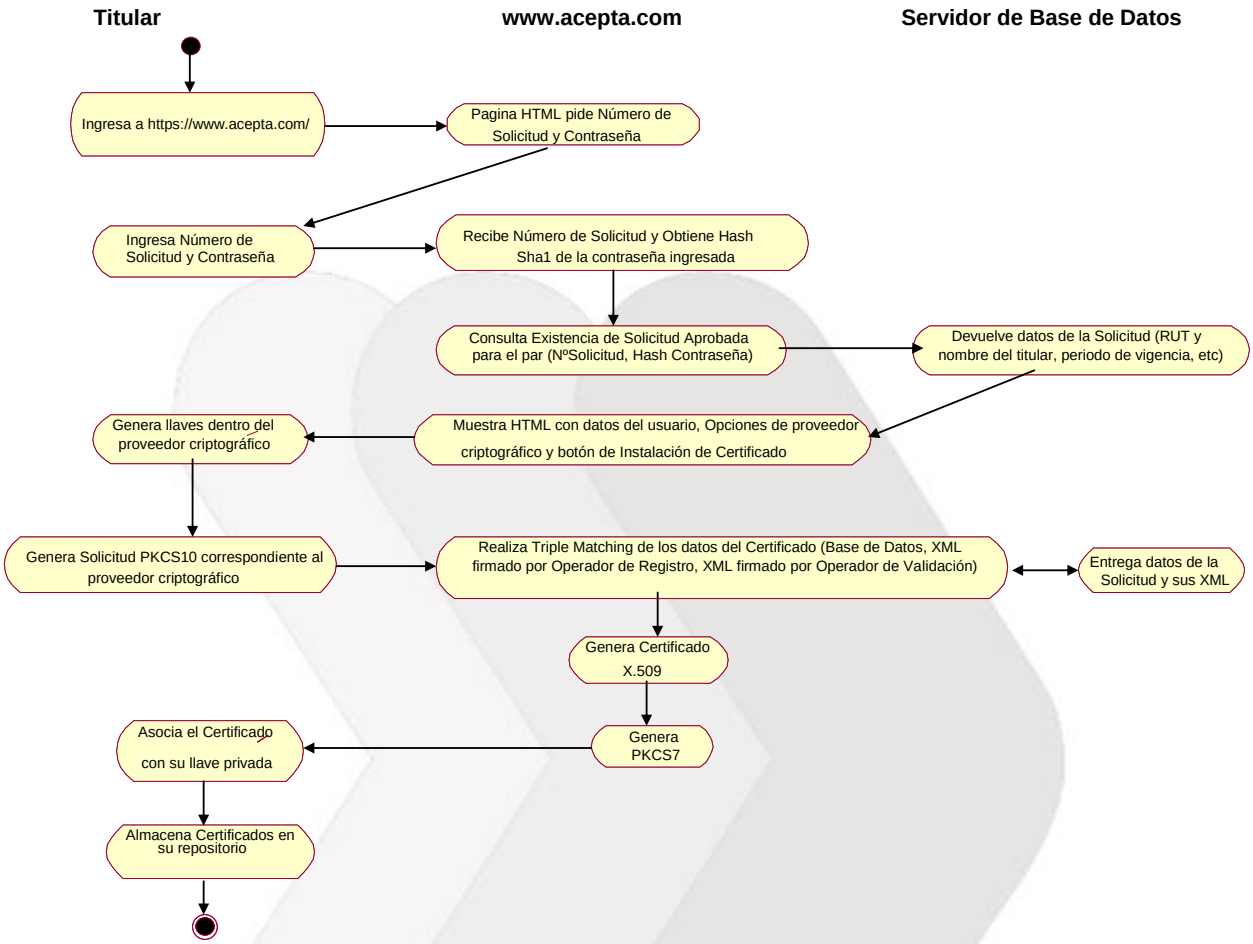
Acepta solicita la conformidad expresa del titular respecto a la emisión de los certificados solicitados ya sea el representante legal o suscriptor autorizado, a través de la firma del contrato de suscripción. Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.2.2.17 Tiempo de procesamiento

Para mayor detalle remítase a Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.3 Emisión de Certificados

El proceso seguido para la emisión, recuperación e instalación de un certificado de firma digital, o firma electrónica es descrito a continuación:



Una vez que el suscriptor ha recibido por e-mail la notificación de que su solicitud de certificado ha sido aprobada, éste debe conectarse a una página web de emisión de certificados. Luego, el suscriptor deberá proporcionar la clave de activación (definida en el registro presencia) y el número de solicitud (recibido por e-mail).

Todos los datos digitados por el usuario son enviados de manera segura (cifrada) al sitio de Acepta a través de Internet, en donde se realiza la validación necesaria para comprobar que dichos datos correspondan efectivamente a una solicitud previamente requerida, y que hasta ese momento se encuentra en estado pendiente y aprobada. Esto garantiza que el certificado será instalado sólo en el equipo del suscriptor que corresponde a la solicitud, y cuyos antecedentes de registro se encuentran en Acepta.

Siguiendo con el proceso, Acepta le envía al usuario una página con los antecedentes del certificado requerido y se los presenta al usuario para su confirmación.

Si el usuario reconoce, se genera el par de llaves pública y privada, lo que es realizado íntegramente en el equipo computacional del suscriptor, dentro del dispositivo de almacenamiento de llaves privadas.

La clave pública generada es enviada de manera segura al sitio de Acepta. La información correspondiente de la llave pública, se transmite usando el formato estándar PKCS#10.

En los servidores de Acepta se prepara un certificado en formato X.509v3 se envía a servidores de firma. Los servidores de firma son administrados con los más altos niveles de seguridad y no tienen acceso a Internet.

Antes de firmar el certificado X.509v3, en los servidores de firma se realiza un “Triple matching", el cual valida los siguientes elementos:

- Que los datos del certificado que se generará coincidan con los datos de la base de datos que apoyan los procesos de Acepta. Esto se hace indirectamente al usar los datos de la base de datos de Acepta para preparar el archivo X.509v3 y tomar sólo la clave pública del archivo PKCS#10.
- Que los datos del certificado que se generará coincidan con una solicitud de registro firmada con la firma digital de un operador de registro autorizado por Acepta.
- Que los datos del certificado que se generará coincidan con una autorización firmada con la firma digital de un operador de validación central autorizado por Acepta.

La lista de Operadores de Registro y Operadores de Validación autorizados por Acepta se encuentra firmada por la AC intermedia de Acepta y es generada con los mismos estándares de seguridad con los que se generan los certificados de las Autoridades Certificadoras intermedias de Acepta.

Si estas 3 verificaciones resultan exitosas, se firma el certificado X.509v3 y es enviado como respuesta al browser del usuario.

Posteriormente dicho certificado es instalado en el dispositivo de almacenamiento de llave privada de Acepta.

4.4 Aceptación de Certificados

La aceptación de los certificados por parte de los firmantes se produce en el momento de la firma del contrato de suscripción asociado a cada Política de Certificación. La aceptación del contrato implica el conocimiento y aceptación por parte del suscriptor de la Política de Certificación asociada.

El contrato de suscripción es un documento que debe ser firmado por el suscriptor, y cuyo fin es vincular a la persona a certificar con la acción de la solicitud, con el conocimiento de las normas de uso y con la veracidad de los datos presentados.

4.5 Uso del par de claves y del certificado

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.6 Re-emisión de certificados.

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.7 Renovación de claves

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.8 Modificación de certificados.

No aplica.

4.9 Suspensión y Revocación de Certificado

Los certificados de firma electrónica o digital, podrán ser revocados principalmente bajo las siguientes circunstancias:

a) Solicitud del titular del certificado.
b) Fallecimiento del titular.
c) Resolución judicial ejecutoriada.
d) Que el titular haya proporcionado al momento de solicitar el certificado información inexacta o incompleta.
e) Que el titular no custodie adecuadamente los mecanismos de seguridad de funcionamiento del sistema de certificación provistos por Acepta.
f) Si el titular no actualiza los datos proporcionados a Acepta al momento de solicitar el certificado.

Frente a cualquiera de estas circunstancias, un operador de validación de Acepta podrá ingresar a una aplicación especial y firmar electrónicamente la autorización de revocación.

Esta aplicación alimenta la base de datos de Acepta con la que se generan las listas de revocación (CRL) y respuestas a consultas en línea, ya sea a través del sitio web o de OCSP.

Respecto a la suspensión, su efecto será el invalidar un certificado durante el tiempo que permanece suspendido. Pudiendo ser solicitada por el suscriptor del certificado, por Acepta como AC o en caso excepcionales a través de una orden judicial

Para un mayor detalle respecto a revocación y/o suspensión de certificados, remítase a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.9.1 Circunstancias de Revocación

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.9.2 Solicitud de Revocación

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.9.3 Procedimiento de Revocación

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.9.4 Motivos de Suspensión

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.9.5 Solicitud de Suspensión

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.9.6 Descripción de Procedimiento de Suspensión

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.9.7 Límite de Suspensión

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.9.8 Listado de Certificados Revocados

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.10 Servicios de comprobación de estado de certificados.

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

4.11 Finalización de la suscripción.

La suscripción finaliza con el término de vigencia de un certificado o la revocación del mismo.

4.12 Depósito y recuperación de claves.

Acepta no genera las claves de sus suscriptores, y por lo tanto no tiene la posibilidad de almacenar ni recuperar sus claves.

Acepta mantiene los certificados emitidos, los cuales contienen sólo la llave pública del titular. Estos certificados pueden ser descargados por la comunidad para los fines que estime conveniente.

5 Controles de Personas, Físicos y de Procedimientos

5.1 General

En este capítulo se describen los controles físicos, de procedimientos y de personal que utiliza la AC en los procesos de identificación, emisión, revocación, auditoría y almacenamiento de sus certificados.

5.2 Data Center

Los sistemas e infraestructura del Servicio de Emisión de Certificados, se encuentra alojado en un Sitio Principal y uno secundario. Las características generales del recinto Principal comprenden una Zonificación en Alta Criticidad (Sitio de Producción) y una Zona de Media Criticidad (recintos de Operaciones y Cintoteca).

- Zona Alta Criticidad: Sitio de Producción:
  - El espacio físico blindado en su perímetro desprotegido de muros estructurales del edificio.
  - Sistema de esclusas mediante puerta corta fuego y blindada opaca y vidriada blindada.
  - Acceso restringido.
  - Sistema de video vigilancia.
  - Piso falso de 30cm de altura con cámara plena para distribución de aire para climatización de todos los equipos de la sala.
  - Acceso por rutas físicas redundantes para fibras ópticas carriers.
  - Equipos de Climatización precisa redundantes en configuración 1+1.
  - Equipos de energía ininterrumpida UPS redundantes en configuración 1+1 . La iluminación de la sala se encuentra respaldada por el sistema UPS y el grupo electrógeno.
  - Sistema autónomo de detección y extinción de incendios en base a gas FM-200.
  - Soporte generación autónoma de energía de emergencia mediante Grupo Electrógeno de operación continua. Todos los equipos están respaldados.

- Zona Criticidad Media: Operaciones:
  - Espacio cerrado de oficinas dotado de puestos de trabajo para personal operación y administración.
  - Acceso restringido mediante tarjeta magnética u botonera con clave.
  - Sistema de Video Vigilancia.
  - Iluminación y puestos de trabajo respaldados por el grupo electrógeno.

- Zona Criticidad Media: Cintoteca:
  - El espacio físico blindado en su perímetro desprotegido de muros estructurales del edificio, alejado del Sitio de Producción.
  - Puerta de acceso corta fuego y de seguridad.
  - Acceso restringido mediante cerradura de seguridad.
  - Sistema autónomo de detección y extinción de incendios en base a gas FM-200.
  - Iluminación respaldada con grupo electrógeno.

Respecto al sitio secundario sus principales características son:

- Acceso restringido y controlado.
- Climatización full redundante calculada de acuerdo a la carga térmica de la sala.

- Alimentación del sistema eléctrico independiente de otros consumos propios del lugar en que se encuentra ubicado el sitio secundario.
- Sistema de respaldados con UPS redundante y grupo electrógeno.
- Sistema de detección temprana de incendio y extinción vía agente limpio FM-200
- Sistema de detección de sobre temperatura para monitorear permanentemente el funcionamiento del sistema de Aire Acondicionado.
- Sistema de detección de intrusos
- Acceso por rutas físicas redundantes para fibras ópticas carriers
- Acceso a través de una puerta cortafuego de características para resistencia al fuego F-60.
- Sistemas de Circuito Cerrado de Televisión.

Los controles definidos en ambos sitios, para proteger los elementos que forman parte de la solución de Acepta, se basan en procedimientos y estándares de seguridad física para las instalaciones informáticas. Estos a su vez se encuentran elaborados según la norma ISO 27001, para la cual ambos sitios se encuentran certificados.

5.2.1 Seguridad Física Data Center
De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.2.2 Sistema de Energía Eléctrica
De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.2.3 Sistema de Control Ambiental
De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.2.4 Sistema de Extinción y Control de Incendios
De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.2.5 Telecomunicaciones
De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.2.6 Seguridad Lógica Data Center
De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.3 Controles de procedimientos
Los sistemas de información y los servicios de Acepta se operan de forma segura, siguiendo procedimientos preestablecidos.

5.3.1 Papeles de confianza
Los roles definidos para el control y gestión del sistema son:

- Administrador de Sistemas
- Administrador de Seguridad
- Operador de Registro
- Operador de Validación
- Responsable de formación, soporte y comunicación

- Responsable de Seguridad
- Auditor
- Responsable de Documentación

Para un mayor detalle remítase a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.4 Controles de seguridad del personal

5.4.1 Requerimientos de antecedentes y experiencia

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.4.2 Comprobación de antecedentes

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.4.3 Requerimientos de formación y reentrenamiento

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.4.4 Frecuencia de rotación de tareas

No aplica.

5.4.5 Sanciones

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.4.6 Requerimientos de contratación

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.4.7 Documentación entregada al personal

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.4.8 Control de cumplimiento

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.4.9 Finalización de contratos

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.4.10 Definición de roles

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.5 Procedimientos de auditoría de seguridad

5.5.1 Tipos de eventos registrados

Los tipos de eventos registrados dependen de las políticas señaladas para cada tipo de certificado. En particular para certificados digitales se registra:

- Intentos exitosos o fracasados de cambiar los parámetros de seguridad del sistema operativo.
  - Inicio y detención de la CA.
  - Intentos exitosos o fracasados de inicio y fin de sesión de administradores.
  - Intentos exitosos o fracasados de crear, modificar o borrar cuentas del sistema.

- Intentos exitosos o fracasados de crear, modificar o borrar usuarios del sistema autorizados.
- Intentos exitosos o fracasados de solicitar, generar, firmar, emitir o revocar claves y certificados.
- Intentos exitosos o fracasados de generar, firmar o emitir una CRL.
- Intentos exitosos o fracasados de crear, modificar o borrar información de los titulares de certificados.
- Intentos exitosos o fracasados de acceso a los sitios principal y secundario por parte de personal autorizado o no.
- Backup, archivo y restauración.
- Cambios en la configuración del sistema.
- Actualizaciones de software y hardware.
- Mantenimiento del sistema.

Para mayor detalle remítase a la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.5.2 Frecuencia de procesamiento del log
De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.5.3 Periodo de Retención para el log de auditoría
De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.5.4 Protección del log de auditoría
De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.5.5 Procedimientos de respaldo del log de auditoría
De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.5.6 Evaluaciones de vulnerabilidad
De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.5.7 Identidad/calificaciones de asesores
De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.6 Políticas para archivo de registros

5.6.1 Documentos archivados
Con el fin de mantener un adecuado respaldo de la información involucrada en el proceso de certificación, así como para brindar seguridad y garantía a todas las partes involucradas, se almacenaran en un medio seguro una serie de documentos relevantes al proceso de certificación. Ellos son:

- Los registros de auditoría especificados en el punto 5.5 de esta Declaración de Prácticas de Certificación.
- Los soportes de backup de los servidores que componen la infraestructura de la AC de Acepta.
- Documentación relativa al ciclo de vida de los certificados

- Acuerdos de confidencialidad
- Contratos suscritos por la Acepta en su función de CA
- Autorizaciones de acceso a los Sistemas de Información

5.6.2 Requerimientos para "marca de tiempo" de registros

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.6.3 Sistema de colección de archivos

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.6.4 Procedimientos para obtener y verificar información de archivos

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.7. Compromiso de clave de una entidad

En el caso de compromiso de la clave de una entidad perteneciente a la PSC de Acepta, se procederá a su revocación inmediata y se informará del hecho al resto de entidades dependientes

Para un mayor detalle remítase a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.8 Recuperación en caso de compromiso de una clave o de desastre

5.8.1 Alteración de los recursos hardware, software y/o datos

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.8.2 La clave pública de una entidad se revoca

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.8.3 La clave de una entidad se compromete

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.8.4 Instalación de seguridad después de un desastre natural u otro tipo de desastre

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

5.9 Cese de la actividad del PSC

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

6 Controles de Seguridad Técnica

6.1 General

En este punto Acepta describe las medidas de seguridad que ha tomado para proteger tanto las llaves generadas, como los datos de activación de dichas llaves (Clave creada por el usuario al momento de la solicitud), a fin de que dicha información sea sólo accesible a las personas autorizadas. También se describe los aspectos técnicos relacionados con la generación de llaves, la identificación de los usuarios, el registro de certificados, su revocación, auditoria y almacenamiento.

6.2 Instalación y Generación de Pares de Llaves

6.2.1 Generación del par de claves

Los pares de claves para todos los componentes internos de Acepta, se generan en módulos de hardware criptográficos con certificación FIPS 140-2 Nivel 3.

- **Certificados Propios de la PSC:** Los pares de claves para todos los componentes internos de Acepta, se generan en módulos de hardware criptográficos con certificación FIPS 140-2 Nivel 3.
    - AC raíz: La máquina donde reside la AC raíz dispone de un dispositivo criptográfico (HSM) para la generación de claves de la AC raíz. Esta raíz una vez generada las llaves subsiguientes y CRL respectiva, queda fuera de línea a menos que se requiera generar la CRL de las llaves subsiguientes.
    - AC intermedias: La máquina donde residen las AC intermedias dispone de un dispositivo criptográfico (HSM) para la generación de claves de las distintas AC intermedias.
- **Certificados subscriptores**: Las claves de los certificados de subscriptores pueden ser generadas empleando:
    - Dispositivo de software criptográfico en posesión del suscriptor (Firma Digital).
    - Dispositivo criptográfico (HSM) en Acepta con control exclusivo del suscriptor (Firma Digital).
    - En cualquier almacén de llaves que no cumpla características FIPS 140-2 Nivel 3 (Firma Electrónica)

Para mayor detalle remítase a la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

6.2.2 Entrega de la clave privada a la entidad

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

6.2.3 Entrega de la clave pública al emisor del certificado

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

6.2.4 Entrega de la clave pública de la AC a los usuarios

Las claves públicas de todas las EC pertenecientes a la jerarquía de confianza de Acepta se pueden descargar del sitio https://asistencia.acepta.pe/certificado-digital.html ("Complementos de instalación del Certificado Digital").

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Registro o Verificación (RPS) de Acepta.

6.2.5 Tamaño de las claves

Las claves de la AC raíz y las autoridades de certificación que se encuentran en la misma jerarquía son claves RSA de 2048 bits de longitud.

El tamaño de las claves para cada tipo de certificado emitido por la CA, se establece en la Política de Certificación que le es de aplicación. En todo caso, su tamaño nunca será inferior a 2048 bits para los certificados emitidos con la nueva versión de la AC. Todos aquellos certificados que fueron emitidos con un largo de clave de 1024 bits, continuarán en operación durante su periodo de vigencia o hasta su revocación.

Para mayor detalle remítase a la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

6.2.6 Parámetros de generación de la clave pública

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

6.2.7 Comprobación de la calidad de los parámetros

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

6.2.8 Hardware/software de generación de claves

Las claves son generadas, según el caso, de la siguiente forma:

- CA: En el propio dispositivo HSM.
- Entidad final (suscriptor): En los propios dispositivos o sistemas que las soportan.

Para mayor detalle remítase a la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

6.2.9 Fines del uso de la clave

Todos los certificados emitidos por Acepta contienen la extensión KEY USAGE definidas por el estándar X.509 v3 para la definición y limitación de fines.

Las claves definidas por la presente política se utilizarán para usos descritos en el punto de este documento, 1.4.1 Tipos y usos de los certificado.

6.3 Protección de la llave privada

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

6.4 Otros aspectos de gestión del par de claves

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

6.5 Datos de activación

Los datos de activación de las Autoridades de Certificación de Acepta, se generan y almacenan en smart cards criptográficas en posesión de personal autorizado. Sólo este personal conoce las contraseñas para tener acceso a datos de activación.

En relación al dato de activación (PIN) de firma, se requiere a los operadores autorizados de los certificados, memoricen estos y además mantengan su confidencialidad.

Para mayor detalle remítase a la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

6.6 Controles de seguridad informática

Actualmente, Acepta cuenta con un plan de seguridad de la información, el cual contempla distintos controles de seguridad, desde un plan de recuperación de desastres hasta los respectivos controles de acceso. Para mayor detalle remítase a la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

6.7 Controles de Seguridad Técnica

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

6.8 Controles de seguridad de red

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

6.9 Controles de seguridad de los módulos criptográficos

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

6.10 Timestamping

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

6.11 Gestión de Residuos

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

7 Certificado, CRL y OCSP

7.1 Certificado

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

7.2 CRL

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

7.3 OCSP

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

8 Cumplimiento auditoría y otras evaluaciones

8.1. Frecuencia y circunstancias de evaluación

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

8.2. Identidad/Calificaciones de auditores

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

8.3. Relación del auditor con la entidad auditada

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

8.4. Elementos cubiertos por la evaluación

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

8.5. Acciones a ser tomadas frente a deficiencias

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

8.6. Publicación de resultados

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9 Otros negocios y materias legales

9.1 Tarifas

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9.2 Responsabilidad Financiera

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9.3 Confidencialidad de información del negocio

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9.4 Privacidad

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9.5 Propiedad Intelectual

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9.6 Representación y Garantía

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9.7 Exención de Garantías

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9.8 Limitaciones de responsabilidad

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9.9 Indemnizaciones

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9.10 Duración y terminación

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9.11 Noticias individuales y comunicaciones con participantes

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9.12 Enmiendas

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9.13 Resolución de disputas

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9.14 Leyes gubernamentales

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9.15 Cumplimiento con la ley aplicable

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9.16 Misceláneas

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

9.17 Otras provisiones

De acuerdo a lo especificado en la Declaración de Prácticas de Registro y Verificación (RPS) de Acepta.

10 Administración de las RP

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

10.1 Procedimientos para Modificar las RP

Las políticas de registro contenidas en este documento, son administradas y mantenidas rigurosamente por personal especializado y en posiciones de confianza en la compañía.

10.2 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 en https://sovos.com/es/politicas-y-practicas/.

10.3 Procedimientos de aprobación de las RP

Estas RP y las subsecuentes versiones futuras de éste documento están sujetas a la aprobación del Comité de seguridad de Acepta.

11 REVISIÓN Y APROBACIÓN DEL DOCUMENTO

11.1 Revisión

Este documento es revisado anualmente a fin de verificar su validez y eficacia, o en un plazo menor en caso de producirse cambios significativos que ameriten su revisión de acuerdo al marco regulatorio, comercial, legal o técnico.

11.2 Control de cambio

Cada vez que se requiera efectuar una modificación a estas CP, esta debe ser incorporada al documento y reflejada en un historial de cambios. Para ello, se debe ingresar una nueva entrada en el historial de cambios de la portada de este documento conforme se detalla a continuación:

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha

Con esto se logrará mantener una traza respecto a las actualizaciones que ha sufrido este documento. La nueva versión del documento será almacenada en el sistema documental de Acepta, con su respectivo control de versión, posterior a su aprobación.

Además, en caso de existir cambio en la referencia a documentación externa se debe modificar el siguiente cuadro, incorporando este cambio:

REFERENCIAS

Documentos Internos	
Título	**Nombre del archivo**
Documentos Externos	

11.3 Aprobación

Este documento así como sus modificaciones deben ser aprobados por el dueño del documento y en comité de seguridad, a fin de que sea incorporado como la nueva versión vigente al sistema de gestión documental y para posteriormente proceder a su difusión con los empleados y partes externas pertinentes.