ACEPTA

Empresas
a velocidad
digital

PO02

Declaración de Prácticas de Certificación

Entidad de Certificación

EC

Enero 2014

OID 1.3.6.1.4.1.6891.1

MANUEL
ENRIQUE
GODOY
RAMIREZ

Digitally signed by
MANUEL ENRIQUE
GODOY RAMIREZ
Date: 2025.02.14
10:32:53 -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 Prácticas de Certificación - PO02	1.0	Primera versión	23-01-2014
Declaración de Prácticas de Certificación - PO02	1.1	- Cambios en vigencias y diferencia entre vigencia y operación - Ajustes de texto	15-07-2014
Declaración de Prácticas de Certificación - PO02	1.2	Actualización proveedor de data Center	04-03-2015
Declaración de Prácticas de Certificación - PO02	2.0	Segunda versión	29-06-2016
Declaración de Prácticas de Certificación - PO02	4.0	Revisión anual	01-10-2016
Declaración de Prácticas de Certificación - PO02	4.1	Ajustes Perú	04-01-2017
Declaración de Prácticas de Certificación - PO02	4.2	Ajuste a punto 3.4 (revocación por parte de la empresa)	29-05-2017
Declaración de Prácticas de Certificación - PO02	5.0	Revisión anual	01-10-2017
Declaración de Prácticas de Certificación - PO02	5.1	Posibilidad de realizar la operación de registro y validación en base a clave única del SRCeI	07-11-2017
Declaración de Prácticas de Certificación - PO02	5.2	Ajustes Jurisprudencia	02-04-2018

Declaración de Prácticas de Certificación - PO02	5.3	Ajustes Asociados a Certificación 2018	06-04-2018
Declaración de Prácticas de Certificación - PO02	5.4	Ajustes a nombre de Prácticas	11-04-2018
Declaración de Prácticas de Certificación - PO02	5.5	Ajustes contacto, acrónicos y calificación asesores	25-04-2018
Declaración de Prácticas de Certificación - PO02	6.0	Revision anual	11-03-2019
Declaración de Prácticas de Certificación - PO02	6.1	Ajustes a capítulo 9, producto de seguimiento 2019	15-04-2019
Declaración de Prácticas de Certificación - PO02	6.2	Actualización producto de nuevas guías de acreditación INDECOPI	30-09-2019
Declaración de Prácticas de Certificación - PO02	7.0	Revision anual	01-10-2019
Declaración de Prácticas de Certificación - PO02	8.0	Revision anual	01-10-2020
Declaración de Prácticas de Certificación - PO02	8.1	Modifica 4.2 para incorporar solicitudes de firma digital y electrónica con atención remota	08-11-2021
Declaración de Prácticas de Certificación - PO02	8.2	Se elimina referencias a términos usados en Chile, se uniforman términos de EC y ER, se corrige la resolución de conflictos y se elimina legislación Chilena y la firma electrónica	24-11-2021
Declaración de Prácticas de Certificación - PO02	9.0	Revision anual	15-03-2022
Declaración de Prácticas de Certificación - PO02	10.0	Revision anual	15-03-2023
Declaración de Prácticas de Certificación - PO02	10.1	Ajustes a prácticas como parte de Re Acreditación	12-05-2023
Declaración de Prácticas de Certificación - PO02	11.0	Revision anual	30-04-2024
Declaración de Prácticas de Certificación - PO02	12.0	Revision anual	14-02-2025

CLASIFICACIÓN DEL DOCUMENTO

NIVEL DE CRITICIDAD: Baja **NIVEL DE CONFIDENCIALIDAD: Pública**
NOTA DE CONFIDENCIALIDAD: Información de Libre Acceso al Público. ESTE DOCUMENTO NO PUEDE SER REPRODUCIDO, DISTRIBUIDO, COMUNICADO, TRANSMITIDOO ALMACENADO, TOTAL O PARCIALMENTE, EN CUALQUIER FORMA O POR CUALQUIER MEDIO, SIN EL PREVIO CONSENTIMIENTO POR ESCRITO DE ACEPTA.

CONTROL DE DIFUSIÓN

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

Documentos Internos	
Título	**Nombre del archivo**
Tarifas y procedimiento de reembolso	Tarifas y procedimiento de reembolso.docx
PS02 Análisis y Gestión de Riesgos	PS02 Análisis y Gestión de Riesgos.docx
PS04 Plan de Seguridad	PS04 Plan de Seguridad.docx
PS06 Plan de administración de llaves	PS06 Plan de administración de llaves.docx
PO02 Declaración de Prácticas de Registro y Verificación	PO02 Declaración de Prácticas de Registro y Verificación.docx
Documentos Externos	
• Ley N° 27.269, Ley 29.733 (Perú) • SG-Q-01 Política de Seguridad de la información • SG-M-02 Manual de Operaciones de Sistemas • SG-M-03 Manual de Seguridad • SG-P-18 Seguridad de la información y administración de la prestación de servicios de proveedores • CA-M-03 Indicadores de Calidad • SG-Q-06 Política de control de acceso • SG-F-05 Listado de activos de información primarios	

ÍNDICE

1 Introducción

1.1 Presentación

En el siguiente documento se presenta la Declaración de "Prácticas de Certificación" (CPS, por su sigla en inglés Certification Practice Statement) de Acepta para los certificados de firma digital. Estas son una descripción detallada de los procedimientos o prácticas que Acepta declara convenir en la prestación de sus servicios de certificación, cuando emite y gestiona certificados de firma 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 digital (Entidad de Registro).

Es así como la presente Declaración de Prácticas de Certificación (CPS) detalla las normas y condiciones de los servicios de certificación de firma digital que presta Acepta y que están relacionadas con la gestión del ciclo de vida de los certificados de firma, en particular lo relativo a la información utilizada en la emisión, la verificación de los certificados electrónicos y de su firma, las condiciones asociadas a la solicitud, emisión, uso, suspensión y la revocación de dichos certificados. También se describen las medidas de seguridad técnica y organizativa, los perfiles y los mecanismos de información que permiten verificar y administrar la vigencia de los certificados, así como la forma en que se asegura que el proceso de certificación es llevado a cabo en un ambiente seguro capaz de brindar total confianza a la comunidad que interactúa en torno a la firma digital

1.1.1 Sobre las Prácticas de Certificación

Las prácticas de certificación aquí descritas establecen y configuran el ciclo de vida de los certificados de firma digital que comercializa Acepta. Es decir, se trata de una declaración unilateral que hace Acepta por medio de la cual se obliga a desarrollar la actividad de certificación de firma digital, en la forma aquí declarada.

1.1.2 Alcance

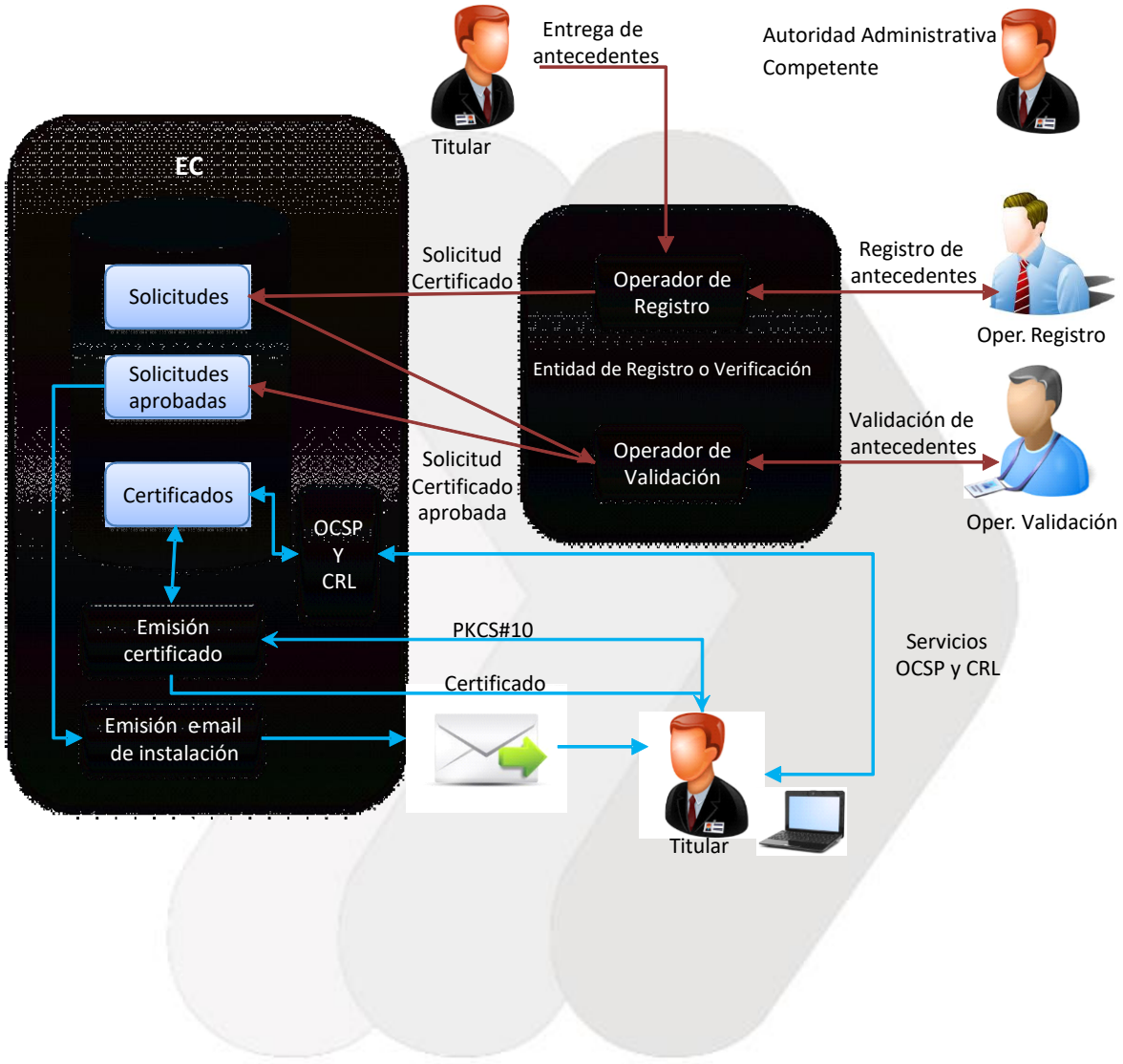
El alcance de esta Declaración de Prácticas de Certificación (CPS) detalla las normas y condiciones de los servicios de certificación que presta Acepta para la emisión de sus certificados de firma digital.

1.1.3 Referencias

La presente Declaración de Prácticas de Certificación 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 digital, 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). La siguiente figura muestra dicha relación:



1.2 Identificación

El presente documento de "Prácticas de Certificación de Acepta", también acá referidas como "CPS", está registrado con el número único internacional (OID) 1.3.6.1.4.1.6891.1.

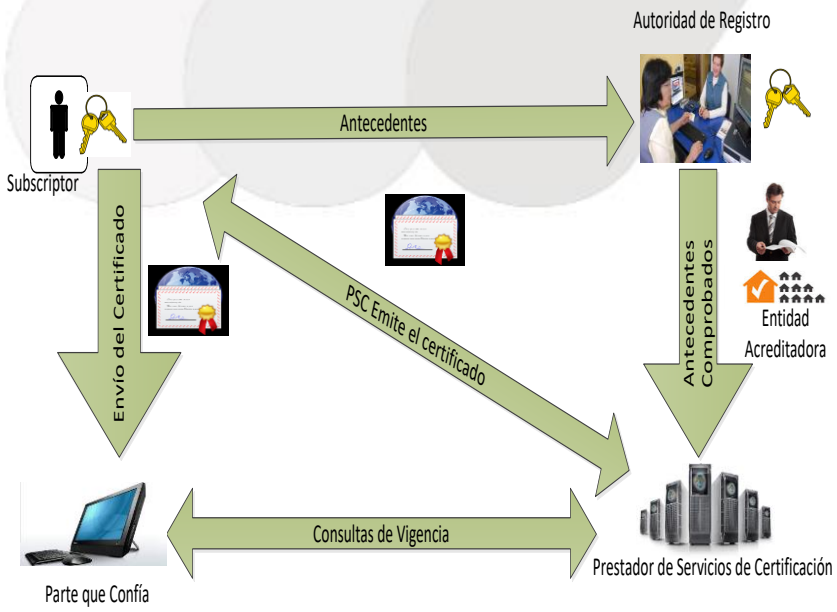
Acepta tiene asignado el identificador (OID) 1.3.6.1.4.1.6891, el cual está registrado en la Internet Assigned Number Authority (IANA). Este número identifica únicamente a Acepta en un contexto global.

Las políticas de las CPS y de cada tipo de certificado están registradas con un número único internacional, llamado Object Identifier (OID). La siguiente tabla resume todos los OID administrados por Acepta:

Descripción	OID
Prácticas de Certificación	1.3.6.1.4.1.6891.1
Políticas de certificados Clase 3	1.3.6.1.4.1.6891.2
Políticas de certificados de firma digital	1.3.6.1.4.1.6891.3
Políticas de certificados de Sitio Web	1.3.6.1.4.1.6891.4
Extensión para indicar declaraciones del titular de un certificado X.509	1.3.6.1.4.1.6891.9
Extensión para certificados X.509 en la que se incluye el XML de un CAF.	1.3.6.1.4.1.6891.50.1
Identificador permanente administrado por Acepta para nombrar Servidores.	1.3.6.1.4.1.6891.100.1
Identificador permanente administrado por Acepta para nombrar Servicios.	1.3.6.1.4.1.6891.100.2

1.3 Comunidad y Aplicabilidad

Los servicios de certificados de firma digital de Acepta están insertos en una infraestructura en que se relacionan distintos sujetos. Básicamente: Prestador de Servicios de Certificación (PSC), Entidad de Registro o Verificación, Titular, 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 digital, completan el formulario de solicitud y proveen todos los antecedentes que exige la ley y esta CPS 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 digital. Los titulares 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 o verificación**: La recepción y procesamiento de las solicitudes de certificados es realizada por la "Entidades de Registro o Verificación" (ER en Perú) de Acepta, sea que lo haga directamente o a través de un mandatario especialmente designado para tal objeto. La Entidad de Registro o Verificación debe realizar la comprobación fehaciente de la identidad de los solicitantes de certificados de firma digital. En caso que sea un tercero el que actúe, en calidad de mandatario de Acepta, como Entidad de Registro o Verificación, 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 digital, de conformidad a la ley, en particular, a lo previsto en la Ley 27.269 (Perú), que en este caso es Acepta.
- **Tercera parte que confía**: Es el receptor de un certificado de firma digital. Normalmente, junto con el certificado este tercero recibe un documento electrónico que se encuentra suscrito con la firma digital del titular. 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:** A INDECOPI, el Prestador de Servicios de Certificación de Firma debe demostrarle que cuenta con las instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados de firma digital, permitiendo su inscripción en el registro de certificadores acreditados.

1.4. Aplicabilidad de los certificados

Los certificados de firma digital emitidos por Acepta podrán ser utilizados por los titulares de conformidad con lo dispuesto en esta Declaración de Prácticas de Certificación y dando especial respeto a cualquier límite funcional que se incorpore en ellos, de conformidad con lo dispuesto en la Ley 27.269 (Perú) y su reglamento.

1.4.1 Tipos y usos de los certificados

Acepta emite distintos tipos de certificados, definiendo para cada tipo un nivel de seguridad, restricciones y requerimientos específicos respecto a las medidas tomadas para la autentificación de la entidad titulara del certificado, mecanismos de emisión, revocación y utilización de los certificados. Los titulares 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 cada tipo de certificado emitido.

A continuación, se muestra un resumen de los tipos de certificados emitidos por Acepta:

Tipo	Características generales	Usos típicos
Firma Electrónica	• Registro presencial. • Certificado para persona natural y/o jurídica. • El medio de almacenamiento de la llave privada es elegido por el titular del certificado. • Estas políticas de certificado han sido acreditadas por el SII y por Aduanas en Chile.	• e-mail firmado • Autenticación del titular en sitios Web, como el del SII o SUNAC. • Factura electrónica. • Operaciones aduaneras. • Otros en que las partes elijan libremente confiar en estos certificados.
Firma Digital	• Registro presencial. • Certificado para persona natural y/o jurídica. • El medio de almacenamiento de la llave privada debe ser un dispositivo especializado que cumpla con la norma FIPS-140-2 nivel 3 o superior. • Estas políticas de certificado y la forma de cumplirlas han sido acreditadas por INDECOPI en Perú	• Todos los usos de los certificados Firma Electrónica • Firma electrónica de instrumentos públicos. • Firma electrónica de documentos privados con el mismo valor probatorio de un instrumento público.

Tabla 1: Tipos de certificados

1.4.2 Limitaciones de Uso y Prohibiciones

Los Certificados de firma digital emitidos por Acepta se utilizarán únicamente conforme a los usos y finalidades que tengan establecida en este documento y en las correspondientes Políticas de Certificación, y de acuerdo a la normativa chilena vigente y a los convenios internacionales ratificados por la República del Perú según corresponda. Cualquier uso diferente del autorizado por ley e indicado en estas prácticas está expresamente prohibido. En consecuencia, será responsabilidad del Titular 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

Este capítulo contiene especificaciones detalladas de los formatos y contenido de los certificados emitidos bajo la arquitectura señalada por estas CPS (campos, básicos y extensiones).

Composición del certificado raíz de Acepta

Campo	Descripción	Ejemplo
Versión	Versión del certificado, que deberá ser versión 2	V3
Nº de Serie	Número que identifica unívocamente al certificado dentro de los emitidos por Acepta	**00**
Algoritmo de Firma	Algoritmo utilizado por el PSC para firmar el certificado	SHA256 With RSAEncryption
Nombre del Emisor	Nombre distintivo (DN) del emisor, en el formato del estándar X.500. Deben incluirse los siguientes tipos: CN =Tipo de certificado E = e-mail del Prestador de Servicios de Certificación emisora Número de serie = Número identificador del Emisor C = País	SERIALNUMBER = 20562999711 E = info@acepta.com CN = Acepta Peru Autoridad Certificadora Raiz - V1 O = ACEPTA PERU S.A.C. C = PE
Periodo de Validez	Fecha de inicio y termino en que es válido el certificado. Para PSC = 10 años, para titulares = 1 año, para servidores = 2 años. Codificado en formato YYMMDDHHMMSSZ	Fecha inicio = miércoles, 18 de abril de 2018 11:54:31 Fecha termino = domingo, 18 de abril de 2038 11:54:31
Nombre del titular	Nombre distintivo (DN) del titular del certificado, en el formato del estándar X.500. Deben incluirse los siguientes tipos: CN = Nombre distintivo del titular T = Profesión E = dirección de correo del titular C = País	SERIALNUMBER = 20562999711 E = info@acepta.com CN = Acepta Peru Autoridad Certificadora Raiz - V1 O = ACEPTA PERU S.A.C. C = PE
Clave pública	Clave pública del titular del certificado	30 82 01 0a 02 82 01 01 00 b3 9e a4 3b 7a f4 a6 ab 4b 4b ca 94 aa 6f d3 c7 8c 9a e8 5e 74 2f 0f f5 ca f4 ff 57 dc 65 6c 13 c3 b3 83 35 12 34 e8 c6 5c e8 98 1e 54 0c 0b 79 77 6d 7b 5c 2f 43 29 6c e8 d9 1c d2 37 8d 5f 92 0a d9 d4 17 33 ff ff ae cf 83 e5 7d a2 a8 79 2b 9f 64 2e a5 4a f9 96 39 c9 76 6a 20 f0 54 88 88 a8 1e 42 47 1c bc 58 a6 83 b5 a6 bf f0 30 07 33 3c be 5c 51 ae 05 f3 f6 71 0b 81 f5 1c 12 b1 cf 64 df a9 93 1b 79 d4 e5 c1 d5 1d dc 9f 9d 8a 94 23 b4 be 4c 38 97 a4 63 cf d9 ff fd 1b 18 41 55 2f 8e 6f 57 99 cf 73 de cb c5 af 7d 34 14 2e bb 4c 6d b5 fc 7a d4 10 45 90 77 ae ae 53 5f 80 f8 7f a1 6c 50 af e4 7f 97 3e e9 fd bb d6 bc 4e d3 fc 40 a9 e9 70 3f c8 83 2e cc 3c d5 3d 48 c9 d2 9c 17 5a e3 ac a2 14 62 40 73 aa d2 52 aa 07 17 5f f8 de 12 97 8b 4e e4 79 61 2c b9 93 16 60 e5 02 03 01 00 01

Tabla 2: Composición del certificado Raíz de Acepta

Tipo	Nombre	Descripción	OID	Valor
RES	KeyUsage	Esta extensión define el propósito para el cual deben ser usadas las claves correspondientes al certificado. El certificado debe ser utilizado sólo para los propósitos definidos por esta extensión.	2.5.29.15	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
RES	BasicConstrains	Permite diferenciar entre un certificado de PSC y uno de titular final.	2.5.29.19	Tipo de asunto=CA Restricción de longitud de ruta=Ninguno
RES	AuthorityKeyIdentifier	Medio para identificar la llave pública de Acepta El campo KeyId es idéntico al valor de la extensión SubjectKeyIdentifier		KeyID=7da80d687b38269de59b82489c6c73cd30e81d0c
RES	SubjectKeyIdentifier	Identificador único de la llave pública del PSC, conteniendo el hash de 160bit de la llave pública		7da80d687b38269de59b82489c6c73cd30e81d0c
RES	CertificatePolicy	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Ver sección 4.2.1.4		[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.6891.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://acpev1.acepta.pe/CPS-PE-V1-Aceptape [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Reference: Organization=ACEPTA PERU S.A.C. Notice Number=1 Notice Text=La utilizacion de este certificado esta sujeta a las politicas de certificado (CP) y practicas de certificacion (CPS) establecidas por Acepta, y disponibles publicamente en www.acepta.pe.
INF	IssuerAltName	Identificador alternativo del emisor, corresponde al RUT de Acepta, en formato análogo a SubjectAltName		Other Name: 1.3.6.1.4.1.8321.2=16 0b 32 30 35 36 32 39 39 39 37 31 31Other Name: 1.3.6.1.5.5.7.8.3=30 17 0c 0b 32 30 35 36 32 39 39 39 37 31 31 06 08 2b 06 01 04 01 c1 01 02
INF	SubjectAltName	Permite definir términos que identifican al titular del certificado, adicionalmente a lo establecido en el campo estándar Subject. Se podrán registrar los siguientes campos adicionales: OtherName: Para certificados de identidad de individuos, aquí se registra el RUT, en la siguiente estructura: Type-id = 1.3.6.1.4.1.8321.1 Value =’xx.xxx.xx-v’		Other Name: 1.3.6.1.4.1.8321.1=16 0b 32 30 35 36 32 39 39 39 37 31 31 Other Name: 1.3.6.1.5.5.7.8.3=30 17 0c 0b 32 30 35 36 32 39 39 39 37 31 31 06 08 2b 06 01 04 01 c1 01 02

Tabla 3: Extensiones del certificado raíz de Acepta

1.4.3.1 Contenido de los Certificados Personas Juridicas

Para aquellos certificados de personas jurídicas, su organización y atribución de responsabilidad, quedarán reflejados en los campos OU y O del certificado tal como se muestra:

- SERIALNUMBER = 44310188
- E = JUANMENDOZABAY@GMAIL.COM
- CN = JUAN ANDRES MENDOZA BAY
- T = PERSONA NATURAL
- OU = 20602550932
- O= Quality & Innovation Services
- STREET = Jiron Soledad 425
- L = Lince
- S = Lima
- C = PE

1.5 Detalle de los contactos y administración de la PSC

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

- **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

- ACR: Entidad Certificadora Raíz
- AFIS: Automated Fingerprint Identification System
- CA: Certification Authority
- CP: Certificate Policy
- CP-FA: Políticas de Certificado de Firma Digital
- CPS: Certification Practice Statement
- CRL: Certificate Revocation List
- DNI: Documento Nacional de Identificación
- ER: Entidad de Registro o Verificación
- 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
- 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 de firma digital, se obliga a realizar las siguientes actividades en la prestación de sus servicios:

1. Contar con reglas sobre prácticas de certificación que sean objetivas y no discriminatorias y comunicadas a los usuarios de manera sencilla y en idioma castellano.
2. Contar con un registro fidedigno de los antecedentes proporcionados por los solicitantes de los certificados de firma digital al momento de comprobarse fehacientemente su identidad.
3. Comprobar fehacientemente la identidad del solicitante de los certificados de firma digital. En el caso de Perú, la solicitud no podrá ser cursada en caso de no poder verificar la identidad contra RENIEC.
4. Mantener un registro de acceso público de certificados, en el que quede constancia de los emitidos y los que queden sin efecto, sea por revocación o suspensión de los mismos.
5. Tratar los datos personales recolectados con ocasión de la actividad de certificación dando cumplimiento a lo dispuesto en la Ley 29.733 sobre protección de datos personales.
6. En el caso de cesar voluntariamente en su actividad, comunicarlo previamente a los titulares de los certificados de firma digital emitidos y, en caso de no existir oposición de los titulares, transferir los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, deja sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia.
7. Publicar en el home del sitio web de Acepta las resoluciones de la Entidad Acreditadora que la afecten.
8. Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Entidad Acreditadora, con una antelación no inferior a un mes cuando vayan a cesar su actividad, y comunicarle el destino que dará a los datos de los certificados, especificando, de ser el caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto.
9. Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento concursal de liquidación o que se encuentre en cesación de pagos.
10. Cumplir con las demás obligaciones legales, especialmente las establecidas el país donde se realice la función.
11. Ejecutar la actividad de certificación de conformidad a lo dispuesto en esta Declaración de Prácticas de Certificación (CPS).
12. Emitir los certificados de firma digital con mecanismos tecnológicos y criptográficos que garanticen que el proceso de certificación es realizado adecuadamente y que cumplen con los requisitos establecidos por la Entidad Acreditadora.
13. Revocar los certificados de firma digital en los cuales se vea comprometida la confianza respecto a la veracidad de su contenido.

2.1.1 Obligaciones de la Entidad de Certificación Raíz (ACR)

El certificado raíz de Acepta permite firmar certificados de distintas comunidades. Es así como Acepta, a partir de su certificado raíz, genera la jerarquía de confianza para distintas comunidades, cada una de ellas encargadas de emitir certificados específicos de firma. Así es como a partir de la ACR, Acepta genera un conjunto de EC intermedias, cada una de las cuales posee su propia vigencia. La tabla siguiente da a conocer dicha jerarquía de confianza:

Tipo	Bits de la llave privada	Años de operación
Raíz de Acepta	RSA 2.048	10.
Firma Electrónica	RSA 2.048	10.
Firma digital	RSA 2.048	10.
Sitio Web	RSA 2.048	10.

Los certificados de las entidades certificadoras intermedias y el certificado raíz de Acepta tienen una fecha de vigencia de 10 años contados desde la fecha de generación de la raíz de Acepta. En el caso que el certificado de Acepta sea vulnerado durante su vigencia, Acepta procederá a su revocación inmediata conforme a lo indicado en la Sección 5.7 de estas CPS. Cuando se reemplazan estos certificados, se generan nuevos certificados, pertenecientes a una estructura jerárquica completamente nueva, cumpliendo con todas las formalidades de generación de llaves definidas para cada nueva entidad certificadora intermedia.

Las entidades certificadoras intermedias reemplazadas dejan de firmar certificados nuevos desde el momento de su revocación.

Las claves de las entidades certificadoras reemplazadas siguen generando listas de revocación y respondiendo a consultas OCSP por un plazo de 10 años de disponibilidad adicional, por lo que todos los certificados firmados por estas entidades certificadoras podrán cumplir su período de vigencia antes de que expire el certificado de alguna entidad certificadora presente en su cadena de certificación.

2.1.2 Obligaciones de la Entidad de Registro o Verificación (ER) y la Entidad de Certificación (EC)

Acepta para el desarrollo de la actividad de certificación de firma digital desarrolla actividades que son propias de una entidad certificadora de firma y otras que son propias de las entidades de registro. Así, realiza actividades tales como: aprobar o rechazar solicitudes de certificados de firma digital; emitir y publicar los certificados de firma digital emitidos; proveer su llave pública de manera segura a terceros, de modo que ellos puedan verificar la validez de los certificados que Acepta ha emitido (modelo de confianza), así como informar la revocación de dicha llave; proveer información del estado de los certificados emitidos así como de la lista de revocación; proveer la infraestructura necesaria para proveer los servicios de firma digital, procedimientos, seguridad física y personal adecuado para llevar a cabo las funciones asociadas a la certificación; y, en general cumplir las obligaciones legales, reglamentarias y las que emanan de estas CPS.

Las actividades que desarrolla en su calidad de entidad certificadora las ejecuta personalmente y no son delegables bajo ninguna circunstancia. Por su parte, las actividades que desarrolla en su calidad de Entidad de Registro o Verificación, las realiza en forma personal o representada.

ACEPTA no representa a ninguna ER distinta a la propia ER de ACEPTA, la cual cuenta con una resolución de operación vigente y publicada en sitio web, y que demuestran el logro de las acreditaciones de la EC y ER de Acepta. Así mismo ACEPTA en el Registro Oficial de Prestadores de Servicio de Certificación Digital (ROPS) mantiene vigente a la fecha, los siguientes servicios que entrega, todos bajo su misma persona jurídica:

ACEPTA Perú S.A.C. (RUC Nro. 20562999711)

- *Entidad de Certificación*
- *Entidad de Registro o Verificación (*Venta de Certificados Digitales)*
- *Prestador de Servicio Añadido (Sellado de Tiempo)*
- *Software de Firma Digital (Librería Firmador Acepta)*

Obligaciones de la Entidad de Registro o Verificación (ER):

- Comprobar fehacientemente la identidad de los solicitantes de los certificados de firma digital, de conformidad a lo dispuesto en estas CPS. En particular para el caso de Perú, de no estar disponible la verificación de identidad contra RENIEC, no podrá cursarse la solicitud.
- Entregar a la Entidad Certificadora (EC) los antecedentes exigidos por estas CPS que sirvieron de base para comprobar fehacientemente la identidad de los solicitantes de los certificados de firma digital.
- Custodiar los antecedentes que sirvieron de base para comprobar fehacientemente la identidad de los solicitantes de los certificados de firma digital mientras la EC no tome el control de éstos.
- Mantener los controles de seguridad física, de procedimiento y personales definidos para el desarrollo de la actividad de registro, de acuerdo a lo establecido en estas CPS y en la documentación de seguridad de Acepta.
- Contar con la infraestructura requerida para prestar el servicio de certificación, conforme al nivel de calidad comprometido.

Obligaciones de la Entidad Certificadora (EC):

- Hacer públicas las políticas y prácticas de certificación a que están sujetos los certificados de firma digital.
- Custodiar los datos de creación de firma con los cuales Acepta suscribe los certificados de firma digital que comercializa de conformidad con las normas técnicas fijadas por la Entidad Acreditadora.
- Contar con la infraestructura requerida para prestar el servicio de certificación, conforme al nivel de calidad comprometido y los requisitos y obligaciones que impone la ley.
- Generar y firmar los certificados de firma digital a partir de la información que le proporciona la Entidad de Registro o Verificación (ER).
- Entregar en la forma establecida en estas CPS los certificados de firma digital a los titulares.

- Procesar y reportar los requerimientos de revocación y suspensión de los certificados de firma digital.
- Proveer el estado de revocación de certificados a las partes interesadas.
- Mantener un registro de acceso público de los certificados de firma digital, en el que quedará constancia de los emitidos y los que han quedado sin efecto.

Para asegurar el cumplimiento de las obligaciones señaladas precedentemente, Acepta ha definido:

- Prácticas de Certificación de firma digital.
- Controles respecto a la generación de llaves, que aseguran que ellas son generadas en una infraestructura segura (con múltiples sitios), con roles definidos y con un doble control (operadores de registro y validación).
- Algoritmos reconocidos por la industria para la generación de claves.
- Un largo de llave de al menos 2048 bits.
- Procedimientos para generación de llave de la EC ante expiración de la misma, sin que ello implique interrupción de los servicios.
- Procedimientos para el respaldo, almacenamiento y recuperación de las llaves de la EC sólo por personal autorizado y en base al quórum que se ha definido para esta acción.
- Un canal seguro para la distribución de la llave pública de la EC que permita verificar a los terceros interesados, los certificados que Acepta a firmado.
- Que los certificados de firma estén asociados sólo al propósito para el cual han sido definido (Campo CN en Nombre de Emisor).
- Que la llave privada no puede ser usada de manera posterior a su fecha de expiración.
- Que existe un procedimiento para el control del ciclo de vida de los elementos criptográficos.
- Que la llave privada del cliente debe ser almacenada en un dispositivo que no comprometa su seguridad.
- Que la entrega de los datos de creación de firma al titular no debe comprometer su seguridad.

2.1.3 Obligaciones del Solicitante

Los solicitantes de certificados de firma digital se encuentran obligados a:

- Conocer y aceptar estas CPS.
- Conocer y aceptar el propósito y alcance de los certificados de firma digital que le vaya a emitir Acepta.
- Brindar a la Entidad de Registro o Verificación (ER) declaraciones exactas y completas respecto a su identidad personal y otras circunstancias objeto de certificación por parte de Acepta.
- Notificar a Acepta cualquier cambio en las declaraciones, respecto a su identidad personal u otras circunstancias objeto de certificación y que hayan sido proporcionadas a la Entidad de Registro o Verificación al momento de la comprobación fehaciente de la identidad.
- Custodiar adecuadamente los datos de creación de firma del certificado de firma digital que Acepta le emita, así como cualquier otro mecanismo de seguridad de funcionamiento del sistema de firma.
- Suscribir el contrato de prestación de servicios de certificación digital.
- Abonar la tarifa o precio establecido para el servicio solicitado.

2.1.4 Obligaciones del Titular de la Llave

Las obligaciones del Titular del certificado de firma digital se resumen en:

- Proteger y utilizar el certificado emitido para los fines con que ha sido solicitado; custodiando de manera adecuada dicho certificado, ya que este corresponde a su identidad en el mundo digital, por ende al igual que una Cédula de Identidad, el certificado emitido debe ser protegido de un uso no apropiado dado una pérdida, robo o hurto, informando de manera oportuna a Acepta en caso de presentarse algún inconveniente de seguridad del mismo.
- Solicitar la revocación del certificado en caso de cumplirse condiciones tales como la pérdida del certificado o su dispositivo, la pérdida de la clave de acceso, la cesación del cargo en caso de ser certificados que se han asociado a un cargo específico, a solicitud del titular del certificado, ante la no re-emisión del certificado o ante la necesidad de revocación de dicho certificado por parte de Acepta.
- No revelar la clave privada ni el código de activación del certificado, la que es de exclusiva responsabilidad del titular.
- Verificar y asegurar que la información contenida en el certificado es fidedigna e informar 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.
- Cualquiera otra obligación que derive de la Ley, el Reglamento, este documento o del certificado digital.

2.1.5 Obligaciones los Usuarios

Los usuarios de los certificados de firma digital emitidos por Acepta se obligan a aceptar las siguientes condiciones:

- Comprobar en Acepta que el certificado en el que se pretende confiar se encuentra vigente (no ha sido revocado o suspendido o terminada su vigencia).
- Conocer y aceptar el propósito y alcance del certificado de firma digital en que se pretende confiar.

2.1.6 Confianza en las Firmas y certificados

Las partes que confíen en las firmas emitidas por Acepta deberán considerar:

- Que la operación que se pretende avalar con la firma, está en el ámbito de esta última, no sólo en el uso de la misma, sino en lo que determinan las normas legales y reglamentarias asociadas a la PSC y los distintos tipos de certificados emitidos.
- Que la parte que desea confiar ha tomado los resguardos de verificar la autenticidad de la firma en base a la llave pública de Acepta
- Que la parte que desea confiar ha asegurado la validación de caducidad o revocación de la firma en cuestión en base a los servicios provisto por Acepta.
- Que las partes que confían en los certificados han de:
    - Acotar la fiabilidad de los certificados emitidos, a los usos que se han definido para los mismos, en conformidad con lo definido en las extensiones de los certificados y la Política de Certificación pertinente.

- Verificar la validez de los certificados en el momento de realizar o verificar cualquier operación basada en los mismos.
- Asumir su responsabilidad en la correcta verificación de las firmas digitales.
- Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados en que confía.
- Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

2.1.7 Obligaciones de los Repositorios

El repositorio público de Acepta permite realizar distintas operaciones dependiendo del tipo de certificado con el que se esté trabajando. En este repositorio se llevará un registro actualizado de los certificados vigentes y revocados, estando dichas alternativas explicadas en el documento de políticas de cada tipo de certificado. En el caso de los certificados de firma digital, se contará con el acceso público a las prácticas y políticas del PSC, asociado a este tipo de certificado, así como del estado de un certificado en particular, ya sea por medio de una consulta al servicio en línea OCSP o a través de la lista de revocación publicada por Acepta en su sitio web.

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 digital ocasione y, en ningún caso será responsable del uso incorrecto, indebido o fraudulento de los certificados de firma 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 digital ocasione, debiendo demostrar que actuó con la debida diligencia.

Se deja expresa constancia que, atendida la complejidad de los sistemas informáticos y el riesgo tecnológico que los mismos conllevan, no es posible garantizar que los sistemas operen libres de errores o inconsistencias, no obstante el cuidado y la diligencia empleada por Acepta. Por lo anterior, no otorga garantía alguna en relación al posible compromiso en el futuro del sistema de claves asimétricas o cualquier otro riesgo no predecible de naturaleza similar. En todo caso, a fin propender a mitigar esta clase de riegos, Acepta aplicará los procedimientos previstos en sus planes de contingencia.

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 digital.

2.2.1 Responsabilidad Pecuniaria

Las responsabilidades que afectan la operación de Acepta se encuentran establecidas y limitadas a lo definido en DS 052-2008 para el caso de Perú.

En todo caso, la responsabilidad de Acepta cualquiera sea la naturaleza de la acción o reclamo y salvo que medie dolo o culpa grave atribuible a ésta, quedará limitada como máximo al monto definido en el DS 052-2008.

La actividad de certificación de firma digital se encuentra limitadas al ciclo de vida del certificado, esto es:

1. Solicitud del solicitante. Proveer todas las condiciones necesarias para que el solicitante de un certificado de firma digital pueda requerir y proporcionar toda la información necesaria para la emisión del mismo.

2. Registro del solicitante. Una vez que el prestador de servicios de certificación recibe la solicitud debe proceder a la aprobación de la misma, y para ello deberá comprobar los antecedentes que le han sido declarados, debiendo comprobar en la forma señalada en esta CPS y, especialmente la identidad del solicitante y que los datos de creación de firma son entregados realmente a quien solicitó el certificado de firma.

3. Firma y emisión del certificado. Una vez que se ha efectuado el registro del solicitante y se ha verificado la exactitud de los datos proporcionados, el prestador de servicios de certificación procede a emitir el certificado de firma digital, firmado por medio de la firma digital de la cual es titular.

4. Publicación y archivo. Una vez que el certificado de firma ha sido emitido y firmado por el prestador de servicios de certificación, hacerlo constar en el registro de acceso público.

5. Revocación y suspensión. Hacer cesar la vigencia del certificado, de manera temporal o definitiva, según sea el caso en la forma descrita en esta CPS.

2.2.2 Fuerza Mayor

Acepta no será responsable por daños, pérdidas o perjuicios que provengan de incumplimientos en el desarrollo de la actividad de certificación de firma digital y que sean atribuibles a circunstancias constitutivas de caso fortuito o fuerza mayor.

Las obligaciones de Acepta afectadas por el caso fortuito o la fuerza mayor se suspenderán por el período de tiempo que dure el hecho que lo motivó.

Para los efectos de estas CPS, se entenderá por caso fortuito o fuerza mayor, lo que incluye guerras, desastres naturales, paros, huelgas o suspensión de laborales del personal de Acepta o de sus contratistas o subcontratistas, sin que esta enumeración sea taxativa.

2.2.3 Responsabilidad de la EC y ER

Aplica el régimen de responsabilidad establecido en 2.2, no siendo pertinente diferenciar entre la responsabilidad de la ER y la EC en virtud de la Ley 27269 (Perú).

2.3 Ley Aplicable y Resolución de Conflictos

2.3.1 Ley Aplicable

Estas CPS y las Prácticas de Certificación específicas para cada tipo de certificado se regirán e interpretarán de conformidad con la ley peruana.

2.3.2 Resolución de Conflictos.

Cualquier diferencia, dificultad, problema o controversia que pueda surgir entre Acepta y los titulares o signatarios que suscriban él (los) respectivo(s) contrato(s) de certificación o con los terceros interesados que adhieran a las CPS de Acepta con motivo de la validez, eficacia, interpretación, nulidad, cumplimiento o incumplimiento de estas CPS o de la actividad de certificación de firma digital será resuelta definitivamente por un árbitro mixto, quien tramitará como árbitro arbitrador pero que fallará conforme a derecho. El fallo del árbitro será en única y definitiva instancia, sin que en contra de sus resoluciones y fallo, ya sean de substanciación o de medidas precautorias o bien el fallo definitivo, proceda ningún recurso. El árbitro estará solamente obligado a constituir legalmente el arbitraje, a oír a las Partes en conjunto o separadamente, según él lo decida, a recibir las pruebas que se presenten y a dictar su sentencia oportunamente. Las resoluciones se notificarán por carta certificada dirigidas a las Partes o a sus representantes designados en esta escritura o en el respectivo proceso, a las direcciones que ellos señalen en tales instrumentos, salvo la primera notificación del proceso y la de la sentencia definitiva que deberán notificarse. El árbitro designado podrá actuar cuantas veces fuere requerido, por asuntos diferentes, promovidos por cualquiera de las Partes, y en caso de ausencia o impedimento acreditada a juicio del sustituto, éste podrá intervenir de inmediato, en carácter de subrogante, en el estado en que el asunto se encuentre, sin otro requisito que aceptar el cargo. El respectivo proceso podrá continuarse incluso en una copia autorizada de los autos que cualquiera de las Partes presentare ante el sustituto. La evidencia de haberse ausentado del país el árbitro en ejercicio por más de treinta días sin haber regresado, o de impedimento de otra naturaleza acreditado ante el sustituto por medios idóneos y que dure más de treinta días será considerado como ausencia del árbitro.

El árbitro, deberá ser designado por las partes de común acuerdo y, en caso de no haberlo dentro de 15 días de la solicitud escrita de cualquiera de ellas, será designado por los Juzgados de Primera Instancia, debiendo en tal caso recaer la designación en una persona que sea o haya sido miembro del cuerpo arbitral de Centro de Arbitraje de la Cámara de Comercio de Lima, excluidos los que hubieren prestado sus servicios a cualquier título a alguna de las partes.

2.4 Publicación y Repositorios

Acepta mantiene publicadas en su sitio web (https://sovos.com/es/politicas-y-practicas/) esta Declaración de Prácticas de Certificación (CPS).

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

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

La disponibilidad de los servicios señalados no podrá ser inferior a un 99,5 % al año, excluyendo de este compromiso, los tiempos de mantención programados o casos de fuerza mayor indicados en 2.2.2.

La información de validación del estado de los certificados de firma digital (vigente, revocado o suspendido) se mantiene permanentemente actualizada.

Las listas de revocación de todos los tipos de certificados son actualizadas cada 24 horas, siendo ellas publicadas inmediatamente al momento de ser generada.

El registro de acceso público de certificados funciona bajo las siguientes normas:

a. La información relativa a los certificados de firma digital es publicada, a través de sistemas automatizados, en el mismo momento en que éstos son emitidos.
b. La información relativa a la revocación de los certificados de firma digital es publicada dentro de un plazo que no puede exceder de 6 horas laborales (entre 9:00 y 18:00 horas), contada desde la solicitud de revocación realizada de conformidad con el procedimiento indicado en 4.9.3 de estas CPS.

La información relativa a la suspensión de los certificados de firma digital es publicada, a través de sistemas automatizados, en el mismo momento en que ésta es solicitada de conformidad con el procedimiento indicado en 4.9.6 de estas CPS.

ACEPTA cuenta con una política de control de acceso, definida para proteger contra modificación no autorizada a los objetos de información publicados, incluyendo sus CP, CPS, certificados, estado de los certificados y CRL. Acepta ha documentado su política de control de acceso a través del documento "SG-Q-06 Política de control de acceso", en base a los requisitos del negocio y la seguridad de información requerida; definiendo las condiciones mínimas que deben poseer los sistemas de información, aplicaciones, servicios y servidores que hacen parte del alcance del SGSI, de manera tal de dar el acceso a sólo la información e instalaciones de procesamiento que el rol requiere. Para mayor detalle remítase al documento "SG-M-03 Manual de Seguridad", en su punto "9.1.1 política de control de acceso".

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 manera complementaria a lo dispuesto en las Políticas de Privacidad de Acepta, la empresa protege especialmente la siguiente información:

- Información propia de la operación de Acepta y de sus llaves
  - 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.
  - 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".
- Información propia del titular capturada durante el registro
  - Toda la información de carácter personal proporcionada a Acepta durante el proceso de registro de los titulares de certificados.

2.5.2 Tipos de Información que puede ser entregada

Acepta considera como información de acceso público y, consecuentemente se encuentra disponible al público en https://sovos.com/es/politicas-y-practicas/ o en las oficinas de la empresa:

- La Declaración de Prácticas de Certificación de Acepta.
- Toda aquella información que y no teniendo un estatuto de protección especial establecido en la ley sea por Acepta clasificada como "PÚBLICA".
- La contenida en el registro de acceso público de certificados de firma digital

Y en https://asistencia.acepta.pe/certificado-digital.html se encuentra:

- La lista de certificados revocados (CRL).
- La contenida en los certificados de firma digital.

Pese a la calificación de la información como de acceso público, Acepta se reserva el derecho de imponer medidas y controles de seguridad adecuados y proporcionales con el fin de asegurarla autenticidad e integridad de los documentos, así como de imponer medidas tecnológicas anti copia y de impresión para aquellos que se encuentren soportados electrónicamente.

2.5.3 Información del Certificado

Los certificados de firma 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.

Campo	Descripción	Ejemplo
Versión	Versión del certificado, que deberá ser versión 3	v3
Nº de Serie	Número que identifica unívocamente al certificado dentro de los emitidos por Acepta	0090 0001
Algoritmo de Firma	Algoritmo utilizado por el PSC para firmar el certificado	SHA256 WithRSAEncryption
Nombre del Emisor	Nombre distintivo (DN) del emisor, en el formato del estándar X.500. Deben incluirse los siguientes tipos: CN =Tipo de certificado E = e-mail del Prestador de Servicios de Certificación Número de serie = Número identificador del certificado, se utiliza el RUT de Acepta. C = País	CN = Acepta Autoridad Certificadora Firma digital E = info@acepta.com SN = 96919050-8 C = PE
Periodo de Validez	Fecha de inicio y termino en que es válido el certificado. Para PSC = 10 años, Para titulares = 1 a 3 años, Codificado en formato YYMMDDHHMMSSZ	Fecha inicio = 040914140522Z Fecha termino = 050914140522Z
Nombre del titular	Nombre distintivo (DN) del titular del certificado, en el formato del estándar X.500. Deben incluirse los siguientes tipos: CN = Nombre distintivo del titular T = Profesión E = dirección de correo del titular Número de serie = Número identificador del certificado. Se utiliza el RUT del titular del certificado. C = País	CN = Nombre Apellido1 Apellido2 T = Profesión E = persona@sitio.com SN = 99999999-9 C = PE

Clave pública	Clave pública del titular del certificado	3081 8902 8181 009D ECC1 62F4 FE2D 73DD BE6D 53C3 E578 7F98 38AE ED42 B03D A804 F4D5 CA86 9563 2757 D556 7A4F 0C94 DBBA 8F4E 80B0 C334 6B01 B85D 1872 635F 40C3 F294 24E9 FD92 C97A D3B4 798E 680C 7F92 5889 4786 41DC 1AB0 80D4 CCDE 1280 9334 90F1 A1BE 9E96 72AF AA28 3BEA 2DCC 13BC 685C 7782 E869 A7C4 98B6 9094 43FF 574F 3025 5A2C 8880 3F02 0301 0001

2.5.4 Entrega de Información sobre la Revocación o Suspensión del Certificado

La información relativa a la revocación o suspensión de certificados se proporciona vía CRL por parte de Acepta. Esta información también se encuentra disponible en el servidor de validación OCSP de Acepta.

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

Acepta sólo podrá comunicar informaciones calificadas como confidenciales o que contengan datos de carácter personal en aquellos casos en los que así se le requiera por la autoridad pública competente y bajo los procedimientos que se han previstos legalmente por el Poder Judicial de Perú, o de sus tribunales competentes.

Las obligaciones, prohibiciones y responsabilidades de custodia de información sujeta a secreto, reserva o confidencialidad de acuerdo con la ley y estas CPS no regirán si media alguna disposición legal o resolución judicial que obligue a entregar al conocimiento de los Tribunales de Justicia, organismos, instituciones o entidades facultadas por la ley para solicitarlos y que actúen dentro del ámbito de sus atribuciones.

Sin perjuicio de lo cual, Acepta le informará al titular al correo electrónico contenido en el certificado de firma digital la existencia del requerimiento de información, de modo que el titular pueda ejercer sus derechos ante la autoridad competente.

2.5.6 Entrega de Información a Petición del Titular

Acepta entregará la información del titular del certificado que mantiene en sus registros previo ejercicio del derecho de acceso por éste, en la forma establecida en las Políticas de Privacidad de Acepta.

En virtud de lo dispuesto en la Ley 29.733 (Perú), Acepta mantendrá a disposición de cualquier interesado, a través del registro de acceso público de los certificados emitidos, el nombre, DNI, correo electrónico y cualquier otra circunstancia que haya sido objeto de la certificación de la firma digital.

2.6 Derechos de Propiedad Intelectual e Industrial

La prestación de los servicios de certificación de firma digital en ningún caso otorga a los partícipes de la comunidad descritos en 1.3 de estas CPS derecho de propiedad intelectual o industrial alguno. Así, Acepta retiene todos sus derechos de propiedad intelectual e industrial sobre las obras creadas, desarrolladas o modificadas. Ningún derecho de propiedad intelectual o industrial preexistente o que se adquiera o licencie a o por Acepta, se entenderá conferido a los miembros de la comunidad antes citada.

Salvo acuerdo previo, específico y por escrito en contrario celebrado con algún miembro de la comunidad descrita en 1.3 de estas CPS, ninguno de ellos puede publicar o usar logotipos, marcas, marcas registradas, incluso marcas de servicio y patentes, nombres, redacciones, imágenes, símbolos o palabras de Acepta.

Los documentos definidos cómo públicos pueden ser reproducidos respetando las restricciones indicadas en cada documento:

- Políticas de privacidad
- Políticas de certificados
- Prácticas de certificación

2.7 Entidades de certificación afiliadas a la EC

2.7.1 Publicación de Entidades

La EC de Acepta publica la lista de Entidades de certificación a las cuales representan o tienen afiliación, para realizar las actividades de registro, como parte de este mismo documento. En particular la EC de Acepta sólo representa o tiene afiliación, para realizar las actividades de registro, con las ER indicadas en 2.1.2 de sus CPS

2.7.2 Publicación de CP y CPS

La EC de Acepta publica en su página web los documentos RP y RPS vigentes de las Entidades de Registro a las cuales representan o tienen afiliación para realizar las actividades de registro, y que están limitadas a las indicadas en 2.1.2. Para mayor detalle de este punto, remítase a 2.4.

2.7.3 Publicación certificaciones

La EC de Acepta publica en su página web las Resoluciones de Acreditación correspondientes a las Entidades de Certificación a las que se encuentra vinculada, y que están limitadas a las indicadas en 2.1.2. Para mayor detalle de este punto, remítase a 2.4.

2.7.4 Publicación de un documento que acredite representación de la ER

La EC de Acepta declara en su CPS, punto 2.1.2, su vinculación con cada Entidad de Registro o Verificación a la cual representa. Esta misma CPS, además es publicada en la página web de Acepta, tal como se indica en el punto “2.4 Publicación y Repositorios“.

2.7.5 Limitación de responsabilidades

Tal como se indica en 2.1.2 - ACEPTA no representa a ninguna ER distinta a la propia ER de ACEPTA, la cual cuenta con una resolución de operación, cuyo registro es el “064-2018/CFE-INDECOPI” – Dicho esto, tanto la EC como la ER de Acepta declaran en sus CPS y RPS, punto 9.8, las limitaciones de responsabilidad para cubrir los temas de compensación y garantías ofrecidas a los usuarios por casos de suplantación de identidad ocasionados por las operaciones de la Entidad de Registro o Verificación o por las Entidades de Certificación.

3 Identificación y Autenticación

La identificación de los solicitantes y titulares de certificados de firma digital se realiza de acuerdo con las normas y procedimientos contenidas en esta sección de las CPS, con independencia de que la actividad de registro sea realiza directamente por ACEPTA o por un mandatario. En particular, actualmente la función de identificación y autenticación se realizar a través de la ER de ACEPTA, cuyo proceder está definido en la "Declaración de Prácticas de Registro y Verificación" publicadas en la página web de ACEPTA. En particular en estas prácticas, en los puntos 4.2, se describe las solicitudes de certificados de persona natural y jurídica, en su punto 4.6 su re-emisión y en su punto 4.9 la suspensión y revocación.

3.1 Registro Inicial

3.1.1 Registro de Nombres

De conformidad con la Ley 29.733 (Perú), los certificados de firma digital deberán contener como menciones mínimas: El nombre del solicitante, su DNI en Perú; su RUT o RUC, en caso de emitirse el certificado a una persona jurídica y una dirección de correo electrónico.

El nombre corresponderá al nombre completo del solicitante en los términos consignados en su cédula de identidad (nombres y apellidos) del país emisor. Este deberá ser registrado por Acepta, personalmente o a través de mandatario, en los términos definidos en el estándar X.509 y será incluido en el certificado en el campo Common Name (CN). 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.

El DNI en Perú corresponderá a aquel que se encuentre consignado en la cédula de identidad del solicitante del país emisor.

La dirección de correo electrónico será aquel que declare el solicitante al momento de realizarse la comprobación fehaciente de su identidad.

Acepta sólo incorporará en los certificados de firma digital el nombre y el DNI consignado en la cédula de identidad de Perú. Asimismo, incorporará la dirección de correo electrónico que haya sido declarada en la solicitud del certificado y no resolverá disputa alguna relativa a la titularidad de los nombres, números de DNI en Perú, ni dominios de las direcciones de correo electrónico.

3.1.2 Verificación General

Todas las menciones incorporadas en los certificados de firma digital son comprobadas por Acepta, de manera de asegurar que el nombre y DNI en Perú, incluido en éstos se encuentre efectivamente agregado en idénticos términos a los consignados en la cédula de identidad del solicitante del país emisor. Respecto a la dirección de correo electrónico o cualquier otra mención certificable (RUC en caso de persona jurídica), Acepta se asegurará que se adicione en idénticos términos consignados en la solicitud del certificado o en la documentación acreditativa de la respectiva mención.

Respecto a la verificación de identidad, en caso de no estar disponible el servicio de verificación de identidad en línea con RENIEC – Para el caso del registro en Perú – la solicitud no podrá ser ingresada.

Para mayor detalle remítase a capítulos 3 y 4 de este documento.

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

La revocación es el mecanismo a través del cual Acepta deja sin efecto de manera permanente un certificado de firma digital emitido por él, cesando permanentemente los efectos jurídicos del certificado conforme a los usos que le son propios impidiendo el uso legítimo del mismo.

Tendrá lugar cuando Acepta constate alguna de las siguientes circunstancias:

a) 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).
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.

Las solicitudes de revocación son realizadas directamente por la ER de Acepta. Para mayor detalle remítase a “PO02 Declaración de Prácticas de Registro y Verificación ER”, en su punto 4.9, publicado en la página web de Acepta.

3.5 Re-emisión de certificados

Las solicitudes de re-emisión son realizadas directamente por la ER de Acepta. Para mayor detalle remítase a “PO02 Declaración de Prácticas de Registro y Verificación ER”, en su punto 4.6, publicado en la página web de Acepta.

4 Requisitos Operacionales

En este capítulo se describen los requisitos operativos de Acepta, dentro de su prestación de servicios asociados a su PSC, la cual cuenta con los siguientes componentes de sistema:

- **Interfaces:** Acepta, para su emisión de certificados, establece una relación entre la EC la ER y el titular. Esta relación se inicia en la captura de los datos relevantes para la emisión del certificado de firma desde el solicitante, los cuales son comprobados por la Entidad de Registro o Verificación. De ser aprobada esta solicitud, ella se envía a través de un canal seguro a la Entidad de Certificación, de manera que el titular pueda realizar la generación de su par de llaves así como solicitar la generación de su certificado de firma, elementos a ser almacenados y controlados por el titular en su dispositivo criptográfico.

  La comunicación entre la ER y la EC, con posterioridad a la generación de las llaves, sólo ocurre en el registro de las revocaciones y suspensiones, las que son ingresadas por el operador de validación y cuyo efecto es el modificar la CRL y el servicio OCSP.

- **Sistema de directorios para los certificados de firma**: En caso de requerir información asociada a la emisión de certificados, los interesados pueden acceder, a través de un servidor web, al repositorio que contiene los certificados de firma mediante la siguiente URL:
  - https://acpev1.acepta.pe/cgi-bin/consultar_certificados_pev1

- **Procesos de Auditoría:** La auditoría sobre la PSC de Acepta, se realizará al menos una vez al año, para garantizar el funcionamiento y seguridad, de acuerdo a las disposiciones contenidas en la Declaración de Prácticas de Certificación de esta PSC.

- **Bases de datos**: La información relevante incluida en la Base de Datos de la PSC de Acepta, que está asociada al proceso de emisión de certificados incluye:
  - Solicitudes de Certificado y su estado
  - Certificados emitidos y su estado

- **Privacidad:** Acepta mantiene un compromiso respecto al uso de los datos personales, el cual asegura la confidencialidad de los datos personales de los titulares que se faciliten, ya sea mediante el o los formulario(s) establecido(s) para esos efectos o bien los que sean recogidos por el hecho mismo de navegar por la web. Acepta únicamente recolectará aquellos datos que han sido entregados voluntariamente por los usuarios, los que serán usados o tratados únicamente para los fines para los cuales dichos datos fueron proporcionados.

- **Entrenamiento del personal:** Como parte de sus actividades, Acepta realiza cursos de capacitación, los cuales en contenido, duración y fechas estimadas se encuentran descritos en el plan de capacitación anual de su PSC. Este plan incluye labores de reentrenamiento de existir cambios tecnológicos, en las políticas o prácticas de certificación o cualquier documento que se considere relevante de ser informado.

De igual forma, Acepta para estos requisitos, considera un plan de auditoría que verifica que su modelo incluye:

- **Seguridad y dispositivos de seguridad**: El hardware criptográficos utilizado por la PSC de Acepta cuenta con la certificación FIPS 140-2 Nivel 3, para el caso de los certificados digitales.

- **Restricciones de personal**: Acepta filtra adecuadamente los candidatos para el empleo, los contratistas y sus usuarios especialmente en las tareas sensibles y se asegura de que estos sean aptos para los roles que están siendo considerados, de tal forma de disminuir los riesgos de hurto, fraude o mal uso de las instalaciones. Para esto, la Gerencia de Recursos Humanos utiliza procedimientos de requerimiento y comprobación de antecedentes, entregando a cada empleado, al momento del contrato, del Reglamento Interno el cual en uno de sus capítulos indica deberes, obligaciones y sanciones en caso de incumplimiento de las obligaciones del cargo. Todo trabajador de la PSC Acepta, firma un acuerdo de confidencialidad.

- **Procedimientos de recuperación de desastres**: El Plan de Continuidad de Negocio y Gestión de Contingencias de Acepta, tiene por objetivo el proveer un conjunto de políticas y procedimientos, tanto para prevenir como para enfrentar una situación de emergencia en los sistemas de información, así como también, de mantener la continuidad de las operaciones y asegurar la capacidad de responder eficazmente ante un desastre y otras situaciones de emergencia. Este plan contempla un conjunto de escenarios de contingencia, así como una frecuencia de revisión de dicho Plan.

- **Procedimiento de respaldo**: Los respaldos de servidores centrales de la PSC de Acepta, son realizados haciendo uso de medios magnéticos que aseguran la permanencia de la información a lo menos en 5 años. Los respaldos se realizan diariamente, incluyendo un respaldo incremental de los datos administrados por los sistemas de información, así como un respaldo total semanal. Los respaldos mensuales, son mantenidos como históricos.

Finalmente, Acepta considera los siguientes requerimientos de seguridad:

- **Seguridad física de las instalaciones:** Acepta concibe la seguridad física como parte de una política global, que garantiza la protección de los activos del negocio, mitigando el riesgo asociado a las amenazas y vulnerabilidades, de aquellos activos que pueden protegerse físicamente. Estos recursos incluyen el personal, el sitio donde ellos laboran, los datos, equipos y los medios con los cuales los empleados interactúan, en general los activos asociados al mantenimiento y procesamiento de la información. Acepta desarrolla sus operaciones en 3 lugares físicos, siendo ellos su Casa Matriz, Sitio Principal y el Sitio Secundario.

- **Seguridad del Personal:** Acepta, con el objeto de favorecer un uso adecuado de la información y de los sistemas que la apoyan, cuenta con políticas de seguridad de la información vinculadas al recurso humano. Esas políticas, en la medida que se refieran a obligaciones o prohibiciones que afecten al personal de Acepta, deberán encontrarse alineadas, entre otras, con las normas

laborales vigentes, en especial, con los contratos de trabajo y el reglamento interno de orden, higiene y seguridad.

- **Seguridad del módulo criptográfico**: 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.

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 los siguientes puntos, se procede a describir y detallar el proceso antes mencionado. Las especificaciones contenidas en estos puntos lo son sin perjuicio de las estipulaciones previstas en cada una de las distintas Políticas de Certificación para los distintos tipos de certificados emitidos por Acepta.

4.2 Solicitud de Certificado

Las solicitudes de certificados son realizadas directamente por la ER de Acepta. Para mayor detalle remítase a "PO02 Declaración de Prácticas de Registro y Verificación ER", en su punto 4.2, publicado en la página web de Acepta.

Para solicitar un certificado de firma digital el solicitante debe comparecer personalmente o ingresar su solicitud de manera remota ante la Entidad de Registro o Verificación de Acepta.

En caso de ser una solicitud presencial, deberá además completar el formulario de solicitud de acuerdo a:

- Para Personas Naturales o Jurídicas se presentará la cédula de identidad vigente del país emisor, a los efectos de que Acepta compruebe:
  a. El DNI en Perú
  b. Nombres y apellidos. Se hace presente que en el registro y por razones de compatibilidad con el estándar X.509v3, las letras acentuadas son reemplazadas por letras sin acento y las "ñ" son reemplazadas por "n".
- Cuando el registro presencial es de una persona jurídica (Sólo Perú) se verificará adicionalmente:
  - Razón social
  - Número de RUC
  - Dirección oficial de correo electrónico de la persona jurídica
- Indicar una dirección de correo electrónico.

El solicitante también podrá solicitar un certificado de firma digital de forma remota. En caso de que el solicitante realice su solicitud de manera remota (opción de solicitud válida en Perú), se solicitará que el solicitante ingrese la siguiente información en el formulario de solicitud disponible en el sitio web de ACEPTA:

- Para personas naturales se solicitarán los siguientes documentos:
  - Nombres y apellidos
  - Dirección
  - DNI
  - Teléfono
  - Dirección correo electrónico
  - Foto anverso y reverso DNI
  - Verificación biométrica facial a través de servicios de RENIEC (realizada en línea en el sitio de ACEPTA)

- Para personas jurídicas se solicitarán los siguientes documentos:
  - Nombres y apellidos
  - Dirección
  - DNI
  - Teléfono
  - Dirección correo electrónico
  - Datos comerciales:
  - RUC
  - Razón social
  - Cargo del titular
  - Dirección comercial
  - Correo electrónico comercial
  - Foto anverso y reverso DNI
  - Ficha RUC desde SUNAT
  - Vigencia de Poderes
  - Verificación biométrica facial a través de servicios de RENIEC (realizada en línea en el sitio de ACEPTA)

Para un mayor detalle de este proceso, remítase a “PO02 Declaración de Prácticas de Registro y Verificación ER”, en su punto 4.2, publicado en la página web de Acepta.

En caso que el solicitante desea que el certificado cuente con una mención especial, de las que son susceptibles de certificación, deberá presentar la documentación acreditativa de dicha circunstancia (Régimen de poderes para persona jurídica).

Si el registro presencial es hecho por un operador de registro de Acepta, se almacena la siguiente documentación:

- Imagen escaneada de la cédula de identidad por ambos lados.
- Foto del solicitante.
- Contrato de suscripción, con firma manuscrita e impresión dactilar.

El tiempo comprometido para la solicitud será de acuerdo a lo declarado en el indicador específico contenido en el documento CA-M-03.

4.2.1 Verificación General

Las menciones exigidas por la Ley 29.733 (Perú), para los certificados de firma digital deben ser comprobados fehacientemente por 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 titular del certificado. Para el caso de persona jurídica se solicitará el RUC, razón social y documentación que soporte dicha declaración.

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

El tiempo comprometido para la validación será de acuerdo a lo declarado en el indicador específico contenido en el documento “CA-M-03 Indicadores de Calidad”.

4.2.2 Labores de EC y ER

A la Entidad de Registro o Verificación propia o designada por Acepta para esta labor, le corresponde la comprobación de la identidad del solicitante, la verificación de la documentación por él presentada y la constatación de que el solicitante ha firmado el contrato de suscripción. Este contrato incluye tanto las obligaciones de la ER, EC como las del titular, las cuales están dadas por sus respectivas prácticas y políticas de certificación. Para mayor detalle de este contrato remítase a “PO02 Declaración de Prácticas de Registro y Verificación ER”, en sus puntos “4.2.1.8 Contrato del titular”, “4.2.2.8 Contrato del titular” y “4.2.2.16 Conformidad del titular”, publicado en la página web de Acepta. Una vez completa la solicitud, la Entidad de Registro o Verificación remitirá esta solicitud al operador de validación de Acepta.

Este proceso de validación consiste en la centralización de las solicitudes con la información proporcionada por el titular de una firma digital, en el proceso de registro presencial de la identidad. Para cumplir esta función, el operador de validación, ubicará el registro a validar y sólo si los datos se encuentran correctos, al compararlo con la imagen del documento de identidad presentado, procederá a aceptar dicha solicitud. En caso contrario, o exista alguna inconsistencia en la solicitud, ella puede quedar en un estado pendiente o ser rechazada definitivamente. Así, la validación aplicada se resume en:

1. Cuando el registro presencial fue hecho por un operador de registro:
    - Verifica que la información del nombre y DNI en Perú asociados a la solicitud correspondan con las copias electrónicas de la Cédula Nacional de Identidad.
    - Verifica que el nombre, DNI en Perú, y dirección de e-mail de la solicitud correspondan a los datos estipulados en la copia electrónica del contrato del titular.
    - Verifica que la copia electrónica del contrato de suscripción esté debidamente firmada y con impresión dactilar, y que dicha firma corresponda a la de la Cédula Nacional de Identidad.
2. Cuando el registro presencial es de una persona jurídica (Sólo Perú) se verificará adicionalmente:
    - Razón social
    - Número de RUC
    - Dirección oficial de correo electrónico de la persona jurídica

El objetivo de esta segunda validación es contar con un quórum de dos operadores distintos en la aprobación de una solicitud.

Una vez aprobada la solicitud, se procederá a enviar un mensaje electrónico al titular, a fin de que proceda a emitir su certificado de firma, a través de la EC de Acepta.

4.3 Emisión de Certificados

Acepta sólo emite certificados de firma digital cuando ha sido comprobada fehacientemente la identidad del solicitante en la forma señalada en esta Declaración de Prácticas de Certificación.

Para mayor detalle remítase a “PO02 Declaración de Prácticas de Registro y Verificación ER”, que en sus puntos 4.2.1.4, 4.2.2.6 y 4.2.2.13, detallan la verificación de la solicitud, envío de ella a la EC de Acepta, la notificación al titular, la recepción de la generación de certificado vía la solicitud PKCS#10 y su validación con respecto a los datos almacenado en el repositorio, todo esto publicado en las prácticas de registro y verificación, en la página web de Acepta.

4.4 Aceptación de Certificados

Los procedimientos mediante los cuales el titular de cada tipo de certificado acepta el certificado emitido, están indicados en las políticas de cada tipo de certificado.

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 titular de la Política de Certificación asociada.

4.5 Uso del par de claves y del certificado

El titular sólo puede utilizar los datos de creación de firma y el certificado de firma digital para los usos autorizados en este instrumento y de acuerdo con lo establecido en los campos "Key Usage" y "Extended Key Usage" del certificado.

Tras la expiración o revocación del certificado, el titular debe cesar en el uso de los datos de creación de firma.

Todo uso del certificado fuera del ámbito o uso autorizado indicado en éste, es de exclusiva responsabilidad del titular y representan usos ilegítimos.

4.6 Re-emisión de certificados.

Acepta permite solicitudes de re-emisión de certificados, clasificándose ellas en:

a. **Rutinarias**: Durante el período de vigencia, el titular podrá siempre solicitar otro certificado, sin necesidad de repetir el registro presencial. El titular podrá enviar un e-mail firmado electrónicamente solicitando un nuevo certificado o conectarse a una página Web usando su Password de activación, lo que asegura la identidad puesto que ésta fue comprobada cuando se realizó el primer registro presencial

   En ambos casos, el titular recibirá un e-mail de Acepta comunicándole un nuevo número de solicitud. Con este número de solicitud y su Password de activación el Titular podrá crear un nuevo certificado.

b. **Producto de una revocación:** La política de identificación y autenticación para la re-emisión de un certificado después de una revocación y sin compromiso de la clave será la misma que para el registro inicial, o bien se empleará algún método electrónico que garantice de manera fiable e inequívoca la identidad del solicitante y la autenticidad de la solicitud.

Para mayor detalle, remítase a "PO02 Declaración de Prácticas de Registro y Verificación ER", que en su punto 4.6, detalla la re-emisión de certificados.

4.7 Renovación de claves

La renovación de claves implica necesariamente la emisión de un nuevo certificado de firma digital. Las claves no son recuperables. Para mayor detalle remítase a punto 3.5.

4.8 Modificación de certificados.

No aplica.

4.9 Suspensión y Revocación de Certificado

Las alternativas disponibles para suspender o revocar cada tipo de certificado están disponibles en las políticas de certificación correspondientes. Para mayor detalle remítase a "PO02 Declaración de Prácticas de Registro y Verificación ER", en su punto "4.9 Suspensión y Revocación de Certificado".

4.9.1 Circunstancias de Revocación

Aplica lo dispuesto en 3.4.

4.9.2 Solicitud de Revocación

Aplica lo dispuesto en 3.4.

4.9.3 Procedimiento de Revocación

La revocación se realiza en forma presencial en oficinas de Acepta, entregando los antecedentes que comprueben la identidad del titular, mencionando los motivos de la revocación.

En el caso de no ser presencial, el cliente debe enviar un correo indicando la solicitud de revocación, señalando los motivos y una copia de cédula de identidad por ambos lados con su firma manuscrita.

4.9.4 Motivos de Suspensión

La suspensión implica invalidar un certificado durante el tiempo que permanece suspendido. La suspensión únicamente se puede efectuar ante:

- Una solicitud de revocación de un certificado en que no ha sido posible verificar de inmediato la identidad del solicitante.
- Cuando Acepta tiene convencimiento que se ha podido comprometer la clave privada asociada al certificado de un usuario.
- Cuando una autoridad judicial lo establezca.
- Una solicitud del propio titular del certificado.

4.9.5 Solicitud de Suspensión

La solicitud de suspensión de un certificado se puede instar tanto por el titular del certificado, por Acepta como EC o, en caso excepcionales, a través de una orden judicial.

4.9.6 Procedimiento de Suspensión

Para solicitar la suspensión de un certificado, el titular o un tercero deberán enviar un e-mail a la casilla admin-suspensiones@acepta.com, indicando el número de serie del certificado que desea suspender. La casilla de e-mail usada para este envío debe coincidir con la casilla del certificado.

Acepta enviará al titular un e-mail de confirmación de lectura cuando se haya recibido la solicitud y un segundo e-mail avisando cuando se haya procesado la solicitud. El plazo transcurrido entre la recepción de la solicitud y su procesamiento no podrá ser superior a 6 horas, considerando lunes a viernes de 9:00 a 18:00 horas.

Para aquellos casos que se encuentren fuera del horario indicado, la PSC de Acepta, a través de su página web provee un formulario que permite suspender temporalmente el certificado, por un plazo máximo de 72 horas, pasado este periodo el certificado quedará automáticamente vigente a menos que se repita el proceso de suspensión temporal, acción que se podrá repetir sólo 1 vez más. De confirmarse por parte del usuario esta solicitud, se procederá a suspender el certificado inmediatamente de recibida esta confirmación.

Las solicitudes de suspensión no tendrán costo para el usuario.

4.9.7 Límite de Suspensión

La suspensión de un certificado es un estado temporal de 72 horas corridas, salvo que la resolución judicial que lo dictamine imponga un plazo superior o inferior, después del cual el certificado puede ser revocado permanentemente o puede recuperar su estado de vigente. El proceso de suspensión podrá realizarse sólo 2 veces consecutivas.

4.9.8 Listado de Certificados Revocados

Acepta publicará una nueva CRL en su repositorio en intervalos de 24 horas, aunque no se hayan producido modificaciones en la misma (cambios de estado de certificados) durante dicho periodo.

4.10 Servicios de comprobación de estado de certificados.

Acepta cuenta con dos servicios para la comprobación de los certificados, el primero es la CRL o lista de revocación, la que se actualiza tal como se indica en 4.9.8; la segunda es el servicio OCSP, el cual entrega el estado actual de un certificado.

4.11 Finalización de la suscripción.

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

Para mayor detalle, remítase a ”PO02 Declaración de Prácticas de Registro y Verificación ER”, que en su punto 4.9, detalla la revocación de certificados.

4.12 Depósito y recuperación de 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 EC en los procesos de identificación, emisión, revocación, auditoría y almacenamiento de sus certificados.

Para mayor detalle de los controles de seguridad física, remítase a “SG-M-03 Manual de Seguridad”, capítulo 11.

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 configuración1+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 se 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 gasFM-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.

5.2.1 Seguridad Física Data Center

Los sistemas de Acepta, como Entidad de Certificación, se encuentran alojados en un Sitio Principal y uno secundario. Ambos sitios cuentan con niveles de protección y solidez de la construcción adecuado y con vigilancia durante las 24 horas al día, los 7 días a la semana.

Ambos sitios cuentan con diversos perímetros de seguridad, diferentes requerimientos de seguridad y autorizaciones. Entre los equipos que protegen los perímetros de seguridad se encuentran sistemas de control de acceso físico, sistemas de video vigilancia y de grabación, de detección de intrusiones entre otros.

Los sitios además cuentan con un sistema central de vigilancia mediante circuito cerrado de televisión, distribuidas en lugares estratégicos del piso, las que permanentemente están grabando las actividades y registrando los accesos de personas a lugares que requieren acceso restringido. El centro de control es monitoreado por guardias de seguridad las 24 horas del día, todos los días de la semana, lo que permite llevar un registro y control total de acceso.

Se ha reforzado el control del ingreso a áreas de alta seguridad, como es el área de servidores, a través de la instalación de puertas reforzadas que permanecen constantemente cerradas y que sólo pueden ser abiertas por personas previamente autorizadas por la Gerencia del CGSI, bajo la estrecha supervisión de Guardias de Seguridad.

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.

5.2.2 Sistema de Energía Eléctrica

El suministro eléctrico para el sitio principal está garantizado con un grupo electrógeno dimensionado para proporcionar energía eléctrica a todas las instalaciones del sitio, ante fallas de los proveedores de energía. Todo el sistema de suministro eléctrico está reforzado por una serie de UPS's instaladas en cascada, tiempo más que suficiente para activar el generador y asegurar la continuidad del servicio.

También se cuenta con tableros eléctricos redundantes de modo de asegurar el funcionamiento antes fallas de la distribución de los equipos.

Respecto a los sitios principal y secundario, sus instalaciones disponen de sistemas de alimentación ininterrumpida con una potencia suficiente para mantener autónomamente la red eléctrica durante los períodos de apagado controlado del sistema y para proteger a los equipos frente a fluctuaciones eléctricas que los pudieran dañar. Ambos sitios cuentan con todos los resguardos necesarios para mantener una continuidad de energía suficiente y su operación por largos periodos de tiempo.

5.2.3 Sistema de Control Ambiental

Ambos sitios cuentan con un suministro continuo de climatización (aire acondicionado, humedad, polvo en suspensión) en modalidad 24x7x365, garantizando el buen funcionamiento de los equipos. Las especificaciones son:

- Temperatura: 21°C+/-3°C.
- Humedad relativa: 45%+/-10%.
- Polvo en suspensión: 75 Microgramos por m3, como máximo.

Para cumplir esta función los sitios cuentan con equipos de climatización precisa que detectan y controlan la humedad relativa del ambiente, lo que permite mantener ambientes óptimos de temperatura y humedad, en las distintas salas. Ambos cuentan además con un sistema redundante de climatización dimensionado para asegurar una temperatura estable y continua a las salas de equipamiento y a las áreas de operación. En caso de fallas del sistema de aire acondicionado, éste cuenta con un sistema de respaldo que garantiza la continuidad del servicio.

5.2.4 Sistema de Extinción y Control de Incendios

Dado los riesgos de incendio a que pueden estar sujetos los sitios, es que tanto el sitio principal como el secundario cuentan con el suministro e instalación de un sistema de protección contra incendios sobre la base de detección temprana que se realiza bajo vía un sistema de aspiración de partículas del ambiente y de extinción automática con FM-200, aprobación UL, e instalado bajo norma NFPA.

5.2.5 Telecomunicaciones

Tomando en cuenta la importancia que tiene la infraestructura de comunicaciones para el negocio de Acepta, es que se ha diseñado en ambos sitios una plataforma robusta, segura y escalable, utilizando como base para ello los servicios WAN, estos servicios provistos por los principales carriers del país, nos aseguran, redes confiables y con tecnología de última generación.

El objetivo principal de este diseño es cumplir con los niveles de servicio comprometidos por Acepta, por lo que se contempla respaldos en todos los puntos críticos. Adicionalmente, cabe destacar que las redes de transporte del carrier están diseñadas para entregar una alta disponibilidad, con una arquitectura redundante interna, lo cual permite garantizar el servicio de conectividad sobre su red.

5.2.6 Seguridad Lógica Data Center

Ambos sitios cuentan los siguientes aspectos de seguridad lógica:

- Múltiple tecnología de firewall
- Sistema de detección de intrusos
- Sistemas de análisis de seguridad activos

5.3 Controles de procedimientos

Los sistemas de información y los servicios de Acepta se operan de forma segura, siguiendo procedimientos preestablecidos. Cabe mencionar que todos los controles de seguridad y procedimientos, están definidos en el "SG-M-03 Manual de Seguridad", el cual en su capítulo 11, define los controles asociados a la seguridad física. Adicionalmente, en el documento "SG-M-02 Manual de Operaciones de Sistema" se describen los procedimientos operativos y de seguridad que realiza la EC. En particular, el documento "SG-M-03 Manual de Seguridad", el cual en su capítulo 11, punto 11.2.5 indica cómo se implementan los controles que impiden el retiro no autorizado de equipos, información, medios de almacenamiento, software y otros activos de la EC.

5.3.1 Papeles de confianza

Los roles definidos para el control y gestión del sistema son:

- Administrador de Sistemas: A cargo de
  - La instalación y configuración de sistemas operativos, de productos de software y del mantenimiento y actualización de los productos y programas instalados. Cuentan con capacidad para configurar y mantener los sistemas, pero sin acceso a los datos.
  - Activar los servicios de CRL, OCSP.
  - Establecer y documentar los procedimientos de monitorización de los sistemas y de los servicios que prestan.
  - Son responsables de la correcta ejecución de la Política de Copias, y en particular, de mantener la información suficiente que permita restaurar eficientemente cualquiera de los sistemas.
  - Debe mantener el inventario de servidores y equipamiento que compone el núcleo de la plataforma de certificación.
- Administrador de Seguridad
  - Debe cumplir y hacer cumplir las políticas de seguridad de Acepta, y debe encargarse de cualquier aspecto relativo a la seguridad de la EC de Acepta, desde seguridad física hasta la seguridad de las aplicaciones, pasando por seguridad de la red. Esta función estará soportada a través de una oficina de seguridad técnica, además del oficial de seguridad.
- Operador de Registro
  - Responsable de realizar el registro presencial ante la solicitud de un certificado de firma digital, preocupándose de la verificación de identidad del solicitante y la tramitación del certificado.

- Operador de Validación
    - Tiene por función validar el correcto ingreso de una solicitud de certificado, validando la identidad ingresada versus la imagen de los documentos que respaldan dicha identidad. También verificará el pago de la solicitud antes de aprobar la misma.
    - Adicionalmente se encarga de gestionar las suspensiones, revocaciones y re-emisiones de certificados.
- Responsable de formación, soporte y comunicación
    - Se encarga del mantenimiento de contenidos de la web de Acepta.
    - Se encarga de definir el plan de formación para usuarios finales, para agentes de Call Center y para personal implicado directamente en la operación y administración de la plataforma de certificación de la EC de Acepta.
    - Debe revisar mensualmente los ficheros de incidencias y respuestas de Call Center, y revisar los registros de los agentes de Call Center.
    - El Responsable de formación, soporte y comunicación contará con la colaboración de las áreas de RRHH, Marketing o Post venta de estimarse necesario.
- Responsable de Seguridad
    - Se asigna esta tarea al Comité de Seguridad de la Información de Acepta, asumiendo la responsabilidad general en cuanto a la actualización e implantación de las políticas y procedimientos de seguridad que han sido aprobadas.
    - Gestionará que los sitios donde se encuentran los sistemas de Acepta, cumplan con gestionar los sistemas de protección perimetral y la correcta gestión de los sistemas de detección de intrusiones (IDS) y de las herramientas asociadas a éstos.
    - Es el responsable de resolver o hacer que se resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, y otras tareas relacionadas.
    - Es responsable de autorizar movimientos de material fuera de las instalaciones de la EC.
    - Debe encargarse de efectuar la selección y determinar la contratación de terceros especialistas que puedan colaborar en la mejora de la seguridad de la EC de Acepta.
- Auditor
    - Encargado de realizar auditorías internas. En definitiva, debe comprobar todos los aspectos recogidos en la política de seguridad, políticas de copias, prácticas de certificación, políticas de certificación, etc. tanto en el núcleo de sistemas de la EC de Acepta y su personal como en los puntos de Registro. Para esta labor se hará uso de Auditores internos como también la contratación de una auditoría externa anual.
- Responsable de Documentación
    - Se encargará de mantener el repositorio de documentación y los archivos de documentación en papel.
    - Controlará que cada área lleve a cabo la actualización de documentos cuando se requiera.
    - Se encargará de mantener actualizado el fichero de índice de documentos y será el único habilitado para almacenar, borrar o modificar documentos en el repositorio de documentación.

5.4 Controles de seguridad del personal

El detalle de los criterios para los controles del personal se encuentra detallado en el documento "SG-M-03 Manual de Seguridad" capítulo 7.

5.4.1 Requerimientos de antecedentes y experiencia

Acepta requiere que todo el personal asociado a la EC cuente con una calificación y experiencia acorde a la prestación de servicios de certificación, de acuerdo a la Ley 29.733 (Perú), sobre documentos electrónicos firma electrónica y certificación de dicha firma.

5.4.2 Comprobación de antecedentes

Mediante CV y entrevistas realizadas al momento de la vinculación.

5.4.3 Requerimientos de formación y reentrenamiento

Como parte de las recomendaciones en que Acepta ha trabajado, se considera para el personal asociado a la EC, cursos de capacitación, los cuales en contenido, duración y fechas estimadas se encuentran descritos en el plan de capacitación anual de Acepta para la EC. Este plan incluirá labores de reentrenamiento de existir cambios tecnológicos, en las políticas o prácticas de certificación o cualquier documento que se considere relevante de ser informado.

5.4.4 Frecuencia de rotación de tareas

No aplica.

5.4.5 Sanciones

Acepta informa y entrega a cada empleado el Reglamento Interno de Orden, Higiene y Seguridad de la empresa, en el cual se establecen las obligaciones de los trabajadores y las sanciones aplicables en caso de incumplimiento de las mismas, atendidas las responsabilidades o funciones de éstos.

5.4.6 Requerimientos de contratación

Todo trabajador de la EC asume obligaciones de confidencialidad, las que están descritas en su contrato de trabajo.

5.4.7 Documentación entregada al personal

El personal de la EC tendrá a su disposición el siguiente material:

- Declaración de Prácticas de Certificación
- Políticas de certificación
- Política de privacidad
- Política de Seguridad de la Información
- Organigrama y funciones del personal

Adicionalmente, se facilitará el acceso a la documentación técnica necesaria para llevar a cabo sus funciones.

5.4.8 Control de cumplimiento

De acuerdo al Plan de seguridad se mide el control de cumplimiento de las actividades programadas de manera anual.

5.4.9 Finalización de contratos

El oficial de seguridad con el apoyo del área de sistemas y RRHH, procederá a:

- Suprimir los privilegios de acceso del individuo a las instalaciones de la organización
- Suprimir los privilegios de acceso del individuo a los Sistemas de Información de la organización
- Supresión de acceso a toda información, a excepción de la considerada PÚBLICA
- Informar al resto de la organización claramente de la marcha de individuo y de su pérdida de privilegios.
- Informar a los proveedores y entidades externas a Acepta la marcha de individuo y de que ya no representa a la EC de Acepta.
- Verificar la devolución del material proporcionado por la Acepta. Por ejemplo:
    - Equipo computacional
    - Llaves mobiliario oficinas
    - Teléfono móvil
    - etc.

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 avanzados se registra:

- Intentos exitosos o fracasados de cambiar los parámetros de seguridad del sistema operativo en los servidores.
- Inicio y detención de la EC.
- 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.

Adicionalmente Acepta mantiene los siguientes registros:

- Como parte del proceso de Registro y Validación, Acepta mantiene en su base de datos de solicitudes:

- Información de contacto de los solicitantes de los servicios de la ER de Acepta, incluyendo a titulares
- Solicitudes de emisión, re-emisión, revocación o suspensión de certificados digitales, realizadas mediante un medio no repudiable por parte del titular de los certificados.
- Resultados y evidencias de cada proceso de validación de identidad de persona jurídica o natural, incluyendo procesos con resultados positivos como procesos fallidos en los que se denegó el servicio a un cliente. Para mayor detalle remítase al documento "AD02 Manual de operaciones de la ER" Contratos del titular.
- Registros o evidencias de las solicitudes de emisión, re-emisión, revocación o suspensión de certificados digitales realizadas por parte de los operadores de registro y validación de la ER de Acepta que se envían a la EC de Acepta, indicando el operador de registro y validación que realizó la transacción.

- Registro de contratación de operadores de registro y de operadores de validación

5.5.2 Frecuencia de procesamiento del log

Acepta implementa una infraestructura y sistema de certificación de tal modo que permita monitorear continuamente las operaciones realizadas; y poder detectar cualquier situación errónea, así como cualquier intento de uso o ingreso no-autorizado al sistema. Dicho monitoreo se realiza continuamente por personal autorizado.

Adicionalmente, se cuenta con una serie de herramientas de prevención y detección de posibles intentos de penetración indebida a los sistemas de certificación y datos o funciones del back-end del sistema. Dichos registros son revisados al menos mensualmente.

5.5.3 Periodo de Retención para el log de auditoría

Todos los registros correspondientes al registro de eventos con el fin de auditoría se mantienen de tal forma que se permita una adecuada consulta y revisión de tales registros por personal autorizado. Por tanto, varios de dichos registros se mantienen on-line, realizándose respaldos increméntales diariamente, así como respaldos completos con una base mensual.

Cada mes se obtiene un respaldo completo el cual es custodiado de manera segura. Para ello, Acepta cuenta con servicios de custodia electrónica de documentos, los cuales se retienen por un período no inferior a 10 años, cuya destrucción se lleva a cabo con la autorización de INDECOPI.

5.5.4 Protección del log de auditoría

Toda la información pertinente a auditorías de seguridad, así como los registros indicados en 5.5.1, se mantiene de manera segura y no es accesible por cualquier persona o proceso computacional, salvo por aquellos estrictamente autorizados. Para mayor detalle, remítase al documento "SG-M-03 Manual de seguridad", en sus puntos "6.1.1 Roles y responsabilidades de la seguridad de la información", "9.1.1 Políticas de control de acceso", "11.1.2 Control de Acceso Físico" y "12.3.1 Respaldo de la información"

5.5.5 Procedimientos de respaldo del log de auditoría

Los respaldos de la información de auditoría se realizan acorde a un detallado programa de respaldos aplicable por igual al resto de los datos generados en las operaciones del PSC. Dicho programa

contempla respaldos incrementales diarios y respaldos completos una vez al mes. Respecto a los procesos de respaldo, ellos pueden ser revisados en los documentos "SG-M-03 Manual de seguridad", en su punto "12.3.1 Respaldo de la información" y el documento "SG-M-02 Manual de Operaciones de Sistemas", en su punto de respaldos.

Cada mes se obtiene un respaldo completo el cual es custodiado de manera segura. Para ello, Acepta cuenta con servicios de custodia electrónica de documentos, los cuales se retienen por un período no inferior a 10 años, cuya destrucción se lleva a cabo con la autorización de INDECOPI.

El acceso a la información y respaldos antes mencionado, se encuentra limitada sólo al personal autorizado, el cual es controlado a través de sus roles, controles de acceso lógico y físico, tal como detalla en el documento "SG-M-03 Manual de seguridad", en sus puntos "6.1.1 Roles y responsabilidades de la seguridad de la información", "9.1.1 Políticas de control de acceso" y "11.1.2 Control de Acceso Físico"

Los registros generados por Acepta, son archivados y conservados de manera íntegra en un lugar seguro, los que poseen los controles ambientales y físicos necesarios que garantizan su duración en el tiempo, incluyendo controles anti-incendios, acceso físico e inundaciones. Para mayor detalle remítase al documento "SG-M-03 Manual de seguridad", en cláusula "11 Seguridad Física y Ambiental"

5.5.6 Evaluaciones de vulnerabilidad

Con el propósito de mantener un ambiente seguro y confiable, Acepta y sus PSC acreditadas tienen un accionar sistemático y pro-activo respecto a la detección y evaluación de posibles vulnerabilidades que puedan atentar contra dicha seguridad.

Para ello, se mantienen aplicaciones específicas de monitoreo permanente de las operaciones del sistema. Además, se efectúa una adecuada capacitación de todo el personal, sobre sus responsabilidades y conductas respecto a la conservación de un ambiente seguro.

5.5.7 Identidad/calificaciones de asesores

ACEPTA declara que el personal que realiza las auditorías o evaluaciones de conformidad, bajo el marco de la "Infraestructura Oficial de Firma Electrónica", lo efectúan de acuerdo a lo declarado por el organismo a cargo de este marco (En la actualidad INDECOPI).

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:

- Registros de auditoría especificados en el punto 5.5 de esta Declaración de Prácticas de Certificación.
- Soportes de backup de los servidores que componen la infraestructura de la EC de Acepta.
- Documentación relativa al ciclo de vida de los certificados, entre la que se encuentra:
  - Contrato de certificación

- Copia de la documentación de identificación aportada por el solicitante del certificado
- Identidad del operador de registro y validación que participaron en la emisión del certificado
- Fecha de solicitud y verificación de identidad del titular

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

5.6.2 Requerimientos para "marca de tiempo" de registros

Todos los registros de auditoría contienen la fecha y hora del servidor de la PSC, sincronizado con la TSA de Acepta, para la ocurrencia del evento pertinente.

5.6.3 Sistema de colección de archivos

Los documentos electrónicos aludidos se mantienen en custodia electrónica cerrada para su conservación segura. Cada archivo estará firmado digitalmente por su emisor.

5.6.4 Procedimientos para obtener y verificar información de archivos

La consulta de los documentos electrónicos dejados en custodia electrónica en Acepta, se hace mediante el uso de certificados digitales debidamente autorizados, para garantizar la confidencialidad de la información y autorización requerida.

La verificación de la autenticidad de los documentos electrónicos está dada por la verificación de la firma digital del emisor.

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.

Los certificados firmados por la entidad comprometida, en el periodo comprendido entre el compromiso de la clave y la revocación del certificado correspondiente, serán a su vez revocados, informando a sus titulares el hecho y el procediendo para emitir nuevos certificados.

Acepta comunicará inmediatamente a la AAC del INDECOPI el motivo del compromiso de la clave de la entidad, así como las acciones realizadas.

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

Acepta para este proceso cuenta con procedimientos tanto para la gestión de incidentes ["PS07 Gestión de Incidentes de seguridad de la información"; y "SG-M-03 (Capítulo 16)"]; como para mantener su continuidad del negocio ["PS03 Plan de continuidad de negocios y recuperación de desastres" y "SG-M-03 (Capítulo 17)"].

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

En caso de sospecha de haber sido alterados uno de estos recursos, de responsabilidad de Acepta, se detendrá el funcionamiento de los servicios de Acepta hasta el restablecimiento de un entorno seguro, con la incorporación de nuevos componentes. De forma paralela se realizará una auditoría para identificar la causa de la alteración y asegurar la no repetición de la misma.

En el caso de verse afectados certificados emitidos, se notificará del hecho a los titulares de los mismos y se procederá a emitir los nuevos certificados.

5.8.2 La clave pública de una entidad se revoca

En el caso de la revocación del certificado de una entidad de Acepta, se generará y publicará la correspondiente lista de revocación y se detendrá el funcionamiento de la entidad, hasta que se proceda a la generación, certificación y puesta en marcha de una nueva entidad con la misma denominación que la eliminada y con un nuevo par de claves.

Las entidades dependientes de la entidad renovada serán informadas del hecho y se solicitará que realicen su re certificación con la nueva instancia de la entidad.

5.8.3 La clave de una entidad se compromete

En el caso de compromiso de la clave de una entidad perteneciente a Acepta, se procederá a su revocación inmediata (como se indica en 5.8.2) y se informará del hecho al resto de entidades dependientes.

Los certificados firmados por entidad comprometida, en el periodo comprendido entre el compromiso de la clave y la revocación del certificado correspondiente, serán a su vez revocados, informando a sus titulares y procediendo a emitir ellos.

El mecanismo que puede ser usado, por todos los titulares y terceros que confían, para identificar los certificados que han sido comprometidos, será por medio de los servicios CRL y OCSP, así como de la notificación que generará Acepta a sus titulares.

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

En caso de desastre natural que afecte a las instalaciones del sito principal de Acepta y sus servicios, se procederá a activar el Plan de Continuidad del Servicio y recuperación de desastres.

5.9 Cese de la actividad del PSC

En el evento que Acepta vaya a descontinuar sus operaciones como prestador de servicios de certificación de firma digital, deberá comunicar tal situación a los titulares de los certificados por ella emitidos en la siguiente forma:

a) Si el cese es voluntario, con una antelación de a lo menos dos meses y señalando al titular que de no existir objeción a la transferencia de los certificados a otro prestador de servicios de certificación, dentro del plazo de 15 días hábiles contados desde la fecha de la comunicación, se entenderá que el usuario ha consentido en la transferencia de los mismos. En este caso, si el prestador es acreditado, se traspasará los certificados, necesariamente, a un certificador acreditado.

b) Si el cese no es voluntario, la cancelación de la acreditación se comunicará inmediatamente a los titulares. En caso que el prestador de servicios de certificación esté en situación de traspasar los certificados a otro prestador acreditado, se informará tal situación en la forma y plazo señalado en la letra a).

Si el titular del certificado se opone a la transferencia, el certificado quedará sin efecto sin más trámite, que deberá estar acreditado si aquel lo fuera, o a una empresa especializada en la custodia de datos

electrónicos, por el tiempo faltante para completar los 6 años desde la emisión de cada certificado. Esta situación deberá verse reflejada en el registro público de prestadores acreditados de servicios de certificación, el que deberá contener el número de la resolución que concede la acreditación, el nombre o razón social del certificador, la dirección social, el nombre de su Representante Legal, el número de su teléfono, su sitio de dominio electrónico y correo electrónico así como la compañía de seguros con que ha contratado la póliza de seguros.

En caso que el cese en la prestación del servicio sea por voluntad del Acepta, deberá solicitar a la Entidad Acreditadora, con al menos un mes de anticipación, la cancelación de su inscripción en el registro público mencionado en párrafo anterior, comunicándole el destino que dará a los datos de los certificados, especificando, en su caso, los que va a transferir y a quién, cuando proceda. El cese de la actividad será registrado como nota de cancelación de la inscripción de la acreditación por la Entidad Acreditadora en el registro público mencionado.

ACEPTA realizará la protección de los registros de auditoría, y transferirá los mismos a la AAC u otra Entidad de Registro o Verificación, por el periodo establecido por la AAC de 10 años luego de generado el registro (5.5.3 Periodo de retención para log de auditoría).

En cualquiera de estos casos, las relaciones entre la PSC y los usuarios seguirán rigiéndose por lo señalado en estas CPS mientras no se ponga en conocimiento de los usuarios un nuevo documento por escrito que venga a sustituir este documento (ver 9.11).

En paralelo a estos pasos, Acepta procederá a la revocación del certificado de su EC.

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 titular 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 titulares, 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

- **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.
    - EC raíz: La máquina donde reside la EC raíz dispone de un dispositivo criptográfico (HSM) para la generación de claves de la EC raíz.
    - EC intermedias: La máquina donde residen las EC intermedias dispone de un dispositivo criptográfico (HSM) para la generación de claves de las distintas EC intermedias.

  Para mayor detalle remítase a los documentos “PS06 Plan de administración de llaves”, “Gestión de llaves criptográficas de la EC” y “Procedimiento de generación de CRL Raíz y mantención de raíces”.

- **Certificados de titulares:** Las claves del titular son generadas por él mismo, siendo él quien selecciona dónde son almacenadas dichas claves, entre las siguientes alternativas
    - **Dispositivo de hardware con software criptográfico (Token) en posesión del titular (Firma Digital)**: El proceso de generación de llaves es realizado por el propio titular, quien determina los datos de generación de firma que empleará. Para esta generación se utilizará el número de solicitud proporcionado por Acepta al titular, vía correo electrónico; además de un pin que es ingresado por el propio titular al momento de realizar el registro. La firma podrá ser instalada en cualquier dispositivo (token) que cumpla el estándar mencionado en el punto 6.2.6 de estas prácticas de certificación, así como también con el largo de llave especificado en el punto 6.2.5 del mismo documento; debiendo este dispositivo ser accesible por el software de instalación del certificado de firma. En cuanto al proceso de firma, este se realiza totalmente en el equipo del titular.
    - **Dispositivo criptográfico (HSM) de Acepta**: El proceso de generación de llaves es realizado por el propio titular, quien determina los datos de generación de firma que empleará. Para esta generación se utilizará el número de solicitud proporcionado por Acepta al titular, vía correo electrónico; además de un pin que es ingresado por el propio titular al momento de realizar el registro. Las claves generadas se almacenan en el dispositivo HSM externo, el cual es custodiado y cumple con el estándar mencionado en el punto 6.2.6 de estas prácticas de certificación, así como también con el largo de llave especificado en el punto 6.2.5 del mismo documento. El certificado queda

almacenado bajo una OCS virtual proporcionada por el hardware criptográfico, para cada uno de los titulares y sólo serán accesibles al titular dueño de la clave.

6.2.2 Entrega de la clave privada a la entidad

No aplica.

6.2.3 Entrega de la clave pública al emisor del certificado

La clave pública es generada por el titular y es entregada a la EC de Acepta mediante el envío de una solicitud de generación de certificado en un formato apropiado (El formato mencionado corresponde al CSR: Certificate Signing Request, formato que sigue la especificación PKCS#10 y que es firmado digitalmente con la clave privada del titular). El certificado solicitado es generado a partir de este requerimiento y firmado digitalmente por la PSC.

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

Las claves públicas de todas las EC pertenecientes a la jerarquía de confianza de Acepta se pueden descargar del sitio web https://asistencia.acepta.pe/certificado-digital.html ("Complementos de instalación del Certificado Digital"), en la que se presenta la Jerarquía completa de certificados, es decir, raíz e intermedias. Particularmente, los certificados intermedios son firmados con la llave privada de la EC raíz a fin de asegurar su autenticidad e integridad.

6.2.5 Tamaño de las claves

Las claves de la EC raíz y las Entidades 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 EC, 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 EC. 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.

6.2.6 Parámetros de generación de la clave pública

Las claves de las Entidades de certificación EC raíz, así como las diferentes EC intermedias en cada una de las dos jerarquías están creadas con el algoritmo RSA

Los parámetros de generación de claves siguen las recomendaciones FIPS 140-2 Nivel 3.

6.2.7 Comprobación de la calidad de los parámetros

El identificador de algoritmo (AlgorithmIdentifier) que emplea Acepta para firmar los certificados es SHA-2 (algoritmo de hash) con RSA (algoritmo de firma) que corresponde al identificador para "Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc." Aquellos certificados firmados con SHA-1 seguirán vigentes hasta su vencimiento o revocación.

Las claves de la EC de Acepta no son utilizadas cuando los algoritmos empleados o el tamaño de las claves han sido vulnerados, procediendo Acepta a generar una nueva jerarquía con los algoritmos válidos.

6.2.8 Hardware/software de generación de claves

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

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

6.2.9. Fines del uso de la clave

Los usos de la clave para cada tipo de certificado emitido por Acepta, vienen definidos por la Política de Certificación que corresponda, siendo el propósito de este par de llaves el identificar al titular y permitirle firmar electrónicamente documentos electrónicos, así como cifrar dichos documentos.

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.

6.3 Protección de la llave privada

Respecto a la protección de las llaves se tiene que:

- **Módulos criptográficos**: El HSM "Hardware Security Module" (Módulo de Seguridad Hardware), es un dispositivo hardware de seguridad criptográfica que genera y protege claves privadas. Los nuevos HSM de Acepta cumplan el criterio FIPS 140-2 Nivel 3 o equivalente.
- **Control multipersona de la llave privada**: Las claves privadas utilizadas por las Entidades de certificación de Acepta y sus jerarquías se encuentran bajo control multipersona, es decir, es necesario un mínimo de 3 personas de un total de 8 para modificar el ambiente criptográfico.
- **Depósito de la llave privada**: La clave privada está cifrada y queda contenida en el repositorio asociado a dispositivo HSM.
- **Copia de respaldo de la llave privada**: Existe un procedimiento de recuperación de claves de los módulos criptográficos HSM de la EC (raíz o intermedias) que se puede aplicar en caso de contingencia. El procedimiento de recuperación de claves de módulos criptográficos corresponde al contexto de procesos certificados que posee el dispositivo HSM.
- **Introducción de la clave privada en el módulo criptográfico**: Las claves privadas se crean en el módulo criptográfico HSM en el momento de la creación de cada una de las entidades de Acepta que hacen uso de dichos módulos.
- **Método de activación de la clave privada**: Las claves privadas de las Entidades de certificación de Acepta y que componen su jerarquías, se activan mediante la inicialización del software de EC y la activación del hardware criptográfico que contiene las claves.
- **Método de desactivación de la clave privada**: Un Administrador puede proceder a la desactivación de la clave privada de las EC de Acepta, mediante la detención del software de la EC.
- **Método de destrucción de la clave privada**: Existe un procedimiento de destrucción de claves de la EC. Los dispositivos criptográficos que contienen las claves privadas creadas por los titulares, poseen un procedimiento de destrucción de claves.

6.4 Otros aspectos de gestión del par de claves

- **Archivo de la clave pública**: Los certificados generados por la EC, son almacenados durante el periodo de tiempo mínimo de 10 años.
- **Periodos de utilización de las claves pública y privada**: Corresponde al periodo de vigencia de cada uno de los certificados. Posterior a este periodo dichas claves no son utilizadas. En el caso particular de claves de titulares, una clave de 2048 bit tiene un periodo de uso que es el menor valor entre el máximo de tres (3) años o el que defina su ciclo de vida.

6.5 Datos de activación

Los datos de activación de las Entidades 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.

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 y Plan de Seguridad de Acepta. Para mayor detalle remítase a los documentos “SG-M-02 Manual de Operaciones de Sistemas” y “SG-M-03 Manual de Seguridad”, que describen:

- La continuidad y seguridad de las operaciones a ser monitoreadas de acuerdo a “SG-M-03 Manual de Seguridad” capítulo 17.
- Como los usos no autorizados de los sistemas de Acepta son detectados y registrados, existiendo medios de monitoreo y alarmas, implementados para detectar, registrar y actuar oportunamente sobre accesos no autorizados o intentos irregulares de acceso a recursos, de acuerdo con “SG-M-03 Manual de Seguridad” capítulo 9.
- Los registros de auditoría y los reportes de eventos sobre errores y advertencias en el funcionamiento de los sistemas de la EC de Acepta que son monitoreados como se indica en 5.5 y “SG-M-03 Manual de Seguridad” capítulo 12.

6.7 Controles de Seguridad Técnica

Acepta, en lo referente al dominio de la EC, hace uso de procedimientos de pruebas y paso a producción de cualquier cambio que afecta al software de la EC. Estos cambios están regulados por un procedimiento de control de cambio administrado por el área de desarrollo de Acepta. Asimismo, la aplicación del procedimiento para el almacenamiento seguro del hardware criptográfico y los materiales de activación se materializa después de la ceremonia de generación de claves. Para mayor detalle remítase a “SG-M-03 Manual de Seguridad” capítulo 14, en lo que respecta a desarrollo de software y el capítulo 12 respecto al control de cambio.

6.8 Controles de seguridad de red

Acepta limita el acceso de sus redes al personal debidamente autorizado. En particular:

- Se implementan controles para proteger la red interna de acceso por terceras partes
- Los datos sensibles son cifrados al momento ser intercambiado a través de redes no seguras. Se garantiza que los componentes locales de red están ubicados en entornos seguros

Para mayor detalle, remítase al documento “SG-M-03 Manual de Seguridad de la Información (Cláusula 13)” y el documento “ET01 Evaluación de la plataforma tecnológica”, en su capítulo 8.

6.9 Controles de seguridad de los módulos criptográficos

Acepta utiliza módulos criptográficos con hardware y software disponibles comercialmente, los cuales son desarrollados por terceros.

Los módulos criptográficos utilizados cuentan con un nivel de certificación de seguridad suficiente para la funcionalidad y seguridad que se exige.

6.10 Timestamping

De acuerdo a lo definido en las prácticas de certificación de Sello de tiempo de ACEPTA.

7 Certificado, CRL y OCSP

7.1 Certificado

Los certificados de firma digital o electrónica emitidos por la EC de Acepta están en conformidad con el formato X.509v3 definido en ITU-T X.509v3 y las recomendaciones de la IETF RFC-3280, es decir la estructura del certificado emitido por Acepta cumple con los siguientes contenidos:

- **Version**: Versión del certificado
- **Serial Number**: Número de serie que identifica de manera única al certificado emitido por Acepta
- **Algorithm ID:** Algoritmo de firma del certificado (SHA-2 con Encriptación RSA)
- **Issuer**: Nombre del emisor en formato X.500
- **Validity**: Periodo en el cual el certificado es válido
- **NotBefore**: Fecha de inicio de validez
- **NotAfter**: Fecha de término de la validez
- **Subject**: Nombre distintivo del titular del certificado en formato X.500
- **SubjectPublicKeyInfo**: Este campo es usado para almacenar la llave pública e identificar el algoritmo con el cual la clave es usada
  - **Public Key Algorithm**
  - **Subject Public Key**
- **Extensions (optional):** Extensiones del certificado (Por ejemplo ubicación de las políticas de certificación, lista de revocación o servicio OCSP)
- **CertificateSignatureAlgorith**: Algoritmo de firma del certificado
- **CertificateSignature**: Firma del certificado

7.1.1. Versión

Los perfiles de los certificados digitales emitidos por ACEPTA cumplen con el estándar x.509 versión 3.

7.1.2. Extensiones del certificado digital

Adicional a la información básica y obligatoria que contiene un certificado de firma digital o electrónica, existen extensiones definidas por el estándar X.509 V3, el que permite incorporar atributos adicionales al certificado para la administración de las relaciones entre las distintas EC. Este mismo estándar permite incorporar extensiones privadas de ámbito de uso restringido a la comunidad que las ha solicitado.

La siguiente tabla muestra los campos que constituyen la extensión de un certificado emitido por Acepta para certificados de Firma Digital o electrónica. En esta tabla se entrega el nombre de campo, su contenido y un valor para un certificado de ejemplo específico.

A continuación se detallan las extensiones incluidas en los certificados de firma electrónica digital o electrónica.

Nombre	Descripción	OID	Valor
KeyUsage	Esta extensión define el propósito para el cual deben ser usadas las claves correspondientes al certificado. El certificado debe ser utilizado sólo para los propósitos definidos por esta extensión.	2.5.29.15	Digital Signature, Non-Repudiation (c0)
ExtendedKeyUsage	Esta extensión define una serie de propósitos respecto al uso del certificado, adicionalmente a las definidas en KeyUsage. El certificado debe ser utilizado sólo para los propósitos definidos por esta extensión.	2.5.29.37	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
AuthorityKeyIdentifier	Medio para identificar la llave pública de Acepta El campo KeyId es idéntico al valor de la extensión SubjectKeyIdentifier		KeyID=e5ea517d8f5e00f4de965ee4aae0325408b49d6f
SubjectKeyIdentifier	Identificador único de la llave pública de el PSC, conteniendo el hash de 160bit de la llave pública.		b547d4e868a48e2a8c537b1660f04aca96a82732
CertificatePolicy	Ver sección 7.1.6		[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.6891.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://acpev1.acepta.pe/CPS-PE-V1-Aceptape [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Reference: Organization=ACEPTA PERU S.A.C. Notice Number=3 Notice Text=
CrlDistributionPoint	En este campo se establece la localización del CRL correspondiente para consultar sobre revocaciones. Contiene la sgte. estructura: DistribuitonPoint: Un URI para identificar el CRL	2.5.29.31	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=https://acpev1.acepta.pe/pev1/crl/Digital-V1.crl
AuthorityInfoAccess	En esta extensión se establece información de acceso a servicios de información del Prestador de Servicios de Certificación. En este momento, establece el acceso para consultas de revocaciones on-line. Contiene la siguiente estructura: AccessMethod: OID identificando el método de acceso. En este caso, corresponde al protocolo OCSP, con OID=13.6.1.48.1 AccessLocation: Ubicación del servicio de consulta OCSP	13.6.1.5.5.7.1.1	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=https://acpev1.acepta.pe/pev1/ocsp/Digital-V1

7.1.3. Identificadores de objeto de algoritmos

Los certificados digitales emitidos por ACEPTA usan los algoritmos de firma sha256RSA.

7.1.4. Formas de nombres

Se respeta la forma de nombres de acuerdo a la familia de estándares ISO/IEC 9594 (recomendación X.500) para DistinguishedName.

Los certificados digitales emitidos por ACEPTA, además de lo establecido en el artículo 7º de la Ley de Firmas y Certificados Digitales – Ley 27269, incluyen lo siguiente:

- Razón social o nombre de la entidad
- Número de RUC de la entidad

7.1.5. Restricciones de nombre

Los certificados digitales para PSC emitidos por la ACEPTA indican un nombre que permite el reconocimiento de la persona jurídica asociada y se cumple con lo establecido en el estándar RFC 5280.

7.1.6. Identificador de objeto de la política de certificados digitales

ACEPTA consigna su identificador de objeto como lo definido en 1.2.

7.1.7. Uso de la extensión "Restricciones de Políticas" (PolicyConstraints)

No aplica.

7.1.8. Semántica y sintaxis de los calificadores de política (PolicyQualifiers)

No aplica.

7.1.9. Semántica de procesamiento para la extensión "Políticas de Certificado Digital" (CertificatePolicy)

No aplica.

7.2 CRL

Las listas de revocación de los certificados de firma digital emitidos por Acepta están en conformidad con el formato CRLv2 definido en ITU-T X.509v3 y las recomendaciones de la IETF RFC-5280.

Nombre	*Descripción*	*Valor*
Versión	Corresponde a versión 2	V2
Issuer	Descripción de el Prestador de Servicios de Certificación emisora de la CRL	SERIALNUMBER = 20562999711 E = info@acepta.com CN = Acepta Peru Autoridad Certificadora Digital - V1 O = ACEPTA PERU S.A.C. C = PE
Effective Date	Fecha de publicación de la CRL	martes, 9 de mayo de 2023 21:54:53
NextUpdate	Fecha de próxima publicación	miércoles, 10 de mayo de 2023 21:54:53

Acepta usa las siguientes extensiones en las listas de revocación de certificados:

Nombre	Descripción
AuthorityKeyIdentifier	Identificador de la clave del Prestador de Servicios de Certificación KeyID=e5ea517d8f5e00f4de965ee4aae0325408b49d6f
CRL Number	Número de secuencia de la CRL, CRL Number=0786

Respecto a la lista de certificados revocados que contiene la CRL, cada uno de estos registros está compuesto por:

Nombre	Descripción
UserCertificate	Número de serie del certificado
RevocationDate	Fecha de revocación del certificado

Esta lista de revocación puede ser recuperada en el sitio seguro de Acepta, a través de la siguiente URL:

- https://acpev1.acepta.pe/pev1/crl/Digital-V1.crl

7.3 OCSP

El servicio web OCSP publicado por Acepta, cumple con el estándar RFC 2560 "*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol*" y actualizado según RFC 6277 "*Online Certificate Status ProtocolAlgorithmAgility*", conteniendo la siguiente estructura:

Request

- Versión del protocolo
- Lista de Identificación de certificados
    - ID certificado
        - Algoritmo Hash
        - Nombre emisor del Hash
        - Clave emisor hash
        - Número de serie
    - Extensión
- Extensiones opcionales que pueden ser procesadas por el servicio OCSP

Response

- Status de Response
- Tipo de Response
- Versión de la respuesta
- Identificador de quien responde
- Fecha de response
- Respuesta para certificado consultado del request
    - Identificador del certificado
        - Algoritmo
        - Nombre de emisor en HASH
        - Llave del emisor en HASH
        - Serie del certificado
    - Estado del certificado
    - Fecha de actualización
    - Extensiones opcionales
- Extensiones opcionales
- Algoritmo de firma
- Firma calculada con Hash de la respuesta

Este servicio se encuentra publicado en:

- https://acpev1.acepta.pe/pev1/ocsp/Digital-V1

8 Cumplimiento auditoría y otras evaluaciones

Acepta declara el cumplimiento de este punto a través del capítulo 5.5 de este documento, además del capítulo 6.11 de la Política General de Seguridad de La información y del documento "SG-M-03 Manual de Seguridad", en su punto "12.7.1 Controles de auditoría de sistemas de información"

8.1. Frecuencia y circunstancias de evaluación

Acepta está sujeta al menos a una auditoría externa e interna anual. En particular, en esta revisión anual, los registros, archivos, procedimientos y controles son revisados como parte de la auditoría de la AAC.

Respecto a las auditorías internas y de tercera parte Acepta las lleva a cabo, como mínimo, una vez al año. Para mayor detalle remítase al documento "SG-M-03 Manual de Seguridad", en su punto "12.7.1 Controles de auditoría de sistemas de información"

8.2. Identidad/Calificaciones de auditores

Respecto a la identidad del Auditor, la EC de Acepta sólo considera para sus procesos de auditoria, relacionadas con los seguimientos de la AAC, a aquellos auditores autorizados por INDECOPI a través de la lista de auditores por ellos aprobados.

Respecto a las credenciales y calificaciones de los auditores a ser contratados para la ejecución de auditorías internas o tercera parte Acepta, no relacionadas con la auditoría anual de la AAC, hace uso del procedimiento "GG-P-01 Auditar gerencias", el cual describe el proceso de auditoría en los pasos mínimos a cubrir; así como del procedimiento "GG-P-05 Procedimiento de control de auditoría de sistemas de información"; en que este último documento, entre otros tópicos cubre la selección del auditor y sus calificaciones.

8.3. Relación del auditor con la entidad auditada

Para aquellas auditorias relacionadas con los seguimientos de la AAC, la ER de Acepta, restringe su selección, de los indicados en 8.2, a aquellos que no hayan tenido ninguna relación comercial con la misma, ni de efectos de auditoría en el mismo alcance de evaluación, en los últimos 2 años.

Respecto los auditores a ser contratados para la ejecución de auditorías internas o tercera, no relacionadas con la auditoría anual de la AAC, la ER de Acepta hace uso del procedimiento "GG-P-01 Auditar gerencias", el cual describe la independencia del equipo auditor respecto a los elementos a auditar, y que es reforzado en el documento "PS01 Política General de Seguridad de la Información", en su punto 6.11.5.

8.4. Elementos cubiertos por la evaluación

Las auditorías externas verifican, como mínimo, los siguientes aspectos considerados como críticos:

Alineación de la CP y CPS Acepta a las Guías de Acreditación de la IOFE.

- Alineación de las medidas efectivas existentes.
- Evaluación y cumplimiento de los niveles de seguridad física.
- Revisión de los procedimientos de contingencia.
- Revisión de los controles de seguridad de la información.

- Revisión de los controles de acceso a la Base de Datos.

8.5. Acciones a ser tomadas frente a deficiencias

Tanto en las auditorías internas como externas, Acepta toma acciones inmediatas frente a las no conformidades, observaciones y oportunidades de mejora encontradas por los auditores.

8.6. Publicación de resultados

Acepta tiene potestad en relación a la publicación de resultados de auditoría.

9 Otros negocios y materias legales

9.1 Tarifas

Las tarifas de los distintos servicios, así como el procedimiento de reembolso, se presentan en la página web de Acepta, en documento “Tarifas y Procedimiento de Reembolso”.

9.1.1. Tarifas para la emisión o re-emisión de certificados

Las tarifas de los distintos servicios se presentan en la página web de Acepta.

9.1.2. Tarifas de acceso a certificados

No aplica ninguna tasa por el empleo de los certificados digitales, ni por el acceso a los repositorios públicos donde se encuentran la CRL y los certificados digitales emitidos.

9.1.3. Tarifas para información sobre cancelación o estado

No aplica ninguna tasa por el empleo de los certificados digitales, ni por el acceso a los repositorios públicos donde se encuentran la CRL y los certificados digitales emitidos.

9.1.4. Tarifas para otros servicios

Las tarifas de los distintos servicios se presentan en la página web de Acepta.

9.1.5. Políticas de reembolso

Es política de Acepta, sólo reembolsar al solicitante la tasa respectiva por la emisión del certificado digital, en caso su solicitud no hubiese sido atendida por responsabilidad atribuible a ACEPTA, ello acorde a lo definido en la Ley del consumidor N° 29571. Mayor detalle se presenta en el sitio web de ACEPTA.

9.2 Responsabilidad Financiera

Acepta cuenta con un seguro de responsabilidad civil y un respaldo económico descrito en sus estados financieros.

9.3 Confidencialidad de información del negocio

De acuerdo a plan de privacidad y política de privacidad de Acepta publicada en su página web.

9.4 Privacidad

De acuerdo a plan de privacidad y política de privacidad de Acepta publicada en su página web.

9.5 Propiedad Intelectual

Remítase a 2.6 de este documento.

9.6 Representación y Garantía

Para Acepta, remítase a 2.2. Respecto al resto de la comunidad de la IOFE remítase a 2.1 de este documento.

9.7 Exención de Garantía

De acuerdo al alcance de la póliza vigente.

9.8 Limitaciones de responsabilidad

Remítase a 2.2 de este documento.

9.9 Indemnizaciones

Acepta dispondrá de una garantía con cobertura suficiente de responsabilidad civil, a través del seguro contratado.

9.10 Duración y terminación

9.10.1 Comunicación a sus clientes y comunicación a la AAC

El presente documento entra en vigencia desde el momento en que es aprobado por la AAC de la IOFE, y su periodo de vigencia es de 05 años al ser este el plazo de las acreditaciones otorgadas por la AAC de acuerdo a la legislación vigente. Esto sin perjuicio que en el trascurso de este tiempo este documento pueda ser modificado por decisión propia de Acepta o determinación de la AAC. Respecto a la terminación se regirá de acuerdo a 5.9 de este documento. En caso de modificaciones a estas CPS, ello será registrado tal como se indica en 11.

9.10.2 Protección de los registros de auditoría.

Remítase a puntos Remítase a puntos "5.5.4 Protección del log de auditoría" y "5.5.5 Procedimientos de respaldo del log de auditoría y registros"

9.10.3 Transferencia de log de auditoría

ACEPTA transferirá los registros de auditoría a la AAC u otra Entidad de Registro o Verificación, por el periodo establecido por la AAC de 10 años luego de generado el registro (5.5.3 Periodo de retención para log de auditoría).

9.10.4 Transferencia de solicitudes, revocaciones o reemisiones

ACEPTA transferirá las solicitudes, revocaciones o re-emisiones ante el cese de sus actividades (remítase a 5.9 Cese de la actividad de la PSC) a otro prestador de servicios de certificación, de no existir objeción a la transferencia dentro del plazo de 15 días hábiles contados desde la fecha de la comunicación; en cuyo caso se entenderá que el usuario ha consentido en la transferencia de los mismos.

9.11 Noticias individuales y comunicaciones con participantes

Toda notificación o comunicación se hará mediante correo electrónico o por escrito dirigido a la dirección señalada en el contacto del presente documento (punto 1.5). Para todo cambio de las políticas y prácticas, Acepta notificará el cambio a través de la publicación de una versión del documento en su página web. De requerirse una notificación a un titular o titular que cause un evento, Acepta usará el mail registrado como parte de la solicitud del titular.

9.12 Enmiendas

9.12.1. Procedimiento para enmendaduras

En caso se actualice algún procedimiento o se requiera hacer alguna enmendadura Acepta presentará a la AAC la nueva versión del documento para su respectiva aprobación y posterior publicación.

9.12.2. Mecanismos y periodos de notificación

Acepta pondrá a disposición de la comunidad de usuarios, así como a otras infraestructuras que la reconocen, la nueva versión de su CPS, una vez que la misma haya sido aprobada por la AAC.

Acepta comunicará a los participantes de la IOFE, así como a otras infraestructuras que la reconocen, aquellas modificaciones que impliquen cambios en los términos y condiciones básicas de la prestación de los servicios de certificación que brinda.

El mecanismo de comunicación se efectuará a través de la publicación en la página WEB de Acepta, surtiendo los efectos de una notificación válidamente emitida.

9.12.3. Circunstancias bajo las cuales debe ser cambiado el OID

Cualquier cambio en el OID de cualquiera de los certificados y políticas o declaraciones de prácticas será aprobado previamente por la AAC.

9.13 Resolución de disputas

Remítase a 2.3.2 de este documento

9.14 Leyes gubernamentales aplicables

Estará sujeto a la normatividad que resulte aplicable y en especial a las disposiciones siguientes:

- Ley N° 27269, Ley de Firmas y Certificados Digitales.
- Decreto Supremo Nº 004-2007-PCM que aprobó el Reglamento de la Ley de Firmas y Certificados Digitales
- Reglamento de la Ley de Firmas y Certificados aprobado mediante el Decreto Supremo Nº 052-2008-PCM y sus modificaciones.
- Guía de Acreditación de Entidades de Certificación EC.
- Ley N° 29733, Ley de Protección de Datos Personales.

Así como a las disposiciones que sobre la materia dicte el INDECOPI como Autoridad Administrativa Competente en el marco de la IOFE.

9.15 Cumplimiento con la ley aplicable

Es responsabilidad de Acepta en la prestación de sus servicios, el cumplimiento de la legislación recogida en numeral 9.14.

9.16 Misceláneas

Respecto al acuerdo integro remítase a 2.3.2 de este documento. El resto de los puntos No aplica

9.16.1 Clasificación y gestión de activos

La EC mantiene un inventario de todos los activos de información relevantes, en concordancia con el análisis de riesgos de ACEPTA. EL detalle se encuentra en el documento "SG-M-03 Manual de Seguridad", capítulo 8 y en el documento "SG-F-05 Listado de activos de información primarios".

9.16.2 Política de Seguridad de la Información

ACEPTA define, a través del documento "SG-Q-01 Política de Seguridad de la información", un sistema de gestión de seguridad de la información, cuyo alcance considera tanto los servicios de Entidad de Registro o Verificación, Entidad de Certificación y Servicio de Valor Agregado. Esta política se encuentra publicada en la página web de ACEPTA.

9.16.3 Planificación

La planificación y gestión de la seguridad de la información de Acepta, está orientada a generar y ejecutar un plan que permita mitigar las amenazas detectadas, que sean producto de la gestión de riesgos definida en 9.16.4.

9.16.4 Gestión de Riesgos

Se realiza de acuerdo a lo declarado en el documento "SG-P-06 Procedimiento de Evaluacion de Riesgos".

9.16.5 Seguridad en el trato con terceros

ACEPTA realiza su gestión con terceros de acuerdo a lo declarado en "SG-P-18 Seguridad de la información y administración de la prestación de servicios de proveedores".

9.16.6 Manejo de medios y seguridad

ACEPTA realiza el manejo de medios de acuerdo a lo descrito en "SG-M-03 Manual de Seguridad" capítulo 8.

9.16.7 Planificación del sistema

ACEPTA realiza análisis de sus sistemas, a través de análisis de capacidad periódicos, con el fin de gestionar los mismos de acuerdo de futuras demandas. El detalle se encuentra en "SG-M-03 Manual de Seguridad", punto 12.1.3.

9.16.8 Intercambio de datos y software

ACEPTA evalúa los riesgos del intercambio de información que realiza, de acuerdo a la clasificación de la información que es intercambiada; y a partir de este análisis se determina el medio a utilizar para el intercambio. El detalle de este accionar se encuentra definido en "SG-M-03 Manual de Seguridad", punto 13.2.1.

9.16.9 Gestión de accesos a los sistemas

ACEPTA limita el acceso a sus sistemas, sólo a personal autorizado y dependiendo de las funciones que realice. El detalle de la gestión de acceso se encuentra en "SG-M-03 Manual de Seguridad", capítulo 9.

9.16.10 Sistemas operativos

Todos los sistemas operativos de ACEPTA son actualizados y/o parchados regularmente, de acuerdo a lo definido en "SG-M-02 Manual de Operaciones de Sistemas".

9.16.11 Gestión de Continuidad del negocio

La continuidad de negocio de ACEPTA es realizada de acuerdo a “SG-M-03 Manual de Seguridad” capítulo 17.

9.16.12 Organización de la seguridad de la información

La responsabilidad de organizar y dirigir la seguridad de la información en ACEPTA, es realizada de acuerdo a “SG-M-03 Manual de Seguridad” punto 5.3.

9.17 Otras provisiones

No aplica

10 Administración de las CPS

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

10.1 Procedimientos para Modificar las CPS

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

10.2 Publicación y notificación

Cualquier cambio, significativo en el contenido de estas prácticas será comunicado al público y titulares mediante su publicación en el sitio Web de Acepta https://sovos.com/es/politicas-y-practicas/.

10.3 Procedimientos de aprobación de las CPS

Estas CPS 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 CPS, 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. Para un cambio mayor que afecte los procesos de la EC, se presentará la nueva versión a la AAC, ello antes de publicar la nueva versión del documento, para su aprobación.