Declaración de Prácticas y Políticas de Certificación

Entidad de Certificación para el Estado Peruano

Peruano - ECEP

Versión: 2.1	**Año:** 2015

Elaborado por: Sub Gerencia de Certificación Digital	**Revisado por:** Sub Gerente de Certificación Digital Comité para Acreditación	**Aprobado por:** Gerente de Certificación y Registro Digital

Historial de Cambios				
Ver.	**Fecha**	**Descripción**	**Responsable**	**Estado**
1.0	22/06/2012	Elaboración y Aprobación	GCRD	Aprobado
2.0	05/12/2012	Se recoge observaciones del evaluador de INDECOPI.	GCRD	Aprobado
2.1	28/12/2015	Se recoge observaciones del evaluador de INDECOPI.	GCRD	Aprobado

INDICE

1. Introducción

El Registro Nacional de Identificación y Estado Civil (en adelante el RENIEC) es un organismo constitucional y autónomo con personería jurídica de derecho público interno, creado por mandato de la Constitución Política del Perú mediante Ley Orgánica N° 26497, goza de atribuciones en materia registral, técnica, administrativa, económica y financiera. Está encargado de organizar y mantener el Registro Único de Identificación de las Personas Naturales e inscribir los hechos y actos relativos a su capacidad y estado civil.

Mediante la Ley Nº 27269 - Ley Firmas y Certificados Digitales[1] se regula en el Perú la utilización de la firma electrónica y los certificados digitales, así como el establecimiento de los prestadores de servicios de certificación digital. Su Reglamento vigente, aprobado mediante el Decreto Supremo Nº 052-2008-PCM[2], reglamentó el empleo de la firma digital para los sectores público y privado, otorgando a la firma digital generada dentro la Infraestructura Oficial de Firma Electrónica (en adelante IOFE) la misma validez y eficacia jurídica que el uso de una firma manuscrita, así mismo, estableció el régimen de la IOFE, definida[3] como un sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente (en adelante AAC), provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de:

(i) La integridad de los documentos electrónicos,
(ii) La identidad de su autor.

Este sistema incluye la generación de firmas digitales, en las que participan Entidades de Certificación y Entidades de Registro o Verificación acreditadas ante la AAC, incluyendo a la Entidad de Certificación Nacional para el Estado Peruano, las Entidades de Certificación para el Estado Peruano y las Entidades de Registro o Verificación para el Estado Peruano y los Prestadores de Servicios de Valor Añadido para el Estado Peruano.

El artículo 47º del Reglamento de la Ley de Firmas y Certificado Digitales designó al RENIEC como Entidad de Certificación Nacional para el Estado Peruano (en adelante ECERNEP), Entidad de Certificación para el Estado Peruano (en adelante ECEP) y Entidad de Registro o Verificación para el Estado Peruano (en adelante EREP-RENIEC), disponiendo se realicen los trámites correspondientes ante la AAC, con el fin de acreditarse como Prestador de Servicios de Certificación Digital y formar parte de la IOFE.

Mediante el Artículo 57° del Reglamento acotado se designó al Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI como AAC.

En dicho orden de ideas, y con la finalidad de dar cumplimiento a lo dispuesto por el Reglamento de la Ley de Firmas y Certificado Digitales, el presente documento describe las prácticas y funciones que observará el RENIEC en su calidad de ECEP.

Entenderemos por prácticas de certificación al conjunto de procedimientos,

[1] Publicada en el Diario Oficial el peruano el 28 de mayo de 2000.
[2] Publicada en el Diario Oficial el peruano 19 de julio de 2008.
[3] Décimo Cuarta Disposición Complementaria Final del Reglamento de la Ley de Firmas y Certificados Digitales.

estándares o normas técnicas y/o disposiciones legales definidos y aplicados por la ECEP en el marco de sus funciones dentro de la IOFE.

El presente documento es aplicable y de obligado cumplimiento para toda la comunidad de usuarios a la que se alude en la sub sección 1.3.

1.1. Visión general.

De acuerdo al Decreto Supremo 052-2008-PCM "Reglamento de la Ley de Firmas y Certificados Digitales" aprobado el 19 de julio del 2008 y al amparo de la Ley N° 27269 "Ley de Firmas y Certificados Digitales", el RENIEC tiene las funciones de Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), Entidad de Certificación para el Estado Peruano (ECEP), Entidad de Registro o Verificación para el Estado Peruano (EREP-RENIEC).

El presente documento contiene la Declaración de Prácticas y Políticas de Certificación de la Entidad de Certificación para el Estado Peruano (ECEP) del que rige el funcionamiento y operaciones de la Infraestructura de Clave Pública del RENIEC, mediante la cual se emiten certificados digitales dirigidos a entidades finales (personas naturales y jurídicas).

El presente documento se aplica a todas las Autoridades Intermedias (exceptuando Autoridad Raíz - ECERNEP) de la jerarquía PKI del RENIEC y da cumplimiento a todos los requerimientos exigidos por las Guías de Acreditación para Entidades de Certificación publicadas por la AAC.

A fin de dotar al documento de uniformidad, facilidad de lectura y análisis, se incluyen las secciones establecidas en el RFC 3647 y en las Guías de Acreditación para Entidades de Certificación. Se indicará entre comillas y en cursiva documentos a los cuales se hace referencia.

Cabe precisar que en el presente documento se usará de forma genérica el acrónimo EREP para referirse tanto a la EREP-RENIEC como a otras Entidades de Registro o Verificación acreditas por la AAC y que hayan suscrito convenios con la ECEP para la emisión conjunta de certificados digitales.

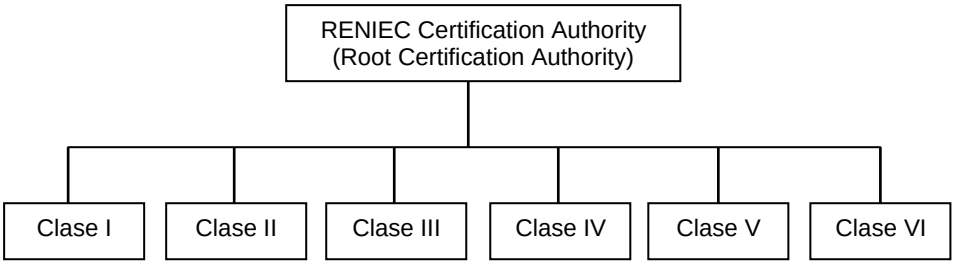
Cabe precisar también, que la Declaración de Prácticas de Registro o Verificación (DPR) es el documento oficialmente presentado por una Entidad de Registro o Verificación a la AAC, mediante el cual define sus Prácticas de Registro o Verificación. En el presente documento se usará el acrónimo DPR cuando se haga referencia a cualquiera de los siguientes documentos:

i. "*Declaración de Prácticas de Registro - Entidad de Registro o Verificación para el Estado Peruano – Persona Natural*" para certificados digitales autorizados por la EREP-RENIEC contenidos en el DNIe.
ii. "*Declaración de Prácticas de Registro - Entidad de Registro o Verificación para el Estado Peruano*" para certificados digitales distintos al del numeral anterior y autorizados por la EREP-RENIEC.
iii. "*Declaración de Prácticas de Registro o Verificación*" para certificados digitales autorizados por alguna otra Entidad de

Registro o Verificación acreditada por la AAC.

1.1.1. Clases de Certificados

La infraestructura de clave pública del RENIEC emite y gestiona diferentes clases de certificados digitales según el tipo de suscriptor o entidad final. Bajo esta premisa la clasificación es la siguiente:



Autoridad	Aplicación
RENIEC Certification Authority (Root Certification Authority)	Es la raíz de la jerarquía de Autoridades de Certificación (ECERNEP) del RENIEC. Esta EC puede certificar a cualquier EC subordinada, TSA y Autoridad de Validación OCSP previa acreditación ante la AAC.
Clase I "Persona Natural – 1 año"	Se utiliza SOLO para certificados de entidad final emitidos para Persona Natural con periodo de validez de 1 año.
Clase II "Persona Natural – 2 años"	Se utiliza SOLO para certificados de entidad final emitidos para Persona Natural con periodo de validez de 2 años.
Clase III "Persona Jurídica"	Se utiliza SOLO para certificados de entidad final emitidos para Persona Jurídica con periodo de validez de 1 y 2 años.
Clase IV "Persona Jurídica – Dispositivo Servidor SSL"	Se utiliza SOLO para certificados de entidad final emitidos para Dispositivos Servidores de Persona Jurídica, utilizado para autenticar dispositivos servidores en clientes o viceversa.
Clase V "Persona Jurídica – Sistemas SIE"	Se utiliza SOLO para certificados de entidad final emitidos para Sistemas SIE de Persona Jurídica, para validar el real compromiso del contenido firmado, tal como una firma digital en acuerdos o transacciones.
Clase VI "Persona Jurídica – Entidades de Certificación"	Se utiliza SOLO para certificados de Entidades de Certificación emitidos para Personas Jurídicas.

Para mayor detalle de la clasificación, puede recurrir a los perfiles de certificados digitales emitidos por la ECEP consignados en el documento

"*Perfiles de Certificado Digital ECEP***"**.

La emisión de certificados digitales de las mencionadas clases está sujeta a la inclusión del respectivo servicio en el TUPA del RENIEC.

1.2. Nombre e identificación del documento

Nombre del documento	Declaración de Prácticas y Políticas de Certificación Entidad de Certificación para el Estado Peruano Peruano - ECEP
OID	1.3.6.1.4.1.35300.1.1.1.1
Versión del documento	2.0
Estado del documento	Aprobado
Fecha de emisión	05/12/2012
Publicación de la CPS.	http://www.reniec.gob.pe/repository/

1.3. Participantes de la PKI

La comunidad de usuarios se compone por aquellas personas naturales y jurídicas que obtienen y utilizan un certificado digital emitido por una EC acreditada con la intervención de una ER acreditada, dichos usuarios deben cumplir los requerimientos especificados en las siguientes secciones de este documento y otros, como la correspondiente DPR**.**

1.3.1. Entidades de Certificación

La Entidad de Certificación Nacional para el Estado Peruano - ECERNEP es la entidad encargada de emitir los certificados raíz para las Entidades de Certificación para el Estado Peruano que lo soliciten, además de proponer a la Autoridad Administrativa Competente, las políticas y estándares de las Entidades de Certificación para el Estado Peruano y Entidades de Registro o Verificación para el Estado Peruano, según los requerimientos de la Autoridad Administrativa Competente[4]

El Registro Nacional de Identificación y Estado Civil - RENIEC es la única ECERNEP y actúa también como Entidad de Certificación para el Estado Peruano (ECEP) y Entidad de Registro o Verificación para el Estado Peruano (EREP-RENIEC). Todas las Entidades de Certificación para el Estado Peruano y las Entidades de Registro o Verificación para el Estado Peruano deben seguir las políticas y estándares propuestos por la Entidad de Certificación Nacional para el Estado Peruano y aprobados por la Autoridad Administrativa Competente.

[4] Reglamento de la Ley de Firmas y Certificados Digitales aprobado mediante el decreto supremo N 052-2008-PCM

La ECEP es la entidad encargada de la generación y cancelación de certificados digitales de:

i. Personas naturales y jurídicas.
ii. Funcionarios, empleados y servidores públicos para el ejercicio de sus funciones y la realización de actos de administración interna e interinstitucional, y de las personas expresamente autorizadas por la entidad pública correspondiente.

La ECEP recepciona a través de un medio seguro, con las debidas validaciones de identidad por parte de la EREP, las autorizaciones para la emisión y cancelación de certificados digitales.

La ECEP cuenta con certificados digitales denominados certificados digitales de autoridades intermedias, los cuales pueden ser generados por la ECERNEP usando algoritmos de firma SHA-1 ó SHA-256. Estos certificados de autoridades intermedias tienen una vigencia de diez (10) años.

1.3.2. Entidades de Registro

La ECEP tiene vínculos con la EREP, lo cual implica que los procesos descritos en el presente documento son compatibles con los procesos descritos en la DPR de la EREP, delineando específicamente y claramente los procedimientos que corresponden a cada entidad.

1.3.3. Titulares de certificados

Son titulares de certificados digitales aquellas personas naturales o entidades de la Administración Pública, a quienes se les atribuye de manera exclusiva dicho documento credencial electrónico.

En el caso de las entidades de la Administración Pública, éstas son titulares del certificado digital. Los suscriptores son las personas naturales responsables de la generación y uso de la clave privada, con excepción de los certificados digitales para su utilización en un Servidor y Sistemas de Intermediación Electrónico (SIE), situación en la cual dichas entidades asumen las facultades de titulares y suscriptores del certificado digital.[5]

1.3.4. Tercero que confía

Los terceros que confían o terceros usuarios son aquellas personas naturales o jurídicas (diferentes al titular o suscriptor del certificado digital), equipos, servicios o cualquier otro ente que decide aceptar y confiar en un certificado digital emitido por la ECEP, y actúa basado en la confianza sobre la validez de un certificado digital y/o verifica la firma digital en la que se utiliza dicho documento.[6]

1.3.5. Otros participantes

Todas las funciones, operaciones y actividades de la ECEP, dentro de los procesos de emisión y cancelación están a cargo del RENIEC en

[5] Artículo 9º del Reglamento de la Ley de Firmas y Certificados Digitales.
[6] Décimo Cuarta Disposición Complementaria del Reglamento de la Ley de Firmas y Certificados Digitales.

su calidad de Prestador de Servicios de Certificación Digital. Cabe mencionar que adicionalmente a la EREP-RENIEC, la ECEP podrá hacer uso de los servicios de otras EREP acreditas por la AAC con las cuales suscribirá los respectivos convenios.

La AAC faculta a las Entidades de Certificación acreditadas para que puedan realizar certificaciones cruzadas con Entidades de Certificación Extranjeras a fin de reconocer los certificados digitales que éstas emitan en el extranjero, incorporándolos como suyos dentro de la IOFE, siempre y cuando obtengan autorización previa de la AAC.

No obstante, en la eventualidad que el RENIEC requiera la tercerización de los servicios de directorio o repositorio y/o servicios de producción de certificados; entre otros, la ECEP se reserva su derecho de suscribir el acuerdo de tercerización respectivo, el mismo que contará con las cláusulas especificas relacionadas con la confidencialidad de la información y la protección de los datos personales.

1.3.5.1. SVAs

No aplica para la ECEP.

1.4. Uso del certificado

El siguiente cuadro resume los tipos de certificados y sus usos:

Clase	Tipo de persona que lo usa	Vigencia	Longitud de clave	Modo de generación	Uso
Clase I	Natural	1 año	2048	Automático	• Firma • Autenticación • Autenticación y firma
Clase II	Natural (DNIe)	2 años	2048	Automático	• Firma • Autenticación
Clase III	Jurídica	1 año	2048	Automático	• Firma • Autenticación • Autenticación y firma
		2 años	2048	Automático	• Firma • Autenticación
Clase IV	Jurídica (Servidor SSL)	2 años	2048	Generación manual de CSR	• Autenticación
Clase V	Jurídica (Sistema de Intermediación Electrónico)	2 años	2048	Generación manual de CSR	• Firma
Clase VI	Jurídica (Entidad de Certificación)	Depende de la entidad que la acredita *	Mínimo 2048	Automático	• Firma

* La vigencia máxima de estos certificados no podrá superar a la de los certificados digitales que se encuentran en niveles superiores.

Detalle de los tipos de certificados emitidos por la ECEP y su clasificación:

a) Por el titular:

- Certificados de Persona Natural

  Se caracteriza porque el poseedor de la clave privada es una persona natural, que actúa a nombre propio y representación. La persona natural solicitante se constituirá en titular y suscriptor del certificado digital.

  Dentro de este tipo existen 2 clases:
  - Clase I caracterizado por tener 1 año de duración.
  - Clase II caracterizado por tener 2 años de duración. El DNIe contiene este tipo de certificado digital.

- Certificados de Persona Jurídica

  Se caracteriza porque el poseedor actúa a nombre y representación de la persona jurídica. La persona jurídica considera los siguientes actores: titular que es el representante legal y funcionarios autorizados que son los suscriptores del certificado digital.

  Dentro de este tipo existen 4 clases:
  - Clase III con una duración de 1 ó 2 años para personas naturales que actúan en representación de la persona jurídica.
  - Clase IV con una duración de 2 años, emitidos para equipos servidores (persona jurídica), para motivos de autenticación.
  - Clase V con una duración de 2 años, emitidos para Sistemas de Intermediación Electrónico - SIE (persona jurídica).
  - Clase VI para Entidades de Certificación cuyo período de vigencia es determinado por el ente que lo acredita. La vigencia máxima de estos certificados no podrá superar a la de los certificados digitales que se encuentran en niveles superiores.

  Los certificados de Persona Jurídica pueden ser sub-agrupados en:

  (i) Certificado de Atributos: se caracteriza porque el titular del certificado es la persona jurídica que actúa a través de su representante legal y faculta a una persona natural de atributos que le permiten actuar en nombre de aquella.
  En la solicitud respectiva se deberá indicar claramente quién es la persona natural que será el suscriptor.
  Estos certificados digitales son emitidos bajo la Clase III.

  (ii) Certificado de Dispositivo: se caracteriza porque la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponden a la persona jurídica, quien asumirá la responsabilidad por el uso de dicho certificado digital.
  Existen dos casos de Certificado de Dispositivo:

  - Certificado de dispositivo servidor: Estos certificados permiten determinar que un sitio web es genuino, son los denominados certificados SSL.

Estos certificados son utilizados para establecer una comunicación segura (intercambio de datos cifrados entre cliente y servidor). Así se tiene la certeza que la información se transmite de forma confidencial y preservando la integridad.
Por otro lado, si es necesario, un servidor web puede configurarse para que funcione con protocolo SSL y pedir al cliente que intenta conectarse que se identifique mediante su certificado digital. Siendo esta una forma de establecer un mecanismo de control de acceso a un sitio web.
El pedido de este tipo de certificado debe considerar que su clave privada y el pedido de certificado (archivo CSR o request) deben ser generados en el equipo servidor para el cual se requiere el certificado digital.
Estos certificados digitales son emitidos bajo la Clase IV.

- Certificado de generación de cargos para los Sistemas de Intermediación Electrónicos: Este certificado se almacena en un dispositivo criptográfico y se emplea para firmar un cargo o acuse por cada transacción electrónica que realice dicho servidor.

  No es un certificado personal, sino que está vinculado al servidor y actúa de manera "automática", por lo que no requiere intervención "humana".

  Se debe dimensionar apropiadamente el hardware donde residirá este certificado, ya que podría saturarse al realizar los procesos de firma asimétrica. Sin embargo, el acceso al hardware debe estar restringido y protegido para evitar posibles usos fraudulentos del certificado.

  El pedido de este tipo de certificado debe considerar que su clave privada y el pedido de certificado (archivo CSR o request) deben ser generados en el equipo servidor para el cual se requiere el certificado digital.
  Estos certificados digitales son emitidos bajo la Clase V.

b) Por el uso:

Por el uso que se le da al certificado digital, este se puede clasificar en:

(i) Certificados de firma: utilizados en transacciones electrónicas que requieren la firma digital del suscriptor del certificado.
(ii) Certificados de autenticación: son utilizados en procesos de control de acceso y permisos donde se requiera autenticar a un suscriptor.
(iii) Certificados de autenticación y firma digital: son utilizados para control de acceso y permisos donde se requiera autenticar a un suscriptor, y adicionalmente pueden ser utilizados en transacciones electrónicas que requieran la firma digital del suscriptor del certificado.

1.4.1. Uso apropiado del certificado

Los certificados digitales emitidos por la ECEP tendrán como finalidad lo siguiente:

- **Certificado de Autenticación**: Garantizar electrónicamente la identidad de la persona natural o jurídica al realizar una transacción electrónica. El Certificado de Autenticación asegura que la comunicación electrónica se realiza con la persona que dice que es. El titular o suscriptor podrá a través de su certificado acreditar su identidad frente a cualquiera, ya que se encuentra en posesión del certificado y de la clave privada asociada al mismo.
  El uso de este certificado no está habilitado en operaciones que requieran no repudio de origen, por tanto, los terceros que confían y los prestadores de servicios telemáticos no tendrán garantía del compromiso del titular o suscriptor del certificado digital con el contenido firmado. Su uso principal será para generar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos (mediante establecimiento de canales privados y confidenciales con los prestadores de servicio telemáticos).

- **Certificado de Firma:** Mediante este certificado el titular o suscriptor va a poder firmar documentos electrónicos con pleno valor legal. Según la Ley de Firmas y Certificados Digitales y su Reglamento (D.S 052-2008-PCM) la firma digital generada por un Prestador de Servicios de Certificación Digital acreditado ante la Autoridad Administrativa Competente – INDECOPI, tiene la misma validez y eficacia jurídica que el uso de la firma manuscrita[7].
  El certificado de firma generado por la ECEP es un certificado reconocido por la IOFE, permitiendo sustituir la firma manuscrita por la firma digital en las relaciones del titular o suscriptor con la administración pública y/o terceros a través de medios electrónicos.
  Por lo antes descrito, este certificado no deberá ser empleado para generar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos (mediante establecimiento de canales privados y confidenciales con los prestadores de servicio telemáticos).

- **Certificado de Autenticación y Firma**: El uso conjunto de ambos certificados proporciona las siguientes garantías:

  (i) Autenticidad de origen
  El titular o suscriptor podrá, a través de su Certificado de Autenticación, acreditar su identidad frente a cualquiera, demostrando la posesión y el acceso a la clave privada asociada a la pública que se incluye en el certificado que

[7] Artículo 6to. del Reglamento de la Ley de Firmas y Certificados Digitales.

acredita su identidad.

(ii) No repudio de origen
Asegura que el documento proviene del titular o suscriptor de quien dice provenir. Esta característica se obtiene mediante la firma digital realizada por medio del Certificado de Firma.
Además, según lo señalado en el Reglamento acotado, el suscriptor no podrá repudiar o desconocer un documento electrónico que ha sido firmado digitalmente usando su clave privada[8]. Por consiguiente, se garantiza el "no repudio legal".

(iii) Integridad
Con el empleo del Certificado de Firma, se permite comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación. Para garantizar la integridad, la criptografía ofrece soluciones basadas en funciones de características especiales, denominadas funciones resumen, que se utilizan siempre que se realiza una firma digital. El uso de este sistema permite comprobar que un mensaje firmado no ha sido alterado entre el envío y la recepción. Para ello, se firma con la clave privada un resumen único del documento de forma que cualquier alteración del mensaje revierte en una alteración de su resumen.

Existe un registro de *"Preguntas Frecuentes"*, disponible en la dirección: *http://portales.reniec.gob.pe/web/identidaddigital/faqPKI*,al cual pueden acceder los usuarios en caso de dudas sobre el uso de sus certificados digitales.

1.4.2. Prohibiciones del uso del certificado

El certificado no se puede usar para aplicaciones no contempladas en numeral 1.4.1 y las no contempladas en:

- Ley N° 27269 "Ley de Firmas y Certificados Digitales" y Decreto Supremo 070-2011-PCM.
- D.S. 052-2008-PCM "Reglamento de la Ley de Firmas y Certificados Digitales".
- Disposiciones de la Autoridad Administrativa Competente (AAC).
- Documento de **"***Perfiles de Certificado Digital ECEP***"**.
- Declaración de Prácticas y Políticas de Certificación de la ECEP.

De igual modo, tal y como se recoge en el ítem 1.4 inciso b) y en el ítem 1.4.1 del precedente documento, el certificado de autenticación no deberá emplearse para la firma de trámites y documentos en los que se precise dejar constancia del compromiso del firmante con el contenido firmado. Igualmente el certificado de firma no deberá ser empleado para firmar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos (mediante el establecimiento de canales privados y confidenciales con los

[8] Artículo 8vo. del Reglamento de la Ley de Firmas y Certificados Digitales.

prestadores de servicios telemáticos).
Asimismo, no deberá ser utilizado un certificado digital de Persona Natural para representar una Institución, ni un certificado digital de Persona Jurídica para firmar a nombre personal o individual.

1.5. Administración de políticas

1.5.1. Organización que administra los documentos de CPS o CP

La organización encargada de la administración (elaboración, registro, mantenimiento y actualización) de este documento es:

Nombre: Registro Nacional de Identificación y Estado Civil - RENIEC.
Dirección de correo: identidaddigital@reniec.gob.pe
Dirección: Jr. Bolivia 109, Centro Cívico - Cercado de Lima.
Teléfono: 01-3152700 anexos 1192 y 1194.

1.5.2. Persona de contacto

De parte del Registro Nacional de Identificación y Estado Civil:
Sub Gerente de Certificación Digital.

Dirección de correo electrónico: identidaddigital@reniec.gob.pe
Número de teléfono: 01-3152700 anexos 1192 y 1194.
Dirección: Jr. Bolivia 109, Centro Cívico - Cercado de Lima.

1.5.3. Persona que determina la conformidad de la CPS con las políticas

El INDECOPI es la AAC, responsable de acreditar y determinar si una Entidad de Certificación está dentro de la Infraestructura Oficial de Firma Electrónica (IOFE), asimismo, es quien aprueba la presente Declaración de Prácticas y Políticas de Certificación durante el proceso de acreditación.

1.5.4. Procedimiento de aprobación de CPS

La AAC decidirá la aprobación de la CPS de la ECEP mediante los procedimientos establecidos en la "Guía de Acreditación para Entidades de Certificación Digital - EC".

1.6. Definiciones y acrónimos

DEFINICIONES:
Se ha tomado como referencia:

- Definiciones establecidas en el D.S. 052-2008-PCM “Reglamento de la Ley de Firmas y Certificados Digitales”.
- Otras definiciones que no han sido tomadas del mencionado reglamento están identificadas con un asterisco (*).

Acreditación.- Es el acto a través del cual la Autoridad Administrativa Competente, previo cumplimiento de las exigencias establecidas en la Ley, el Reglamento y las disposiciones dictadas por ella, faculta a las entidades solicitantes a prestar los servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica.

Acuse de Recibo.- Son los procedimientos que registran la recepción y validación de la Notificación Electrónica Personal recibida en el domicilio electrónico, de modo tal que impide rechazar el envío y da certeza al remitente de que el envío y la recepción han tenido lugar en una fecha y hora determinada a través del sello de tiempo electrónico.

Agente Automatizado.- Son los procesos y equipos programados para atender requerimientos predefinidos y dar una respuesta automática sin intervención humana, en dicha fase.

Ancho de banda.- Especifica la cantidad de información que se puede enviar a través de una conexión de red en un período de tiempo dado (generalmente un segundo). El ancho de banda se indica generalmente en bits por segundo (bps), kilobits por segundo (Kbps), o megabits por segundo (Mbps). Cuánto más elevado el ancho de la banda de una red, mayor es su aptitud para transmitir un mayor caudal de información.

Archivo.- Es el conjunto organizado de documentos producidos o recibidos por una entidad en el ejercicio de las funciones propias de su fin, y que están destinados al servicio.

Archivo Electrónico.- Es el conjunto de registros que guardan relación. También es la organización de dichos registros.

Autenticación.- Es el proceso técnico que permite determinar la identidad de la persona que firma digitalmente, en función del documento electrónico firmado por éste y al cual se le vincula; este proceso no otorga certificación notarial ni fe pública.

Autoridad Administrativa Competente (AAC).- Es el organismo público responsable de acreditar a las Entidades de Certificación, a las Entidades de Registro o Verificación y a los Prestadores de Servicios de Valor Añadido, públicos y privados, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, y las otras funciones señaladas en el presente Reglamento o aquellas que requiera en el transcurso de sus operaciones. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI.

Autoridad Raíz (*).- Se encuentra en la cima de la pirámide de las Autoridades permitidas para emitir certificados, su tarea específica es la de emitir certificados para Autoridades Intermedias y generar la CRL para éstas. En el marco de la IOFE esta autoridad toma el nombre de ECERNEP.

Autoridad Intermedia (*).- Se encuentra por debajo de una Autoridad Raíz y es la encargada de emitir certificados para entidades finales (Personas Naturales o Jurídicas). En el marco de la IOFE estas autoridades toman el nombre de ECEP.

Canal seguro.- Es el conducto virtual o físicamente independiente a través del cual se pueden transferir datos garantizando una transmisión

confidencial y confiable, protegiéndolos de ser interceptados o manipulados por terceros.

Cancelación de certificado digital (*).- Anulación definitiva de un certificado digital a petición del suscriptor, un tercero o por propia iniciativa de la autoridad de certificación en caso de duda de la seguridad de las claves o por cualquier motivo permitido y debidamente sustentado descritos en la Declaración de Prácticas de Registro o Verificación.

Certificación Cruzada.- Es el acto por el cual una Entidad de Certificación acreditada reconoce la validez de un certificado emitido por otra, sea nacional, extranjera o internacional, previa autorización de la Autoridad Administrativa Competente; y asume tal certificado como si fuera de propia emisión, bajo su responsabilidad.

Certificado Digital.- Es el documento credencial electrónico generado y firmado digitalmente por una Entidad de Certificación que vincula un par de claves con una persona natural o jurídica confirmando su identidad.

Clave privada.- Es la clave en un sistema de criptografía asimétrica que es usada por el destinatario de un documento electrónico para firmar un documento. La clave privada sólo debe permanecer en propiedad del suscriptor.

Clave pública.- Es la otra clave en un sistema de criptografía asimétrica que es usada por el destinatario de un documento electrónico para verificar la firma digital puesta en dicho documento. La clave pública puede ser conocida por cualquier persona.

Código de verificación o resumen criptográfico (hash).- Es la secuencia de bits de longitud fija obtenida como resultado de procesar un documento electrónico con un algoritmo, de tal manera que:
(1) El documento electrónico produzca siempre el mismo código de verificación (resumen) cada vez que se le aplique dicho algoritmo.
(2) Sea improbable a través de medios técnicos, que el documento electrónico pueda ser derivado o reconstruido a partir del código de verificación (resumen) producido por el algoritmo.
(3) Sea improbable por medios técnicos, que se pueda encontrar dos documentos electrónicos que produzcan el mismo código de verificación (resumen) al usar el mismo algoritmo.

Controlador de dispositivo (driver).- Es el programa informático que permite a un Sistema Operativo entender y manejar diversos dispositivos electrónicos físicos que se conectan o forman parte de la computadora.

Criptografía Asimétrica.- Es la rama de las matemáticas aplicadas que se ocupa de transformar documentos electrónicos en formas aparentemente ininteligibles y devolverlas a su forma original, las cuales se basan en el empleo de funciones algorítmicas para generar dos “claves” diferentes pero matemáticamente relacionadas entre sí. Una de esas claves se utiliza para crear una firma numérica o transformar datos en una forma aparentemente ininteligible (clave privada), y la otra para verificar una firma numérica o devolver el documento electrónico a su forma original (clave

pública). Las claves están matemáticamente relacionadas, de tal modo que cualquiera de ellas implica la existencia de la otra, pero la posibilidad de acceder a la clave privada a partir de la pública es técnicamente ínfima.
Declaración de Prácticas de Certificación (CPS).- Es el documento oficialmente presentado por una Entidad de Certificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Certificación.

Declaración de Prácticas de Registro o Verificación (DPR).- Documento oficialmente presentado por una Entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Registro o Verificación.

Nota: en el presente documento se usará el acrónimo DPR para representar a los siguientes documentos:

i. "*Declaración de Prácticas de Registro - Entidad de Registro o Verificación para el Estado Peruano – Persona Natural*" para certificados digitales autorizados por la EREP-RENIEC contenidos en el DNIe.
ii. "*Declaración de Prácticas de Registro - Entidad de Registro o Verificación para el Estado Peruano*" para certificados digitales distintos al del numeral anterior y autorizados por la EREP-RENIEC.
iii. "*Declaración de Prácticas de Registro o Verificación*" para certificados digitales autorizados por alguna otra Entidad de Registro o Verificación acreditada por la AAC.

Depósito o Repositorio de Certificados.- Es el sistema de almacenamiento y recuperación de certificados, así como de la información relativa a éstos, disponible por medios telemáticos.

Dirección oficial de correo electrónico.- Es la dirección de correo electrónico del usuario, reconocido por el Gobierno Peruano para la realización confiable y segura de las notificaciones electrónicas personales requeridas en los procesos públicos. Esta dirección recibirá los mensajes de correo electrónico que sirvan para informar al usuario acerca de cada notificación o acuse de recibo que haya sido remitida a cualquiera de sus domicilios electrónicos. A diferencia del domicilio electrónico, esta dirección centraliza todas las comunicaciones que sirven para informar al usuario que se ha realizado una actualización de los documentos almacenados en sus domicilios electrónicos. Su lectura es de uso obligatorio.

Documento electrónico.- Es la unidad básica estructurada de información registrada, publicada o no, susceptible de ser generada, clasificada, gestionada, transmitida, procesada o conservada por una persona o una organización de acuerdo a sus requisitos funcionales, utilizando sistemas informáticos.

Documento oficial de identidad.- Es el documento oficial que sirve para acreditar la identidad de una persona natural, que puede ser:

a) Documento Nacional de Identidad (DNI);
b) Carné de extranjería actualizado, para las personas naturales extranjeras domiciliadas en el país; o,

c) Pasaporte, si se trata de personas naturales extranjeras no residentes.

Domicilio electrónico.- Está conformado por la dirección electrónica que constituye la residencia habitual de una persona dentro de un Sistema de Intermediación Digital, para la tramitación confiable y segura de las notificaciones, acuses de recibo y demás documentos requeridos en sus procedimientos. En el caso de una persona jurídica el domicilio electrónico se asocia a sus integrantes.

Para estos efectos, se empleará el domicilio electrónico como equivalente funcional del domicilio habitual de las personas naturales o jurídicas.

En este domicilio se almacenarán los documentos y expedientes electrónicos correspondientes a los procedimientos y trámites realizados en el respectivo Sistema de Intermediación.

Entidad de Certificación.- Es la persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.

Entidad de Certificación Extranjera.- Es la Entidad de Certificación que no se encuentra domiciliada en el país, ni inscrita en los Registros Públicos del Perú, conforme a la legislación de la materia.

Entidades de la Administración Pública.- Es el organismo público que ha recibido del poder político la competencia y los medios necesarios para la satisfacción de los intereses generales de los ciudadanos y la industria.

Entidad de Registro o Verificación.- Es la persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.

Entidad final.- Es el suscriptor o propietario de un certificado digital.

Estándares Técnicos Internacionales.- Son los requisitos de orden técnico y de uso internacional que deben observarse en la emisión de certificados digitales y en las prácticas de certificación.

Estándares Técnicos Nacionales.- Son los estándares técnicos aprobados mediante Normas Técnicas Peruanas por la Comisión de Reglamentos Técnicos y Comerciales - CRT del INDECOPI, en su calidad de Organismo Nacional de Normalización.

Equivalencia funcional.- Principio por el cual los actos jurídicos realizados por medios electrónicos que cumplan con las disposiciones legales vigentes poseen la misma validez y eficacia jurídica que los actos realizados por medios convencionales, pudiéndolos sustituir para todos los

efectos legales. De conformidad con lo establecido en la Ley y su Reglamento, los documentos firmados digitalmente pueden ser presentados y admitidos como prueba en toda clase de procesos judiciales y procedimientos administrativos.

Expediente electrónico.- El expediente electrónico se constituye en los trámites o procedimientos administrativos en la entidad que agrupa una serie de documentos o anexos identificados como archivos, sobre los cuales interactúan los usuarios internos o externos a la entidad que tengan los perfiles de accesos o permisos autorizados.

Gobierno Electrónico.- Es el uso de las Tecnologías de Información y Comunicación para redefinir la relación del gobierno con los ciudadanos y la industria, mejorar la gestión y los servicios, garantizar la transparencia y la participación, y facilitar el acceso seguro a la información pública, apoyando la integración y el desarrollo de los distintos sectores.

Hardware Security Module (*).- Traducido al español es módulo de seguridad de hardware. Es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas. Aporta aceleración en las operaciones criptográficas.

Identidad digital (*): Es el reconocimiento de la identidad de una persona en un medio digital (como por ejemplo Internet) a través de mecanismos tecnológicos seguros y confiables, sin necesidad de que la persona esté presente físicamente.

Identificador de objeto (OID).- Es una cadena de números, formalmente definida usando el estándar ASN.1 (ITU-T Rec. X.660 | ISO/IEC 9834 series), que identifica de forma única a un objeto. En el caso de la certificación digital, los OIDs se utilizan para identificar a los distintos objetos en los que ésta se enmarca (por ejemplo, componentes de los Nombres Diferenciados, CPS, etc.).

Infraestructura Oficial de Firma Electrónica (IOFE).- Sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de:

1) La integridad de los documentos electrónicos;
2) La identidad de su autor, lo que es regulado conforme a Ley.

El sistema incluye la generación de firmas digitales, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la Autoridad Administrativa Competente incluyendo a la Entidad de Certificación Nacional para el Estado Peruano, las Entidades de Certificación para el Estado Peruano, las Entidades de Registro o Verificación para el Estado Peruano y los Prestadores de Servicios de Valor Añadido para el Estado Peruano.

Integridad.- Es la característica que indica que un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción

por el destinatario.

Interoperabilidad.- Según el OASIS Forum Group la interoperabilidad puede definirse en tres áreas:

- Interoperabilidad a nivel de componentes: consiste en la interacción entre sistemas que soportan o consumen directamente servicios relacionados con PKI.
- Interoperabilidad a nivel de aplicación: consiste en la compatibilidad entre aplicaciones que se comunican entre sí.
- Interoperabilidad entre dominios o infraestructuras PKI: consiste en la interacción de distintos sistemas de certificación PKI (dominios, infraestructuras), estableciendo relaciones de confianza que permiten el reconocimiento indistinto de los certificados digitales por parte de los terceros que confían.

Ley.- Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley Nº 27310.

Lista de Certificados Digitales Cancelados (CRL).- Es aquella en la que se deberá incorporar todos los certificados cancelados por la entidad de certificación de acuerdo con lo establecido en el presente Reglamento.

Mecanismos de firma digital.- Es un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma digital. Dichos mecanismos varían según el nivel de seguridad que se les aplique.

Medios electrónicos.- Son los sistemas informáticos o computacionales a través de los cuales se puede generar, procesar, transmitir y archivar documentos electrónicos.

Medios electrónicos seguros.- Son los medios electrónicos que emplean firmas y certificados digitales emitidos por Prestadores de Servicios de Certificación Digital acreditados, donde el intercambio de información se realiza a través de canales seguros.

Medios telemáticos.- Es el conjunto de bienes y elementos técnicos informáticos que en unión con las telecomunicaciones permiten la generación, procesamiento, transmisión, comunicación y archivo de datos e información.

Neutralidad tecnológica.- Es el principio de no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente; asimismo, implica la no discriminación, preferencia o restricción de ninguna de las diversas técnicas o tecnologías que pueden utilizarse para firmar, generar, comunicar, almacenar o archivar electrónicamente información.

Niveles de seguridad.- Son los diversos niveles de garantía que ofrecen las variedades de firmas digitales, cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma digital para enviar o recibir documentos electrónicos.

No repudio.- Es la imposibilidad para una persona de desdecirse de sus actos cuando ha plasmado su voluntad en un documento y lo ha firmado en forma manuscrita o digitalmente con un certificado emitido por una Entidad de Certificación acreditada en cooperación de una Entidad de Registro o Verificación acreditada, salvo que la misma entidad tenga ambas calidades, empleando un software de firmas digitales acreditado, y siempre que cumpla con lo previsto en la legislación civil.

En el ámbito del artículo 2º de la Ley de Firmas y Certificados Digitales, el no repudio hace referencia a la vinculación de un individuo (o institución) con el documento electrónico, de tal manera que no puede negar su vinculación con él ni reclamar supuestas modificaciones de tal documento (falsificación).

Nombre Común - Common Name (CN) (*).- Es un atributo que forma parte del Nombre Distinguido (Distinguished Name - DN).

Nombre de Dominio totalmente calificado - Fully Qualified Domain Name (FQDN) (*).- Es el identificador que incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo que puede identificar de forma única a un equipo servidor (o arreglo de estos) en el internet.

Nombre Diferenciado (X.501) - Distinguished Name (DN).- Es un sistema estándar diseñado para consignar en el campo sujeto de un certificado digital los datos de identificación del titular del certificado, de manera que éstos se asocien de forma inequívoca con ese titular dentro del conjunto de todos los certificados en vigor que ha emitido la Entidad de Certificación. En inglés se denomina “Distinguished Name”.

Nombre distinguido (*).- Es equivalente a Nombre diferenciado.

Norma Marco sobre Privacidad.- Es la norma basada en la normativa aprobada en la 16º Reunión Ministerial del APEC, que fuera llevada a cabo en Santiago de Chile el 17 y 18 de noviembre de 2004, la cual forma parte integrante de las Guías de Acreditación aprobadas por la Autoridad Administrativa Competente.

Notificación electrónica personal.- En virtud del principio de equivalencia funcional, la notificación electrónica personal de los actos administrativos se realizará en el domicilio electrónico o en la dirección oficial de correo electrónico de las personas por cualquier medio electrónico, siempre que permita confirmar la recepción, integridad, fecha y hora en que se produce. Si la notificación fuera recibida en día u hora inhábil, ésta surtirá efectos al primer día hábil siguiente a dicha recepción.

Par de claves.- En un sistema de criptografía asimétrica comprende una clave privada y su correspondiente clave pública, ambas asociadas matemáticamente.

Planta de Certificación Digital (*).- Instalación física tecnológica de la ECEP que también alberga a la ECERNEP.

Políticas de Certificación.- Documento oficialmente presentado por una Entidad de Certificación a la Autoridad Administrativa Competente, mediante el cual se establece, entre otras cosas, los tipos de certificados digitales que podrán ser emitidos, cómo se deben emitir y gestionar los certificados, y los respectivos derechos y responsabilidades de las Entidades de Certificación. Para el caso de una Entidad de Certificación Raíz, la Política de Certificación incluye las directrices para la gestión del Sistema de Certificación de las Entidades de Certificación vinculadas.

Prácticas de Certificación.- Son las prácticas utilizadas para aplicar las directrices de la política establecida en la Política de Certificación respectiva.

Prácticas de Registro o Verificación.- Son las prácticas que establecen las actividades y requerimientos de seguridad y privacidad correspondientes al Sistema de Registro o Verificación de una Entidad de Registro o Verificación.

Prestador de Servicios de Certificación.- Es toda entidad pública o privada que indistintamente brinda servicios en la modalidad de Entidad de Certificación, Entidad de Registro o Verificación o Prestador de Servicios de Valor Añadido.

Prestador de Servicios de Valor Añadido.- Es la entidad pública o privada que brinda servicios que incluyen la firma digital y el uso de los certificados digitales. El presente Reglamento presenta dos modalidades:

a. Prestadores de Servicio de Valor Añadido que realizan procedimientos sin firma digital de usuarios finales, los cuales se caracterizan por brindar servicios de valor añadido, como Sellado de Tiempo que no requieren en ninguna etapa de la firma digital del usuario final en documento alguno.
b. Prestadores de Servicio de Valor Añadido que realizan procedimientos con firma digital de usuarios finales, los cuales se caracterizan por brindar servicios de valor añadido como el sistema de intermediación electrónico, en donde se requiere en determinada etapa de operación del procedimiento la firma digital por parte del usuario final en algún tipo de documento.

Prestador de Servicios de Valor Añadido para el Estado Peruano.- Es la Entidad pública que brinda servicios de valor añadido, con el fin de permitir la realización de las transacciones públicas de los ciudadanos a través de medios electrónicos que garantizan la integridad y el no repudio de la información (Sistema de Intermediación Digital) y/o registran la fecha y hora cierta (Sello de Tiempo).

Reconocimiento de Servicios de Certificación Prestados en el Extranjero.- Es el proceso a través del cual la Autoridad Administrativa Competente, acredita, equipara y reconoce oficialmente a las entidades de certificación extranjeras.

Reglamento.- Reglamento de la Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley Nº 27310.

Servicio de Valor Añadido.- Son los servicios complementarios de la firma digital brindados dentro o fuera de la Infraestructura Oficial de Firma Electrónica que permiten grabar, almacenar, y conservar cualquier información remitida por medios electrónicos que certifican los datos de envío y recepción, su fecha y hora, el no repudio en origen y de recepción. El servicio de intermediación electrónico dentro de la Infraestructura Oficial de Firma Electrónica es brindado por persona natural o jurídica acreditada ante la Autoridad Administrativa Competente.

Servicio OCSP (Protocolo del estado en línea del certificado, por sus siglas en inglés).- Es el servicio que permite utilizar un protocolo estándar para realizar consultas en línea (on line) al servidor de la Autoridad de Certificación sobre el estado de un certificado.

Sistema de Intermediación Digital.- Es el sistema WEB que permite la transmisión y almacenamiento de información, garantizando el no repudio, confidencialidad e integridad de las transacciones a través del uso de componentes de firma digital, autenticación y canales seguros.

Sistema de Intermediación Electrónico.- Es el sistema WEB que permite la transmisión y almacenamiento de información, garantizando el no repudio, confidencialidad e integridad de las transacciones a través del uso de componentes de firma electrónica, autenticación y canales seguros.

Suscriptor.- Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

Tercero que confía o tercer usuario.- Se refiere a las personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado.

Titular.- Es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

Usabilidad.- En el contexto de la certificación digital, el término Usabilidad se aplica a todos los documentos, información y sistemas de ayuda necesarios que deben ponerse a disposición de los usuarios para asegurar la aceptación y comprensión de las tecnologías, aplicaciones informáticas, sistemas y servicios de certificación digital de manera efectiva, eficiente y satisfactoria.

Usuario final.- En líneas generales, es toda persona que solicita cualquier tipo de servicio por parte de un Prestador de Servicios de Certificación Digital acreditado.

WebTrust.- Certificación otorgada a prestadores de servicios de certificación digital - PSC, específicamente a las Entidades Certificadoras - EC, que de manera consistente cumplen con estándares establecidos por el Instituto Canadiense de Contadores Colegiados (CICA por sus siglas en inglés - ver Cica.ca) y el Instituto Americano de Contadores Públicos Colegiados (AICPA). Los estándares mencionados se refieren a áreas como privacidad, seguridad, integridad de las transacciones, disponibilidad, confidencialidad y no repudio.

ACRÓNIMOS:

Vocablo	Significado
AAC	Autoridad Administrativa Competente (en concreto la Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias (CNB) del INDECOPI)
CRL	Certicate Revocation List (Lista de certificados revocados o Lista de certificados cancelados)
CP	Certification Policy (Políticas de Certificación)
CPS	Certification Practice Statement (Declaración de Prácticas de Certificación)
DN	Distinguished Nane (Nombre distinguido o diferenciado)
DNIe	Documento Nacional de Identidad electrónico
DPC	Declaración de Prácticas de Certificación
DPR	Declaración de Prácticas de Registro o Verificación
EC	Entidad de Certificación
ECERNEP	Entidad de Certificación Nacional para el Estado Peruano
ECEP	Entidad de Certificación para el Estado Peruano
ER	Entidad de Registro o Verificación
EREP	Entidad de Registro o Verificación para el Estado Peruano
HSM	Hardware Security Module (Módulo de seguridad de hardware)
INDECOPI	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual

IOFE	Infraestructura Oficial de Firma Electrónica
ISP	Internet Service Provider (Proveedor de servicios de internet)
OCSP	Online Certificate Status Protocol (Protocolo del estado en línea del certificado)
PKI	Public Key Infrastructure (Infraestructura de Clave Pública)
PSC	Prestador de Servicios de Certificación Digital
RENIEC	Registro Nacional de Identificación y Estado Civil
SIE	Sistema de Intermediación Electrónico.
TSL	Trusted Services List (Lista de servicios de confianza)

2. Responsabilidades de publicación y repositorio

2.1. Repositorios

La ECEP dispone de repositorios, accesibles desde la Internet, donde se publican las distintas CRLs, las vigentes y el histórico de éstas, las políticas y prácticas de certificación, así como los certificados emitidos por la ECEP y los certificados de las autoridades.

Según la información publicada los repositorios son:

i. Repositorios para la lista de certificados cancelados.
ii. Repositorio de certificados de Autoridades de la ECEP.
iii. Repositorio de certificados emitidos por la ECEP.
iv. Repositorio del documento de Declaración de Prácticas y Políticas de Certificación.

Toda la información ubicada en nuestros repositorios es considerada pública y contemplan los derechos a la privacidad de la información considerando las restricciones mencionadas en la ley N° 29733 de Protección de Datos Personales, el Plan de Privacidad y la Política de Privacidad del RENIEC.

Los documentos e información contenida en estos repositorios se encuentran firmados digitalmente para garantizar su no repudio y su legitimidad.

La disponibilidad de estos repositorios son soportados tecnológicamente por el RENIEC, acorde a lo mencionado por la Autoridad Administrativa Competente en el Anexo 1 “Marco de la política de emisión de certificados digitales” de su Guía de Acreditación para Entidades de Certificación, la cual indica que es conveniente una disponibilidad mínima de 99%

anual, con un tiempo programado de inactividad máximo de 0.5% anual.

2.2. Publicación de información sobre certificación

La ECEP es la responsable de la publicación de toda información referente a los certificados digitales emitidos por ésta. Por lo cual, en los repositorios de la ECEP está disponible la siguiente información:

i. Repositorios para la lista de certificados cancelados
Especificados en el campo **Punto de distribución de CRL** de los certificados digitales emitidos, donde se indican las direcciones URL de descarga de la última CRL emitida.
http://crl.reniec.gob.pe/ y http://crl2.reniec.gob.pe
También se cuenta con un repositorio histórico de las CRL emitidas en orden cronológico.
http://crl.reniec.gob.pe/historicocrl/

ii. Repositorio de certificados de Autoridades de la ECEP
Especificado en el campo del certificado digital **Directivas del certificado**, donde se indica la dirección URL de descarga de certificados de las autoridades de la ECEP.
http://www.reniec.gob.pe/crt/

iii. Repositorio de certificados emitidos por la ECEP
El servicio de búsqueda de certificados digitales emitidos se brinda a través de un sistema de directorio en el cual se almacenan los certificados digitales emitidos por las autoridades de la ECEP. Los accesos se determinan según lo indicado por la *"Política de Privacidad".*

Para ubicar un certificado digital específico se deberá brindar los datos mínimos requeridos por el buscador como: número de DNI (Documento Nacional de Identidad) o número de RUC (Registro Único de Contribuyente) según sea el tipo de suscriptor o propietario del certificado.
http://crl.reniec.gob.pe/ldap/

iv. Repositorio de CP y CPS:
La ubicación donde se publican dichos documentos está especificada en el campo del certificado digital directivas del certificado, donde se indica la dirección URL de descarga de la última versión aprobada por la AAC y versiones previas.
http://www.reniec.gob.pe/repository/

La AAC es la encargada de operar y publicar la relación de Prestadores de Servicios de Certificación Digital acreditados.

2.3. Tiempo o frecuencia de publicación

i. Repositorios para la lista de certificados cancelados.
La frecuencia de publicación de la CRL vigente es cada 24 horas.

ii. Repositorio de certificados de Autoridades de la ECEP.
El repositorio de certificados de Autoridades es actualizado de acuerdo

a los requerimientos de la ECEP, siendo algunos motivos para su modificación:

- Creación de una nueva Autoridad Intermedia.
- Adicionar un nuevo formato de descarga para un certificado digital de una Autoridad ya existente.

Dichas actualizaciones son poco frecuentes.

iii. Repositorio de certificados emitidos por la ECEP.
Este repositorio es actualizado apenas es generado un nuevo certificado digital, tal como está indicado en el documento "*Generación y cancelación de certificado digital*".

iv. Repositorio de CP y CPS.
Los cambios de la CPS o CP de la ECEP, están sujetas a la necesidad de modificación y la respectiva aprobación por parte de la AAC para su puesta en vigencia y publicación respectiva.

2.4. Controles de acceso a los repositorios

El acceso a los repositorios (indicados en los items 2.1 y 2.2 del presente documento) donde la ECEP almacena información de interés público, sólo permite la lectura y/o descarga, quedando restringidas las operaciones de actualización del contenido. A las operaciones de actualización sólo tienen acceso las aplicaciones internas con usuarios previamente autorizados y desde puntos de la red interna de la ECEP.
Cabe mencionar además, que los repositorios indicados están protegidos por equipos de seguridad de red (firewall), que impiden una manipulación no autorizada.

El RENIEC hará uso de mecanismos técnicos que permitan mantener controlados estos accesos según lo detallado en el documento "*Control de Acceso Lógico*".

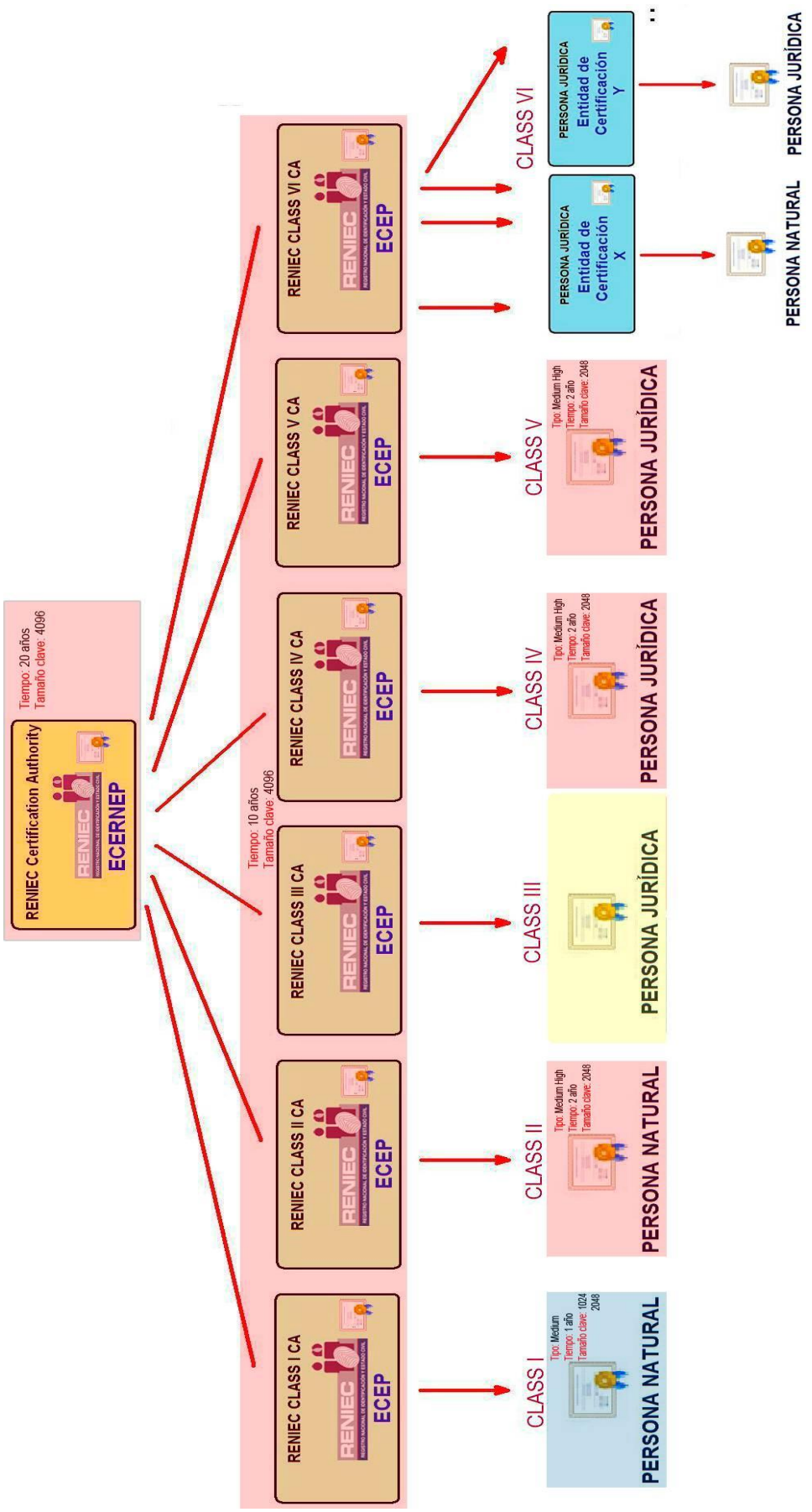
3. Identificación y autenticación

3.1. Nombre

3.1.1. Tipos de nombres

Tipos de nombres asignados al Nombre Distinguido (Distinguished Name - DN):

i. Nombres Distinguidos (Distinguished Names - DN) X.509:


RENIEC Certification Authority
ECERNEP
Tiempo: 20 años
Tamaño clave: 4096
Tiempo: 10 años
Tamaño clave: 4096
RENIEC CLASS I CA
RENIEC CLASS II CA
RENIEC CLASS III CA
RENIEC CLASS IV CA
RENIEC CLASS V CA
RENIEC CLASS VI CA
ECEP
CLASS I
CLASS II
CLASS III
CLASS IV
CLASS V
CLASS VI
Tipo: Medium
Tiempo: 1 año
Tamaño clave: 1024
2048
Tipo: Medium High
Tiempo: 2 año
Tamaño clave: 2048
PERSONA NATURAL
PERSONA JURÍDICA
PERSONA JURÍDICA
Entidad de Certificación X
PERSONA JURÍDICA
Entidad de Certificación Y
PERSONA NATURAL
PERSONA JURÍDICA

AUTORIDADES DEL RENIEC CERTIFICATION AUTHORITY

- Tipo: Certificado de Autoridad Jerárquica

Ítem	Sub - tipo de certificado	Subject [Distinguished Names Attributes]
1	Autoridad de certificación raíz (SHA-1)	commonName = RENIEC Certification Authority organizationName = Registro Nacional de Identificación y Estado Civil countryName = PE
2	Autoridad de Certificación raíz (SHA-256)	commonName = RENIEC High Grade Certification Authority organizationName = Registro Nacional de Identificación y Estado Civil countryName = PE
3	Clase I Autoridad de Certificación Subordinada (SHA-1)	SerialNumber = <Número de Identificación Peruano registrado por RENIEC> commonName = RENIEC Class I CA organizationalUnitName = RENIEC Certification Authority organizationName = Registro Nacional de Identificación y Estado Civil countryName = PE
4	Clase I Autoridad de Certificación Subordinada (SHA-256)	SerialNumber = <Número de Identificación Peruano registrado por RENIEC> commonName = RENIEC Class I High Grade CA organizationalUnitName = RENIEC Certification Authority organizationName = Registro Nacional de Identificación y Estado Civil countryName = PE
5	Clase II Autoridad de Certificación Subordinada (SHA-1)	SerialNumber = <Número de Identificación Peruano registrado por RENIEC> commonName = RENIEC Class II CA organizationalUnitName = RENIEC Certification Authority organizationName = Registro Nacional de Identificación y Estado Civil countryName = PE
6	Clase II Autoridad de Certificación Subordinada (SHA-256)	SerialNumber = <Número de Identificación Peruano registrado por RENIEC> commonName = RENIEC Class I High Grade CA organizationalUnitName = RENIEC Certification Authority organizationName = Registro Nacional de Identificación y Estado Civil countryName = PE
7	Clase III Autoridad de Certificación Subordinada	SerialNumber = <Número de Identificación Peruano registrado por RENIEC> commonName = RENIEC Class III CA organizationalUnitName = RENIEC Certification

	(Autoridad intermedia) (SHA-1)	Authority organizationName = Registro Nacional de Identificación y Estado Civil countryName = PE
8	Clase III Autoridad de Certificación Subordinada (SHA-256)	SerialNumber = <Número de Identificación Peruano registrado por RENIEC> commonName = RENIEC Class III High Grade CA organizationalUnitName = RENIEC Certification Authority organizationName = Registro Nacional de Identificación y Estado Civil countryName = PE
9	Clase IV Autoridad de Certificación Subordinada (SHA-1)	SerialNumber = <Número de Identificación Peruano registrado por RENIEC> commonName = RENIEC Class IV CA organizationalUnitName = RENIEC Certification Authority organizationName = Registro Nacional de Identificación y Estado Civil countryName = PE
10	Clase IV Autoridad de Certificación Subordinada (SHA-256)	SerialNumber = <Número de Identificación Peruano registrado por RENIEC> commonName = RENIEC Class IV High Grade CA organizationalUnitName = RENIEC Certification Authority organizationName = Registro Nacional de Identificación y Estado Civil countryName = PE
11	Clase V Autoridad de Certificación Subordinada (SHA-1)	SerialNumber = <Número de Identificación Peruano registrado por RENIEC> commonName = RENIEC Class V CA organizationalUnitName = RENIEC Certification Authority organizationName = Registro Nacional de Identificación y Estado Civil countryName = PE
12	Clase V Autoridad de Certificación Subordinada (SHA-256)	SerialNumber = <Número de Identificación Peruano registrado por RENIEC> commonName = RENIEC Class IV High Grade CA organizationalUnitName = RENIEC Certification Authority organizationName = Registro Nacional de Identificación y Estado Civil countryName = PE
13	Clase VI Autoridad de Certificación Subordinada (SHA-1)	SerialNumber = <Número de Identificación Peruano registrado por RENIEC> commonName = RENIEC Class VI CA organizationalUnitName = RENIEC Certification Authority

		organizationName = Registro Nacional de Identificación y Estado Civil countryName = PE
14	Clase VI Autoridad de Certificación Subordinada (SHA-256)	SerialNumber = <Número de Identificación Peruano registrado por RENIEC> commonName = RENIEC Class VI High Grade CA organizationalUnitName = RENIEC Certification Authority organizationName = Registro Nacional de Identificación y Estado Civil countryName = PE

CERTIFICADOS OFRECIDOS

- Certificados de Entidad Final Clase I

Ítem	Sub - tipo de certificado	Subject [Distinguished Names Attributes]
1	Firma digital para persona natural (Seguridad Media)	E (emailAddress) = <dirección de correo electrónico> [opcional] CN (commonName)= APELLIDOS Nombres (FIR[Número de DNI/Número de carné de extranjería]) SERIALNUMBER = <DNI: número de DNI- RUC:número de RUC/ CEX: número de carné de extranjería- RUC:número de RUC> G (givenname) = <Nombres> SN (surname) = <APELLIDOS> L (localityName) = <Distrito> S (stateOrProvinceName) = <Provincia-Departamento> C (countryName) = PE T (title) =XX [opcional]
2	Autenticación para persona natural (Seguridad Media)	CN (commonName)= APELLIDOS Nombres (AUT[Número de DNI/Número de carné de extranjería]) SERIALNUMBER = <DNI: número de DNI- RUC:número de RUC/ CEX: número de carné de extranjería- RUC:número de RUC> G (givenname) = <Nombres> SN (surname) = <APELLIDOS> L (localityName) = <Distrito> S (stateOrProvinceName) = <Provincia-Departamento> C (countryName) = PE T (title) =XX [opcional]
3	Autenticación y firma digital para persona natural (Seguridad Media)	E (emailAddress) = <dirección de correo electrónico> [opcional] CN (commonName)= APELLIDOS Nombres ([FAU[Número de DNI/Número de carné de extranjería]) SERIALNUMBER = <DNI: número de DNI-

		RUC:número de RUC/ CEX: número de carné de extranjería- RUC:número de RUC> G (givenname) = <Nombres> SN (surname) = <APELLIDOS> L (localityName) = <Distrito> S (stateOrProvinceName) = <Provincia-Departamento> C (countryName) = PE T (title) =XX [opcional]

- Certificados de Entidad Final Clase II

Ítem	Sub - tipo de certificado	Subject [Distinguished Names Attributes]
1	Firma digital para persona natural (Seguridad Media-Alta)	E (emailAddress) = <dirección de correo electrónico> [opcional] CN (commonName)= APELLIDOS Nombres (FIR[Número de DNI/Número de carné de extranjería]) SERIALNUMBER = <DNI: número de DNI-RUC:número de RUC/ CEX: número de carné de extranjería- RUC:número de RUC> G (givenname) = <Nombres> SN (surname) = <APELLIDOS> L (localityName) = <Distrito> S (stateOrProvinceName) = <Provincia-Departamento> C (countryName) = PE T (title) =XX [opcional]
2	Autenticación para persona natural (Seguridad Media-Alta)	CN (commonName)= APELLIDOS Nombres (AUT[Número de DNI/Número de carné de extranjería]) SERIALNUMBER = <DNI: número de DNI-RUC:número de RUC/ CEX: número de carné de extranjería- RUC:número de RUC> G (givenname) = <Nombres> SN (surname) = <APELLIDOS> L (localityName) = <Distrito> S (stateOrProvinceName) = <Provincia-Departamento> C (countryName) = PE T (title) =XX [opcional]
3	Autenticación y firma digital para persona natural (Seguridad Media)	E (emailAddress) = <dirección de correo electrónico> [opcional] CN (commonName)= APELLIDOS Nombres ([FAU[Número de DNI/Número de carné de extranjería]) SERIALNUMBER = <DNI: número de DNI-RUC:número de RUC/ CEX: número de carné de extranjería- RUC:número de RUC> G (givenname) = <Nombres> SN (surname) = <APELLIDOS> L (localityName) = <Distrito>

		S (stateOrProvinceName) = <Provincia-Departamento> C (countryName) = PE T (title) =XX [opcional]

- Certificados de Entidad Final Clase III

Ítem	Sub - tipo de certificado	Subject [Distinguished Names Attributes]
1	Firma digital para persona jurídica (Seguridad Media)	E (emailAddress) = <dirección de correo electrónico> CN (commonName)= APELLIDOS Nombres (FIR[Número de RUC]) SERIALNUMBER = <DNI:número de DNI-RUC:número de RUC-PARTIDA ELECTRONICA:número de partida electrónica / CEX:número de carné de extranjería-RUC:número de RUC-PARTIDA ELECTRONICA:número de partida electrónica> G (givenname) = <Nombres> SN (surname) = <APELLIDOS> L (localityName) = <Distrito de la entidad> S (stateOrProvinceName) = <Provincia-Departamento de la entidad> C (countryName) = PE O (organizationName) = <Nombre de la Organización o Razón Social> OU (organizationalUnitName) =<Área o dependencia de la entidad> [opcional] OU (organizationalUnitName) = <Sub área o dependencia de la entidad> [opcional] T (title) =<Cargo o función> [opcional]
2	Autenticación para persona jurídica (Seguridad Media)	CN (commonName)= APELLIDOS Nombres (AUT[Número de RUC]) SERIALNUMBER = <DNI:número de DNI-RUC:número de RUC-PARTIDA ELECTRONICA:número de partida electrónica / CEX:número de carné de extranjería-RUC:número de RUC-PARTIDA ELECTRONICA:número de partida electrónica> G (givenname) = <Nombres> SN (surname) = <APELLIDOS> L (localityName) = <Distrito de la entidad> S (stateOrProvinceName) = <Provincia-Departamento de la entidad> C (countryName) = PE O (organizationName) = <Nombre de la Organización o Razón Social> OU (organizationalUnitName) =<Área o dependencia de la entidad> [opcional]

		OU (organizationalUnitName) = <Sub área o dependencia de la entidad> [opcional] T (title) =<Cargo o función> [opcional]
3	Autenticación y firma digital para persona jurídica (Seguridad Media)	E (emailAddress) = <dirección de correo electrónico> CN (commonName)= APELLIDOS Nombres (FAU[Número de RUC]) SERIALNUMBER = <DNI:número de DNI-RUC:número de RUC-PARTIDA ELECTRONICA:número de partida electrónica / CEX:número de carné de extranjería-RUC:número de RUC-PARTIDA ELECTRONICA:número de partida electrónica> G (givenname) = <Nombres> SN (surname) = <APELLIDOS> L (localityName) = <Distrito de la entidad> S (stateOrProvinceName) = <Provincia-Departamento de la entidad> C (countryName) = PE O (organizationName) = <Nombre de la Organización o Razón Social> OU (organizationalUnitName) =<Área o dependencia de la entidad> [opcional] OU (organizationalUnitName) = <Sub área o dependencia de la entidad> [opcional] T (title) =<Cargo o función> [opcional]
4	Firma digital para persona jurídica (Seguridad Media-Alta)	E (emailAddress) = <dirección de correo electrónico> CN (commonName)= APELLIDOS Nombres (FIR[Número de RUC]) SERIALNUMBER = <DNI:número de DNI-RUC:número de RUC-PARTIDA ELECTRONICA:número de partida electrónica / CEX:número de carné de extranjería-RUC:número de RUC-PARTIDA ELECTRONICA:número de partida electrónica> G (givenname) = <Nombres> SN (surname) = <APELLIDOS> L (localityName) = <Distrito de la entidad> S (stateOrProvinceName) = <Provincia-Departamento de la entidad> C (countryName) = PE O (organizationName) = <Nombre de la Organización o Razón Social> OU (organizationalUnitName) =<Área o dependencia de la entidad> [opcional] OU (organizationalUnitName) = <Sub área o dependencia de la entidad> [opcional] T (title) =<Cargo o función> [opcional]

5	Autenticación para persona jurídica (Seguridad Media-Alta)	CN (commonName)= APELLIDOS Nombres (AUT[Número de RUC]) SERIALNUMBER = <DNI:número de DNI-RUC:número de RUC-PARTIDA ELECTRONICA:número de partida electrónica / CEX:número de carné de extranjería-RUC:número de RUC-PARTIDA ELECTRONICA:número de partida electrónica> G (givenname) = <Nombres> SN (surname) = <APELLIDOS> L (localityName) = <Distrito de la entidad> S (stateOrProvinceName) = <Provincia-Departamento de la entidad> C (countryName) = PE O (organizationName) = <Nombre de la Organización o Razón Social> OU (organizationalUnitName) =<Área o dependencia de la entidad> [opcional] OU (organizationalUnitName) = <Sub área o dependencia de la entidad> [opcional] T (title) =<Cargo o función> [opcional]
6	Autenticación y firma digital para persona jurídica (Seguridad Media-Alta)	E (emailAddress) = <dirección de correo electrónico> CN (commonName)= APELLIDOS Nombres (FAU[Número de RUC]) SERIALNUMBER = <DNI:número de DNI-RUC:número de RUC-PARTIDA ELECTRONICA:número de partida electrónica / CEX:número de carné de extranjería-RUC:número de RUC-PARTIDA ELECTRONICA:número de partida electrónica> G (givenname) = <Nombres> SN (surname) = <APELLIDOS> L (localityName) = <Distrito de la entidad> S (stateOrProvinceName) = <Provincia-Departamento de la entidad> C (countryName) = PE O (organizationName) = <Nombre de la Organización o Razón Social> OU (organizationalUnitName) =<Área o dependencia de la entidad> [opcional] OU (organizationalUnitName) = <Sub área o dependencia de la entidad> [opcional] T (title) =<Cargo o función> [opcional]

- Certificados de Entidad Final Clase IV

Ítem	Sub - tipo de certificado	Subject [Distinguished Names Attributes]
1	Firma Digital para Personas Jurídicas [Server Devices] (Seguridad Media)	C (countryName) = PE CN (commonName)= <Nombre FQDN/Nombre WINS/Dirección IP> SERIALNUMBER = <RUC:número de RUC-PARTIDA ELECTRÓNICA:número de Partida Electrónica> O (organizationName) = <Nombre de la Organización o Razón Social> S (stateOrProvinceName) = <Provincia-Departamento de la entidad> L (localityName) = <Distrito de la entidad>
2	Firma Digital para Personas Jurídicas [Server Devices] (Seguridad Media-Alta)	C (countryName) = PE CN (commonName)= <Nombre FQDN/Nombre WINS/Dirección IP> SERIALNUMBER = <RUC:número de RUC-PARTIDA ELECTRÓNICA:número de Partida Electrónica> O (organizationName) = <Nombre de la Organización o Razón Social> S (stateOrProvinceName) = <Provincia-Departamento de la entidad> L (localityName) = <Distrito de la entidad>

- Certificados de Entidad Final Clase V

Ítem	Sub - tipo de certificado	Subject [Distinguished Names Attributes]
1	Firma Digital para Personas Jurídicas [Sistemas SIE] (Seguridad Media)	C (countryName) = PE CN (commonName)= <Nombre FQDN/Nombre WINS/Dirección IP> SERIALNUMBER = <RUC:número de RUC-PARTIDA ELECTRÓNICA:número de Partida Electrónica> O (organizationName) = <Nombre de la Organización o Razón Social> S (stateOrProvinceName) = <Provincia-Departamento de la entidad> L (localityName) = <Distrito de la entidad>
2	Firma Digital para Personas Jurídicas [Sistemas SIE] (Seguridad Media-Alta)	C (countryName) = PE CN (commonName)= <Nombre FQDN/Nombre WINS/Dirección IP> SERIALNUMBER = <RUC:número de RUC-PARTIDA ELECTRÓNICA:número de Partida Electrónica> O (organizationName) = <Nombre de la Organización o Razón Social> S (stateOrProvinceName) = <Provincia-Departamento de la entidad> L (localityName) = <Distrito de la entidad>

El campo DN (Nombre Distinguido) deberá identificar de forma única y plena a una entidad final, es potestad de la EREP realizar las validaciones necesarias para que esta regla se cumpla.

ii. Nombres RFC-822 : No aplica.
iii. Nombres X.400 : No aplica.

3.1.2. Necesidad de que los nombres tengan un significado

Los nombres deben ser "significativos" debido a que el suscriptor o titular del certificado debe contar con una identificación única.

Los campos del certificado mostrado en las tablas del ítem 3.1.1 para cada clase son "significativos" debido a que garantizan que se pueda determinar la identidad del suscriptor.

3.1.3. Anonimato o seudónimo de los suscriptores

La ECEP no emite certificados digitales anónimos. Sin embargo, para el caso de certificados digitales de agentes automatizados se permite el uso de seudónimos.

3.1.4. Reglas para interpretar las diferentes modalidades de nombres

La regla utilizada para interpretar los Nombres Distinguidos (Distinguished Name - DN) de certificados que se emite es, ISO/IEC 9595 (X.500) Distinguished Name, lo cual se puede verificar en el perfil del certificado (ver ítem. 7.1).

3.1.5. Singularidad de los nombres

Los nombres de los suscriptores o titulares son únicos para poder identificarlos plenamente. Para garantizar la unicidad en el Nombre Distinguido (Distinguished Name - DN) de los suscriptores o titulares se utiliza una combinación de valores.

3.1.6. Reconocimiento, autentificación y rol de marcas registradas

Para mayor detalle revisar el ítem 3.1.6 de la correspondiente DPR.

3.2. Validación inicial de la identidad

Para mayor detalle revisar el ítem 3.2 de la correspondiente DPR.

3.2.1. Método para probar la posesión de la clave privada

En caso, la clave privada asociada a un certificado se genere en las instalaciones de la EREP, este procedimiento se realizará en presencia del titular o suscriptor del certificado utilizando un medio seguro (FIPS 140-2 nivel 1), garantizando que en todo momento la clave privada está bajo el control del titular o suscriptor. Para el caso del DNIe el procedimiento utilizará un medio seguro (FIPS 140-2 nivel 1), garantizándose el control de la clave privada según se indica en la

correspondiente DPR.

En el caso que el certificado digital sea generado directamente por el suscriptor, el request o pedido de certificado debe ser firmado por la clave privada de éste, como prueba de posesión de la clave privada.

3.2.2. Autenticación de la identidad de la persona jurídica

Para mayor detalle revisar el ítem 3.2.2 de la correspondiente DPR.

3.2.3. Autenticación de la identidad individual

Para mayor detalle revisar el ítem 3.2.3 de la correspondiente DPR.

3.2.4. Información no verificada del suscriptor

Para mayor detalle revisar el ítem 3.2.4 de la correspondiente DPR.

3.2.5. Validación de la Autoridad

Para mayor detalle revisar el ítem 3.2.5 de la correspondiente DPR.

3.2.6. Criterios para la interoperación (Con una CA externa)

La ECEP acreditada, con su Declaración de Prácticas y Políticas de Certificación aprobadas y conforme a las Guías de Acreditación emitidos por la AAC, está facultada para poder interactuar en el marco de la IOFE y realizar el reconocimiento cruzado.

Antes de establecer una interoperabilidad con Entidades de Certificación Externas, éstas deben cumplir los siguientes requisitos:

- La Entidad de Certificación Externa ha de proporcionar un nivel de seguridad en la gestión de los certificados, a lo largo de su ciclo de vida, como mínimo, igual al de la ECEP. Esta exigencia se recogerá en la CPS y CP correspondientes, y en su cumplimiento por la Entidad de Certificación Externa.
- Deberá contar con un informe de auditoría de una Entidad Externa de reconocido prestigio y el documento de aprobación emitido por la AAC, relativa a sus operaciones como medio de verificación del nivel de seguridad existente.
- Establecer un convenio en el que se fijen los compromisos adquiridos en materia de seguridad para los certificados incluidos en la interacción.

La AAC puede ampliar estos requisitos.

3.3. Identificación y autenticación para solicitudes de re-emisión de certificados

La ECEP no brindará el servicio de re-emisión de certificados digitales.

3.3.1. Identificación y autenticación para solicitudes de re-emisión de certificado rutinaria

No se brindara servicio de re-emisión.

3.3.2. Identificación y autenticación para la re-emisión de certificado luego de la cancelación

No se brindara servicio de re-emisión.

3.4. Identificación y autenticación de la solicitud de cancelación

La ECEP procesa los requerimientos de cancelación de certificados digitales requeridos por la EREP, ésta última es la encargada de realizar las verificaciones previas para garantizar el no repudio. Una EREP sólo puede solicitar la cancelación de un certificado digital cuya generación haya sido autorizada por ella.

Para mayor detalle revisar el ítem 3.4 de la correspondiente DPR.

4. Requisitos operacionales del ciclo de vida de los certificados

Los procesos del ciclo de vida de un certificado digital ECEP, tanto para una persona natural, como jurídica, se definen en:

4.1. Solicitud del certificado

El solicitante que desee gestionar la emisión de un certificado digital deberá apersonarse a una oficina autorizada de la EREP-RENIEC o de otra EREP acreditada por la AAC y que haya suscrito un convenio con la ECEP. El solicitante debe entregar la información solicitada por la EREP y asume la responsabilidad por la veracidad y exactitud de la información proporcionada, sin perjuicio de la respectiva comprobación de la información por parte de la EREP.

4.1.1. Habilitados para presentar la solicitud de un certificado.

No se procesarán las solicitudes de certificado de Personas Naturales o Personas Jurídicas que tengan alguna solicitud anterior pendiente sin su respectiva generación de certificado digital (pendiente la generación de certificado) para un mismo tipo de uso de certificado (Firma, Autenticación, Firma y Autenticación).

Para mayor detalle revisar el ítem 4.1.1 de la correspondiente DPR.

4.1.2. Proceso de solicitud y responsabilidades

Es atribución de la EREP encaminar la solicitud con datos correctos declarados por el suscriptor en cuanto al tipo de usuario (Persona Natural, Persona Jurídica) de certificado digital y al uso que se le dará (Firma, Autenticación, Firma y Autenticación).

Para mayor detalle revisar el ítem 4.1.2 de la correspondiente DPR.

4.2. Procesamiento de la solicitud del certificado

4.2.1. Realización de las funciones de identificación y autenticación

Para mayor detalle revisar el ítem 4.2.1 de la correspondiente DPR.

4.2.2. Aprobación o rechazo de la solicitud de emisión de un certificado

El solicitante que desee gestionar la emisión de un certificado digital deberá apersonarse a una oficina autorizada de la EREP-RENIEC o de otra EREP acreditada por la AAC y que haya suscrito un convenio con la ECEP. El solicitante debe entregar la información solicitada por la EREP y asume la responsabilidad por la veracidad y exactitud de la información proporcionada, sin perjuicio de la respectiva comprobación de la información por parte de la EREP.

La ECEP únicamente procesará las solicitudes encaminadas por la EREP y que hayan sido previamente autorizadas por ésta.

Para mayor detalle revisar el ítem 4.2.2 de la correspondiente DPR**.**

4.2.3. Tiempo para el procesamiento de la solicitud del certificado

Una vez autorizada la solicitud por la EREP, y comunicada a la ECEP, ésta última estará en condiciones de emitir el certificado digital de forma inmediata, a través de un proceso automático.

4.3. Generación de claves y emisión del certificado

4.3.1. Acciones de la EC durante la emisión del certificado

Una vez que la EREP envíe a la ECEP la autorización para el certificado digital del suscriptor con la información requerida, la ECEP estará en condiciones de emitir el certificado digital de forma automática, y en los casos que corresponda, el suscriptor podrá iniciar la conexión con la plataforma de emisión de certificados digitales. Para facilitar el uso de la plataforma, la ECEP proporcionará guías de referencia en la dirección:
http://portales.reniec.gob.pe/web/identidaddigital/faqPKI

La ECEP deberá realizar las siguientes acciones:

- Autenticación del suscriptor con las credenciales entregadas
- Recepción de pedido de certificado (request) firmado con la clave privada recién generada del suscriptor.
- Emisión del certificado asociado al uso operativo solicitado y el Nombre Distinguido (Distinguished Name - DN) asociado con el suscriptor.
- Proteger la confidencialidad e integridad de los datos del solicitante del certificado.

- Publicar en el repositorio el certificado emitido, utilizando los controles establecidos para garantizar la seguridad de la información. El detalle está indicado en el documento "*Gestión de repositorios*".
- Almacenar de forma automática en los registros de la ECEP, la fecha y hora en la que se expidió el certificado.

En caso el certificado se genere en un medio portador proporcionado por la EREP, ésta debe garantizar su entrega al suscritor.

4.3.2. Notificación al suscriptor por parte de la EC respecto a la emisión de un certificado

Una vez generado el certificado digital, el suscriptor recibirá en la misma pantalla de generación la confirmación de la descarga del certificado y de su instalación. En caso de presentarse inconvenientes en este paso, el suscritor deberá comunicarse con el Centro de Contacto que se muestra en la página web oficial de la entidad: http://www.reniec.gob.pe

Para el caso de certificados del DNIe la notificación se realizará a través de la EREP-RENIEC según se indique en su correspondiente DPR.

4.4. Aceptación del certificado

4.4.1. Conducta constitutiva de la aceptación de un certificado

El Contrato firmado por el suscriptor garantiza el reconocimiento y acuerdo con los términos y condiciones contenidos en dicho documento que rige los derechos y obligaciones de la EREP, ECEP y del suscriptor, además de reconocer la presente Declaración de Prácticas y Políticas de Certificación, que rige técnica y operativamente los servicios de certificación digital prestados por la ECEP.

4.4.2. Publicación del certificado por parte de la EC

La información concerniente a los certificados digitales emitidos será publicada en el Repositorio de la ECEP, tal como está señalado en el documento "*Generación y cancelación de certificado digital*".

4.4.3. Notificación de la EC a otras entidades respecto a la emisión de un certificado

La ECEP, posterior la emisión del certificado procederá a publicar el mismo, como prueba de su generación satisfactoria, permitiendo el acceso al suscriptor y terceros que confían respetando la **"***Política de Privacidad***".** Esta operación está especificada en el documento "*Generación y cancelación de certificado digital*".

4.5. Par de claves y uso del certificado

4.5.1. Uso de la clave privada y certificado por parte del suscriptor

La ECEP exige al suscriptor y titular, lo siguiente:

- Emplear el certificado de acuerdo con lo establecido en la CPS de la ECEP u otro documento relevante y el contrato del suscriptor.
- Ser razonablemente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados.
- Notificar a la correspondiente EREP a través de la cual solicitó su certificado digital, sin retraso injustificable:
  - La pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada (computador, token criptográfico o tarjeta inteligente).
  - El compromiso potencial de su clave privada.
  - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación o por cualquier otra causa.
  - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- Dejar de utilizar la clave privada, transcurrido el plazo de vigencia del certificado digital.

4.5.2. Uso de la clave pública y el certificado por el tercero que confía

La IOFE permite al tercero que confía el acceso a los certificados publicados en el Repositorio.

La ECEP requiere del tercero que confía, como mínimo lo siguiente:

- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de la IOFE.
- No comprometer la seguridad de la Jerarquía de la IOFE.
- Aplicar los criterios de verificación adecuados para la validación de un certificado digital durante su uso en las transacciones electrónicas.
- Denunciar cualquier situación en la que se deba cancelar el certificado de un titular, siempre y cuando se tengan pruebas fehacientes del compromiso de la clave privada o de un uso ilegal del manejo de la misma. Por ejemplo, debe denunciar la pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena una clave privada que no le pertenece (computador, token criptográfico o tarjeta inteligente, DNIe).

Adicionalmente la ECEP brinda información actualizada a través de la página web del RENIEC y a través de sus repositorios (ver ítem 2.1).

4.6. Renovación del certificado

Por medidas de seguridad, según CWA 14167-1, esto no es aplicable en el marco de la IOFE.

4.6.1. Circunstancias para la re-certificación de los certificados

Por medidas de seguridad, según CWA 14167-1, esto no es aplicable en el marco de la IOFE.

4.6.2. Personas habilitadas para solicitar la renovación

Por medidas de seguridad, según CWA 14167-1, esto no es aplicable en el marco de la IOFE.

4.6.3. Procesamiento de la solicitud de renovación de certificado.

Por medidas de seguridad, según CWA 14167-1, esto no es aplicable en el marco de la IOFE.

4.6.4. Notificación al suscriptor respecto a la emisión de un nuevo certificado

Por medidas de seguridad, según CWA 14167-1, esto no es aplicable en el marco de la IOFE.

4.6.5. Conducta constitutiva de aceptación de renovación de certificado

Por medidas de seguridad, según CWA 14167-1, esto no es aplicable en el marco de la IOFE.

4.6.6. Publicación de la renovación por parte de la EC de un certificado

Por medidas de seguridad, según CWA 14167-1, esto no es aplicable en el marco de la IOFE.

4.6.7. Notificación de la EC a otras entidades respecto a la renovación del certificado

Por medidas de seguridad, según CWA 14167-1, esto no es aplicable en el marco de la IOFE.

4.7. Re-emisión de certificado.

Este servicio no es brindado por la ECEP.

4.7.1. Circunstancias para la re-emisión de un certificado

Este servicio no es brindado por la ECEP.

4.7.2. Personas habilitadas para solicitar la re-emisión de certificado

Este servicio no es brindado por la ECEP.

4.7.3. Procesamiento de las solicitudes para re-emisión de certificados

Este servicio no es brindado por la ECEP.

4.7.4. Notificación al suscriptor sobre la re-emisión de un certificado

Este servicio no es brindado por la ECEP.

4.7.5. Conducta constitutiva de la aceptación de una re-emisión de certificado

Este servicio no es brindado por la ECEP.

4.7.6. Publicación por parte de la EC del certificado re-emitido

Este servicio no es brindado por la ECEP.

4.7.7. Notificación por parte de la EC a otras entidades respecto a la emisión de certificados

Este servicio no es brindado por la ECEP.

4.8. Modificación del certificado

Este servicio no es brindado por la ECEP.

4.8.1. Circunstancias para la modificación de un certificado

Este servicio no es brindado por la ECEP.

4.8.2. Personas habilitadas para solicitar la modificación de un certificado

Este servicio no es brindado por la ECEP.

4.8.3. Circunstancias para la modificación de un certificado

Este servicio no es brindado por la ECEP.

4.8.4. Notificación al suscriptor sobre la emisión de un nuevo certificado

Este servicio no es brindado por la ECEP.

4.8.5. Conducta constitutiva de la aceptación de un certificado modificado

Este servicio no es brindado por la ECEP.

4.8.6. Publicación por parte de la EC del certificado modificado

Este servicio no es brindado por la ECEP.

4.8.7. Notificación por parte de la EC a otras entidades respecto a la emisión de certificados modificados

Este servicio no es brindado por la ECEP.

4.9. Cancelación y suspensión del certificado

4.9.1. Circunstancias para la cancelación

La ECEP aceptará el pedido de cancelación del certificado digital realizado por la EREP que aprobó su emisión, el pedido de cancelación debe ser autorizado por ésta y enviado únicamente mediante canales seguros. El detalle del proceso se indica en el documento "*Generación y cancelación de certificado digital*".

Para mayor detalle revisar el ítem 4.9.1 de la correspondiente DPR.

4.9.2. Personas habilitadas para solicitar la cancelación

Para mayor detalle revisar el ítem 4.9.2 de la correspondiente DPR.

4.9.3. Procedimiento para la solicitud de cancelación

La ECEP aceptará el pedido de cancelación del certificado digital realizado por la EREP que aprobó su emisión, el pedido de cancelación debe ser autorizado por ésta y enviado únicamente mediante canales seguros. El detalle del proceso se indica en el documento "*Generación y cancelación de certificado digital*".

Para mayor detalle revisar el ítem 4.9.3 de la correspondiente DPR.

4.9.4. Periodo de gracia de la solicitud de cancelación

Autorizada la solicitud de cancelación por parte de la EREP, la ECEP procederá de manera automática a cancelar el certificado digital y a publicar su nuevo estado en el repositorio correspondiente, según lo especificado en el ítem 2.3 del presente documento.

Autorizada la solicitud de cancelación por parte de la EREP y comunicada a la ECEP, ésta última procede a cancelar de manera inmediata el certificado digital. Por tanto, luego de efectuada la comunicación a la ECEP no existe ningún periodo de gracia asociado a este proceso durante el que se pueda anular la cancelación de un certificado. Esta especificación se encuentra descrita en el documento "*Generación y cancelación de certificado digital*".

4.9.5. Tiempo dentro del cual una EC debe procesar la solicitud de cancelación

La ECEP procesará de manera inmediata cualquier pedido de cancelación indicado por la EREP una vez que sea de su conocimiento y bajo el cumplimiento del numeral 4.9.2 y 4.9.3 del presente documento. El proceso se encuentra descrito en el documento "*Generación y cancelación de certificado digital*".

Es potestad de la EREP realizar las validaciones necesarias para proceder a la cancelación de un certificado digital.

4.9.6. Requerimientos para la verificación de la cancelación de certificados por los terceros que confían

Una vez realizada la cancelación de un certificado por parte de la ECEP, ésta publica el estado del certificado en sus repositorios de acuerdo a lo señalado en el ítem 2.3 del presente documento, notificando de esta manera a todo aquel interesado. El detalle de la publicación se encuentra descrito en el documento "*Gestión de repositorios*".

4.9.7. Frecuencia de emisión de CRL

La ECEP actualiza su lista de certificados cancelados (CRL) cada 24 horas y es publicada en sus repositorios según lo mencionado en el ítem 2.1 del presente documento. Para esta actividad la ECEP hace uso del documento denominado "*Gestión de la lista de certificados revocados de la Planta de Certificación Digital*".

La ECEP brinda el servicio de CRL, con una disponibilidad mínima del 99% anual y con un tiempo programado de inactividad máximo de 0.5% anual.

4.9.8. Máxima Latencia para CRLs

La latencia entre la generación y la publicación de una CRL es contada en segundos debido a que la publicación se realiza de forma inmediata, solo en caso de inconvenientes el tiempo máximo entre la generación de la CRL y su publicación es de una (01) hora.

4.9.9. Disponibilidad de la verificación en línea cancelación /estado

La ECEP no brinda servicio de verificación en línea OCSP para ningún tipo o clase de certificado.

4.9.10. Requisitos para la verificación en línea de la cancelación

La ECEP no brinda servicio de verificación en línea OCSP para ningún tipo o clase de certificado.

4.9.11. Otras formas disponibles de publicar la cancelación

La lista de certificados cancelados (CRL) emitidos por la ECEP son publicados en más de un repositorio especificados en cada uno de los certificados digitales emitidos por ésta.

Como las guías de acreditación para Entidades de Certificación refiere: "Cuando la publicación de una cancelación pueda reducir el daño potencial a los terceros que confían, INDECOPI permite que una EC o un suscriptor afectado puedan emplear diferentes formas para realizar dicha publicación.", por lo expuesto la ECEP se permitirá publicar en algún otro repositorio adicional de requerirlo para satisfacer el requerimiento y necesidad.

4.9.12. Requisitos especiales para el caso de compromiso de la clave privada

La ECEP notificará en un lapso máximo de 24 horas a INDECOPI respecto a incidencias que produzcan el compromiso de sus claves o su imposibilidad de uso, de acuerdo a lo detallado en el documento "*Gestión de claves de entidad raíz y de nivel intermedio*".

En caso de compromiso de las claves privadas de la ECEP, ésta cancelará los certificados emitidos y comunicará a la EREP para que informe a los suscriptores afectados, los cuales estarán en la facultad de apersonarse a las oficinas de la correspondiente EREP para solicitar la emisión de un nuevo certificado digital.

4.9.13. Circunstancias para la suspensión

La ECEP no brinda servicio de suspensión de certificados digitales.

4.9.14. Personas habilitadas para solicitar la suspensión

La ECEP no brinda servicio de suspensión de certificados digitales.

4.9.15. Procedimiento para solicitar la suspensión

La ECEP no brinda servicio de suspensión de certificados digitales.

4.9.16. Límite del periodo de suspensión

La ECEP no brinda servicio de suspensión de certificados digitales.

4.10. Servicios de estado de certificado

La ECEP mantiene una copia de la lista de entidades acreditadas (TSL) que le es proporcionada por INDECOPI.

- Dirección donde se mantiene la copia: http://crl.reniec.gob.pe/tsl
- Dirección original de publicación por parte de la AAC: https://iofe.indecopi.gob.pe/TSL/tsl-pe.xml

La ECEP, publica en la CRL el estado de los certificados digitales según lo señalado en el ítem 2.2 del presente documento.

4.10.1. Características Operacionales

Cualquier información publicada por la ECEP respecto al estado de uno de sus certificados (a través de la CRL) es firmada digitalmente por la ECEP. La hora y fecha son consignadas por la ECEP las cuales son obtenidas del servidor NTP con el que cuenta la ECEP. Para garantizar estas operaciones, se cuentan con los documentos "*Sincronización de hardware y software con servicio NTP*" y "*Pruebas de operatividad de servicios y funcionalidades de hardware y software*".

4.10.2. Disponibilidad del servicio

La ECEP brinda el servicio de información sobre el estado del certificado a través de las correspondientes CRLs, con una disponibilidad mínima del 99% anual y con un tiempo programado de inactividad máximo de 0.5% anual.

4.10.3. Rasgos Operacionales

La ECEP no brinda servicio de verificación en línea OCSP para ningún tipo o clase de certificado.

4.11. Finalización de la suscripción

La ECEP dará por extinguida la validez de un certificado digital en los siguientes casos:

- Caducidad de la vigencia del certificado digital.
- Por cancelación del certificado por cualquiera de las circunstancias señaladas en el ítem 4.9.1 del presente documento.
- Por fallecimiento del suscriptor o extinción de la persona jurídica que es titular del certificado.

El primer caso es de reconocimiento automático por las aplicaciones que hacen uso de certificados digitales; los otros casos son tratados por la EREP, según lo indicado en el ítem 4.9.1 de su correspondiente DPR**.**

4.12. Depósito y recuperación de claves

4.12.1. Políticas y prácticas de recuperación de Depósito de claves

No se almacenará la clave privada de ningún certificado digital de suscriptor que genere firmas digitales y/o que sirva para autenticación.

4.12.2. Políticas y prácticas para la encapsulación de claves de sesión

Se encuentra fuera del alcance del presente documento, el hecho de que un suscriptor realice una encapsulación de la clave de sesión para las transacciones de los titulares representados por dicho suscriptor. No obstante, sí le serán aplicables a este suscriptor, todas las obligaciones referidas a la protección de las claves privadas correspondientes a los certificados digitales emitidos por la ECEP, que pudieran ser utilizadas en la encapsulación.

5. CONTROLES DE LAS INSTALACIONES, DE LA GESTIÓN Y CONTROLES OPERACIONALES

5.1. Controles físicos

5.1.1. Ubicación y construcción del local

Las características de las instalaciones de la ECEP son:

- Puertas cortafuego blindadas para el acceso del personal autorizado.
- La puerta de acceso principal cuenta con personal de seguridad que verifica que sólo personas autorizadas puedan acceder a la misma.
- El acceso a zonas de alta seguridad como la sala de máquinas (lugar de procesamiento de información sensible), está restringida por controles biométricos.
- Los ambientes que constituyen las instalaciones de la ECEP, cuentan con las estructuras y secciones necesarias, que garantizan que sólo el personal autorizado las puede acceder.

Para el caso del personal que labora al interior de la Planta de Certificación Digital, se realiza una identificación previa y registro en el sistema de control de acceso, lo cual le permitirá el acceso a las instalaciones de la Planta. El ingreso de visitas y proveedores se efectúa previo permiso y conforme a lo establecido en el documento "*Control de acceso físico*".

Las instalaciones de la ECEP cuentan con las siguientes medidas de prevención:

i. Ante desastres naturales:

- Inundación: protección mediante tarrajeo impermeabilizado y hermetizado; además detectores de aniego debajo del piso técnico.
- Terremoto: se cuenta con bases antisísmicas para los gabinetes de los equipos ubicados en la sala de máquinas.

ii. Desastres accidentales creados por el hombre:

- Incendios: se cuenta con sistema de extinción de fuego FM-200 y puertas corta fuego con barra anti-pánico desde el interior.
- Explosiones: se cuenta con sistema de extinción de fuego FM-200, cerramiento del perímetro mediante paredes, piso, techo de concreto y metálico, y puerta cortafuego.
- Disturbios civiles: los ambientes cuentan con un sistema de puertas blindadas, sistema de cámaras que graban las actividades tanto al personal como a los invitados desde su ingreso a las instalaciones de la ECEP, además se cuenta con un sistema de control de acceso, que garantiza que sólo el personal autorizado pueda ingresar a las instalaciones de la ECEP.

5.1.2. Acceso físico

Perímetros de seguridad física:
Centro de datos principal: cerramiento del perímetro mediante paredes, piso y techo de concreto, y puerta cortafuego.
Centro de datos de contingencia: cerramiento del perímetro mediante paredes de metal, piso y techo de concreto reforzados con metal.

Controles físicos de entrada:
Se dispone de un completo sistema de control de acceso físico de personas a la entrada y a la salida que conforman varios niveles de control, lo cual se encuentra detallado en el documento "*Control de acceso físico*".

Los visitantes son identificados y registrados, además de tener a un coordinador permanente durante la visita a las instalaciones de la ECEP, como es especificado en el documento **"***Control de acceso físico***".**

5.1.3. Energía y aire acondicionado

El equipo de energía y aire acondicionado, incluyendo el equipo de seguridad de los mismos, están protegidos y en constante mantenimiento a efectos de asegurar su correcto funcionamiento. Mayor información se encuentra en el documento denominado "*Infraestructura de Centros de Datos*".

5.1.4. Exposición al agua

El cerramiento del perímetro de la ECEP en su Centro de Datos Principal ha sido construida con material de concreto, además cuenta con protección por medio de impermeabilizado para lograr un mayor margen de seguridad ante un evento de aniego en la zona superior, además se cuenta con detectores de agua debajo del piso técnico. En caso del Centro de Datos de Contingencia este se encuentra en un ambiente hermético. Mayor información se encuentra en el documento denominado "*Infraestructura de Centros de Datos*".

5.1.5. Prevención y protección contra fuego

El Centro de Datos Principal de la ECEP cuenta con sensores de humo. Los ambientes donde labora permanentemente el personal (operadores y supervisores) cuentan con extintores de mano en ubicaciones señalizadas. Las salas de máquinas cuentan con un sistema de detección y extensión automático de fuego mediante un sistema FM200.
El Centro de Datos de Contingencia de la ECEP cuenta con un sistema de extinción de fuegos.

5.1.6. Archivo de material

Los sistemas de registro de los servidores de la ECEP cuentan con mecanismos de control de acceso que permiten prevenir el

acceso y las modificaciones a los datos no autorizados.
Los controles de acceso al sistema de archivos de los servidores restringen:

- Acceso a áreas del sistema.
- Adición de software o servicios.
- Tener acceso a los archivos de otros usuarios (en los sistemas operativos principales).

El control de acceso a sistemas de información y servicios cubre todas las etapas del ciclo de vida de acceso del usuario, registro de nuevos usuarios, registro de los usuarios que necesitan el acceso. Según los procedimientos especificados en el documento "*Control de Acceso Lógico*".

Los servidores que contienen información sensible son:

- Físicamente protegidos, detallado en el documento "*Control de Acceso Físico*"
- Lógicamente protegidos, detallado en el documento "*Control de Acceso Lógico*".
- Supervisados para evitar el empleo inadecuado, detallado en el documento "*Operación de la Planta de Certificación Digital"*.

5.1.7. Gestión de residuos

La información contenida en formato papel, así como en soportes magnéticos u ópticos, para ser eliminada es destruida tanto física como lógicamente, a fin de evitar la posibilidad de recuperar dicha información desde los formatos que la contuvieron, tal como está establecido en el documento "*Borrado seguro y destrucción de medios de almacenamiento*".

Para el caso de medios de almacenamiento, antes de ser desechados, se someten a un proceso de destrucción controlada, según lo indicado en el documento "*Borrado seguro y destrucción de medios de almacenamiento"*.

5.1.8. Copia de seguridad externa

La ECEP, dispone de copias de seguridad en tres locales distintos:

- Centro principal.
- Centro de contingencias.
- Centro de custodia externa al RENIEC.

El detalle de las actividades desarrolladas para la ejecución de las copias de seguridad se encuentra descrito en el documento "*Respaldo de información de la Planta de Certificación Digital*"

5.2. Controles procesales

5.2.1. Roles de confianza

Se define "rol de confianza" como aquel rol cuyas funciones o actividades conllevan a un riesgo en el manejo, uso o acceso a la información y por ende a la continuidad de las operaciones.

Dichos roles se describen en el documento "Asignación de roles".

5.2.2. Número de personas requeridas por labor

La asignación de roles en la ECEP ha sido aprobado, documentado y estandarizado de acuerdo al documento **"***Asignación de roles***".**

5.2.3. Identificación y autenticación para cada rol

Los requerimientos de cada rol, competencias y el detalle de sus actividades se encuentran descritos en el documento denominado **"***Asignación de roles***"**.

5.2.4. Roles que requieren funciones por separado

Con el fin de mantener una adecuada separación de funciones, se han definido diferentes roles, los cuales se detallan en el documento "*Asignación de roles*".

5.3. Controles de personal

En esta sección se establecen los controles implementados por el RENIEC en relación con el personal que desempeña funciones en la ECEP; comprende, entre otros, los requisitos a cumplir para su incorporación, la forma como éstos deben ser comprobados, la capacitación a los que estarán sujetos y las sanciones por acciones no autorizadas.

En lo que corresponda, el presente ítem alcanza también, al personal a cargo de terceros y contratistas que realicen labores por tiempo determinado en las instalaciones de la ECEP.

En ambos casos, el personal que ejerza labores en la ECEP y que para el desarrollo de sus actividades necesite tener acceso a información clasificada como "confidencial" o "sensible" debe suscribir previamente el respectivo acuerdo de confidencialidad de no divulgación de la información, conforme a lo establecido en el documento *"Lineamientos generales de seguridad de la información".*

5.3.1. Cualidades y requisitos, experiencia y certificados

Los procedimientos dispuestos por el RENIEC para la gestión del personal que desarrolla funciones en la ECEP, buscan asegurar que se acredite de manera suficiente y fehaciente las cualificaciones y experiencia profesional.

Las prácticas de selección y reclutamiento de personal se llevan a cabo en la Gerencia de Recursos Humanos del RENIEC tomándose como referencia lo establecido en el *"Reglamento Interno de Trabajo"*, y lo

requerido en los perfiles fijados por la ECEP, donde se considera requisitos de experiencia y cualificación para cada personal, además del rol que desempeñará.

El personal que ocupa un rol de confianza deberá encontrarse libre de intereses personales que entren en conflicto con el desarrollo del rol que tenga encomendado.

El contrato de trabajo respectivo regulará las relaciones de trabajo entre el RENIEC y su personal.

En caso de personal a cargo de terceros, será responsabilidad del contratista acreditar la formación y experiencia de aquellos, de acuerdo con los requerimientos de la ECEP, debiendo (durante el proceso de contratación) presentar la documentación que evidencie el cumplimiento de dicho aspecto.

5.3.2. Procedimiento para verificación de antecedentes

El RENIEC verifica la documentación aportada por el personal aspirante a realizar labores al interior de la entidad, tomándose como referencia lo establecido en el *"Reglamento Interno de Trabajo"*.

A tal efecto, la Gerencia de Recursos Humanos ejecuta los controles mínimos siguientes:

- Verificación de la identidad personal.
- Confirmación de las referencias.
- Confirmación de empleos anteriores.
- Revisión de referencias profesionales.
- Confirmación de grados académicos obtenidos.
- Verificación de antecedentes penales y policiales.
- En los casos de roles de confianza, verificación de antecedentes crediticios.

Corresponde al contratista realizar la verificación de los antecedentes de sus empleados, conforme a sus procedimientos.

5.3.3. Requisitos de capacitación

Toda persona que desarrolla funciones al interior de la ECEP recibe desde su ingreso una instrucción (inducción) acorde con la función a desempeñar. Así mismo, el personal se encuentra sujeto a un plan de capacitación continúo con el fin de que las responsabilidades asumidas como parte de los servicios de certificación digital se desarrollen en forma competente.

El contenido de los programas de capacitación se controla y refuerza periódicamente, llevándose un registro y archivo de las materias impartidas para los efectos de las re-capacitaciones a las que se alude en la sub sección 5.3.4 del presente documento.

El "*Plan de capacitaciones ECERNEP-ECEP*", adecuado a las funciones a desempeñar en la ECEP, contiene como mínimo los siguientes

conceptos básicos:

- Uso y operación del hardware y software empleado.
- Aspectos relevantes de la Política General de Certificación, Declaración de Prácticas y Políticas de Certificación, Política de Seguridad, Plan de Privacidad, Política de Privacidad y otra documentación que comprenda sus funciones.
- Marco regulatorio de la prestación de los servicios de certificación digital.
- Procedimientos en caso de contingencias.
- Procedimientos de operación y administración para cada rol específico.
- Procedimientos de seguridad para cada rol específico.

La ECEP cuando estime conveniente o por disposición legal expresa, podrá incluir otros temas en la capacitación con la finalidad de lograr una apropiada formación y alcanzar un adecuado proceso de mejora continua del personal.

En lo que corresponda, los contratistas que realicen labores por tiempo determinado en las instalaciones de la ECEP, tienen la obligación de capacitar de manera continua a su personal en temas relacionados con las actividades que desarrollan.

5.3.4. Frecuencia y requisitos de las re-capacitaciones

Tal como está indicado en el "*Plan de capacitaciones ECERNEP-ECEP*", la capacitación se efectuará necesariamente cuando el personal sea sustituido o rotado, así como cuando se realicen cambios en los procedimientos de operaciones o en la Política General de Certificación, Declaración de Prácticas y Políticas de Certificación, Política de Seguridad, Plan de Privacidad, Política de Privacidad o en cualquier otro documento que resulte relevante para la ECEP– RENIEC y que comprometa los aspectos funcionales de las labores del personal.

Sin perjuicio de lo antes expuesto, la ejecución del "*Plan de capacitaciones ECERNEP-ECEP*" resulta ser un proceso de formación continua del personal, encontrándose sus requisitos dispuestos en la sub sección 5.3.3 del presente documento.

Tratándose de un aspecto inherente a la ECEP, y en consideración a los servicios de certificación digital que ofrecerá, la "*Política de Seguridad*" manifiesta que la capacitación en tópicos relacionados con la seguridad de la información se realizará en forma permanente.

5.3.5. Frecuencia y secuencia de la rotación en el trabajo

La ECEP, en caso lo determine conveniente, podrá establecer métodos de rotación laboral para la prestación del servicio. La frecuencia de la rotación y su comunicación al personal se describe en el documento "*Operación de la Planta de Certificación Digital*".

5.3.6. Sanciones por acciones no autorizadas

Le es aplicable a todo el personal del RENIEC la Ley N° 27815 – Código de Ética de la Función Pública, y normas complementarias, independientemente de la modalidad de contratación. El procedimiento sancionador es regulado por la Ley N° 27444 – Ley del Procedimiento Administrativo General.

Con relación a las operaciones de la ECEP, se considerarán acciones no autorizadas las que contravengan, de manera negligente o malintencionada, al presente documento, la Política de Seguridad, la Política de Privacidad y el Plan de Privacidad, así como, los documentos normativos de alcance a su personal, que emita el RENIEC.

La ECEP, a través de la Gerencia de Recursos Humanos del RENIEC, contempla los términos para las acciones no autorizadas (de acuerdo a la legislación peruana pertinente y vigente), así como las sanciones correspondientes, contemplándose su cese de acuerdo a la gravedad de las mismas, esto sin perjuicio del procedimiento administrativo formal.

De otro lado, es aplicable a los servidores y funcionarios públicos del RENIEC la Ley Nº 29622 - Ley que modifica la Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, y Amplía las Facultades en el Proceso para Sancionar en Materia de Responsabilidad Administrativa Funcional y, su Reglamento aprobado por el Decreto Supremo N° 023-2011-PCM, que establece las infracciones y sanciones por responsabilidad administrativa funcional.

5.3.7. Requerimientos de los contratistas

En caso que el RENIEC, en su calidad de ECEP, estime conveniente el empleo de contratistas, éstos y sus empleados que realicen funciones al interior de la entidad, se encuentran sujetos a lo establecido en la presente documento en el ítem 5.3 en lo que resulte aplicable, en los mismos criterios de funciones y seguridad aplicados a empleados de la ECEP en posición similar.

Los contratos especifican las sanciones y reparaciones para las acciones llevadas a cabo por los contratistas y sus empleados.

5.3.8. Documentación suministrada al personal

La ECEP suministra a todo su personal, en función a los cargos y roles que desempeñe, la documentación mínima siguiente:

- Reglamento de Organizaciones y Funciones (ROF) y Manual de Organizaciones y Funciones (MOF).
- Política General de Certificación.
- Declaración de Prácticas y Políticas de Certificación de la ECEP.
- La documentación que define las obligaciones y procedimientos de cada rol.
- Manual de funcionamiento de equipos y software que debe

operar en la ECEP.
- Normas Legales y marco regulatorio aplicables a sus funciones en la ECEP.
- Documento relativo al ciclo de vida de los certificados digitales e instructivos o procedimientos de trabajo.
- Documentación aplicable respecto a su rol dentro del "*Plan de Recuperación y Continuidad de la Planta de Certificación Digital*".

5.4. Procedimiento de registro de auditorías

5.4.1. Tipos de eventos registrados

La ECEP mantiene registros de auditoría de los eventos que puedan impactar en la seguridad de sus operaciones.
Estos incluyen lo siguiente:

- Encendido y apagado de los equipos servidores (registro de eventos en servidores).
- Registro de sucesos del módulo criptográfico (registro de eventos de modulo criptográfico).
- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios (registro de eventos en servidores).
- Intentos de entrada y salida a los servidores (registro de eventos en servidores).
- Intentos no autorizados de acceso a la base de datos (registro de eventos de base de datos).
- Cambios en los perfiles de emisión de certificados (registro de eventos en plataforma PKI).
- Intentos no autorizados de ingresos a la red de la ECEP (registro de eventos en plataforma PKI).
- Generación de claves de la ECEP (registro de eventos de modulo criptográfico).
- Intentos nulos de lectura y escritura en un certificado y en los repositorios (registro de eventos en plataforma PKI).
- Eventos relacionados con el ciclo de vida del certificado: emisión y cancelación (registro de eventos en plataforma PKI).
- Tal como está indicado en la "*Política de seguridad*", los registros de auditoría de eventos registran la hora, fecha e identificadores software/hardware.
- La ECEP registra de manera manual o electrónica, como mínimo, la siguiente información:
  - Mantenimientos y cambios de configuración del sistema según **"***Control de cambios en sistemas***".**
  - Acceso físico a las áreas sensibles según **"***Control de acceso físico***".**
  - Cambios en el personal.
  - Informes completos de los intentos de intrusión física a las instalaciones de la Planta PKI según **"***Gestión de Incidentes de Seguridad***".**

5.4.2. Frecuencia del procesamiento del registro

LA ECEP ha establecido fechas, frecuencias, objetivos, estándares, guías, procedimientos y documentación pertinente, para verificar los registros de auditoría ante algún tipo de actividad sospechosa o inusual.

Los registros de auditoría deben ser procesados y revisados una vez al mes como mínimo según **"***Gestión de registros de auditoría***".**

5.4.3. Periodo de conservación del registro de auditorías

En cumplimiento de lo establecido por la AAC, la conservación de los registros de auditoría señalados en el ítem 5.4.1., será como máximo por un periodo de diez (10) años, tal como lo indica la **"***Gestión de registros de auditoría***"**.

5.4.4. Protección del registro de auditoría

Los registros de auditorías, tanto físicos como electrónicos, cuentan con medidas de protección física y lógica, tales como:

- Controles de acceso a lectura.
- Protección contra modificaciones.
- La destrucción de un archivo de auditoría sólo se podrá llevar a cabo con la autorización de la AAC, siempre y cuando haya transcurrido un periodo mínimo de 10 años.

5.4.5. Procedimiento de copia de seguridad del registro de auditorías

En la ECEP, se realizan dos tipos de copias de seguridad del registro de auditorías, conforme a la criticidad de la información, de acuerdo al documento **"***Respaldo de información de la Planta de Certificación Digital***"**:

- Completas.
- Incrementales.

Estas copias de seguridad serán almacenadas externamente.

5.4.6. Sistema de realización de auditoría (Interna vs Externa)

La frecuencia de las auditorías internas se realiza conforme a lo establecido en el "*Plan Anual de Auditorias*". Las auditorías externas se realizan una vez al año o cuando la AAC lo requiera.

Se tiene establecido que la auditoria se realiza sobre temas específicos como: Planificación de Contingencias, Seguridad Física, Control de accesos, entre otros.

5.4.7. Notificación al titular que causa un evento

Los sistemas de información de la ECEP generan informes de eventos, incidentes y errores, en los cuales se indica e identifica al usuario que generó el evento.

La persona designada para realizar una auditoría a un evento de seguridad no comunicará el hecho al autor del mismo, sino informará inmediatamente al Oficial de Seguridad de Información para que proceda en función de la gravedad del evento o hecho.

5.4.8. Valoración de vulnerabilidad

La ECEP cuenta con hardware y software que cumplen con altos estándares de seguridad, tales como Common Criteria EAL4+ y FIPS 140-2 nivel 3. El análisis de las vulnerabilidades es efectuado por los fabricantes, quienes al identificarlas efectúan los ajustes necesarios para ser puestas a disposición del usuario del hardware o software.

Además es responsabilidad del personal de la ECEP informar al Oficial de Seguridad de Información, cualquier tipo de evento que pueda producir (o potencialmente producir) alguna vulnerabilidad en el hardware o software de la ECEP.

5.5. Archivo de registro

5.5.1. Tipos de eventos registrados

Los eventos que la ECEP mantendrá serán:

- Datos del certificado digital (Número de serie, estado e información del suscriptor).
- Lista de Certificados digitales cancelados.
- Claves públicas de la ECEP.
- Estado de acreditación de la ECEP.
- Registros de auditorías.

La ECEP es responsable del correcto archivamiento de estos registros. Para ello se guiará de lo indicado en los documentos “Gestión de registros de auditoría” y “Respaldo de información de la Planta de Certificación Digital”.

5.5.2. Periodo de conservación del archivo

De acuerdo a la Legislación Peruana vigente los archivos deben ser mantenidos por un periodo de diez (10) años.

5.5.3. Protección del archivo

Los archivos de registro son:

i. Físicamente protegidos.
ii. Lógicamente protegidos.
iii. Supervisados para evitar el empleo inadecuado.

La protección de los archivos se establece de acuerdo al tipo de información que contiene, conforme a lo establecido en el documento *“Lineamientos de Clasificación de la Información”*.

5.5.4. Procedimientos para copia de seguridad del archivo

La ECEP realiza copias de seguridad, tanto de la información como del software primordial para el funcionamiento de la ECEP. Estas copias son probadas con regularidad por el personal autorizado.

5.5.5. Requisitos para los archivos de sellado de tiempo

Los sistemas de la ECEP para proteger los archivos de registro realizan una marca de tiempo en el instante en que se genera el registro. El tiempo de los sistemas proviene de una fuente confiable de hora, a través del protocolo NTP (Network Time Protocol) con el que cuentan todos los sistemas de la ECEP, para ello se ejecuta lo indicado en "*Sincronización de hardware y software con servicio NTP*" y en "*Pruebas de operatividad de servicios y funcionalidades de hardware y software*".

5.5.6. Sistema de recolección del archivo (interna o externa)

Las copias de seguridad de la ECEP, se mantienen tanto interna (almacenada en dispositivos al interior de la Planta de Certificación Digital – PKI) como de forma externa. El detalle es especificado en **"***Respaldo de información de la Planta de Certificación Digital***".**

5.5.7. Procedimiento para obtener y verificar la información del archivo

Dependiendo de la naturaleza de la información contenida en el archivo, el acceso a ésta se efectuará de acuerdo a los privilegios asignados a los usuarios autorizados, conforme a la clasificación de la información establecida en el documento "Lineamientos para la clasificación de la información", y conforme a lo indicado en los ítems 9.3 y 9.4 del presente documento.

La verificación de la información se efectuará utilizando mecanismos de seguridad basados en criptografía de acuerdo a lo establecido en el documento **"***Gestión de registros de auditoría***"**.

5.6. Cambio de clave

El procedimiento para proporcionar, en caso de cambio de claves, una nueva clave pública de Autoridad de Certificación raíz o intermedia, a los titulares y terceros aceptantes de los certificados que emite la ECEP, es el mismo que para proporcionar la clave pública en vigor, lo cual se encuentra detallado en "*Gestión de claves de entidad raíz y de nivel intermedio*". En consecuencia, la nueva clave se publicará en el repositorio que gestiona la ECEP (ver ítem 2.2. apartado ii del presente documento)

5.7. Recuperación frente al compromiso y desastre

En el documento **"***Plan de Recuperación y Continuidad de la Planta de Certificación Digital***",** la ECEP establece los procedimientos para el restablecimiento y mantenimiento de la continuidad del negocio y la

recuperación frente a desastres.

5.7.1. Procedimiento de manejo de incidentes y compromisos

La ECEP ha establecido mecanismos de comunicación, registro y de respuesta a incidentes, indicando la acción que ha de emprenderse al tomarse conocimiento de un incidente.

Dichos mecanismos contemplan que ante la detección de un supuesto incidente o violación de la seguridad de información, deberán ser comunicados a través de canales pre-establecidos tan pronto como se haya tomado conocimiento, al Oficial de Seguridad de Información para las acciones correspondientes.

Para el desarrollo de lo indicado en este ítem se tomará en cuenta lo descrito en "*Gestión de Incidentes de Seguridad*".

5.7.2. Adulteración de los recursos computacionales software y/o datos.

En el documento **"***Plan de Recuperación y Continuidad de la Planta de Certificación Digital***"** de la ECEP, se identifican fuentes alternativas de recursos computacionales, software y datos, las cuales serán empleadas en los casos de adulteraciones o fallas en los mismos.

5.7.3. Procedimientos en caso de compromiso de la clave privada de la Entidad

En caso, la clave de la ECEP fuera comprometida de manera real o potencial, ésta deberá ser inmediatamente cancelada, notificándose el hecho en un lapso máximo de 24 horas al INDECOPI, de acuerdo a lo detallado en el documento "*Gestión de claves de entidad raíz y de nivel intermedio*".

Asimismo, se comunicará a la EREP para que informe a los suscriptores afectados, que los certificados suministrados con la clave comprometida de la ECEP, han dejado de ser válidos; estando los usuarios en la facultad de apersonarse a las oficinas de la correspondiente EREP para solicitar la emisión de un nuevo certificado digital.

5.7.4. Capacidad de continuidad del negocio luego de un desastre

La ECEP mantiene un "*Plan de Recuperación y Continuidad de la Planta de Certificación Digital***"** afín de garantizar la continuidad de las operaciones en caso de compromiso de su clave privada u otras situaciones que podrían ocasionar la interrupción del servicio; permitiendo la continuidad de las siguientes actividades:

- Recepción de solicitudes autorizadas para emisión de certificados digitales, encaminadas por la EREP mediante canales seguros.
- Emisión de certificados digitales.

- Recepción de solicitudes de cancelación, encaminadas por la EREP mediante canales seguros.
- Cancelación de certificados digitales.
- Generación y publicación de la lista de certificados cancelados.

5.8. Finalización de la EC o ER

En caso que la ECEP comunique a la correspondiente EREP la finalización de sus actividades, ésta última adoptará las medidas posibles para minimizar el impacto que pueda causar en los miembros de la comunidad de usuarios a la que se alude en la sub sección 1.3 del presente documento.

En dicho supuesto, la ECEP y la EREP, según les corresponda, informarán a la AAC, así como a los titulares, suscriptores y terceros que confían sobre el cese de las operaciones de la ECEP, con un mínimo de treinta (30) días calendario de anticipación, y conforme a lo indicado en el documento “Cese de actividades de entidad raíz y de nivel intermedio”.

6. Controles de seguridad técnica

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

Para la generación de claves la ECEP emplea hardware criptográfico certificado bajo el estándar FIPS 140-2 nivel 3 y Common Criteria EAL4+.

El par de claves de las entidades finales deben ser generadas en medios criptográficos que cumplan con el estándar FIPS 140-2 nivel 2 ó Common Criteria EAL4+ de acuerdo al nivel de acreditación de la ECEP y a los requerimientos exigidos en las Guías de Acreditación para Entidades de Certificación.

6.1.2. Entrega al suscriptor de la clave privada

En caso que las claves se entreguen al suscriptor en las instalaciones de la EREP, esto se llevará a cabo en un ambiente que garantice la confidencialidad en la entrega de la clave privada.

Nota: este proceso se sigue para certificados digitales destinados a personas naturales y jurídicas.

6.1.3. Entrega de la clave pública para el emisor de un certificado

Cuando un titular o suscriptor genere su propio par de claves, la solicitud que incluye la correspondiente clave pública, debe ser entregada a la ECEP, a través de un canal seguro establecido por ésta.

Es responsabilidad del suscriptor la correcta generación del par de claves y la solicitud.

Haciendo uso de la clave pública la ECEP procederá de manera automática, a verificar si la firma de la solicitud fue realizada con la correspondiente clave privada, asegurándose de esta manera la autenticidad del suscriptor.

6.1.4. Entrega de la clave pública de la EC al tercero que confía.

La clave pública de la ECEP está consignada en la lista TSL, la cual es gestionada por el INDECOPI y se encuentra en la página web oficial de la TSL (website de INDECOPI), en la dirección https://iofe.indecopi.gob.pe/TSL/tsl-pe.xml

Se mantiene una copia de la TSL en el repositorio que gestiona la ECEP, en la dirección http://crl.reniec.gob.pe/tsl a la cual podrán acceder los terceros que confían.

6.1.5. Tamaño de claves

La ECEP mantiene los siguientes tamaños de claves:

i. Certificados Intermedios

Certificados Intermedios de la ECEP		
Algoritmo de Firma	**SHA-1**	**SHA-256**
Nombre del Certificado	**reniecclassX**	**reniecclassXHG**
Tamaño de clave	**4096**	**4096**

ii. Certificado de suscriptor o titular

Certificados Intermedios de la ECEP		
Algoritmo de Firma	**SHA-1**	**SHA-256**
Tamaño de clave	**2048**	**2048**

Nota: la ECERNEP determinará la utilización del algoritmo de firma SHA-256 cuando las aplicaciones que interactúen con los certificados digitales (sistemas operativos, software de firma, entre otros), que soporten este algoritmo, sean usados masivamente.

6.1.6. Generación de parámetros de las claves públicas y verificación de la calidad

La clave pública de los certificados emitidos por la ECEP está codificada de acuerdo con el RFC 3280 y PKCS#1. El algoritmo de generación de claves es el RSA.

La ECEP valida la clave pública del pedido del certificado y se asegura que no pertenezca a otro usuario, a través de un mecanismo automático que tiene implementada la plataforma que utiliza la ECEP para gestión de certificados digitales.

6.1.7. Propósitos del uso de las claves (conforme a lo establecido en el campo de uso de X.509 v3)

Los propósitos de claves permitidas y establecidas por la ECEP para las entidades finales son determinados de acuerdo a los **"***Perfiles de Certificado Digital ECEP***"** y a lo indicado en el ítem 1.4 del presente documento.

6.2. Controles de ingeniería para protección de la clave privada y módulo criptográfico

6.2.1. Estándares y controles para el módulo criptográfico

La ECEP utiliza los siguientes estándares como parte de los controles de ingeniería del módulo criptográfico:

- FIPS 140-2 nivel 2.
- Common Criteria EAL4+

O aquellos requeridos de acuerdo al nivel de acreditación de la ECEP, especificados en la Guía de Acreditación del INDECOPI.

6.2.2. Control multipersonal (k de m) de la clave privada

Conforme a lo establecido en el documento "*Gestión de claves de entidad raíz y de nivel intermedio*", para la generación y acceso físico a las claves privadas se requiere de la concurrencia de 2 personas de un conjunto de 5 autorizadas.

Nota: k de m, donde:
k = número de personas concurrentes.
m = total de personas autorizadas.

6.2.3. Depósito de clave privada

La ECEP no admite el depósito, almacenamiento o copia de claves privadas de firma y autenticación de los usuarios finales, ni de los módulos hardware que los contienen; conforme se establece en el "*Plan de Seguridad y Administración de claves*".

6.2.4. Copia de seguridad de la clave privada de los PSCs

Existe más de un dispositivo criptográfico que contiene las claves privadas de la ECEP. Estas claves se encuentran dentro de los equipos HSM y están protegidas por los estándares de seguridad FIPS 140-2 nivel 3 y Common Criteria EAL4+.

No se realiza copia de seguridad (backup) de la clave privada de la ECEP y éstas no pueden ser utilizadas fuera del HSM.

6.2.5. Archivo de la clave privada

Las claves privadas de suscriptores o titulares no serán archivadas. Por ello la plataforma de la ECEP no tiene habilitada esta funcionalidad tal como se indica en el documento "*Configuraciones de Seguridad*".

6.2.6. Transferencia de la clave privada de o hacia un módulo criptográfico

La clave privada de la ECEP ha sido generada y es mantenida en el módulo criptográfico (HSM) en un lugar seguro según *"Gestión de claves de entidad raíz y de nivel intermedio"*.

La ECEP, en caso de necesidad para mantener la continuidad de sus servicios, podrá realizar una migración de sus claves privadas a otro equipo HSM, manteniendo los niveles de seguridad especificados en el ítem 6.2.2 del presente documento.

6.2.7. Almacenamiento de la clave privada en un módulo criptográfico

La clave privada de la ECEP es generada y mantenida en el módulo criptográfico (HSM) de la Planta de Certificación Digital.

Los módulos criptográficos usados por la ECEP están certificados bajo los estándares FIPS 140-2 nivel 3 y Common Criteria EAL4+.

6.2.8. Método de activación de la clave privada

En el caso de que los certificados digitales sean generados por el suscriptor, las claves privadas no requerirán activación posterior, debido a que estas se activan automáticamente al momento de ser generadas.

El procedimiento de activación de la clave privada de un suscriptor para el caso del DNIe se indicará en la correspondiente DPR del EREP-RENIEC que autorizó su emisión.

6.2.9. Método de desactivación de la clave privada

El suscriptor o titular debe desactivar su clave privada mediante el mecanismo especificado por el fabricante del componente (del medio portador) que almacena dicha clave.

6.2.10. Método de destrucción de la clave privada

En caso se requiera la destrucción de la clave privada por parte del

suscriptor o titular, primero deberá realizarse el procedimiento de cancelación del certificado (ver ítem 3.4 del presente documento), y luego debe eliminar su clave privada mediante el mecanismo especificado por el fabricante del componente (del medio portador) que almacena dicha clave.

6.2.11. Clasificación del módulo criptográfico

- Para la ECEP:
  Los módulos criptográficos usados por la ECEP cumplen los siguientes requerimientos, según lo indicado en el documento "*Gestión de claves de entidad raíz y de nivel intermedio*":
  - FIPS 140-2 nivel 3
  - Common Criteria EAL4+

- Para el Suscriptor o titular del certificado:
  Los módulos criptográficos usados por los suscriptores de certificados deben cumplir con los estándares FIPS 140-2 nivel de seguridad 1 como mínimo o Common Criteria EAL4 o aquel exigido de acuerdo al nivel de acreditación de la ECEP.

6.3. Otros aspectos de la gestión del par de claves

6.3.1. Archivo de la clave publica

Las claves públicas o los certificados que las contengan, son almacenados en la base de datos principal de la ECEP y son custodiadas según lo establecido en el documento **"***Control de Acceso Lógico***".**

6.3.2. Periodos operacionales del certificado y periodo de uso de claves

A continuación se muestra los periodos operacionales de los certificados:

Clase	Tipo de persona	Tiempo	Tamaño de clave
Clase I	Persona Natural	1 año	2048
Clase II	Persona Natural	2 años	2048
Clase III	Persona Jurídica	1 año	2048
		2 años	2048
Clase IV	Persona Jurídica (Servidor SSL)	2 años	2048
Clase V	Persona Jurídica (Sistema de Intermediación Electrónico)	2 años	2048
Clase VI	Persona Jurídica (Entidad de	Depende del tamaño de la	Mínimo 2048 Máximo 10

	Certificación)	clave y del período autorizado*	años.

* La vigencia máxima de estos certificados no podrá superar a la de los certificados digitales que se encuentran en niveles superiores.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

La activación del acceso a la clave privada debe ser realizada por el suscritor como mínimo mediante el uso de PIN o patrones de las impresiones dactilares, de acuerdo a lo soportado por el componente que contiene la clave.

6.4.2. Protección de los datos de activación

Corresponde al suscriptor la responsabilidad de proteger los datos de activación de acceso a la clave privada, lo cual debe estar en concordancia con el valor de los activos protegidos por la clave privada.

Debe configurarse el componente para que el acceso a la clave privada se bloquee como mínimo luego de tres (03) intentos consecutivos fallidos. Para los casos donde la EREP no provea el componente, es responsabilidad del suscriptor la configuración de esta característica. Para el desbloqueo del componente el suscriptor deberá seguir el procedimiento indicado por el fabricante del componente o acudir a la entidad o empresa que le proporcionó el medio, según corresponda.

6.4.3. Otros aspectos de los datos de activación

Corresponde al usuario determinar que otros aspectos son necesarios considerar, para una mejor protección de la clave privada. Como ejemplo, se puede mencionar “requerirse el cambio de PIN y contraseña cada 30 días”, esto dependerá de la capacidad de configuración que tenga el medio portador que almacena la clave privada.

6.5. Controles de seguridad computacional

6.5.1. Requisitos técnicos específicos para seguridad computacional

La ECEP cumple los controles establecidos en:

- La norma ISO/IEC 17799 “Information technology – Code of practice for information security management” y la norma ISO/IEC TR13335 “Information technology - Guidelines for the management of IT Security”.
- La norma ISO/IEC 27001:2005 “Information technology - Security techniques - Information security management systems - Requirements”.
- La norma ISO/IEC 15408 “Information technology - Security techniques - Evaluation criteria for IT security”.

En lo que fuera aplicable de acuerdo a lo señalado en la "*Política de Seguridad*", "*Plan de Privacidad*" y "*Plan de Seguridad y Administración de Claves*".

6.5.2. Evaluación de la seguridad computacional

La evaluación de los controles de la seguridad computacional ha sido realizada de manera compatible con los siguientes estándares internacionales:

- La norma ISO/IEC 15408 "Information technology -- Security techniques - Evaluation criteria for IT security".
- La norma ISO/IEC 17799 "Information technology – Code of practice for information security management" y la norma ISO/IEC TR13335 "Information technology - Guidelines for the management of IT Security"
- La norma ISO/IEC 27001:2005 "Information technology - Security techniques - Information security management systems - Requirements".
- FIPS PUB 140-2 – "Security Requirements for Cryptographic Modules" o Common Criteria EAL 4.

En lo que fuera aplicable de acuerdo a lo señalado en la *"Política de Seguridad"* y *"Plan de Seguridad y Administración de Claves"*.

6.6. Controles técnicos del ciclo de vida

Estos controles aplican a los componentes de hardware y software que conforman la plataforma tecnológica de la ECEP usados para proporcionar servicios de certificación digital.

6.6.1. Controles de desarrollo del sistema

La ECEP cuenta con hardware y software que cumplen con estándares de seguridad, como:

- Sistema Operativo con Common Criteria EAL4+
- HSM con certificación FIPS 140-2 nivel 3 y Common Criteria EAL4+

El control de calidad del hardware y software es efectuado por los fabricantes, durante su elaboración.

El software y hardware que utiliza la ECEP, así como las configuraciones de los mismos, han pasado por una fase de pruebas antes de ser puestos en producción, considerando lo indicado en "Operación de la Planta de Certificación Digital".

6.6.2. Controles de gestión de la seguridad

La configuración del software ECEP se encuentra en su base de datos principal, sobre ésta se aplican algoritmos de comparación y se controlan las versiones, y es registrada según lo indicado en el

documento "C*ontroles para la Seguridad de Información*".

6.6.3. Evaluación de seguridad del ciclo de vida

Los controles de seguridad establecidos para la ECEP serán revisados a través de las auditorías o evaluación de compatibilidad con la IOFE. Todos los controles aplicados se encuentran en el documento "C*ontroles para la Seguridad de Información*"

6.7. Controles de seguridad de la red

Los sistemas de registro del servidor tienen mecanismos de control de acceso para prevenir el acceso no autorizado o el cambio de datos.

Los controles de acceso al sistema de archivos de los servidores, a través de la aplicación del "*Control de Acceso Lógico*" restringen:

- Acceso a áreas del sistema.
- Adición de software o servicios.
- Tener acceso a los archivos de otros usuarios.

Se asignan a los usuarios de los sistemas los privilegios de acceso necesarios para la realización de sus roles y funciones.

Las cuentas de administrador del sistema son asignadas y usadas de forma cuidadosa y restringida.

Los servidores que contienen información sensible se encuentran:

- Físicamente protegidos (sistemas biométricos).
- Lógicamente protegidos (a través de contraseñas o uso de certificados digitales).
- Supervisados para evitar el empleo inadecuado. (video vigilancia y control de históricos de acceso).

Las contraseñas deben ser seguras, pero capaces de ser recordadas. Estas deben garantizar un proceso de manejo formal. Estas contraseñas son concedidos por un proceso de entrega formal, donde los usuarios están de acuerdo con mantenerlos confidenciales. El detalle se encuentra especificado en "*Control de Acceso Lógico*" y "*Control de Acceso Físico*".

Además el sistema de telecomunicaciones y conexión remota se encuentra protegida por equipos firewall con reglas de acceso para usuarios externos a la ECEP y reglas que dividen la red interna en segmentos protegidos. El detalle se encuentra indicado en el "*Control de Acceso Lógico*".

6.8. Sello de tiempo

La información publicada en los repositorios (directorios, CRLs, copias archivadas y otros) indica la fecha y hora de su generación, los cuales son obtenidos de un servidor NTP.
Para garantizar estas operaciones, se cuentan con el documento "*Sincronización de hardware y software con servicio NTP*".

7. Perfiles del certificado

7.1. Perfil del certificado

7.1.1. Número(s) de versión(es)

Se soporta y emplea X.509 v3.
El certificado generado por la ECEP contempla el contenido y campos descritos en el ítem 3.1.1 del presente documento, además de los siguientes:

- Número de serie, que será un código único con respecto al Nombre Distinguido (Distinguished Name - DN) del emisor.
- Algoritmo de firma.
- El Nombre Distinguido (Distinguished Name - DN) del emisor.
- Inicio de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 3280.
- Fin de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 3280.
- Nombre distinguido del suscriptor.
- Clave pública del suscriptor, codificada de acuerdo con RFC 3280.
- Firma, generada y codificada de acuerdo con RFC 3280.
- Uso autorizado del certificado digital.

7.1.2. Extensiones del certificado

Se soporta y usa las extensiones de certificado X.509 v3.

El detalle de las extensiones utilizadas se describe en el documento **"***Perfiles de Certificado Digital ECEP***"**.

7.1.3. Identificadores de objeto de algoritmo

Los algoritmos OIDs están de conformidad con el RFC 3279 y RFC 3280.
El identificador de Objeto (OID) de los algoritmos Criptográficos es: *SHA-1 with RSA Encryption* (1.2.840.113549.1.1.5)

7.1.4. Forma de nombres

La forma de nombres está de acuerdo al formato de Nombres distinguidos X.501 tal como se implementa en el RFC 3739 y como se especifica en el ítem 3.1.1 del presente documento.

7.1.5. Restricciones de Nombre

Las restricciones de nombre están soportadas tal como se establece en el RFC 3280.

Los nombres contenidos en los certificados están restringidos a

distinguished names (DN) X.500, únicos y no ambiguos.

Los atributos que componen el DN, permitirán diferenciar a los DN entre sí.

7.1.6. Identificador de objeto de la política de certificados

La Declaración de Prácticas y Políticas de Certificación de la ECEP tiene un identificador de objeto (OID), el cual es: 1.3.6.1.4.1.35300.1.1.1.1.

7.1.7. Extensión de restricciones de uso de la política.

No se hace uso de las restricciones de políticas (policy constraints).

7.1.8. Sintaxis y semántica de los calificadores de la política

Los calificadores de políticas son soportados tal como se encuentran definidos en el RFC 3280.
La extensión "CERTIFICATE POLICIES" contiene el siguiente calificador de política ("Policy Qualifiers"):

- "CPS POINTER": reservada para contener la URL de la CPS y la CP que rigen el certificado.

7.1.9. Procesamiento de semántica para la extensión de políticas de certificados críticos

La ECEP es capaz de aceptar certificados que contengan cualquiera de las extensiones estandarizadas definidas en el RFC 3280 sea que estas se encuentren marcadas o no como críticas.

7.2. Perfil CRL

7.2.1. Número(s) de versión(es)

Se usan CRLs X.509 v2, además de soportar certificados X.509 v3.

7.2.2. CRL y extensiones de entrada CRL

Se soportan las extensiones CRL definidas en el RFC 3280.

7.3. OCSP Profile

7.3.1. Version number(s)

La ECEP no brinda servicio de verificación en línea OCSP para ningún tipo o clase de certificado.

7.3.2. OCSP extensions

La ECEP no brinda servicio de verificación en línea OCSP para ningún tipo o clase de certificado.

8. Auditorías de conformidad y otras evaluaciones

8.1. Frecuencia y circunstancias de la evaluación

La ECEP se someterá a una auditoría anual por parte de la AAC; en caso esta autoridad comunique que no desarrollará la mencionada auditoría, la ECEP podrá realizarla convocando a un tercero independiente.

8.2. Identidad/Calificaciones de asesores

El auditor es independiente a la ECEP.

Los auditores deberán contar con capacitación y experiencia en PKI, seguridad, tecnologías criptográficas y procesos de auditoría, además del conocimiento de la Guía de Acreditación EC, conforme a lo establecido para los perfiles de auditor en el “Plan de Auditorías”.

La ECEP está en la potestad de contratar personal externo especializado para la realización de los controles de auditoría.

8.3. Relación del auditor con la entidad auditada

La ECEP verificará que no exista ninguna relación entre el auditor y ésta, ya sea actual o planificada, o de cualquier otra clase que pueda derivar en un conflicto de intereses.

Si durante el desarrollo de las labores de auditoría, el auditor requiera contar con acceso a la Plataforma de la Planta de Certificación Digital - PKI, se le otorgará el acceso de forma restringida y previa evaluación.

En las labores de auditoría que quiera llevar a cabo en relación a los módulos criptográficos HSM, estos serán siempre operados por el personal de la Planta de Certificación Digital - PKI, proporcionando al auditor la información requerida. El auditor no estará en ningún caso autorizado a la manipulación física de los HSM, ni se le suministrará acceso al hardware que soporta la plataforma de la ECEP.

En el caso de auditores internos, estos no deberán tener relación funcional directa con el área objeto de la auditoría, conforme al perfil de auditor establecido en el “Plan de Auditoría”.

8.4. Elementos cubiertos por la evaluación

La auditoría determinará la conformidad del presente documento, infraestructura, hardware y software de la ECEP con la Guía de Acreditación de la EC, además también determinará los riesgos del no cumplimiento de la referida guía.

Se procederá a auditar, como mínimo, los siguientes aspectos considerados críticos:

- Alineación del presente documento con la CP de la ECERNEP.
- Alineación de las medidas efectivas existentes en la ECEP con los procedimientos marcados en el presente documento.

- Evaluación y cumplimiento de los niveles de seguridad física y lógica.
- Control de las versiones de software y correcta actualización del mismo.
- Revisión del estado de los equipos de TI utilizados por la ECEP.
- Revisión de los procedimientos de contingencia.
- Revisión de las copias de seguridad y estado de la base de datos.
- Validez de alta y acceso del personal que labora en la Planta de Certificación Digital - PKI.

8.5. Acciones a ser tomadas frente a resultados deficientes

Para el caso de las auditorías internas, el auditor elaborará un informe dirigido a la Gerencia de Certificación y Registro Digital con los resultados de su auditoria, procediendo ésta última a disponer la subsanación de las observaciones encontradas.

Para el caso de auditorías externas, si se encuentra un resultado deficiente, se llevarán a cabo las siguientes acciones:

- El auditor realizará un informe con los resultados de su auditoria.
- El auditor notificará la deficiencia al RENIEC y a la AAC.
- La AAC evaluará los resultados y en caso de una:
  a. No conformidad leve
     Indicará las irregularidades (no conformidad), pero permitirá que la ECEP continúe con sus operaciones hasta la próxima auditoría programada.

  b. No conformidad
     Permitirá que la ECEP continúe sus operaciones por un máximo de treinta (30) días naturales, pendientes a que se solucionen los problemas detectados antes de proceder a la suspensión de la ECEP.

  c. No conformidad grave
     Suspender la operación de la ECEP.
     En este caso todos los certificados emitidos por la ECEP serán cancelados antes de la suspensión del servicio.

  En los casos del literal a y b, la ECEP:
  - Ejecutará las acciones correctivas para solucionar la deficiencia, indicando a la AAC, el tiempo estimado para su realización, de acuerdo a la criticidad de la no conformidad.
  - Una vez que la deficiencia sea subsanada, será necesario realizar una nueva auditoría para confirmar la efectividad de las soluciones tomadas.

8.6. Publicaciones de resultados

La AAC publicará los resultados de las auditorías o evaluaciones, como parte de la información del estado de la ECEP.

9. Otras materias de negocio y legales

9.1. Tarifas

9.1.1. Tarifas para la emisión o renovación de certificados

Para mayor detalle revisar el ítem 9.1.1 de la correspondiente DPR.

9.1.2. Tarifas de acceso a certificados

La ECEP 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

La ECEP no aplica ninguna tasa por brindar información sobre la cancelación del estado del certificado, siempre que esta se consulte a través de la CRL.

9.1.4. Tarifas para otros servicios

Las tasas respectivas por la prestación del servicio de certificación digital se encuentran establecidas en el Texto Único de Procedimientos Administrativos (TUPA) del RENIEC.

9.1.5. Políticas de reembolso

Es política del RENIEC, en su calidad de Prestador de Servicios de Certificación Digital para el Estado Peruano, reembolsar al solicitante la tasa respectiva por la emisión del certificado digital, en caso su solicitud no hubiese sido aceptado debido a un trámite que debe regularizar con relación a su documento de identidad, RUC, o la vigencia del poder del representante legal o apoderado.

La política de reembolso del RENIEC, en su calidad de Prestador de Servicios de Certificación Digital, se encuentra establecida en el contrato.

9.2. Responsabilidad Financiera

9.2.1. Cobertura de seguro

La ECEP-RENIEC dispondrá de una garantía con cobertura suficiente de responsabilidad civil, a través del seguro contratado por el RENIEC. El referido seguro cubrirá el riesgo de la responsabilidad por los daños y perjuicios que se pudiese ocasionar a terceros como resultado de las actividades a cargo de la ECEP-RENIEC, cumpliendo de este modo con la obligación señalada en el artículo 31 del Reglamento de la Ley de Firmas y Certificados Digitales.

9.2.2. Otros activos

La ECEP, para la prestación del servicio de certificación digital a su cargo, cuenta con el respaldo económico del RENIEC.

9.2.3. Cobertura de seguro o garantía para entidades finales

El RENIEC en su calidad de Prestador de Servicios de Certificación Digital para el Estado Peruano no otorga seguro o garantía para entidades finales.

9.3. Confidencialidad de información del negocio

9.3.1. Alcances de la información confidencial

La ECEP declara expresamente como información confidencial, que no podrá ser divulgada a terceros y que se mantendrá con carácter reservado, excepto en aquellos supuestos previstos legalmente; la siguiente:

- Las claves privadas de la ECEP.
- Material o información reservada de la ECEP, incluyendo términos contractuales, planes de negocio, e información que versa sobre derechos de propiedad intelectual.
- Información reservada de los titulares y/o subscritores, y de ser el caso, de los terceros que confían.
- La información del negocio suministrada por la ECERNEP, EREP o por sus proveedores y otras personas con las que la ECEP tiene el deber de guardar secreto establecido de modo convencional.
- Información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores, titulares y los terceros que confían.
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían.
- La causal que motivó la cancelación del certificado digital.
- Información personal provista por los titulares y/o suscriptores que no sea la autorizada para estar contenida en los certificados digitales y en la Lista de Certificados Cancelados.
- Toda información relativa a las operaciones internas que lleve a cabo la ECEP.
- Toda información clasificada como "confidencial".
- Y otras mencionadas por la "*Política de Seguridad", "Plan de Privacidad"* y "*Plan de Seguridad y Administración de Claves*".

9.3.2. Información no contenida dentro del rubro de información confidencial

Se considera información pública y por lo tanto accesible por terceros:

- La información contenida en la Declaración de Prácticas y Políticas de Certificación aprobadas por la AAC.
- La contenida en las Políticas de Privacidad aprobadas por la AAC.
- Los certificados digitales emitidos por la ECEP, así como las informaciones contenidas en estos y el estado de los mismos.
- La lista de certificados digitales cancelados (CRL)
- Toda otra información identificada como "PUBLICA"

El acceso a la información no considerada confidencial será permitido sin perjuicio que la ECEP aplique los controles de seguridad pertinentes con el fin de proteger la autenticidad e integridad de los documentos, así como impedir que personas no autorizadas puedan añadir, modificar o suprimir contenidos.

9.3.3. Responsabilidad de protección de la información confidencial

El personal de la ECEP, personal contratado por el RENIEC, y cualquiera que se relacione con alguna actividad de la ECEP, están obligados a guardar secreto sobre la información clasificada como "confidencial".

9.4. Privacidad de la información confidencial

9.4.1. Plan de privacidad

De conformidad con lo establecido en la Ley N° 29733 – Ley de Protección de Datos Personales, se considera como datos personales, toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

La ECEP asegura a los titulares y/o suscriptores el adecuado tratamiento de sus datos personales, los cuales serán tratados para los fines propios de la prestación del servicio de certificación digital o para otros propósitos relacionados con dichos servicios, y que permitan otorgar confianza al tercero que confía o tercer usuario, pudiendo ellos verificar el estado del certificado digital emitido por la ECEP.
La ECEP conjuntamente con la EREP-RENIEC han desarrollado un *"Plan de Privacidad",* el cual recoge los principios de la Ley antes indicada.

El referido *"Plan de Privacidad"* establece, entre otros, las directrices que deben cumplir los colaboradores de la EREP-RENIEC, ECEP, y terceros que presten sus servicios como contratistas, así como las directrices respecto de la recolección de datos personales, uso y tratamiento de los mismos, transferencia de la información, mecanismos de acceso a la información personal y las medidas de seguridad destinadas a garantizar la integridad y confidencialidad de la información.

El *"Plan de Privacidad"* es catalogado como información confidencial y sólo se proporciona a los colaboradores de la EREP-RENIEC, ECEP y a quien acredite la necesidad de conocerlo, como en el caso de las auditorías externas o internas.

Las sanciones que la ECEP aplicará al personal involucrado en la prestación del servicio de certificación digital son las establecidas por el RENIEC.

9.4.2. Información tratada como privada

La ECEP declara expresamente como información personal de carácter privado, a toda aquella información que no se encuentre contenida en los certificados digitales ni en la lista CRL.
La información personal considerada como privada es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizada.

9.4.3. Información no considerada privada

La información que la ECEP considerada no privada es aquella que se incluye en los certificados digitales y en la CRL. Se detalla pero no limita a:

- Certificados digitales emitidos o en trámite de emisión.
- Datos de identificación que figuran en el certificado digital del suscriptor y que sirven para autenticar a aquel.
- Usos y límites de uso de los certificados digitales.

Por consiguiente, la información que se hará pública es la siguiente:

a. Certificados digitales emitidos o en trámite de emisión.
b. Certificados digitales cancelados.
c. Datos de identificación que figuran en el certificado digital del suscriptor, como: nombre completo, número del Documento Nacional de Identidad, Carné de Extranjería y Registro Único de Contribuyente (RUC).
d. Usos y límites de uso de los certificados digitales.
e. Aquella información personal que los titulares o suscriptores soliciten o autoricen que se publique.
f. El periodo de validez del certificado digital, así como la fecha de emisión y la fecha de caducidad del certificado digital.
g. El número de serie del certificado.

9.4.4. Responsabilidad de protección de la información privada

La ECEP consiente de la importancia de la protección de los datos personales, cumple con los principios y las disposiciones establecidas en la Ley N° 29733 – Ley de Protección de Datos Personales.

En tal sentido, ha implementado medidas de seguridad de índoles organizativas y técnicas orientadas a garantizar la protección de los datos personales, así como de la información confidencial que gestiona.

Las medidas de seguridad implementadas por la ECEP se encuentran detalladas en la "*Política de Seguridad*".

9.4.5. Notificación y consentimiento para el uso de información

En los formatos de solicitud de emisión y cancelación se especifican los datos personales de los titulares y/o suscriptores que son recolectados por la correspondiente EREP.

De conformidad con lo dispuesto en el numeral 1 del Artículo 14[9] de la Ley N° 29733 – Ley de Protección de Datos Personales, la ECEP está exceptuado de solicitar el consentimiento al titular de los datos para el tratamiento de sus datos personales.

9.4.6. Divulgación con motivo de un proceso judicial o administrativo

Excepcionalmente, los datos personales de carácter privado o la información confidencial del titular y/o suscriptor serán revelados o comunicados al Poder Judicial cuando una orden judicial así lo exija o cuando ésta sea autorizada, de manera expresa, por el titular y/o suscriptor.

9.4.7. Otras circunstancias para divulgación de información

La ECEP, dentro del marco de colaboración del sector público, podrá comunicar o ceder a otros organismos del Estado los datos personales de los titulares y/o suscriptores.

Asimismo, dentro del marco de la IOFE, los datos personales podrán ser transferidos a otras entidades de certificación.

En todo caso, la cesión o transferencia de datos personales se realizará de acuerdo a la Ley N° 29733 – Ley de Protección de Datos Personales, y en lo que fuese aplicable, en el caso de las entidades de la Administración Pública, según lo señalado en el artículo 55 del Reglamento de la Ley de Firmas y Certificados Digitales.
En todos los casos, la Entidad receptora debe garantizar a la ECEP la confidencialidad de la información transferida.

9.5. Derechos de propiedad intelectual

Todos los derechos de propiedad intelectual, incluyendo los referidos a certificados, repositorios de la ECEP, OIDs, la presente Declaración de Prácticas y Políticas de Certificación, Política de Seguridad, así como cualquier otro documento, electrónico o de cualquier otro tipo son propiedad del RENIEC y de uso exclusivo de la ECEP.

Por tanto, se prohíbe cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son de titularidad de la ECEP, sin la autorización expresa del RENIEC.

Las claves privadas y las claves públicas son propiedad del titular y/o suscriptor, independientemente del medio físico que se emplee para su almacenamiento.

El titular del certificado digital conserva cualquier derecho que pudiere ostentar sobre la marca producto o nombre comercial contenido en el

[9] **Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales**
No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:

1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.

certificado digital.

9.6. Representaciones y garantías

9.6.1. Representaciones y garantías de la EC

Son obligaciones de la ECEP las siguientes:

1. Emitir y cancelar el certificado digital previa aprobación de la solicitud por parte de la EREP.
2. Cancelar el certificado digital al suscitarse alguna de las causales señaladas en el contrato e incluir el certificado digital cancelado en la Lista de Certificados Digitales Cancelados.
3. Mantener la confidencialidad de la información relativa al titular y/o suscriptor, limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o pedido del titular y/o suscriptor.
4. Mantener actualizado el estado de los certificados digitales en la base de datos.
5. Proceder, por medio de la correspondiente EREP, a la entrega del certificado digital al titular y/o suscriptor conforme a las condiciones definidas en el presente documento.
6. En general, es obligación de la ECEP cumplir con todas las obligaciones establecidas en el artículo 26° del D.S N° 052-2008-PCM.

En ese sentido, la ECEP asumirá responsabilidad por la emisión, cancelación y consulta del estado del certificado digital. No obstante, la ECEP no será responsable por:

1. Los daños derivados de o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del titular y/o suscriptor.
2. Cualquier violación a la confidencialidad que en el uso de datos personales pudiera incurrir el propio titular y/o suscriptor.
3. La utilización incorrecta del certificado digital y de las claves, así como de cualquier daño indirecto que pueda resultar de la utilización del certificado digital o de la información almacenada en el procesador del dispositivo criptográfico.
4. Los daños que puedan derivarse de aquellas operaciones en que se hayan incumplido las limitaciones de uso del certificado digital.
5. El contenido de aquellos documentos firmados digitalmente por el titular y/o suscriptor.
6. La falta de diligencia o cuidado del suscritor en la protección de su contraseña o PIN de acceso a su clave privada.

9.6.2. Representaciones y garantías de la ER

No aplica a la ECEP.

9.6.3. Representaciones y garantías de los suscriptores

Para mayor detalle revisar el ítem 9.6.3 de la correspondiente DPR.

9.6.4. Representaciones y garantías de los terceros que confían

Para mayor detalle revisar el ítem 9.6.4 de la correspondiente DPR.

9.6.5. Representaciones y garantías de otros participantes

Es responsabilidad de la ECEP la publicación de información relevante respecto a los certificados digitales emitidos, en sus repositorios.

La ECEP es también la encargada de administrar los repositorios mencionados en el ítem 2.1 del presente documento.

9.7. Exención de garantías

La ECEP está exenta del pago de indemnización alguna en caso que el hecho o circunstancia acaecida no sea consecuencia de lo declarado en la sección 9.9 del presente documento.

9.8. Limitaciones a la responsabilidad

La ECEP no será en ningún caso responsable cuando se encuentra en alguna de las siguientes circunstancias:

- Estado de guerra, desastre natural o cualquier otra causa de fuerza mayor, incluida el funcionamiento defectuoso de los servicios de las redes telemáticas de los ISP (Proveedores de Internet), fluido eléctrico o equipos informáticos de terceros.
- Por el uso que se pueda realizar de los certificados digitales, en especial por el contenido de los mensajes o documentos firmados o cifrados.

9.9. Indemnizaciones

La ECEP-RENIEC dispondrá de una garantía con cobertura suficiente de responsabilidad civil, a través del seguro contratado por el RENIEC. El referido seguro cubrirá el riesgo de la responsabilidad por los daños y perjuicios que se pudiese ocasionar a terceros como resultado de las actividades a cargo de la ECEP-RENIEC, cumpliendo así con lo dispuesto en el artículo 27 del Reglamento de la Ley de Firmas y Certificados Digitales.

9.10. Término y terminación

9.10.1. Término

El presente documento entra en vigencia desde el momento en que es aprobado por la AAC, y su periodo de vigencia es de 05 años de acuerdo a la legislación vigente. Esto sin perjuicio que en el trascurso de este tiempo este documento pueda ser modificado por decisión propia del RENIEC o determinación de la AAC.

9.10.2. Terminación

En caso de cese de actividades de la ECEP, ésta y la EREP, según les

corresponda, informarán a la AAC (INDECOPI), así como a los titulares, suscriptores y terceros que confían sobre el cese de las operaciones de la ECEP, con un mínimo de treinta (30) días calendario de anticipación.

9.10.3. Efecto de terminación y supervivencia

Las obligaciones y restricciones que establecen en esta Declaración de Prácticas y Políticas de Certificación, en referencia a auditorías, información confidencial, obligaciones y responsabilidades, nacidas bajo la vigencia del presente documento, subsistirán tras su sustitución o derogación por una nueva versión en todo en lo que no se oponga a ésta.

9.11. Notificaciones y comunicaciones individuales con los participantes

Toda notificación o comunicación con la ECEP, se hará a través de la correspondiente EREP, mediante correo electrónico o por escrito dirigido a la dirección postal señalada en la ítem 1.5 del presente documento.

Las comunicaciones producirán sus efectos cuando se envíe el acuse de recibo o el escrito se presente a mesa de partes del RENIEC, en la dirección a la que se refiere el párrafo precedente.

9.12. Enmendaduras

9.12.1. Procedimiento para enmendaduras

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

9.12.2. Mecanismos y periodos de notificación

La ECEP 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 el INDECOPI.

La ECEP 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 del RENIEC, 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 será aprobado previamente por la AAC.

9.13. Procedimiento sobre resolución de disputas

En caso el reclamo esté directamente relacionado con el servicio de certificación digital brindado por la EREP, o la ECEP, se deberá acercar a la oficina EREP en la cual solicitó su certificado digital, para presentar su reclamo respectivo.

El reclamo será resuelto por la EREP en primera instancia, y de conformidad con lo establecido en la Segunda Disposición Complementaria Final del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo N° 052-2008-PCM, la AAC – INDECOPI resolverá el recurso de apelación presentado por el titular y/o suscriptor.

9.14. Ley aplicable

El funcionamiento y operaciones de la ECEP, así como el presente documento estarán sujetos a la normatividad que resulte aplicable y en especial a las disposiciones siguientes:

- Ley N° 27269 - 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 Registro 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. Conformidad con la ley aplicable

Es responsabilidad de la ECEP en la prestación de sus servicios, velar por el cumplimiento de la legislación aplicable recogida en el ítem 9.14 del presente documento.

9.16. Clausulas misceláneas

9.16.1. Acuerdo Íntegro

Los titulares y/o suscriptores de certificados digitales, así como los terceros que confían deben observar en su totalidad el contenido del presente documento, así como las actualizaciones que se realice sobre el mismo, las cuales estarán disponibles en la siguiente dirección: http://www.reniec.gob.pe/repository/

Para mayor información sobre los contratos y acuerdos, revisar la DPR utilizada por la EREP en la cual solicitó su certificado.

9.16.2. Subrogación

Las funciones, deberes y derechos asignados al RENIEC, en su calidad de ECEP, no serán objeto de cesión de ningún tipo a terceros, así como ninguna tercera entidad podrá subrogarse en dicha posición jurídica, salvo por disposición legal que expresamente disponga lo contrario.

9.16.3. Divisibilidad

En el caso que alguna estipulación del contrato de prestación de servicios de certificación digital llegase a ser declarada invalida, nula o inexigible legalmente o por orden judicial, se entenderá por no puesta. La invalidez de alguna cláusula no afectará en nada al resto del contrato.

9.16.4. Ejecución (tarifas de abogados y cláusulas de derechos)

No se estipula.

9.16.5. Fuerza Mayor

La ECEP, en ningún caso será responsable por daños o perjuicios causados por:

- Catástrofes naturales;
- Casos de guerra;
- Actos de terrorismo y/o sabotaje;
- Otros actos de fuerza mayor.

Sin perjuicio de lo expuesto, la ECEP dentro de lo posible asegurará la continuidad del negocio y recuperación ante desastres.

9.17. Otras clausulas

No se estipula.

10.- BIBLIOGRAFÍA.

En la redacción del presente documento se utilizó:

- Ley N° 27269, de Firmas y Certificados Digitales.
- Ley N° 29733, de Protección de Datos Personales.
- Reglamento de la Ley de Firmas y Certificados Digitales aprobado mediante el Decreto Supremo Nº 052-2008-PCM, y su modificatoria, el Decreto Supremo N° 070-2011-PCM.
- ANEXO 1: Marco de la Política de Registro para la Emisión de Certificados Digitales de la Guía de Acreditación de Entidades de Registro ER, versión 3.3, expedido por la AAC.
- RFC 3647 “Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framewortk” del Internet Engineering Task Force (IETF) (que sustituye a la RFC 2527).
- Norma Marco sobre Privacidad para los países integrantes del APEC, aprobada en la 16º Reunión Ministerial del APEC, Santiago de Chile, 17 y 18 de noviembre de 2004.

- Norma Técnica Peruana “NTP-ISO/IEC 17799:2001 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición (de uso obligatorio en todas las entidades integrantes del Sistema Nacional de Informática conforme lo dispone la Resolución Ministerial Nº 246-2007-PCM publicada el 25 de junio de 2007).