ALFREDO RAFAEL GALLO MONTANI
Sub Gerente de Regulación Digital (e)
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: GALLO MONTANI Alfredo Rafael (FAU20295613620)
Motivo: Soy el autor del documento
Fecha: 01/12/2017 17:06:23-0500

RICARDO JAVIER ENRIQUE SAAVEDRA MÁVILA
Gerente de Registros de Certificación Digital
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: SAAVEDRA MAVILA Ricardo Javier Enrique (FAU20295613620)
Motivo: En señal de conformidad
Fecha: 04/12/2017 15:56:23-0500

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

POLÍTICA GENERAL DE CERTIFICACIÓN

ENTIDAD DE CERTIFICACIÓN NACIONAL PARA EL ESTADO PERUANO
ECERNEP

Versión: 1.0	**Año: 2017**

Elaborado por:	**Revisado por:**	**Aprobado por:**
Jefe de la ECERNEP	Sub Gerente de Regulación Digital	Gerente de Registros de Certificación Digital

República del Perú
Firma Digital

Firmado digitalmente por ROSALES MAQUERA Cesar Roberto (FAU20295613620)
Motivo: En señal de conformidad
Fecha: 01/12/2017 09:04:26 -0500

ÍNDICE

1. INTRODUCCIÓN

En el Perú, el uso de las firmas y certificados digitales es normado por la Ley Nº 27269 - Ley de Firmas y Certificados Digitales[1] (en adelante la Ley) y su modificatoria la Ley Nº 27310. El reglamento de la Ley, aprobado por Decreto Supremo Nº 052-2008-PCM[2] (en adelante el Reglamento), regula el uso de la firma digital para los sectores público y privado, otorgando a la firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica (en adelante IOFE) la misma validez y eficacia jurídica que la firma manuscrita. En dicho reglamento, se define a la IOFE 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 a la integridad de los documentos electrónicos y la identidad de su autor[3].

El artículo 47º del mencionado Reglamento, designa 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), disponiendo se realicen los trámites correspondientes ante la AAC, con el fin de acreditarse como Prestador de Servicios de Certificación Digital (en adelante PSC[4]) y formar parte de la IOFE.

1.1. Visión general

El presente documento denominado Política General de Certificación (en adelante CP) establece las políticas que rigen a los participantes de la jerarquía PKI determinada por el certificado digital raíz denominado “ECERNEP PERU CA Root 3”.

Acorde con el Reglamento de la Ley, las entidades del gobierno que deseen acreditarse como PSC para el Estado Peruano, operarán directamente subordinadas a la ECERNEP y deberán implementar obligatoriamente las políticas establecidas en la presente CP describiendo la referida implementación en su correspondiente Declaración de Prácticas[5].

La presente CP establece las políticas de operación en el nivel de seguridad establecido por la AAC como “medio”, por lo que los PSC bajo la jerarquía “ECERNEP PERU CA Root 3” operarán en este mismo nivel de seguridad.

Asimismo, la presente CP ha sido desarrollada en conformidad con:

[1] Publicada en el Diario Oficial El Peruano el 28 de mayo de 2000.
[2] El Decreto Supremo Nº 052-2008-PCM es publicado en el Diario Oficial El Peruano el 19 de julio de 2008. El Reglamento es objeto de modificaciones mediante decretos supremos Nº 070-2011-PCM de 26 de julio de 2011, Nº 105-2012-PCM de 20 de octubre de 2012 y Nº 026-2016-PCM.
[3] Decimocuarta Disposición Complementaria Final del Reglamento de la Ley de Firmas y Certificados Digitales.
[4] De acuerdo al Artículo 23º del Reglamento de la Ley, un PSC puede adoptar cualquiera de las modalidades siguientes o todas: (a) Entidad de Certificación, (b) Entidad de Registro y/o (c) Prestador de Servicios de Valor Añadido.
[5] De acuerdo al Artículo 47º y 48º del Reglamento de la Ley, las entidades de la Administración Pública que opten por constituirse como ECEP y/o EREP deberán cumplir con las políticas y estándares que sean propuestos por la ECERNEP y aprobadas por la AAC.

- Lo estipulado en el RFC 3647,
- Los lineamientos dados en el documento de APEC denominado "*Public Key Infrastructure (PKI) Guidelines, Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross-Jurisdiction eCommerce*", en particular en lo referido a su marco de políticas y prácticas de certificación, y
- Las Guías de Acreditación publicadas por la AAC, en particular con lo señalado en el Anexo 1 de la Guía de Acreditación de Entidades de Certificación EC Versión 3.3, Guía de Acreditación de Entidades de Registro ER Versión 3.3 y en la Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA Versión 4.0.

1.2. Nombre e identificación del documento

- **Nombre:** Política General de Certificación ECERNEP PERU
- **Versión:** 3.0
- **OID:** 1.3.6.1.4.1.35300.2.1.3.1.0.101.1000
- **Website:** https://pki.reniec.gob.pe/repositorio/
- **Fecha de elaboración:** 03/05/2017
- **Fecha de última modificación:** 03/05/2017
- **Lugar:** Lima, Perú.

1.3. Participantes

1.3.1. Entidad de Certificación Nacional para el Estado Peruano (ECERNEP)

La ECERNEP es la encargada de administrar los certificados digitales raíz. Asimismo, tiene como función emitir y cancelar los certificados digitales destinados a los PSC del Estado Peruano acreditados ante la AAC y tramitar las solicitudes correspondientes. El certificado digital raíz de la ECERNEP es autofirmado y es el inicio de la cadena de confianza de todos los participantes de la jerarquía.

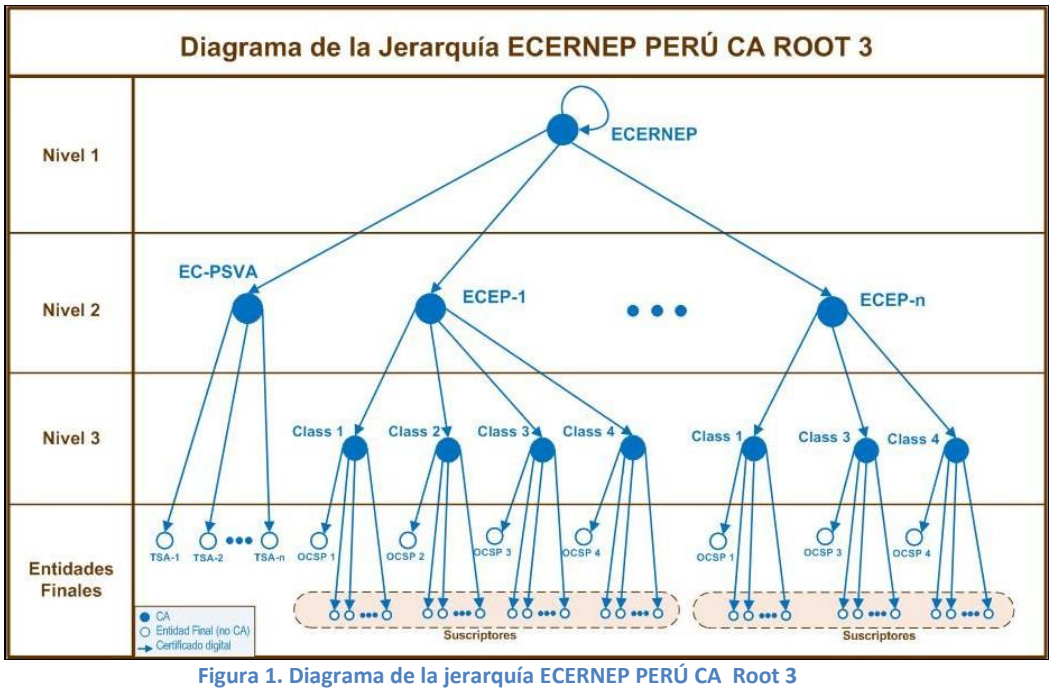

Figura 1. Diagrama de la jerarquía ECERNEP PERÚ CA Root 3

1.3.2. Entidades de Certificación para el Estado Peruano (ECEP)

Las ECEP son Entidades de Certificación acreditadas por la AAC, operan subordinadas a la ECERNEP y tienen como función principal gestionar el ciclo de vida de los certificados digitales de Entidades Finales. Típicamente, el ciclo de vida de un certificado digital comprende su emisión, renovación, reemisión, modificación, cancelación y suspensión. Sin embargo, dentro del marco de esta CP, las ECEP solamente pueden gestionar los servicios de emisión, suspensión y cancelación de certificados digitales. Las ECEP no pueden brindar estos servicios directamente a las Entidades Finales, sino que deben hacerlo únicamente a través de entidades acreditadas ante la AAC como EREP.

Para acreditarse ante la AAC las ECEP deben desarrollar su correspondiente Declaración de Prácticas de Certificación (en adelante CPS), la cual, en conformidad con lo dispuesto en el artículo 48º del Reglamento de la Ley, debe recoger las políticas contenidas en esta CP.

1.3.3. Entidades de Registro o Verificación para el Estado Peruano (EREP)

Una EREP es una entidad que presta sus servicios necesariamente asociada a una ECEP. Las EREP deben acreditarse ante la AAC y deben desarrollar su correspondiente Declaración de Prácticas de Registro (en adelante RPS) alineada a esta CP y a la CPS de su ECEP asociada, de conformidad con lo dispuesto en el artículo 48º del Reglamento de Firmas y Certificados Digitales.

La función principal de una EREP es la verificación de la identidad de los solicitantes, quienes realizan solicitudes de emisión y cancelación de certificados digitales. Una EREP debe realizar el levantamiento de datos y la comprobación de la información brindada por el solicitante. Asimismo, debe aceptar, autorizar o rechazar las solicitudes de emisión o cancelación de certificados digitales, comunicándoselo a la respectiva ECEP con la que se encuentra asociada, de acuerdo a lo estipulado en su correspondiente RPS.

1.3.4. Prestadores de Servicios de Valor Añadido para el Estado Peruano (en adelante PSVA)

En conformidad con lo dispuesto en el Art. 50º del Reglamento de la Ley, un PSVA es aquel que brinda servicios bajo las siguientes modalidades:

- Sistema de Intermediación Digital (SID) cuyo procedimiento concluye con una microforma o microarchivo.
- Sistema de Intermediación Digital (SID) cuyo procedimiento no concluye con una microforma o microarchivo.
- Autoridad de Sellado de Tiempo (TSA).

Las entidades acreditadas por la AAC como PSVA en la modalidad de Autoridad de Sellado de Tiempo deben desarrollar su Declaración de Prácticas en concordancia con la Política de Certificación de PSVA que publica la ECERNEP.

Asimismo, las entidades ECERNEP, ECEP, EREP y PSVA son las responsables de aplicar las disposiciones establecidas en la presente política de certificación.

1.3.5. Entidades Finales

Las Entidades Finales pueden ser personas naturales o personas jurídicas. Las personas naturales se constituyen siempre en titulares y suscriptores del certificado digital, mientras que las personas jurídicas, dependiendo del tipo de certificado digital, se constituyen en titular o en titular y suscriptor.

- Suscriptor: Personas naturales responsables del control y uso de la llave privada asociada a su certificado digital.
- Titular: Persona natural o jurídica sobre la que recae la responsabilidad sobre los efectos jurídicos de sus firmas digitales.

1.3.6. Terceros que confían

Los terceros que confían pueden ser personas naturales, jurídicas, equipos, servicios o cualquier otro ente diferente al suscriptor que decide confiar en un certificado digital emitido por la ECERNEP y por las ECEP y, por lo tanto, en las firmas digitales y mensajes cifrados correspondientes.

1.3.7. Otros participantes

Se considera como otros participantes a aquellas entidades que proveen servicios de soporte a las operaciones del proceso de certificación digital. En caso que un PSC participante de la jerarquía requiera la tercerización de algún servicio, esto deberá estar claramente establecido en su CPS y debe ser comunicado a la AAC para su evaluación dentro del proceso de acreditación. Asimismo, debe suscribir un acuerdo que cuente con las cláusulas específicas relacionadas con la seguridad de la información y la protección de los datos personales de acuerdo a la normativa y legislación del Estado Peruano.

1.4. Uso de un certificado digital

La jerarquía bajo el alcance de la presente CP, denominada “ECERNEP PERU CA Root 3”, ha sido estructurada en tres niveles de Autoridades de Certificación:

- **Nivel 1:** En este nivel se encuentra únicamente el certificado raíz de la ECERNEP, cuya llave privada debe ser operada en modo *offline*.
- **Nivel 2:** En este nivel se encuentran los certificados digitales de los PSC cuyas llaves privadas son operadas en modo *offline*.
- **Nivel 3:** En este nivel se encuentran los certificados digitales de los PSC cuyas llaves privadas son operadas en modo *online*.

1.4.1. Usos apropiados de los certificados digitales

Nivel 1: El certificado raíz de la ECERNEP debe ser usado exclusivamente para la emisión de certificados digitales de Nivel 2.

Nivel 2: Los certificados digitales de las ECEP, deben ser usados exclusivamente para la emisión de sus correspondientes certificados digitales de Nivel 3.

El certificado digital de la EC-PSVA, la misma que es gestionada como una instancia de la ECERNEP, debe ser usado exclusivamente para la emisión de certificados digitales de PSVA bajo la modalidad de TSA.

Nivel 3: Los certificados digitales de este nivel deben ser utilizados únicamente para emitir certificados digitales de Entidad Final solicitados a través de una EREP debidamente acreditada. Se permite a las ECEP emitir certificados bajo su titularidad para firmar las respuestas correspondientes al servicio de verificación del estado del certificado en línea (en adelante OCSP).

Entidad Final: Los certificados de Entidad Final deben ser utilizados únicamente en aplicaciones que se encuentran en concordancia con lo estipulado en la extensión Uso de Llaves (*keyUsage)*, según lo indicado en el numeral **7.1.2, Extensiones del certificado digital,** del presente documento. Las firmas digitales generadas a partir de certificados digitales emitidos para su uso en agentes automatizados permiten garantizar en cierto grado la integridad y la autenticidad de los documentos electrónicos a los que se les asocia, más no pueden implicar una manifestación de voluntad en tanto no existe un suscriptor que directamente las genere.

1.4.2. Usos prohibidos del certificado

Ningún certificado digital perteneciente a la jerarquía debe ser utilizado en situaciones diferentes a las descritas en el numeral **1.4.1, Usos apropiados de los certificados digitales**, del presente documento.

1.5. Administración de la CP

1.5.1. Organización que administra el documento

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 electrónico:** identidaddigital@reniec.gob.pe
- **Dirección:** Jr. Bolivia 109, Centro Cívico - Cercado de Lima.

1.5.2. Persona de contacto

- **Contacto:** Sub Gerente de Regulación Digital.
- **Dirección de correo electrónico:** identidaddigital@reniec.gob.pe
- **Dirección:** Jr. Bolivia 109, Centro Cívico, Cercado de Lima.

1.5.3. Persona que determina la conformidad

Según lo dispuesto en el Art. 48º del Reglamento de la Ley, la AAC es la responsable de aprobar las CP y las declaraciones de prácticas de todos los PSC.

1.5.4. Procedimiento de aprobación

La presente CP así como todas las declaraciones de prácticas son propuestos por los PSC a la AAC, a quien corresponde su aprobación mediante sus procedimientos, según lo dispuesto en el Reglamento de la Ley.

1.6. Definiciones, abreviaturas y acrónimos

Ver Anexo 1.

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

Un repositorio tiene como finalidad el almacenamiento y la recuperación de información de forma irrestricta por medios telemáticos.

Los PSC, y de ser el caso el Proveedor del Servicio de Repositorio, están sujetos a las obligaciones y responsabilidades legalmente establecidas dentro del marco de la IOFE. Las obligaciones y responsabilidades correspondientes al repositorio deben ser registradas en la Declaración de Prácticas del PSC.

Asimismo, los PSC deberán asegurarse de que los terceros que confían tengan conocimiento de sus responsabilidades y de las limitaciones de las mismas con anterioridad a la utilización del Repositorio.

Los PSC deben asegurarse de que los datos relativos a los titulares del certificado, suscriptores y terceros que confían que son obtenidos al momento de la suscripción al servicio, se encuentren protegidos de conformidad con los requisitos establecidos bajo el marco de la IOFE y la Ley N° 29733 - Ley de Protección de Datos Personales y su Reglamento. Asimismo, deberán respetar los principios de privacidad establecidos en el Marco sobre Privacidad, aprobados por la AAC.

2.1. Repositorio

Cada PSC es responsable de gestionar repositorios en la Web como mínimo con la siguiente información:

- Directorio de certificados digitales emitidos (solo Entidades de Certificación)
- Listas de certificados cancelados (solo Entidades de Certificación)
- Política General de Certificación y Política de Prestador de Servicios de Valor Añadido para servicio de sellado de tiempo (solo ECERNEP)
- Declaraciones de Prácticas de Certificación (solo ECEP)
- Declaraciones de Prácticas de Registro (solo EREP)
- Políticas de Privacidad
- Políticas de Seguridad
- Otros instrumentos legales vinculantes con suscriptores, titulares, terceros que confían y cualquier otro PSC.

Los instrumentos legales vinculantes deben ser fácilmente identificables para cada certificado[6].

El directorio de certificados digitales emitidos debe estar disponible las 24 horas de cada día, durante los siete días de cada semana. En caso de indisponibilidad no imputable al PSC, el mismo debe aplicar la máxima diligencia en recuperar la disponibilidad en el periodo indicado en la CPS[7].

Los responsables de los repositorios deben asegurarse que éstos se encuentren disponibles la mayor parte del tiempo en que los terceros que confían requieran acceder a los mismos.

[6] Cfr. la sección 6.1.d) de ETSI EN 319 411-1.
[7] Cfr. sección 6.1.e.ii) de ETSI EN 391 411-1.

Deben asegurar una disponibilidad mínima de 99% anual, con un tiempo programado de inactividad máximo de 0.5% anual. Asimismo, deben asegurar que el Repositorio sea accesible a los potenciales terceros que confían, utilizando para tales efectos protocolos de acceso y tecnologías telemáticas interoperables.

2.2. Publicación de información de certificación

Las modificaciones relativas a las Declaraciones de Prácticas de los PSC deben ser publicadas a la mayor brevedad posible, debiéndose tener cuidado de cumplir con los requisitos para la aprobación de dichas modificaciones. Todas las modificaciones deben ser aprobadas por la AAC antes de su publicación.

Las ECEP deben mantener los repositorios actualizados y disponibles en la Web de tal forma que los terceros que confían puedan verificar la información de los certificados digitales y su estado. Asimismo, deberán proporcionar información de cómo encontrar el repositorio adecuado para verificar el estado del certificado digital mediante la CRL y los servicios de validación en línea (OCSP), las versiones de las políticas que implementan, los perfiles de los certificados digitales y los certificados digitales de la cadena de certificación. Además, deberán utilizar controles apropiados para restringir la posibilidad de modificación no autorizada de la información contenida en los repositorios.

Los certificados sólo se deberán listar en el directorio de certificados digitales emitidos contando con el consentimiento de su suscriptor y de su titular. Asimismo, solo se podrá poner a disposición certificados digitales para su descarga o recuperación contando con el consentimiento de su suscriptor y de su titular[8]. La AAC publica los certificados digitales de los PSC acreditados en el Registro Oficial de Prestadores de Servicio de Certificación Digital (ROPS), encontrándose disponibles para su descarga o recuperación.

Cuando la publicación de algún dato pudiese afectar la seguridad o las operaciones del PSC, este dato puede ser omitido, pero deberá dejarse constancia de su existencia. Un PSC debe indicar en su Declaración de Prácticas si cuenta con información no publicada y de qué manera se deja constancia de su existencia.

2.3. Frecuencia de publicación

Los PSC deben gestionar y mantener actualizados sus repositorios conforme a la siguiente frecuencia:

- Directorio de certificados digitales emitidos: Actualizado cada vez que se emite un nuevo certificado digital.
- Listas de certificados digitales cancelados (CRL): Actualizado cada vez que se cancela un certificado digital de una Entidad de Certificación de Nivel 2 o Nivel 3 o de acuerdo a lo indicado en el numeral **4.9.7, Frecuencia de publicación de la Lista de Certificados Cancelados (CRL)**, del presente documento.
- Repositorio de las Políticas y Declaraciones de Prácticas: Actualizado cada vez que la AAC aprueba una nueva versión de las mismas.

[8] Cfr. la sección 6.1.b) de ETSI EN 319 411-1.

2.4. Control de acceso a los repositorios

Dentro de su comunidad, los PSC no deben limitar el acceso de lectura a la información, pero deben impedir que de forma no autorizada se puedan añadir, modificar o borrar registros del Repositorio.

Los PSC deben emplear sistemas fiables para el Repositorio, de modo tal que:

- Únicamente las personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad e integridad de la información.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Convención de nombres

Todos los certificados digitales de la jerarquía ECERNEP PERU CA Root 3 deben contener información distintiva que permita identificar al emisor y al titular y/o suscriptor. Tal información, debe estar especificada en los campos *IssuerDN (Issuer Distinguished Name)* y *SubjectDN (Subject Distinguished Name)*, respectivamente, conforme a las especificaciones de la familia de estándares ISO/IEC 9594 (recomendación X.500 y X.501).

3.1.1. Tipos de nombres

El campo *SubjectDN* de todos los certificados digitales de la jerarquía ECERNEP PERU CA Root 3 debe identificar de forma única y plena a un titular y/o suscriptor de un certificado digital de cualquier nivel y tipo. En particular, puede ser utilizada la extensión *SubjectAltName y el Campo SubjectDN* con los siguientes atributos.

Campo	Atributos	Nombre en inglés
Subject Distinguished Name	CN	*Common Name*
	SN	*Surname*
	GIVENNAME	*Givenmane*
	O	*Organization*
	OU	*Organization Unit*
	ST	*State*
	L	*Locality*
	C	*Country*
	SERIALNUMBER	*SerialNumber*
SubjectAltName		*Subject Alternative Name*

Tabla 1 – Campos de un DN (*DistinguishedName*)

En los certificados para pruebas, no es obligatoria la verificación de toda la información del titular o suscriptor. Por lo tanto, se puede obviar la inclusión de algunos atributos o pueden contener información ficticia. Los certificados de prueba deben contener un mensaje o frase en el CN que sirva para identificar plenamente la naturaleza del certificado; por ejemplo “IDENTIDAD NO VALIDADA”, “SOLO PARA PRUEBAS”, etc. Las ECEP deben definir en sus perfiles la forma para identificar fehacientemente a los certificados para pruebas.

Para el caso de Entidades Finales, el uso de nombres alternativos en la extensión *SubjectAltName* está permitido de manera opcional. Esta extensión puede contener información adicional sobre el suscriptor, de tal manera que las partes que confían puedan tener información extra que permita identificarlo inequívocamente. Por ejemplo, si se desea incluir una dirección de correo electrónico (e-mail) del suscriptor, esta información se debe colocar en el campo rfc822Name de la extensión “*SubjectAltName* tal como se indica en **ETSI TS 119 412-2 V1.1.1 (2012-04), página 16, sección A.4.7**.

Referenced standard	Section	Requirement or recommendation
RFC 5280 [3]	4.1.2.6	*"Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name in the subject alternative name extension (section 4.2.1.6) to describe such identities".*
RFC 5280 [3]	4.2.1.7	*"When the subjectAltName extension contains an Internet mail address, the address MUST be stored in the rfc822Name".*

Figura 2 - Valor de la extensión Nombre Alternativo del Sujeto *(Subject Alternative Name)*
Fuente: ETSI TS 119 412-2 V1.1.1 (2012-04), página 16, sección A.4.7

3.1.2. Necesidad de nombres significativos

El campo *SubjectDN* de todos los certificados digitales de la jerarquía de certificación debe permitir determinar sin ambigüedad la identidad del suscriptor para quién se emitió el certificado digital.

3.1.3. Anonimato o seudónimo de los suscriptores

No se permite la emisión de ningún certificado digital anónimo dentro de la jerarquía ECERNEP PERU CA Root 3.

El uso de seudónimos está permitido en certificados digitales emitidos para sistemas de información.

Sin embargo, la ECERNEP permite la emisión de certificados de entidades finales para fines de pruebas y auditorias, con información inexacta o no validada en los campos y extensiones relacionados al nombre. Estos certificados no deben tener una vigencia mayor a 45 días, deben ser emitidos bajo un perfil diferente a los certificados que no son para pruebas y deben consignar en el CN la frase “Identidad No Validada”.

3.1.4. Reglas de interpretación de diferentes modalidades de nombres

Las reglas para establecer e interpretar los campos *IssuerDN* y *SubjectDN* en los certificados digitales de la jerarquía son las descritas en la familia de estándares ISO/IEC 9594 (recomendación X.500). Así, la estructura de un DN *(DistinguishedName)* se define en el estándar ISO/IEC 9594-2 (recomendación ITU-T X.501), que es construida con los atributos definidos en el estándar ISO/IEC 9594-6 (recomendación ITU-T X.520). Los numerales 4.1.2.4 y 4.1.2.6 del RFC 5280, indican el conjunto de atributos obligatorios y opcionales que deben contener los campos *IssuerDN* y *SubjectDN.*

3.1.5. Unicidad de Nombres

Se debe garantizar que el *SubjectDN* del certificado digital para un determinado suscriptor sea único no sólo durante el periodo de vigencia del certificado, sino durante la existencia de la jerarquía de certificación digital. Por lo tanto, no se puede reasignar un nombre a un suscriptor que ya hubiera sido asignado a otro diferente.

Para evitar conflictos de nombres en certificados correspondientes a personas naturales, los datos del titular relacionados a su identidad a incorporarse en el *SubjectDN,* deben comprender sus nombres y apellidos más el número de su documento nacional de identidad (DNI).

En certificados digitales para personas jurídicas, los datos de identificación del titular a incorporarse en el *SubjectDN* deben comprender su denominación o razón social y su Registro Único del Contribuyente (RUC), y en el caso del suscriptor, sus nombres y apellidos más el número de su documento oficial de identidad.

En cualquier caso, las ECEP deben utilizar mecanismos que les permitan evitar conflictos de nombres.

3.1.6. Reconocimiento, autenticación y rol de las marcas registradas

La ECERNEP no debe arbitrar, mediar o resolver ninguna disputa concerniente a la propiedad de nombres de instituciones o marcas registradas. La ECERNEP debe utilizar nombres y denominaciones oficiales en los certificados digitales que emite. Está prohibido que los participantes de la jerarquía usen nombres que infrinjan la propiedad intelectual de otros.

No le corresponde a las EREP determinar si un solicitante de certificados posee derecho sobre el nombre que aparece en una solicitud de certificado. Asimismo, no le corresponde resolver ninguna disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales. Sin embargo, una EREP debe cerciorarse, mediante la validación de la documentación e información requerida del solicitante del certificado, que tanto el nombre del titular como del suscriptor correspondan a los solicitantes. Las EREP están facultadas a rechazar una solicitud de certificado a causa de conflicto de nombres.

Se prohíbe a los solicitantes de certificados de Entidad Final de personas jurídicas que incluyan nombres en las solicitudes que puedan suponer infracción de derechos de terceros. En el caso de personas jurídicas, no se podrá volver a asignar un nombre de titular o suscriptor que ya haya sido asignado a un titular o suscriptor diferente, tal como se indica en el numeral **3.1.5 Unicidad de Nombres**.

3.2. Validación inicial de la identidad

A este respecto, deberá cumplirse con lo establecido en el Reglamento de la Ley de Firmas y Certificados Digitales y en el Anexo 1, Marco de la Política de Registro para la emisión de Certificados Digitales, de la Guía de Acreditación de Entidades de Registro ER.

3.2.1. Método para probar la posesión de la llave privada

La ECERNEP no debe generar las llaves de los certificados digitales de sus subordinados. Los PSC subordinados deben generar su propio par de llaves, tal como se indica en el numeral **6.1.1 Generación del par de llaves** y deben demostrar la posesión de su llave privada mediante el envío de un mensaje de prueba de posesión de llave privada, conforme a lo estipulado en el RFC 4210, como por ejemplo un *Certificate Signing Request* (CSR) en formato PKCS#10, según lo estipulado en el RFC2986.

En caso que una Entidad Final solicitante de un certificado digital genere sus propias llaves, deberá demostrar la posesión de la llave privada mediante el envío de un mensaje de prueba de posesión de llave privada, conforme a lo estipulado en el RFC 4210, como el CSR en formato PKCS#10, según lo estipulado en el RFC 2986. No se requiere prueba de posesión en caso de que la generación de llaves de Entidades Finales se encuentre bajo el control directo de una ECEP o EREP.

3.2.2. Autenticación de identidad de personas jurídicas

Los entidades solicitantes de la Administración Pública comprendidas en el Artículo I, del Título Preliminar de la Ley Nº 27444 – Ley del Procedimiento Administrativo General, que requieran certificados digitales subordinados a la ECERNEP deben presentar una solicitud firmada por el máximo representante de la entidad, adjuntando la resolución de acreditación emitida por la AAC, ya sea el caso de una ECEP o un PSVA-TSA.

Para la emisión de certificados digitales de Entidad Final de personas jurídicas se debe proceder de acuerdo a lo establecido en el numeral **3.2.5. Validación de autoridad para efectuar la solicitud** a fin de verificar la identidad de la persona jurídica mediante los documentos sobre su constitución y de acuerdo a lo establecido en la Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias y en las Guías de Acreditación de la AAC.

Las EREP deben definir e indicar en su RPS los procedimientos de autenticación de la identidad de los suscriptores asociados a la persona jurídica, según lo indicado en el numeral **3.2.3. Autenticación de identidad de personas naturales**.

3.2.3. Autenticación de identidad de personas naturales

Para la emisión de certificados digitales de Entidad Final a personas naturales se debe verificar la identidad del solicitante usando el Registro Único de Identificación de Personas Naturales del RENIEC y mediante la comprobación de su Documento Nacional de Identidad (DNI) vigente. Para incrementar la seguridad en el procedimiento de verificación, podrá hacerse uso de los servicios biométricos del RENIEC.

En el caso de tratarse de solicitantes extranjeros deberá efectuarse la verificación de su identidad mediante el correspondiente registro oficial de extranjeros.

Se precisa que los certificados digitales de Entidad Final entregados a los ciudadanos peruanos en el DNI electrónico (ECEP Class II) pueden ser emitidos únicamente por la ECEP del Registro Nacional de Identificación y Estado Civil, en conformidad con lo establecido en el Reglamento de la Ley de Firmas y Certificados Digitales y en la Ley Nº 26497 – Ley Orgánica del Registro Nacional de Identificación y Estado Civil.

3.2.4. Información no verificada del suscriptor

Toda la información a incluirse en un certificado digital debe ser siempre verificada por las EREP durante el proceso de autenticación de la identidad. Cualquier dato o información que no hayan sido verificados no deben incluirse en el certificado digital.

La EREP debe indicar en su RPS los procedimientos de autenticación de la identidad de los solicitantes según lo indicado en el numeral **3.2.1, Método para probar la posesión de la llave privada, 3.2.2, Autenticación de identidad de personas jurídicas** y **3.2.3. Autenticación de identidad de personas naturales**.

3.2.5. Validación de autoridad para efectuar la solicitud

Las EREP deben validar el derecho que posee un solicitante para gestionar un tipo de certificado digital específico. En particular, para el caso de una persona jurídica, la solicitud del certificado digital del cual ésta será titular y el registro o verificación de su identidad deben ser realizados a través de un representante debidamente acreditado y con las atribuciones y los poderes de representación correspondientes.

3.2.6. Criterios de interoperabilidad

La jerarquía de la ECERNEP debe operar independientemente de otras PKI fuera del marco de la IOFE; sin embargo, se debe garantizar la interoperabilidad con las PKI que satisfagan los requisitos técnicos y jurídicos en conformidad con la legislación y normativa nacional, en particular con los artículos 6º y 73º del Reglamento.

3.3. Identificación y autenticación para solicitudes de reemisión con renovación de llaves

3.3.1. Solicitudes rutinarias de renovación de llaves

No aplica

3.3.2. Renovación de llaves luego de la cancelación

No aplica

3.4. Identificación y autenticación para solicitudes de cancelación

La ECERNEP debe verificar y procesar las solicitudes de cancelación de los certificados digitales directamente subordinados a ella.

Lo referido a la verificación y procesamiento de solicitudes de cancelación de certificados digitales de Entidad Final de personas naturales o jurídicas debe contemplarse en la correspondiente RPS de la EREP. El suscriptor o el titular pueden solicitar a la EREP la cancelación de su certificado digital correspondiente utilizando mecanismos que garanticen el no repudio.

4. CICLO DE VIDA DEL CERTIFICADO DIGITAL: REQUISITOS OPERACIONALES

Las operaciones relacionadas al ciclo de vida de los certificados digitales bajo la jerarquía ECERNEP PERU CA Root 3 son: emisión, suspensión y cancelación de certificados y publicación de la CRL. La ECERNEP debe procesar solicitudes de emisión de certificados digitales para los PSC que hayan sido acreditados ante la AAC. La ECERNEP debe asegurarse de que el PSC solicitante haya generado su par de llaves de manera correcta y que la llave pública guarde relación con la llave privada, tal como se indica en el numeral **6.1.1 Generación del par de llaves**. La ECERNEP deberá aceptar únicamente solicitudes de emisión y pedidos de cancelación de certificados digitales a través del representante legal de la entidad, o de apoderado debidamente autorizado por ésta.

Los requisitos operacionales del ciclo de vida de los certificados digitales de Entidad Final son descritos en las siguientes secciones. Se incluyen, en cuanto corresponde, requisitos para los certificados digitales emitidos por la ECERNEP.

4.1. Solicitud de certificado digital

4.1.1. Personas habilitadas para presentar una solicitud de certificado

- Las EREP deben definir en su RPS, en conformidad con la presente CP y la CPS de su ECEP asociada, el conjunto de personas habilitadas para solicitar cada tipo de certificado digital de Entidad Final.
- La solicitud de un certificado digital de Entidad Final, para el caso de personas naturales, debe ser realizada por la misma persona, quien será titular y suscriptor del certificado digital.
- La solicitud de un certificado digital de Entidad Final, para el caso de personas jurídicas, debe ser realizada por el representante legal o su apoderado debidamente acreditado. En este caso, se considera como titular del certificado a la persona jurídica, y las personas naturales debidamente autorizadas son los suscriptores del certificado quienes como tales tienen bajo su control exclusivo las llaves privadas correspondientes.
- En el caso que el certificado digital esté destinado para ser usado por un sistema de información, la solicitud debe ser hecha por el representante legal de la persona jurídica poseedora del agente automatizado o por un apoderado designado por ésta. En este caso, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad para tales efectos corresponde al representante legal que en nombre de la persona jurídica solicita el certificado digital.
- Se puede permitir que múltiples titulares puedan efectuar solicitudes para un mismo suscriptor, siempre y cuando exista entre el titular y el suscriptor una relación de por medio que faculte al suscriptor para proceder de esta manera. De presentarse el caso, los solicitantes bajo el ámbito de la administración pública deberán acreditar que proceden en cumplimiento de lo establecido en la Ley Nº 28175 - Ley Marco del Empleo Público.
- Cada EREP puede establecer limitaciones para la obtención de sus certificados digitales de acuerdo a la comunidad de usuarios que haya especificado en el numeral **1.3.3, Entidades de Registro o Verificación para el Estado Peruano (EREP),** de su RPS.

4.1.2. Proceso de registro de solicitud y responsabilidades

- Las EREP deben establecer en su RPS el procedimiento necesario para realizar la solicitud de los certificados digitales de Entidad Final y las responsabilidades asumidas por el suscriptor para tales efectos.
- Las ECEP a través de las EREP asociadas deben informar a los suscriptores y titulares sobre los términos y limitaciones aplicables a los certificados digitales emitidos a su nombre. Además, deben informar las obligaciones que deben cumplir para garantizar el efecto legal de las transacciones realizadas con los certificados digitales de la jerarquía ECERNEP PERU CA ROOT 3. La entrega de dicha información a los suscriptores y titulares debe ser asumida por las EREP como parte de su convenio con las ECEP.

4.2. Procesamiento de la solicitud de certificado

4.2.1. Identificación y autenticación

Las EREP deben implementar procedimientos para la identificación y autenticación de los usuarios solicitantes, en concordancia con el tipo de certificado digital requerido y con lo establecido en el numeral **3.2.2, Autenticación de identidad de personas jurídicas,** y **3.2.3, Autenticación de identidad de personas naturales**, del presente documento. La revisión de los documentos de identificación debe ser rigurosa:

- Persona natural: los solicitantes deben proveer su documento oficial de identidad, DNI, en caso de ser ciudadanos peruanos y carné de extranjería, en caso de ser extranjeros.
- Persona jurídica: los solicitantes deben proveer los documentos que acrediten la constitución de la entidad, las facultades de su titular y/o representante legal, según el caso, su documento oficial de identidad y el de los suscriptores de los certificados.

4.2.2. Aprobación o rechazo de las solicitudes de certificados

Las EREP deben comunicar a su ECEP asociada la aprobación de la solicitud para la emisión del certificado digital respectivo.

Las EREP deben rechazar solicitudes de solicitantes que no tienen plena capacidad de ejercicio de sus derechos civiles, o si el resultado de la verificación de la identidad fue negativo, y en caso de las personas jurídicas si el representante legal o su apoderado no cuenta con un poder vigente. Una EREP puede decidir establecer en su RPS, circunstancias adicionales para el rechazo de la solicitud.

Las EREP deben requerir al suscriptor la firma de un contrato de conformidad personal y responsabilidades, así como de otro de conformidad por parte del titular y/o representante legal de la persona jurídica en cuyo nombre actúa el suscriptor. El contrato antes aludido, debe contener las obligaciones que deben cumplir los suscriptores y titulares en conformidad con la legislación vigente para garantizar el efecto legal de las transacciones realizadas empleando el certificado emitido por las ECEP, así como las responsabilidades asociadas al uso de la firma digital.

Las EREP deben establecer el contenido del contrato del suscriptor en coordinación con su ECEP asociada, reflejando las responsabilidades de la ECEP, de la EREP y la de los suscriptores y titulares. Como mínimo, se debe requerir al suscriptor y al titular lo siguiente:

- Facilitar a la EREP la información completa y adecuada, conforme a los requisitos especificados en su respectiva RPS u otra documentación relevante.
- Presentar a la EREP una solicitud de emisión de certificado debidamente firmada.
- Cumplir las obligaciones de titular y suscriptor que se establecen en la CPS de la ECEP u otro documento relevante y en el contrato del suscriptor.
- Emplear el certificado de acuerdo con lo establecido en la CPS u otro documento relevante de la ECEP y en el contrato del suscriptor.
- Ser razonablemente diligente en la custodia de su llave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en la CPS u otro documento relevante de la ECEP y en el contrato del suscriptor.
- Notificar al personal de la EREP la ocurrencia de los siguientes eventos, para proceder a la cancelación del certificado digital indicado por el solicitante, sin retrasos injustificables:
    1. La pérdida, robo o extravío del módulo criptográfico que almacena su llave privada (computador, token criptográfico o tarjeta inteligente).
    2. El compromiso potencial de su llave privada.
    3. La pérdida de control sobre su llave privada, debido al compromiso de los datos de activación o por cualquier otra causa.
    4. Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

- Dejar de utilizar la llave privada, transcurrido el plazo de vigencia del certificado.
- No monitorear, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de la IOFE, sin permiso previo por escrito de la AAC.
- No comprometer intencionadamente la seguridad de la Jerarquía de la IOFE.

Además, las ECEP en coordinación con las EREP asociadas, deben incorporar en el contrato la siguiente información para los suscriptores y titulares:

- Política de aplicación del certificado digital, limitaciones y prohibiciones de uso.
- Las responsabilidades del suscriptor y del titular frente a: la actualización de sus datos, cancelar el certificado en caso de que la llave privada se vea comprometida, reemisión de certificado antes de la expiración del certificado.
- Información sobre cómo validar el certificado, incluyendo el requisito de comprobar el estado del mismo y las condiciones en las cuales se puede confiar razonablemente en el certificado, lo cual resulta también aplicable cuando el suscriptor actúa como tercero que confía.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la ECEP acepta o excluye su responsabilidad.
- Ley aplicable y jurisdicción competente.
- Declaración de Prácticas de Certificación de la ECEP y Declaración de Prácticas de Registro de EREP aprobadas por la AAC.
- Información acerca de los módulos criptográficos de usuario final.

El contrato del suscriptor puede elaborarse en formato electrónico y firmarse digitalmente. En este caso, los sistemas informáticos de la EREP deberán soportar esta funcionalidad.

4.2.3. Tiempo límite para el procesamiento de las solicitudes de certificados

Si el resultado de la verificación de identidad del solicitante y de la información proporcionada por este son positivas, la EREP debe enviar a la ECEP correspondiente la autorización para la emisión del certificado digital de manera inmediata**.**

La ECERNEP, las ECEP y las EREP deben establecer en su CPS, en su RPS u otra documentación relevante el plazo necesario para el procesamiento de solicitudes de emisión de certificados. En cumplimiento de lo establecido en el numeral 4.2.3 del Anexo 1 de la Guía de Acreditación de Entidades de Certificación EC en su versión 3.3 y en la Guía de Acreditación de Entidades de Registro ER en su versión 3.3, este plazo no debe ser mayor a 5 días hábiles a partir de la entrevista presencial del solicitante en la EREP, considerando el tiempo requerido para el intercambio de información entre la ECEP y la EREP.

La restricción dada para este plazo podrá adecuarse en la documentación relevante en que se haya consignado siempre que se cuente con el debido sustento y que se cumpla con lo que posteriores versiones de las mencionadas guías establezcan al respecto.

4.3. Emisión del certificado

4.3.1. Acciones durante la emisión del certificado

La ECERNEP debe emitir un certificado digital si recibe una solicitud de emisión acompañada de un mensaje de prueba de posesión de llave privada, conforme a lo estipulado en el RFC 4210, como un (CSR) válido en formato PKCS#10, según lo indicado en el numeral **4.1, Solicitud de certificado digital**4.1**.**

Las ECEP deben emitir un certificado digital si reciben la solicitud de una EREP asociada.

Antes de emitir un certificado digital, los PSC deben asegurarse que el par de llaves se haya generado de manera correcta y que la llave pública guarde relación con la llave privada.

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

Las ECEP deben notificar la emisión y entregar al suscriptor el certificado digital solicitado conforme a lo establecido en su CPS. La notificación de la emisión y entrega puede realizarse mediante medios telemáticos a través del envío del certificado al suscriptor, acompañado para tales efectos de una declaración de la emisión del mismo.

4.4. Aceptación del certificado

4.4.1. Conducta constitutiva de aceptación del certificado

Se deben establecer en las declaraciones de prácticas correspondientes los procedimientos para la aceptación de un certificado digital. La aceptación de un

certificado digital puede ser evidenciada a través de una aceptación formal o de manera tácita mediante el empleo del certificado.

En el caso que el certificado digital sea remitido por medios electrónicos, se puede requerir al receptor que firme digitalmente un mensaje de aceptación utilizando las llaves del certificado remitido.

Una vez que un certificado digital es aceptado, se debe requerir al suscriptor o al titular cumplir con las responsabilidades establecidas en la CPS correspondiente, el contrato y en toda la legislación relevante, según lo señalado en el numeral **4.5.1, Uso de la llave privada y del certificado por parte del suscriptor**.

4.4.2. Publicación del certificado

La información concerniente al certificado digital emitido debe ser publicada por las entidades de certificación en los repositorios correspondientes con previo conocimiento de los suscriptores y titulares de los certificados, debiendo esto haber sido estipulado en el contrato del suscriptor. Mayor información sobre los requisitos de operatividad de los repositorios se encuentra en el numeral **2, RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO,** del presente documento.

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

No se requiere que la entidad de certificación informe a terceros sobre un certificado emitido, basta que los publique en el repositorio correspondiente la clave pública y datos que no comprometan la privacidad de los suscriptores y titulares.

4.5. Uso del par de llaves y del certificado

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

El uso de la llave privada, correspondiente a la llave pública del certificado digital, está permitido luego de que el suscriptor haya aceptado los términos y condiciones establecidos en los contratos y en las políticas y declaraciones de prácticas de certificación de la ECERNEP o de la ECEP, según el caso.

Las ECEP deben requerir del suscriptor y titular, como mínimo, lo siguiente:

- Emplear el certificado de acuerdo con lo establecido en la CPS u otro documento relevante de la ECEP y en el contrato del suscriptor.
- Ser razonablemente diligente en la custodia de su llave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en la CPS u otro documento relevante de la ECEP y en el contrato del suscriptor.
- Dejar de utilizar la llave privada, transcurrido el plazo de vigencia del certificado digital.
- Notificar a la ECEP emisora, sin retrasos injustificables, los hechos indicados a continuación. La ECEP debe indicar en su CPS el procedimiento o canales de comunicación para que el suscriptor y titular realicen la notificación correspondiente.

1. La pérdida, robo o extravío del módulo criptográfico que almacena su llave privada (computador, token criptográfico o tarjeta inteligente).
2. El compromiso potencial de su llave privada.
3. La pérdida de control sobre su llave privada, debido al compromiso de los datos de activación o por cualquier otra causa.
4. Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

Las responsabilidades del suscriptor o titular deben establecerse en el contrato del titular y/o suscriptor y la CPS de la ECEP, en conformidad con el RFC 3647.

En los casos en que la legislación establezca determinadas obligaciones para los suscriptores o titulares a efectos de asegurar las consecuencias legales de las transacciones realizadas utilizando certificados digitales emitidos por la ECEP, el contrato del suscriptor debe recoger expresamente tales obligaciones.

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

Los terceros que confían, deben usar la llave pública contenida en el certificado para realizar las validaciones indicadas únicamente en las extensiones *KeyUsage (KU) y ExtendedKeyUsage (EKU)*, tal como se expone en el numeral **6.1.7, Propósito de uso de la llave (extensión *KeyUsage* X.509 v3),** del presente documento.

La ECERNEP permite al tercero que confía el acceso a los certificados publicados en el Repositorio correspondiente de acuerdo al consentimiento de los suscriptores y titulares, como se expone en el numeral **2.1, Repositorio,** del presente documento.

Las ECEP deben requerir del tercero que confía, como mínimo lo siguiente:

- No monitorear, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de la Jerarquía ECERNEP PERU CA Root 3 de la IOFE, sin su autorización por escrito.
- No comprometer intencionadamente la seguridad de la Jerarquía ECERNEP PERU CA Root 3 de la IOFE.
- Aplicar los criterios de verificación adecuados para la validación de un certificado durante su uso en las transacciones electrónicas.
- Denunciar cualquier situación en la que la ECEP deba revocar el certificado de un titular, siempre y cuando se tengan pruebas fehacientes del compromiso de la llave privada o de su uso ilegal. Por ejemplo, debe denunciar la pérdida, robo o extravío del dispositivo criptográfico que almacena una llave privada que no le pertenece (computador, token criptográfico o tarjeta inteligente).

Las ECEP deben brindar, como mínimo, la siguiente información:

- Política de aplicación del certificado, limitaciones y prohibiciones de uso.
- Las responsabilidades del tercero que confía.
- Información sobre cómo validar el certificado, incluyendo el requisito de comprobar el estado del certificado y las condiciones en las cuales se puede confiar

razonablemente en el certificado, lo cual resulta aplicable cuando el suscriptor actúa como tercero que confía.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la EC acepta o excluye su responsabilidad.
- Ley aplicable y jurisdicción competente.
- Resolución de acreditación de la ECEP por la AAC.

Los terceros que confían deben cumplir con sus respectivas responsabilidades, las cuales deben estar establecidas en la CPS de la ECEP emisora de los certificados utilizados.

Las ECEP deben notificar al tercero que confía acerca de sus responsabilidades a través de la publicación de un documento accesible para éste. El documento debe consignar las consecuencias derivadas del incumplimiento de los términos del mismo.

4.6. Renovación del certificado

De acuerdo a lo establecido en el Anexo 1: Marco de la Política de Emisión de Certificados Digitales de la Guía de Acreditación de Entidades de Certificación EC, este servicio no puede brindarse bajo el marco de la IOFE, por lo tanto no se contempla para la jerarquía objeto de la presente CP.

4.6.1. Circunstancias para la renovación de los certificados
No aplica

4.6.2. Personas habilitadas para presentar una solicitud de renovación
No aplica

4.6.3. Procesamiento de solicitudes de renovación
No aplica

4.6.4. Notificación al suscriptor sobre la emisión de un nuevo certificado
No aplica

4.6.5. Conducta constitutiva de aceptación de renovación de certificados
No aplica.

4.6.6. Publicación del certificado por parte de la EC
No aplica.

4.6.7. Notificación de la EC a otras entidades sobre la renovación de un certificado
No aplica.

4.7. Reemisión de certificado digital con renovación de llaves

De acuerdo a lo establecido en el Anexo 1: Marco de la Política de Emisión de Certificados Digitales de la Guía de Acreditación de Entidades de Certificación EC, este servicio no puede

brindarse bajo el marco de la IOFE para certificados digitales de seguridad media, por lo tanto no se contempla para la jerarquía objeto de la presente CP.

4.7.1. Criterios para la renovación de llaves de un certificado
No aplica.

4.7.2. Solicitantes de renovación de llaves de un certificado
No aplica.

4.7.3. Procesamiento de solicitudes de renovación de llaves de un certificado
No aplica.

4.7.4. Notificación al suscriptor sobre la re-emisión de un nuevo certificado
No aplica.

4.7.5. Conducta constitutiva de aceptación de certificados con renovación de llaves
No aplica.

4.7.6. Publicación del certificado con renovación de llaves
No aplica.

4.7.7. Notificación de la EC a otras entidades sobre la re-emisión de un certificado
No aplica.

4.8. Modificación del certificado

De acuerdo a lo establecido en el Anexo 1: Marco de la Política de Emisión de Certificados Digitales de la Guía de Acreditación de Entidades de Certificación EC, este servicio no puede brindarse bajo el marco de la IOFE, por lo tanto no se contempla para la jerarquía objeto de la presente CP.

4.8.1. Criterios para la modificación de un certificado
No aplica.

4.8.2. Personas habilitadas para la solicitar la modificación de un certificado
No aplica.

4.8.3. Procesamiento de la solicitud de modificación de un certificado
No aplica.

4.8.4. Notificación al suscriptor sobre la modificación de un certificado
No aplica.

4.8.5. Conducta constitutiva de aceptación de modificación de certificados
No aplica.

4.8.6. Publicación del certificado modificado por parte de la EC

No aplica.

4.9. Cancelación y suspensión de certificados digitales

4.9.1. Motivos de cancelación

Las EREP deben especificar en su RPS, las circunstancias en las que los suscriptores, titulares o terceros pueden solicitar la cancelación de un certificado digital. Como mínimo, el titular y el suscriptor del certificado digital están obligados, bajo responsabilidad, a solicitar la cancelación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:

- Por exposición, puesta en peligro o uso indebido de la llave privada.
- Por deterioro, alteración o cualquier otro hecho u acto que afecte la llave privada.
- Cancelación de las facultades de representación y/o poderes de sus representantes legales o apoderados.
- Cuando la información contenida en el certificado digital ya no resulte correcta.
- Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la EC.
- Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometido dentro de la IOFE a través de lo estipulado en el contrato del suscriptor y/o titular.

La revocación supone la cancelación de oficio de los certificados por parte de la ECEP. Las circunstancias bajo las cuales una ECEP puede revocar los certificados de sus usuarios, deben ser claramente especificadas en los contratos de los suscriptores y titulares.

4.9.2. Personas habilitadas para solicitar la cancelación de un certificado

Las ECEP deberán aceptar únicamente el pedido de cancelación del certificado digital realizado por la EREP que aprobó su emisión.

Las personas que pueden solicitar la cancelación de un certificado digital pueden ser:

- El titular o suscriptor del certificado.
- La ECEP que emitió el certificado.
- El juez a través de una resolución judicial que lo ordene.
- La autoridad administrativa competente a través de una resolución administrativa que lo ordene.
- Un tercero que acredite pruebas fehacientes de alguno de los supuestos indicado en el numeral 1 y 2 del artículo 10º de la Ley N° 27269- Ley de Firmas y Certificados Digitales.

4.9.3. Procesamiento de la solicitud de cancelación de un certificado

El suscriptor, el titular o su representante pueden solicitar a la ECEP o EREP asociada la cancelación de su certificado a través de medios telemáticos utilizando un medio que garantice el no repudio, como un mensaje firmado con un certificado válido, la

autenticación a través de una frase secreta conocida sólo por el suscriptor del certificado, entre otros. La ECERNEP, las ECEP y las EREP deben establecer en su CPS y RPS, según corresponda, el procedimiento para realizar las solicitudes de cancelación de los certificados de los suscriptores. El suscriptor también puede realizar la solicitud a la EREP mediante una petición presencial.

Los terceros deben presentarse personalmente o mediante un representante legalmente autorizado en las instalaciones de la EREP para realizar la solicitud de cancelación con la documentación requerida. Se incluyen aquí los casos en que medie una resolución administrativa o judicial. Dicha documentación y el proceso de validación de identidad del solicitante se debe especificar en la RPS de cada EREP.

Una ECERNEP o una ECEP pueden cancelar de oficio los certificados que han emitido, siempre y cuando los motivos de cancelación estén claramente especificados en su CPS y se encuentren contemplados en la legislación vigente.

Cuando una EREP recibe una solicitud para la cancelación de un certificado, debe dejar constancia de la persona que efectúa la solicitud, la relación que tiene ésta con el suscriptor, las acciones tomadas para la verificación de la veracidad de la información, fecha y hora de la cancelación y, de ser el caso, de la notificación a la ECEP.

En caso que no se acepte la cancelación, deberá dejarse constancia de los hechos que motivaron dicha denegatoria.

4.9.4. Periodo de gracia de la solicitud de cancelación de un certificado

Se define como el periodo de tiempo luego de la solicitud de una cancelación dentro del cual el solicitante debe confirmar la cancelación.

Esta CP no exige periodos de gracia para la atención de solicitudes de cancelación de certificados de las ECEP ni de Entidad Final. Al realizarse el pedido de cancelación, podría ejecutarse sin ser necesaria su confirmación.

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

La solicitud de cancelación debe ser procesada dentro de las **24 horas** siguientes a la realización de la solicitud en la EREP o, en caso de existir, a la expiración del periodo de gracia de la misma.

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

Una vez realizada la cancelación de un certificado digital, la ECEP debe almacenar la información de cancelación en el repositorio de la Lista de Certificados Cancelados, de acuerdo a lo indicado en el numeral **2.3, Frecuencia de publicación**, del presente documento, notificando de esta manera a todos los interesados.

Adicionalmente, una ECEP acreditada debe implementar servicios de consulta del Estado de Certificado Digital en Línea *(Online Certificate Status Protocol - OCSP)*.

La integridad y autenticidad de la información de cancelación deben ser aseguradas mediante la firma digital de la CRL y de la respuesta OCSP por parte de la ECEP que las emite.

4.9.7. Frecuencia de publicación de la Lista de Certificados Cancelados (CRL)

Conforme al perfil de CRL indicado en el numeral **7.2, Perfil de la CRL**, existen 3 niveles de listas de certificados cancelados (CRL):

CRL	Certificados digitales cancelados	Emisor	Frecuencia de publicación
Nivel 1	Nivel 2 (EC-PSVA / ECEP)	ECERNEP	1 año
Nivel 2	Nivel 3 / TSA	ECEP / EC-PSVA	6 meses
Nivel 3	Entidad Final	ECEP ONLINE	24 horas

Tabla 2 - Niveles de CRL y frecuencia de publicación

Estas listas deben ser emitidas en la frecuencia establecida incluso si ningún certificado hubiese sido cancelado. Para el caso de las CRL Nivel 1 y Nivel 2, se debe emitir una nueva CRL si ocurre alguna cancelación y publicarla dentro del periodo máximo de latencia especificado en el numeral **4.9.8, Periodo máximo de latencia para las CRL.**

4.9.8. Periodo máximo de latencia para las CRL

La latencia máxima entre la generación de las CRL y su publicación se precisa en la tabla 4 a continuación:

CRL	Certificados digitales cancelados	Emisor	Frecuencia de publicación	Máxima Latencia
Nivel 1	Nivel 2 (EC-PSVA / ECEP)	ECERNEP	1 año	24 horas
Nivel 2	Nivel 3 / TSA	ECEP / EC-PSVA	6 meses	24 horas
Nivel 3	Entidad Final	ECEP ONLINE	24 horas	1 hora

Tabla 3 - Niveles de CRL y máxima latencia

4.9.9. Disponibilidad del servicio online para la verificación del estado de un certificado

Las ECEP deben brindar, de manera obligatoria, el servicio de verificación en línea del estado del certificado (OCSP) para cualquier tipo de certificado que emitan, debiendo ofrecer la misma o mayor disponibilidad que la CRL.

4.9.10. Necesidad de verificación del estado del certificado mediante OCSP

No es obligatorio realizar la verificación en línea del estado del certificado (vía OCSP) al momento de la generación de una firma digital. Los suscriptores pueden utilizar únicamente la CRL de la ECEP emisora. Sin embargo, es recomendable que los terceros que confían usen los servicios OCSP para efectuar la verificación de una firma digital.

4.9.11. Otras formas de publicar la cancelación

Cuando la publicación de una cancelación pueda evitar o reducir el riesgo a potenciales terceros que confían, se permite que una ECEP pueda emplear distintos medios para realizar dicha publicación.

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

Las ECEP deberán notificar en un lapso de 24 horas como máximo a la ECERNEP y a la AAC respecto al compromiso de sus llaves privadas o su imposibilidad de uso.

En caso que la llave privada de una ECEP se vea comprometida, dicha entidad debe cancelar de inmediato todos los certificados emitidos de acuerdo a la legislación vigente, comunicando dicha acción a todos los suscriptores, titulares y terceros que confían.

Según lo estipulado en el numeral **4.9.1, Motivos de cancelación**, en caso que el suscriptor de un certificado digital de Entidad Final sospeche que su llave privada ha sido comprometida, éste debe solicitar de inmediato la cancelación de su certificado digital a través de la EREP donde se solicitó el certificado o directamente a la ECEP emisora.

4.9.13. Circunstancias para una suspensión

Las ECEP pueden realizar la suspensión a pedido del suscriptor por intermedio de la EREP correspondiente, solamente a certificados que se encuentran vigentes (dentro de su periodo de validez y no cancelados).

Aquellas ECEP que deseen implementar este servicio deberán establecer el procedimiento en su respectiva CPS. Las EREP asociadas deben especificar en sus RPS los procedimientos necesarios para la solicitud, procesamiento y consiguiente autorización o negación de una suspensión.

Para el caso de personas jurídicas, sólo se puede solicitar la suspensión cuando el suscriptor se ve impedido temporalmente de cumplir con sus funciones.

4.9.14. Personas habilitadas para solicitar una suspensión

Sólo los titulares de certificados digitales emitidos pueden solicitar la suspensión de los mismos.

4.9.15. Procedimiento para solicitar una suspensión

Una EREP, en coordinación con su ECEP asociada, puede implementar el procedimiento de suspensión de un certificado digital. Los titulares de certificados emitidos a personas jurídicas, pueden solicitar la suspensión de su certificado a la EREP correspondiente a través de su representante legal o apoderado. El solicitante debe especificar las fechas de inicio y fin del periodo de suspensión.

La EREP debe requerir del solicitante la solicitud de suspensión firmada, la cual debe quedar en sus registros. La EREP debe especificar en su RPS los procedimientos necesarios para la solicitud, procesamiento y consiguiente autorización o negación de una suspensión.

Para el caso en que el suscriptor posea dos o más certificados digitales vigentes del mismo tipo y finalidad, las EREP deben brindar la asesoría correspondiente para suspender el certificado deseado.

El certificado suspendido recobrará automáticamente su validez al término del periodo de suspensión solicitado por el titular o el suscriptor del certificado de persona jurídica.

4.9.16. Límite del periodo de suspensión

El tiempo máximo en el que un certificado puede ser suspendido está limitado por su fecha de expiración.

4.10. Servicios de monitoreo de estado del certificado

Las ECEP deben brindar, con carácter obligatorio y de forma irrestricta, el servicio de verificación de estado del certificado mediante la Lista de Certificados Cancelados (CRL) y el servicio de verificación en línea (OCSP). La ECERNEP hará lo propio únicamente mediante la CRL.

4.10.1. Características operacionales

Todas las actualizaciones del estado de cancelación estarán disponibles para todos los métodos, y la información proporcionada por todos los servicios deberá ser coherente en el tiempo teniendo en cuenta los diferentes retrasos en la actualización de la información sobre el estado de cancelación en todos los métodos[9].

Cualquier información publicada respecto al estado de uno de los certificados (a través de la CRL u OCSP) debe ser firmada digitalmente por la ECEP que lo publica, debiendo contar con registro de hora y fecha.

4.10.2. Disponibilidad del servicio

[9] Cfr. sección 6.3.10.f) de ETSI EN 319 411-1.

Se debe brindar el servicio de información sobre el estado del certificado, mediante CRL, con un mínimo de tiempo de disponibilidad del 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

4.10.3. Servicios Opcionales

No aplica.

4.11. Finalización de la suscripción al servicio de certificación

La finalización de la suscripción al servicio de certificación digital puede darse por los siguientes motivos:

- Al cancelarse el certificado digital antes de la fecha de expiración
- Al expirar el certificado digital

El contrato del suscriptor recogerá las obligaciones que éste deberá cumplir a fin de asegurar los efectos legales de las firmas digitales generadas utilizando su certificado digital.

4.12. Custodia y recuperación de llaves

4.12.1. Condiciones y procedimientos para custodia y recuperación de llaves privadas

No está permitido el almacenamiento del original, copia o *backup* de las llaves privadas de suscriptores de certificados digitales de firma y/o autenticación.

El almacenamiento o copia de llaves privadas de cifrado es de carácter opcional y sólo está permitido en caso medie el consentimiento del suscriptor y titular del certificado. Las ECEP que brinden el servicio de almacenamiento de llaves de cifrado deben establecer en su CPS las características y procedimientos relacionados a la custodia y recuperación de las mismas. De ser este el caso, el contrato de suscriptor deberá contemplar las obligaciones de cada parte y el consentimiento de parte del suscriptor de la custodia de las llaves privadas de cifrado.

4.12.2. Condiciones y procedimientos para custodia y recuperación de llaves de sesión

Las llaves de sesión son utilizadas únicamente para operaciones de cifrado. En el caso que el dato a cifrarse se tratase de una llave privada asociada a un certificado de firma, se debe seguir lo indicado en el numeral **4.12.1 Condiciones y procedimientos para custodia y recuperación de llaves privadas**.

5. CONTROLES DE LAS INSTALACIONES, DE GESTIÓN Y OPERACIONALES

5.1. Controles físicos

Los PSC deben mantener controles de seguridad físicos para garantizar la seguridad y calidad de sus operaciones, con especial énfasis en las áreas de sus instalaciones donde se realizan operaciones críticas. A este respecto, se tendrá como guía la aplicación de controles según los estándares NTP-ISO/IEC 27001 (ISO/IEC 27001) y NTP-ISO/IEC 17799 (ISO/IEC 27002).

5.1.1. Ubicación y construcción del local

Las instalaciones donde desarrollan sus operaciones los PSC deben contar como mínimo con las siguientes características:

- Piso, paredes y techo de material noble en su perímetro. Las divisiones interiores, de tipo permanente, podrán efectuarse en material aligerado.
- Puertas sólidas en su perímetro y de estructura aligerada en interiores para impedir y prevenir el acceso a personal no autorizado.
- Medidas de prevención ante desastres naturales y ante desastres accidentales creados por el hombre, incluyendo una ubicación adecuada del local.
- Instalaciones físicas con al menos dos ambientes separados:
  - Las ECEP contarán mínimamente con un área operacional y un área restringida.
  - Las EREP contarán mínimamente con un área operacional y un área de atención al público.
- En el área de atención al público, las EREP contarán con compartimientos o divisiones en sus módulos de atención que garanticen la confidencialidad en el tratamiento de los datos personales.

5.1.2. Acceso físico

Las áreas donde los PSC desarrollan sus operaciones deben mantenerse cerradas para evitar el acceso no autorizado. Se dispondrá asimismo de personal para el control de acceso o control de acceso biométrico, de manera que se posibilite el ingreso sólo a personas autorizadas.

Tanto en las áreas operacionales como en las áreas restringidas debe disponerse de mecanismos de seguridad, entre estos, video vigilancia las 24 horas al día y los 7 días de la semana (24x7). Además, el área restringida de las ECEP debe encontrarse protegida mediante control de acceso biométrico de al menos dos personas.

Las visitas o personal de limpieza, mantenimiento y soporte deben ser escoltados y registrados por el responsable de accesos, debiendo registrarse su identidad, la fecha, hora y motivo de ingreso y la hora de salida. Se verificará su identidad y, en cuanto sea viable, sus antecedentes.

5.1.3. Energía y aire acondicionado

Los centros de datos de las ECEP en los que operan los equipos servidores, los dispositivos HSM, entre otros, deben contar con sistemas de regulación de la energía, incluyendo sistemas de respaldo y puesta a tierra, para asegurar la continuidad y la seguridad de sus operaciones. Además, se debe contar con sistemas de aire acondicionado de precisión capaces de controlar la temperatura y humedad relativa.

Las EREP deben determinar de acuerdo al entorno ambiental en que operan la necesidad de implementar sistemas de aire acondicionado o mecanismos de regulación de energía para asegurar la continuidad y la seguridad de sus operaciones.

5.1.4. Exposición al agua

Las instalaciones deben ser construidas de material noble y protegidas por medio de impermeabilizantes para prevenir inundaciones y otros daños por exposición al agua. Es recomendable la instalación de detectores de humedad.

5.1.5. Previsión y protección contra fuego

Las instalaciones deben ser construidas y equipadas para prevenir, detectar y suprimir incendios o daños producidos por exposición a llamas o humo. Se debe contar con extintores de fuego en ubicaciones señalizadas. Además, los centros de datos deben contar con un sistema de extinción no contaminante especializado, de manera que se prevenga cualquier daño a los equipos.

5.1.6. Almacenamiento de material

Se debe asegurar el almacenamiento, manejo y protección de componentes tecnológicos e información crítica o sensible del sistema. Deben estar protegidos tanto contra acceso no autorizado, como también contra desastres naturales o daños accidentales.

5.1.7. Eliminación de residuos

Se deben implementar controles para la eliminación de residuos tanto físicos como lógicos. La eliminación debe ser realizada de tal manera que se evite la posibilidad de recuperación o restructuración de información.

5.1.8. Copia de seguridad externa

Se deben mantener copias externas de respaldo de toda aquella información considerada como necesaria para la continuidad del negocio y la persistencia de su actividad, incluyendo datos de auditoría.

5.2. Controles procedimentales

5.2.1. Roles de confianza

Se deben definir los roles de confianza en las operaciones que realizan los PSC.

La descripción de los roles debe incluir las labores que pueden como las que no pueden ser realizadas en el ejercicio de tales roles, las mismas que deben ser puestas de manifiesto a las personas que ejercen dichas funciones. Se debe obtener constancia por escrito del conocimiento de las funciones de cada rol.

5.2.2. Número de personas requeridas por labor

Se debe establecer, mantener y ejecutar, procedimientos que detallen estrictamente el número de personas requeridas y necesarias para realizar las labores consideradas como críticas y sensibles.

5.2.3. Identificación y autenticación para cada rol

Deben emplearse controles de acceso tanto físicos como lógicos para verificar la identidad y autorización antes de permitir el acceso para cada rol.

Para el control de acceso físico, como mínimo se contará con personal de seguridad o con control de acceso biométrico, de manera que se posibilite el ingreso sólo a personas autorizadas. Las áreas restringidas de las ECEP, como su centro de datos, deben encontrarse protegidas mediante control de acceso biométrico de al menos dos personas.

El control de acceso lógico debe estar basado en biometría o tarjeta inteligente para operaciones críticas de los PSC.

5.2.4. Roles que requieren separación de funciones

Se deben definir los roles que requieren separación de funciones para la operación de los PSC.

Las personas que se encargan de la implementación de una función, no deben asimismo tener el rol de realización de la auditoría de conformidad, o evaluación o revisión de dicha implementación.

5.3. Controles de personal

Los PSC deben de establecer en su Declaración de Prácticas u otra documentación relevante, los términos de confidencialidad y provisiones de no revelación que gobierna al mismo, así como la legislación que rige a las transacciones que se realizan bajo el marco de la IOFE, la legislación relativa al régimen de los trabajadores y cualquier otra legislación relevante, de conformidad con la Norma Marco sobre Privacidad. Esta información debe ser entregada por escrito a sus empleados y contratistas, debiéndose obtener declaración por escrito por parte de estas personas respecto al de conocimiento de toda esta información.

Esta información debe ser incorporada en todos los contratos de trabajo o servicio.

5.3.1. Requisitos de experiencia, capacidades y autorización

Se deben establecer en su Declaración de Prácticas u otra documentación relevante las cualidades, experiencias y certificados que debe poseer su personal y contratistas.

5.3.2. Procedimiento para verificación de antecedentes

Se deben verificar los antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes vigentes y normatividad pertinente. La precisión de la verificación debe ser proporcional a los requerimientos comerciales, la clasificación de la información a la cual dicho personal tiene acceso y a los riesgos implicados.

Las personas que desempeñan roles de confianza deben de tener en claro el nivel de sensibilidad y valor de los bienes y transacciones protegidos por la actividad de la cual ellas son responsables. Generalmente, esto implica ejecutar, como mínimo, las siguientes verificaciones:

- Verificación de la identidad.
- Confirmación de las referencias.
- Confirmación de empleos anteriores.
- Revisión de referencias profesionales.
- Confirmación de grados académicos obtenidos.
- Verificación de antecedentes penales y policiales.
- Para el caso de roles de confianza, verificación de antecedentes crediticios.

5.3.3. Requisitos de capacitación

Se debe determinar el momento oportuno para impartir capacitación al personal involucrado en las operaciones. Se debe impartir al menos una capacitación al inicio de funciones (inducción) y una actualización anual. La inducción y actualizaciones deben contener al menos los siguientes aspectos:

- Uso y operación del hardware y software empleado.
- Aspectos relevantes de la Política General de Certificación, Declaración de Prácticas, 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.
- Plan de Continuidad del Negocio y Recuperación ante desastres

5.3.4. Requisitos y frecuencia de re-capacitación

Se deben realizar capacitaciones especializadas al personal encargado cuando se realicen cambios significativos, por ejemplo actualizaciones de hardware y software, cambio de los sistemas y/o procedimientos de seguridad.

Se deben realizar capacitaciones con una frecuencia que asegure el adecuado nivel de conocimiento del personal y eficiencia para realizar sus labores de acuerdo a un plan anual de capacitación. De igual manera, cada vez que se sustituya o rote al personal encargado.

5.3.5. Frecuencia y secuencia de rotación de las funciones

Se debe establecer en la Declaración de Prácticas u otra documentación relevante si implementará políticas de rotación en el trabajo, en ese caso se debe establecer documentalmente los procedimientos necesarios, incluyendo los periodos mínimos para realizar la rotación.

5.3.6. Sanciones por acciones no autorizadas

Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.

En caso de una acción real o potencial no autorizada y que haya sido realizada por una persona que desempeña un rol de confianza, dicha persona debe ser inmediatamente

suspendido de todo rol de confianza que pudiera desempeñar y aplicarle otras sanciones que se consideren pertinentes. Dichas sanciones deben estar establecidas en los contratos de cada empleado y/o contratista.

Se consideran acciones no autorizadas las que contravengan, de manera negligente o malintencionada, a este documento, las Declaraciones de Prácticas, la Política de Seguridad, la Política de Privacidad y Plan de Privacidad, así como a los documentos normativos de alcance al personal.

Por otro lado, la Ley Nº 29622 "Ley que modifica la Ley Nº 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República" y su reglamento aprobado por Decreto Supremo N° 023-2011-PCM, "Reglamento de infracciones y sanciones para la responsabilidad administrativa funcional derivada de los informes emitidos por los Órganos del Sistema Nacional de Control", son aplicables a los servidores y funcionarios públicos.

5.3.7. Requisitos para contratistas

En caso se estime conveniente el empleo de contratistas en las instalaciones de los PSC, éstos y sus empleados deben encontrarse sujetos a lo establecido en el numeral **5.3 Controles de personal**, del presente documento en lo que resulte aplicable, en los mismos criterios de funciones y seguridad aplicados a empleados del PSC en posiciones similares. Los contratos deben especificar las sanciones y reparaciones para las acciones llevadas a cabo por los contratistas y sus empleados.

5.3.8. Documentación suministrada al personal

Se debe suministrar al personal, de acuerdo a su rol, la documentación necesaria y suficiente para desempeñar sus funciones. Aquellos documentos confidenciales o con información crítica, deben ser entregados considerando la clasificación de dicha información.

Como mínimo, debe incluirse entre la documentación a suministrarse al personal:

- Una declaración de funciones y autorizaciones.
- Manuales para los equipos y software que deba operar.
- Aspectos de la declaración de prácticas, política de seguridad y otra documentación relevante en relación a sus funciones.
- Legislación aplicable a sus funciones.
- Documentación respecto a sus roles frente a planes de contingencia o de continuidad de negocio y recuperación frente a desastres.

5.4. Procedimientos de registro de eventos

Los PSC deben cumplir con los siguientes requisitos para el registro de eventos en cuanto les resulten aplicables.

5.4.1. Tipos de eventos registrados

Se debe mantener un registro de auditoría de los eventos que puedan impactar en la seguridad de las operaciones. Como mínimo se debe incluir lo siguiente:

- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro de los sistemas o equipos.
- Accesos lógicos al sistema.
- Acceso físico a las áreas críticas de las instalaciones.
- Generación de llaves criptográficas (registro de eventos de módulo criptográfico).
- Eventos relacionados con el ciclo de vida de los certificados digitales: emisión, renovación de llaves y cancelación.
- Encendido y apagado de los sistemas.
- Intentos de entrada y salida del sistema de certificación.
- Intentos no autorizados de acceso a los registros o bases de datos del sistema de certificación.
- Cambios en las políticas de emisión de certificados.
- Intentos no autorizados de entrada a la red de la Entidad.
- Generación de llaves.
- Intentos nulos de lectura y escritura en un certificado y en el repositorio.
- Mantenimientos y cambios de configuración del sistema.
- Acceso físico a las áreas sensibles.
- Cambios en el personal.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al sistema de certificación.

El registro de auditoría de eventos debe registrar la hora, fecha e identificadores de software/hardware. Los relojes del sistema computacional deben estar sincronizados en un sistema que pueda brindar hora exacta (se sugiere el uso del protocolo NTP), para un registro preciso de los eventos.

5.4.2. Frecuencia de procesamiento del registro de eventos

Se deben procesar y revisar los registros de auditoría al menos una vez al mes. Además de las revisiones oficiales, los registros de auditoría deben ser revisados ante una alerta, irregularidades o incidentes. El procesamiento de los registros de auditoría debe incluir la verificación de que dichos registros no hayan sido manipulados.

5.4.3. Periodo de conservación del registro de eventos

La conservación del registro de eventos será como mínimo por un periodo de diez (10) años. Este periodo mínimo de conservación deberá contemplar el establecimiento de acuerdos de reconocimiento cruzado con otras entidades, en cuyo caso deberá ajustarse para que sea igual o mayor al máximo periodo de conservación establecido por las mismas en sus políticas de certificación.

5.4.4. Protección del registro de eventos

Los registros de eventos, tanto físicos como electrónicos, deben contar con controles físicos y lógicos de manera que se prevenga el acceso a estos, su revelación, modificación

o destrucción no autorizados. Los controles deben incluir protección de acceso a lectura y contra modificaciones.

La destrucción de un archivo de auditoría solo se podrá llevar a cabo con la autorización de la AAC, siempre y cuando haya transcurrido un periodo mínimo de 10 años, como se indica en el numeral **5.4.3 Periodo de conservación del registro de eventos.**

5.4.5. Procedimiento de copia de respaldo del registro de eventos

Debe realizarse copias de seguridad del registro de auditorías al menos una vez al mes, la cuales deben archivarse fuera de las instalaciones del PSC.

Debe tomarse en consideración la posibilidad de generar copias de seguridad automatizadas para el caso de eventos auditables significativos.

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

La frecuencia de las auditorías internas debe seguir lo establecido en un "Plan Anual de Auditorias". Las auditorías internas se deben llevar a cabo una vez cada tres (03) meses. Las auditorías externas son efectuadas una (01) vez al año o cuando la AAC lo requiera según los procedimientos establecidos por ésta en la Guía de Acreditación de Entidades de Certificación EC.

5.4.7. Notificación al sujeto que causa el evento

Ante la ocurrencia de un evento, se debe comunicar el hecho al Oficial de Seguridad de Información del PSC para que proceda con las acciones pertinentes, en función a la gravedad y naturaleza del evento.

En los casos en que se establezca que el evento es de índole accidental y puede volver a ocurrir, debe tomarse en consideración la posibilidad de notificar al autor del evento (sujeto que causa el evento).

5.4.8. Evaluación de la vulnerabilidad

Se debe realizar análisis de vulnerabilidades y de *ethical hacking* a los sistemas, en particular aquellos que están expuestos a Internet. Además, se debe evaluar el riesgo al que se expone la organización ante esas vulnerabilidades y se deben tomar medidas para reducir su posible impacto.

5.5. Archivo

5.5.1. Tipos de información archivada

Los PSC deben mantener registro de la información suficiente para establecer la validez de un certificado y la operación de la infraestructura PKI en conformidad con la normatividad vigente y la aplicable a las entidades con las que pueda establecerse acuerdos de reconocimiento cruzado. Como mínimo, debe mantenerse:

- Declaraciones de Prácticas
- Documentos de acreditación
- Modificación de cualquiera de los documentos anteriores

- Registros de eventos
- Las aplicaciones requeridas para tener acceso y lectura a un archivo deben también ser conservadas.

En particular, las ECEP deben mantener además:

- Bases de datos de los certificados digitales emitidos, cancelados o anulados.
- Todas las CRL emitidas desde el inicio de sus operaciones

En particular, las EREP deben mantener además:

- Datos de los suscriptores y titulares, los contratos y documentos que dan constancia de cada solicitud realizada.

5.5.2. Periodo de conservación del archivo

Los archivos deben ser mantenidos por los PSC como mínimo por un período de diez (10) años de acuerdo a lo establecido en las guías de acreditación correspondientes publicadas por la AAC. Este periodo mínimo de conservación debe contemplar el establecimiento de acuerdos de reconocimiento cruzado con otras entidades de certificación, en cuyo caso deberá ajustarse para que sea igual o mayor al máximo periodo de conservación establecido por las mismas en sus políticas de certificación.

5.5.3. Protección del archivo

Los archivos deben ser física y lógicamente protegidos y supervisados para evitar el empleo inadecuado, revelación o copia de información. Se debe establecer en la Política de Seguridad u otra documentación relevante las medidas de protección de la información archivada. Como mínimo las medidas deben prevenir cualquier modificación o eliminación de los datos contenidos en el archivo, e impedir el acceso a personas no autorizadas. Asimismo, debe garantizarse la confidencialidad de los datos proporcionados por los suscriptores y los titulares.

La protección de los archivos se debe establecer de acuerdo al tipo de información que contienen. Los archivos de mayor relevancia, deberán estar firmados digitalmente, contemplando la posibilidad de su refirmado o la generación de microformas según Decreto Legislativo N° 681.

5.5.4. Procedimientos para copia de seguridad del archivo

Se debe contar con procedimientos aprobados y adecuados para las copias de seguridad de los archivos tanto físicos como electrónicos. Las copias de seguridad se deben almacenar en un lugar físicamente separado y deben ser probadas en su integridad con regularidad por el personal autorizado. Los procedimientos deben ser compatibles con los estándares reconocidos por la AAC o basarse en la generación de microformas de acuerdo al Decreto Legislativo N° 681.

5.5.5. Requisitos de fecha y hora de los registros

Los certificados digitales, listas CRL y archivos de registro deben contener información de fecha y hora del instante en que se genera el registro y de ser el caso una firma digital

según el RFC 3161 (Time Stamping), o pueden ser protegidos de cualquier otra forma que pueda demostrar que los datos corresponden a la organización que los ha generado en un determinado instante de tiempo.

5.5.6. Sistema de archivo (interno vs. externo)

Se debe realizar al menos dos copias de seguridad; una de ellas debe almacenarse en un lugar físicamente separado de las instalaciones principales.

5.5.7. Procedimientos para obtener y verificar la información archivada

Se deben establecer procedimientos para la obtención y verificación de la información del archivo, los cuales deben encontrarse en conformidad con los requisitos de confidencialidad y privacidad de la organización.

5.6. Cambio de llaves

El cambio de llaves de una raíz gestionada por la ECERNEP implica el despliegue de una nueva jerarquía de certificación.

Sólo se permiten los cambios de llaves de las ECEP en el caso que sus certificados estén próximos a expirar o por motivos de cancelación. De ser el caso, las llaves antiguas deben mantenerse en su poder hasta la fecha de expiración del certificado asociado, y mientras tanto pueden ser usadas únicamente para firmar las CRL correspondientes. Lo propio aplica a la EC-PSVA gestionada como una instancia de la ECERNEP.

Los PSVA-TSA pueden cambiar sus llaves periódicamente a fin de poder mantener una vigencia prolongada de sus sellos de tiempo. Dicho cambio no implicará la cancelación del certificado vigente de PSVA-TSA[10].

5.7. Recuperación frente al compromiso de las operaciones y los desastres

Se debe establecer en un Plan de Contingencias los lineamientos y procedimientos para el restablecimiento y mantenimiento de la continuidad del negocio y la recuperación frente a desastres. Dicho plan debe asegurar que los aspectos básicos del negocio, tales como servicios de validación o revocación, puedan ser reasumidos dentro de un plazo máximo de 24 horas, el cual constituye el plazo máximo para la emisión de las listas de revocación de certificados. Los planes deben ser evaluados por lo menos una vez durante el periodo de cada auditoría externa establecido en un año.

5.7.1. Procedimiento para el manejo de incidentes y el compromiso de las operaciones

[10] Resulta conveniente disponer de certificados de TSA de larga duración (por ejemplo, 6 años), que se emplean para emitir sellos de tiempo un periodo de tiempo más breve (por ejemplo, 1 año), para garantizar que el sello de tiempo que menos dura tiene una longevidad de 5 años (en el ejemplo).

El Plan de Contingencia debe establecer procedimientos de comunicación, registro y respuesta ante incidentes, indicando la acción que ha de emprenderse. Los incidentes deberán ser comunicados, tan pronto se haya tomado conocimiento, al Oficial de Seguridad de Información para que se tomen las acciones para reducir el impacto de los mismos. Dichos procedimientos deben ser compatibles con los estándares reconocidos por la AAC.

Deben existir mecanismos para permitir cuantificar y monitorear los tipos, cantidad y costos de los incidentes en la seguridad de la información.

Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (civil o penal), se debe recolectar y mantener evidencia para presentarla en cumplimiento de la legislación vigente si así lo estipulara la autoridad judicial competente.

5.7.2. Corrupción de los datos, software y/o recursos computacionales

El Plan de Contingencia debe identificar fuentes alternativas de recursos computacionales, software y datos a emplearse en los casos de adulteraciones o fallas en los mismos.

5.7.3. Procedimiento en caso de compromiso de llave privada

En caso que la llave privada de un PSC fuera comprometida de manera real o potencial, ésta debe ser inmediatamente cancelada y se deberán seguir los procedimientos de notificación detallados anteriormente.

En el caso de las ECEP, se debe notificar a todos los afectados que los certificados y la información sobre su revocación, emitidos usando la llave comprometida, han dejado ser válidos. Los certificacdos subordinados firmados por la ECEP afectada, en el periodo comprendido entre el compromiso de la llave y la cancelación del certificado correspondiente, dejan de ser válidos por lo que sus titulares deben solicitar la emisión de nuevos certificados de asi requerirlo.

En el caso de los PSVA-TSA, se debe notificar a todos los afectados que los sellos de tiempo emitidos usando la llave comprometida, han dejado de ser válidos. Los sellos de tiempo firmados por el PSVA-TSA afectado, en el periodo comprendido entre el compromiso de la llave y la cancelación del cetrtificado correspondiente, dejan de ser válidos por lo que sus titulares deben buscar un proveedor del servicio de sellado de tiempo alternativo de así requerirlo.

5.7.4. Capacidad de continuidad del negocio luego de un desastre

Se debe contar con un Plan de Continuidad del Negocio y Recuperación de Desastres probado y aprobado para garantizar la continuidad de las operaciones en caso de compromiso de su llave privada u otras situaciones que podrían ocasionar la interrupción del servicio; permitiendo la continuidad de las siguientes actividades:

- Recepción de solicitudes de emisión de certificados digitales
- Emisión de certificados digitales.
- Recepción de solicitudes de cancelación de certificados digitales

- Cancelación de certificados digitales.
- Generación y publicación de certificados digitales emitidos y la lista de certificados cancelados (CRL).

El personal afectado por el Plan de Continuidad de Negocio y Recuperación de Desastres debe conocer dicho plan y los procedimientos con él relacionados y será responsable de su cumplimiento de acuerdo a los roles asignados.

5.8. Terminación de un PSC

Se requiere información por parte de los PSC respecto a operaciones de finalización (disolución). Los PSC deben informar a la AAC, a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario de anticipación.

Cuando un PSC finaliza sus operaciones, se debe asegurar que todos los datos necesarios para la continuación de las operaciones bajo el marco de la IOFE son transferidas a la AAC o a otro PSC designado por ésta.

Se debe advertir a todos los suscriptores o terceros que confían, respecto de los cambios y toda condición asociada a la continuidad del uso de los certificados emitidos por un PSC que finaliza sus operaciones.

6. CONTROLES TÉCNICOS DE SEGURIDAD

Los PSC deben mantener controles de seguridad técnicos adecuados a la criticidad de sus operaciones, al valor de los activos de la información a su cargo y a los riesgos identificados, siendo dichos controles compatibles con estándares establecidos por la AAC:

- NTP-ISO/IEC 27001, EDI. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Estándar internacional ISO/IEC 27001.
- NTP-ISO/IEC 17799, EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información, o el estándar internacional ISO/IEC 27002.

6.1. Generación e instalación del par de llaves

6.1.1. Generación del par de llaves

Los PSC deben generar su propio par de llaves utilizando un módulo criptográfico HSM que cumpla los requisitos descritos en el numeral **6.2.1 Estándares y controles para el módulo criptográfico**. Este procedimiento debe ser realizado mediante una ceremonia de generación de llaves.

Tanto la ECERNEP como las ECEP deben tener un procedimiento documentado para la generación de sus llaves. Este procedimiento comprenderá cuando menos lo siguiente:

i) Roles que participan en la ceremonia (internos y externos a la organización);
ii) Funciones a desarrollarse por cada rol en las fases correspondientes;
iii) Responsabilidades durante y después de la ceremonia; y
iv) Requisitos respecto de las evidencias a recogerse durante la ceremonia.

El PSC contará con documentos firmados en los que se consigne que la ceremonia fue llevada a cabo en concordancia con el procedimiento establecido y que se garantizó la integridad y confidencialidad de las llaves.

i) Para la ECERNEP: por el rol responsable de la seguridad de la ceremonia de llaves (por ejemplo el oficial de seguridad) y por una persona confiable independiente de la organización (por ejemplo un notario o un auditor) como testigo de que tales documentos registran fielmente su desarrollo.
ii) Para las ECEP: por el rol de confianza responsable de la seguridad de la ceremonia de llaves (por ejemplo el oficial de seguridad) como testigo de que tales documentos registran fielmente su desarrollo.
iii) Deberá cumplirse con lo señalado en la cláusula 6.1.1.1 del *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates,* en lo que les sea aplicable[11].

[11] Cfr. sección 6.5.1.g) de ETSI EN 319 411-1. Según lo señalado en la norma europea la exigencia de Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum, versión 1.4.9, en su aludida cláusula 6.1.1.1 debe aplicarse a certificados Extended Validation Certificates (EVC), Domain Validation Certificates (DVC) y Organizational Validation Certificates (OVC) a usarse en SSL/TLS o en firma de código, según el caso.

La generación de llaves de Entidad Final debe hacerse utilizando módulos criptográficos que cumplan los requisitos descritos en la sección **6.2.1 Estándares y controles para el módulo criptográfico**. En este caso, las llaves pueden ser generadas por los propios suscriptores, por la EREP o por la ECEP.

Deben establecerse mecanismos que permitan verificar la calidad de los parámetros de las llaves, cuando proceda, del exponente público y el módulo[12].

6.1.2. Entrega de la llave privada al suscriptor

En el caso que una ECEP o EREP genere las llaves de una Entidad Final, éstas deben implementar controles que aseguren la confidencialidad y seguridad en la entrega de la llave privada. La prueba de posesión de la llave privada se realiza según lo indicado en el numeral **3.2.1 Método para probar la posesión de la llave privada**.

6.1.3. Entrega de la llave pública al emisor del certificado digital

Cuando un titular o suscriptor genera su propio par de llaves, la llave pública correspondiente debe ser remitida a la ECEP emisora mediante un mensaje de prueba de posesión de llave privada, conforme a lo estipulado en el RFC 4210, como una petición *(Certificate Signing Request* - CSR) en formato PKCS#10, según lo estipulado en el RFC 2986.

6.1.4. Entrega de la llave pública al tercero que confía

Los certificados digitales de las ECEP, que incluyen su llave pública, serán remitidos por éstas a la AAC para que sean consignados en el registro de PSC de confianza que dicha autoridad gestiona.

Las ECEP deben publicar los certificados digitales de Entidad Final vigentes, los que incluyen su llave pública, en el repositorio correspondiente, según lo indicado en el numeral **2.1 Repositorio**.

6.1.5. Tamaño de llaves

El algoritmo y el tamaño mínimo de las llaves dentro de la jerarquía descrita por la presente CP deben ser los siguientes:

Nivel de la jerarquía PKI	Algoritmo de Firma	Tamaño de llaves RSA
ECERNEP	sha512WithRSAEncryption	4096 bits
EC-PSVA / ECEP offline	sha512WithRSAEncryption	4096 bits
ECEP online	sha512WithRSAEncryption	4096 bits
Entidad final	sha256WithRSAEncryption	2048 bits

Tabla 4 - Algoritmo de firma y tamaño de llave de los niveles de la Jerarquía ECERNEP PERU CA Root 3

[12] Se debe confirmar que el valor del exponente público es un número impar, igual o mayor a 3. Además, el exponente público debe encontrarse en el rango comprendido en [2^16+1 ; 2^256-1]. Asimismo, el módulo debe tener las siguientes características: ser un número impar, que no sea potencia de un primo y no tener factores menores a 752 (Fuente: Section 5.3.3, NIST SP 800-89)

6.1.6. Parámetros de generación de llave pública y verificación de calidad

Se debe generar la llave pública acorde a los lineamientos indicados en el numeral **6.1.1 Generación del par de llaves**. Las auditorías internas o externas verificarán la calidad de las llaves y el cumplimiento de los lineamientos.

6.1.7. Propósito de uso de la llave (extensión *KeyUsage* X.509 v3)

Los usos admitidos de la llave para los certificados digitales están dados por los valores contenidos en las extensiones *KeyUsage* y *ExtendedKeyUsage* de los mismos. Estos valores serán diferentes dependiendo de si se trata de un certificado digital de firma, autenticación o cifrado. El contenido de dichas extensiones para los certificados de cada nivel y los diferentes tipos de certificados digitales se puede consultar en el numeral **7.1.2 Extensiones del certificado digital**, del presente documento.

Los bits *CertSign* y *CRLSign*, en la extensión *KeyUsage,* solo deben ser utilizados en certificados emisores de certificados subordinados y CRL, nunca en certificados de entidad final.

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

6.2.1. Estándares y controles para el módulo criptográfico

Los módulos criptográficos de la ECERNEP, de las ECEP y de los PSVA-TSA deben encontrarse certificados conforme a Common Criteria, perfiles de protección descritos en las normas CEN EN 419 221, partes 2 a 5, según proceda[13]; o según el estándar ISO/IEC 19790 nivel 3, como mínimo, o el estándar FIPS 140-2 nivel 3[14], como mínimo.

Los módulos criptográficos de las EREP deben encontrarse certificados conforme a Common Criteria, perfiles de protección descritos en las normas CEN EN 419 221, partes 2 a 5, según proceda; o según el estándar ISO/IEC 19790 nivel 2, como mínimo, o el estándar FIPS 140-2 nivel 2, como mínimo.

Los módulos criptográficos usados por las entidades finales bajo la jerarquía de la presente CP deben encontrarse certificados y operar bajo el estándar FIPS 140-2 nivel 1 o bajo Common Criteria EAL 4+ conforme a los perfiles de protección referidos por la AAC en la Guía de Acreditación de Entidades de Certificación, como mínimo.

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

Los PSC deben generar sus llaves de tal manera que se proteja su acceso mediante control multipersonal. De un conjunto de “m” personas autorizadas, se debe requerir la concurrencia de “k” para la activación y uso del módulo que contiene dichas llaves.

[13] Cfr. sección 6.5.2 de ETSI EN 319 411-1.

[14] FIPS valida el cumplimiento de su estándar PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, bajo su programa de validación Cryptographic Module Validation Program (CMVP).

6.2.3. Custodia de la llave privada

Los PSC deben custodiar apropiadamente sus llaves privadas.

No se admite la custodia, almacenamiento o copia de llaves privadas de firma y/o autenticación de Entidad Final, ni de los módulos hardware que los contienen. Sólo se permite el depósito de llaves privadas de cifrado (copia de respaldo o backup), siempre que medie el consentimiento del suscriptor.

6.2.4. Respaldo de la llave privada

Está permitido efectuar copias de respaldo de la llave privada de los PSC, siempre que la protección dada a dicha copia de seguridad no sea menor a la establecida para la llave privada original.

6.2.5. Archivo de la llave privada

Los PSC pueden archivar sus llaves privadas garantizando la confidencialidad e integridad de las mismas.

No deberá archivarse las llaves privadas de Entidades Finales empleadas para la firma y/o autenticación, ni los módulos criptográficos o los archivos electrónicos que las contengan. Solamente se permite el archivo de llaves privadas de cifrado, siempre que medie el consentimiento del suscriptor.

6.2.6. Transferencia de la llave privada hacia o desde un módulo criptográfico

De requerirse, las ECEP pueden migrar sus llaves privadas a otro módulo criptográfico HSM adicional. En la migración, estas llaves deben ser ilegibles fuera del HSM y deben estar protegidas por controles de seguridad de igual o de mayor nivel que los establecidos en el módulo criptográfico HSM original y en conformidad con alguno de los estándares indicados en el numeral 6.2.1, **Estándares y controles para el módulo criptográfico**, de este documento.

6.2.7. Almacenamiento de la llave privada en un módulo criptográfico

Las llaves privadas de los PSC deben ser generadas y mantenidas en un módulo criptográfico HSM certificado y que opera bajo alguno de los estándares indicados en el numeral 6.2.1, **Estándares y controles para el módulo criptográfico**, de este documento.

6.2.8. Método de activación de la llave privada

- Para las llaves privadas de los PSC: Los métodos de activación deben contar con mecanismos de autenticación de al menos dos factores de seguridad. Los datos de activación deben estar distribuidos en roles de confianza que ejecutan diversas personas.
- Para las llaves privadas de Entidad Final: Los métodos de activación deben contar con mecanismos de autenticación de al menos un factor bajo el control del titular.

La activación inicial de la llave privada generada para un titular requiere el uso de los datos de activación provistos al mismo por un canal diferente al empleado para la provisión de la llave. Los suscriptores deben hacer uso de sus datos de activación cada vez que requieran utilizar su llave privada para firmar o autenticarse. Se deben tomar las consideraciones necesarias en la provisión de las llaves de tal forma que dicha activación sea requerida.

6.2.9. Método de desactivación de la llave privada

Las llaves privadas correspondientes a entidades de certificación de Nivel 1 y Nivel 2 deben encontrarse en modo *off-line,* es decir no conectadas a una red pública o privada. De la misma manera, las copias de seguridad deben encontrarse en módulos criptográficos *off-line*. Para estos casos se deberán establecer procedimientos de activación y desactivación.

En el caso de las llaves privadas de Nivel 3 (ECEP) que se encuentren *on-line*, la desactivación debe ocurrir al momento del apagado del módulo criptográfico que las contiene, lo cual deberá estar procedimentado.

Para el caso de Entidades Finales, las llaves privadas deben ser desactivadas automáticamente al momento del apagado o luego de un periodo establecido de inactividad de la computadora o del módulo criptográfico. Tal procedimiento debe asegurar que no se permita la recuperación de copias ni en la aplicación, ni en la memoria o en el disco del computador.

6.2.10. Método de destrucción de la llave privada

En caso se requiera la destrucción de una llave privada por parte de un PSC, primero deberá realizarse el procedimiento de cancelación del certificado digital como se indica en el numeral **3.4 Identificación y autenticación para solicitudes de cancelación**, y luego se debe eliminar su llave privada del módulo criptográfico correspondiente, para lo cual debe tener un procedimiento definido y aprobado. El procedimiento debe asegurar que copias recuperables no se mantengan en el dispositivo criptográfico o en zonas de memoria o de disco, incluyendo cualquier copia de seguridad. Además, se debe custodiar los registros de la destrucción de la llave privada.

6.2.11. Clasificación del módulo criptográfico

Los módulos criptográficos de los PSC deben cumplir con la certificación de seguridad de alguno de los estándares indicados en el numeral 6.2.1, **Estándares y controles para el módulo criptográfico**, de este documento.

Los módulos criptográficos de Entidad Final bajo la jerarquía descrita en la presente CP deben cumplir con la certificación de seguridad FIPS 140-2 nivel 1 o Common Criteria EAL 4+, conforme a los perfiles de protección referidos por la AAC en la Guía de Acreditación de Entidades de Certificación, como mínimo.

6.3. Otros aspectos de la gestión del par de llaves

6.3.1. Archivo de la llave pública

Las llaves públicas deben ser archivadas de conformidad con las políticas de archivo de registros establecidas en el numeral **5.5, Archivo,** respecto de los certificados digitales que las contienen, los mismos que a su vez deben publicarse conforme se establece en el numeral **2**, **RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO**.

6.3.2. Periodo operacional del par de llaves y periodo de uso de llaves

El periodo operacional y de uso del par de llaves se determina de acuerdo al en el periodo de validez del certificado digital. Dicho periodo se encuentra comprendido en el intervalo entre los campos *NotBefore* (inicio de la validez) y *NotAfter* (fin de la validez).

El periodo de validez del certificado digital debe ser igual al periodo de uso de las llaves, salvo que se encuentre presente la extensión *PrivateKeyUsagePeriod,* que indica un periodo menor para el uso de la llave privada.

La ECERNEP y las ECEP deberán seguir lo establecido por la AAC respecto de los periodos operacional y de uso de llaves teniendo en cuenta la seguridad de los algoritmos de firma y de resumen, además de la longitud de las llaves.

6.4. Datos de activación

Los PSC deben mantener sus datos de activación bajo controles estrictos, siendo de acceso solamente a los roles de confianza definidos.

6.4.1. Generación e instalación de los datos de activación

La generación de los datos de activación de las llaves de los PSC debe darse de manera que para su utilización siempre se requiera control multipersonal de acceso, como se indica en el numeral **6.2.2 Control multipersonal (k de m) de la llave privada.**

6.4.2. Protección de los datos de activación

La protección de los datos de activación de las llaves de los PSC definida en las Prácticas de Certificación en concordancia con los niveles de seguridad ofrecidos por un dispositivo criptográfico con certificación de seguridad FIPS 140-2 nivel 3. Además, el acceso a dichos datos de activación debe encontrarse bajo control multipersonal, como se indica en el numeral **6.2.2 Control multipersonal (k de m) de la llave privada.**

6.4.3. Otros aspectos de los datos de activación

Si el módulo criptográfico lo permite, los datos de activación de las llaves de los PSC deben ser cambiados al menos una vez cada dos años.

6.5. Controles de seguridad computacional

Los PSC que mantengan o procesen información sensible deberán implementar los controles descritos a continuación.

6.5.1. Requisitos técnicos específicos de seguridad computacional

En relación a la implementación de controles de seguridad y los criterios para su evaluación, deben cumplir con lo estipulado en los siguientes estándares, de acuerdo a su nivel de acreditación:

- NTP-ISO/IEC 27001, EDI. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos, o el estándar internacional ISO/IEC 27001
- NTP-ISO/IEC 17799, EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información, o el estándar internacional ISO/IEC 27002.
- ISO/IEC 15408 “Information technology - Security techniques - Evaluation criteria for IT security”.

6.5.2. Evaluación y clasificación de la seguridad computacional

Deben mantener sus equipos y sistemas críticos en un área restringida. Además, deben mantener los equipos necesarios para el cumplimiento de sus funciones operativas en un área dedicada y aislada de otras actividades, implementando procesos de auditoria interna que ejecuten pruebas de seguridad al menos dos veces al año.

La evaluación y clasificación de la seguridad computacional se realizará de manera compatible con los estándares especificados en el numeral **6.5.1, Requisitos técnicos específicos de seguridad computacional**.

6.6. Controles técnicos del ciclo de vida

Los PSC que mantengan o procesen información sensible deberán implementar los controles descritos a continuación.

6.6.1. Controles para el desarrollo de sistemas

Deben contar con hardware y software que cumplan mínimamente los siguientes estándares de seguridad:

- Módulo de hardware criptográfico con certificación confirme alguno de los estándares indicados en el numeral 6.2.1, **Estándares y controles para el módulo criptográfico**, de este documento.
- Debe especificarse los requisitos de control para los nuevos equipos y sistemas.
- Deben pasar por fase de prueba antes de ser puestos en producción e implementarse control de cambios y la verificación de configuraciones.

- El control de calidad del hardware y software debe ser efectuado por los fabricantes, durante su producción.

6.6.2. Controles de gestión de seguridad

Deben proteger en zonas con acceso físico controlado y contar con los controles indicados en el numeral **6.2.2, Control multipersonal (k de m) de la llave privada**, del presente documento.

6.6.3. Controles de seguridad del ciclo de vida

Deben incluir controles en la gestión de seguridad por medio de herramientas y procedimientos que verifiquen la adherencia a la configuración de seguridad de los sistemas operativos y redes. Los controles de seguridad establecidos serán revisados a través de auditorías externas e internas periódicas desarrolladas según el Plan Anual de Auditorías.

6.7. Controles de seguridad de red

La red de los PSC debe estar protegida contra ataques, accesos no autorizados o alteración de datos. Además, los puertos y servicios que no se requieran deben estar apagados. Se debe trabajar con redes segregadas, con segmentos de red aislados de otras áreas de trabajo de la organización. Los equipos y sistemas de las entidades de certificación que operan de modo *online* deben estar circunscritos a límites de una red interna y publicar solamente aquellos servicios destinados al usuario final.

Las redes de los PSC con niveles críticos de seguridad, deben incluir:

- Cifrado de las conexiones involucradas con las operaciones.
- La red debe estar protegida por controles, incluyendo firewalls (hardware) y sistemas de detección de intrusos y software malicioso.
- Los accesos externos no autorizados a la información en las bases de datos deben estar prohibidos.
- Se debe controlar la ruta de acceso del usuario desde la Terminal hasta los servicios.
- Los componentes de la red local deben mantenerse en un ambiente físicamente seguro y sus configuraciones deben ser auditadas periódicamente.
- Los datos sensibles deben ser intercambiados sobre las redes públicas o no confiables a través de técnicas de canal seguro.

6.8. Fecha y Hora

Los registros del repositorio de certificados digitales emitidos y CRL deben contener la información de fecha y hora confiable.

Para el caso de archivos, se admiten servicios de sellado de hora y tiempo según la norma *ISO/IEC 18014-1 "Information technology -- Security techniques-- Time-stamping Services --*

Part 1: Framework" o la norma ETSI EN 319 421. Para tal efecto debe emplearse una fuente confiable de tiempo y el Prestador de Servicio de Valor Añadido de sellos de tiempo deberá encontrarse acreditado por la AAC.

7. PERFILES DE CERTIFICADOS

7.1. Perfil de los certificados

Los certificados emitidos bajo la jerarquía ECERNEP PERU CA ROOT 3, deben cumplir con el estándar ITU X.509 versión 3 y deben contar, como mínimo, con los siguientes campos y extensiones, de acuerdo a lo indicado en el numeral 4.1 del RFC 5280 y el numeral 7.2 de la recomendación ITU-T X.509:

	Descripción
Version	Indica el número de versión X.509 que aplica al certificado digital.
Serial Number	Número entero, mayor a cero (0), aleatorio, no secuencial de al menos 8 bytes para las entidades finales. En cualquier caso, una CA no debe emitir dos certificados digitales con el mismo número de serie.
Signature Algorithm	Algoritmo de firma con el que fue emitido el certificado digital subordinado.
Issuer	*SubjectDN* del PSC emisor
Validity	Campo que contiene el intervalo de tiempo en que el PSC garantiza que se mantendrá la información sobre el estado del certificado. El campo se representa por dos fechas: notBefore, la fecha y hora (en formato UTC) a partir de la cual el certificado digital es válido; y notAfter, la fecha y hora (en formato UTC) en que finaliza la validez del certificado (expiración).
Subject	*SubjectDN* del certificado digital
Subject Public Key Info	Campo que contiene el algoritmo de llave pública y la llave pública propiamente dicha. El algoritmo de llave debe ser RSA de 4096 bits para las CAs y 2048 bits para las entidades finales.
	EXTENSIONES
Authority Key Identifier	Esta extensión provee un medio (al software de validación) para identificar a la llave pública correspondiente a la llave privada utilizada para firmar este certificado digital. El valor de esta extensión debe estar compuesta del resumen hash SHA-1 (160 bits) de la llave pública del emisor.
Subject Key Identifier	Esta extensión provee un medio (al software de validación) para identificar a la llave pública correspondiente a este certificado digital. El valor de esta extensión debe estar compuesta del resumen hash SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info.
Key Usage	Propósitos y usos permitidos de la llave pública contenida en el certificado digital. Campo crítico. KeyUsage ::= BIT STRING { digitalSignature (0), nonRepudiation (1), -- recent editions of X.509 have -- renamed this bit to contentCommitment keyEncipherment (2), dataEncipherment (3), keyAgreement (4), keyCertSign (5), cRLSign (6), encipherOnly (7), decipherOnly (8) } Los bits keyCertSign (5) y cRLSign(6) solo deben ser utilizados en certificados de CA, nunca en certificados de entidad final.
Certificate Policies	Indica el OID, nombre y URL de acceso a las políticas aplicables al certificado digital y el OID correspondiente al tipo de certificados según el árbol de OID's definido por el PSC.
Subject Alternative Name	Extensión que contiene uno o más nombres adicionales del suscriptor del certificado. SubjectAltName ::= GeneralNames GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

	GeneralName ::= CHOICE { otherName [0] OtherName, rfc822Name [1] IA5String, dNSName [2] IA5String, x400Address [3] ORAddress, directoryName [4] Name, ediPartyName [5] EDIPartyName, uniformResourceIdentifier [6] IA5String, iPAddress [7] OCTET STRING, registeredID [8] OBJECT IDENTIFIER } Las CAs puede incluir el email del suscriptor en rfc822Name[1] (ejemplo@dominio) cuando KeyUsage contenga el bit nonRepudiation (1). Las EC deben incluir el DNS en dNSName[2], al emitir certificados de entidad final de tipo SSL.
Basic Constraints	Indica si el certificado digital es de CA o no (entidad final) y cuántos niveles inferiores de certificados digitales de CA subordinadas se puede emitir. La extensión es una secuencia de dos valores: BasicConstraints ::= SEQUENCE { cA BOOLEAN DEFAULT FALSE, pathLenConstraint INTEGER (0..MAX) OPTIONAL cA toma el valor TRUE cuando el certificado es de CA y el valor FALSE, cuando el certificado es de entidad final. pathLenConstraint no debe estar presente si se trata de un certificado de entidad final.
Extended Key Usage	Extensión que indica propósitos y usos de la llave pública, adicionales a los indicados en la extensión KeyUsage.
CRL Distribution Points	Extensión que identifica cómo se obtiene la información de la Lista de Certificados Cancelados (CRL). Las CAs deben incluir la(s) URL(s) de acceso a la CRL. La CRL debe ser emitida por la misma CA que emite los certificados.
Authority Information Access	Indica un método de acceso a información del emisor del certificado. La extensión puede contener dos métodos de acceso: caIssuers, que debe contener la URL de acceso al certificado de la CA emisor y ocsp, que debe contener la URL del OCSP Responder, si fuera implementado por el PSC. El OCSP responder es opcional para cualquier PSC, pero, de existir, debe indicarse su URL de acceso en esta extensión.

Tabla 5 - Extensiones mínimas de un certificado digital de la Jerarquía ECERNEP PERU CA Root 3

El detalle de perfiles y extensiones de certificados digitales de la jerarquía ECERNEP PERU CA Root 3 se encuentra en el Anexo 2 del presente documento. La ECERNEP define en dicho anexo todos los posibles tipos de certificado que emite la ECERNEP y aquellos que las ECEP pueden emitir.

Es potestad de las ECEP delimitar y declarar la versión final de los perfiles de certificado digital que emitirán. Cabe resaltar que la Class 2 de certificados digitales está reservada únicamente para el Registro Nacional de Identificación y Estado Civil, en conformidad con lo establecido en el Reglamento de la Ley de Firmas y Certificados Digitales y en la Ley N° 26497 – Ley Orgánica del Registro Nacional de Identificación y Estado Civil.

Por cuestiones de seguridad, las ECEP no deben emitir los certificados de entidad final solicitados a través de una EREP haciendo uso de sus llaves que operan en modo offline

vinculadas a certificados de nivel 2, sino que deben hacerlo utilizando sus llaves que operan en modo online vinculadas a certificados de nivel 3.

7.1.1. Versión

Se debe utilizar el estándar x.509 versión 3

7.1.2. Extensiones del certificado digital

El detalle de los campos y las extensiones a ser utilizadas en los certificados digitales dentro del ámbito de aplicación de esta CP se presenta en la Tabla 5 - Extensiones mínimas de un certificado digital de la Jerarquía ECERNEP PERU CA Root 3.

7.1.3.Identificadores de objeto de algoritmos

Los certificados digitales generados dentro del ámbito de aplicación de esta CP deben usar como mínimo los siguientes algoritmos de firma:

- SHA512 con cifrado RSA
    - Notación ASN.1 → OID = {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}
    - Notación numérica → OID = 1.2.840.113549.1.1.13
    - Nombre: sha512WithRSAEncryption

- SHA256 con cifrado RSA
    - Notación ASN.1 → OID = {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
    - Notación numérica → OID = 1.2.840.113549.1.1.11
    - Nombre: sha256WithRSAEncryption

7.1.4.Formas de nombres

Se debe respetar la forma de nombres de acuerdo a la familia de estándares ISO/IEC 9594 (recomendación X.500) para *DistinguishedName* como se especifica en el numeral **3.1.1, Tipos de nombres**, del presente documento.

Los certificados digitales para PSC deben indicar un nombre que permita el reconocimiento de la persona jurídica asociada.

Los certificados digitales para Entidad Final deben contener como mínimo, además de lo establecido en el artículo 7º de la Ley de Firmas y Certificados Digitales – Ley 27269, incluyen lo siguiente:

- Para personas naturales:
    - Nombre completo (nombres y apellidos)
    - Número de documento oficial de identidad
    - Tipo de documento

- Para personas jurídicas:

    - Razón social o nombre de la entidad
    - Número de RUC de la entidad
    - Nombre completo del suscriptor
    - Número de documento oficial de identidad del suscriptor
    - Tipo de documento del suscriptor
    - Correo electrónico oficial del suscriptor (opcional)

Las ECEP podrán incluir información adicional siempre y cuando las EREP comprueben de manera fehaciente la veracidad de ésta.

7.1.5. Restricciones de Nombre

Las ECEP pueden establecer restricciones de nombre como se indica en el estándar RFC 5280.

7.1.6. Identificador de objeto de la política de certificados digitales

De acuerdo al Anexo 1 de la Guía de Acreditación para Entidades de Certificación Digital y Entidades Conexas, el INDECOPI es la Autoridad de Registro Nacional (ARN) para la asignación de los OID en el Perú. Las entidades solicitantes de certificados digitales para ECEP deben hacer uso de los OID emitidos por la ARN en cuanto esta alternativa se encuentre disponible para sus declaraciones de prácticas. Entretanto, podrán incluir en sus certificados el OID identificador de objeto de la presente política de certificados digitales, el mismo que proviene de un nodo o arco asignado por la IANA (Autoridad de Números Asignados en Internet) al RENIEC.

Los PSC podrán también declarar, de forma adicional, los OID de aquellas políticas de línea base a las que se adhieran a efectos de interoperabilidad, como ETSI EN 319 411-1.

7.1.7. Uso de la extensión “Restricciones de Políticas” (*PolicyConstraints*)

No aplica.

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

No aplica.

7.1.9. Semántica de procesamiento para la extensión “Políticas de Certificado Digital” (*CertificatePolicy*)

No aplica.

7.2. Perfil de la CRL

Las CRL emitidas por las ECEP deben cumplir lo estipulado en el numeral *5. CRL and CRL Extensions Profile* del RFC 5280 “*PKIX Certificate and CRL Profile*”. En la jerarquía descrita en la presente CP se cuenta con tres niveles, por lo tanto corresponden 3 niveles de listas de certificados digitales cancelados (CRL), tal como se indica en el numeral **4.9.7 Frecuencia de publicación de la Lista de Certificados Cancelados (CRL)**:

- CRL Nivel 1: Lista CRL donde se encuentran la información de cancelación de los certificados digitales de Nivel 2.
- CRL Nivel 2: Lista CRL donde se encuentran la información de cancelación de los certificados digitales de Nivel 3.
- CRL Nivel 3: Lista donde se encuentran la información de cancelación de los certificados digitales de Entidad Final.

7.2.1.Números de versión

Se debe implementar al menos el perfil de CRL en su versión 2 (X.509 v2) en conformidad con lo especificado en el RFC 5280 "*PKIX Certificate and CRL Profile*".

7.2.2.CRL y extensiones de entrada de CRL

No estipulado

7.3. Perfil de OCSP

Las ECEP deben implementar lo estipulado en el RFC 6960 "*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*".

7.3.1.Números de versión

Se debe implementar al menos la versión del protocolo 1 en conformidad con lo especificado en el RFC 6960 "*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*".

7.3.2.Extensiones OCSP

No aplica.

8. AUDITORÍAS DE CONFORMIDAD Y OTRAS EVALUACIONES

8.1. Frecuencia y circunstancias de evaluación

Los PSC se deben someter a una auditoría externa anual, en conformidad con lo regulado por la AAC.

8.2. Identidad/Calificaciones de auditores

Los auditores externos deberán ser designados por la AAC de acuerdo a su normativa. Además, la ECERNEP está en la potestad de realizar visitas no programadas de auditoría a cualquiera de los participantes de la jerarquía descritos en el numeral **1.3 Participantes**, del presente documento.

8.3. Relación del auditor con la entidad auditada

Los PSC deben garantizar que no exista ninguna relación entre la entidad y el auditor que pueda causar o pueda ser percibida como causante de conflicto de intereses. Para ello, se seguirá el procedimiento definido por la AAC para su designación y se contemplarán además de las restricciones establecidas a las Entidades Públicas bajo el marco legal vigente que sean aplicables para su contrataciónes[15].

En el caso de los auditores internos, estos no deberán tener relación funcional directa con el área objeto de la auditoría, como se indica en el numeral **5.2.4 Roles que requieren separación de funciones**.

8.4. Elementos cubierto por la evaluación

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

- Alineación de las Declaraciones de Prácticas a las Guías de Acreditación de la IOFE, la CP y la CPS de la ECERNEP.
- Alineación de las medidas efectivas existentes
- Evaluación y cumplimiento de los niveles de seguridad física
- Revisión de los procedimientos de contingencia
- Revisión del Plan de Contingencias
- Revisión de los controles de seguridad de la información
- Revisión de los controles de acceso a la base de datos

8.5. Acciones a ser tomadas frente a deficiencias

Al detectarse una irregularidad (no conformidad), y dependiendo de la gravedad de la misma, podrán tomarse entre otras las siguientes acciones:

[15] Ley N° 30225, Ley de Contrataciones del Estado, modificatorias y su Reglamento.
Ley N° 26771, Ley que Establece Prohibición de Ejercer la Facultad de Nombramiento y Contratación de Personal en el Sector Público, en Casos de Parentesco, modificatorias y su Reglamento.

- Indicar las irregularidades, pero permitir al PSC que continúe sus operaciones hasta la próxima auditoría programada.
- Permitir al PSC que continúe sus operaciones por un máximo de treinta (30) días calendario pendientes a la corrección de los problemas antes de suspenderlo.
- Suspender la operación del PSC.

El auditor entregará a la AAC un informe técnico sustentando las acciones a realizar y la AAC determinará cuál de estas acciones deberá ser tomada. Esta decisión estará basada en la severidad de las irregularidades, los posibles riesgos y las consecuencias para los suscriptores y titulares.

La AAC se reserva el derecho de revocar o suspender la acreditación de un PSC cuando luego de su auditoría o evaluación de conformidad se comprueba la existencia de deficiencias significativas con relación al marco establecido de la IOFE.

8.6. Publicación de resultados

Los resultados de las auditorías o evaluaciones de conformidad bajo el marco de la IOFE de los PSC acreditados deben ser publicados como parte de la información de estado de aquellas entidades, la cual es publicada por la AAC.

9. OTRAS MATERIAS DE NEGOCIO Y LEGALES

9.1. Tarifas

En el caso de las entidades de la administración pública las tarifas por la prestación de servicios se consignan como tasas en el Texto Único de Procedimientos Administrativos (TUPA). Alternativamente, se puede dar la prestación de servicios a través de convenios.

9.1.1.Tarifas para la emisión o renovación de certificados

Los PSC deben determinar si procede o no el pago de una tasa por la prestación del servicio de emisión o suspensión de certificados digitales u otros servicios de certificación digital y su monto correspondiente. Dicha tasa, deberá incluirse en el TUPA y encontrarse referenciada en los contratos de suscriptores y de terceros que confían.

9.1.2.Tarifas de acceso a certificados

Los PSC deben determinar si procede o no el pago de una tasa por la prestación del servicio de acceso a certificados digitales y su monto correspondiente. Dicha tasa, deberá incluirse en el TUPA y encontrarse referenciada en los contratos de suscriptores y de terceros que confían.

9.1.3.Tarifas para información sobre cancelación o estado

Los PSC deben determinar si procede o no el pago de una tasa por la prestación del servicio de cancelación o estado de certificados digitales y su monto correspondiente. Dicha tasa, deberá incluirse en el TUPA y encontrarse referenciada en los contratos de suscriptores y de terceros que confían.

9.1.4.Tarifas para otros servicios

Los PSC deben determinar si procede o no el pago de una tasa por la prestación de otros servicios de certificación digital y su monto correspondiente. Dicha tasa, deberá incluirse en el TUPA y encontrarse referenciada en los contratos de suscriptores y de terceros que confían.

9.1.5.Políticas de reembolso

Los PSC deben establecer en su CP, CPS u otra documentación relevante, sus políticas de reembolso. En particular, las políticas deben estar establecidas o referencias en los contratos de suscriptores y terceros que confían.

9.2. Responsabilidad Financiera

9.2.1.Cobertura de seguro

Los PSC deberán presentar para su acreditación, documentación que respalde la contratación de seguros o garantías bancarias para salvaguardar las actividades de certificación.

9.2.2.Otros activos

Para las entidades de la administración pública que presten servicios de certificación digital, no será exigible el sustento económico ni la presentación de estados financieros.

9.2.3.Cobertura de seguro o garantía para entidades finales

En el caso que exista cobertura de seguro o garantía disponibles para los suscriptores o los terceros que confían, esto deberá encontrarse referenciado en la CPS, en donde deben incluirse los términos y condiciones de dicha cobertura.

9.3. Confidencialidad de información del negocio

9.3.1.Alcances de la información confidencial

Los PSC acreditados deben mantener de manera confidencial la siguiente información:

- Material comercialmente reservado de los PSC, de los suscriptores, titulares y de los terceros que confían, incluyendo términos contractuales, planes de negocio y propiedad intelectual;
- 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;
- Se debe asegurar la reserva de toda información que mantiene, la cual pudiera perjudicar la normal realización de sus operaciones.

Se permite la publicación de información respecto a la cancelación o suspensión de un certificado, sin revelar la causal que motivó dicha cancelación o suspensión.

La publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.

9.3.2.Información no contenida dentro del rubro de información confidencial

Los PSC deberán determinar la información considerada como pública.

Se permite la publicación de certificados (siempre que el suscriptor lo autorice en el contrato del suscriptor) e información de estado de certificados, así como de información en relación a la cancelación de un certificado sin revelar la razón de dicha cancelación.

La publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.

9.3.3.Responsabilidad de protección de la información confidencial

Los PSCs acreditados deben cumplir tanto sus requisitos de confidencialidad como las leyes sobre protección de datos, confidencialidad de la información y propiedad intelectual que les fueren aplicables, tal y como está establecido en el Norma Marco sobre Privacidad del APEC. De manera particular, será de aplicación la Ley Nº29733, Ley de Protección de Datos Personales y su reglamento.

9.4. Privacidad de la información personal

Los PSC acreditados deben cumplir con la legislación sobre protección de datos de conformidad con la Norma Marco sobre Privacidad del APEC. De manera particular, será de aplicación la Ley Nº29733, Ley de Protección de Datos Personales y su reglamento.

También debe tomarse en consideración la legislación sobre protección de datos de las jurisdicciones con las que mantengan acuerdos de reconocimiento cruzado y las políticas de protección de datos personales existentes en dichas infraestructuras.

Debe tomarse particular atención a las provisiones relativas a la transferencia internacional de información personal.

Los PSC deben realizar evaluaciones de impacto a la privacidad de sus operaciones, como parte del proceso necesario para su correspondiente acreditación.

9.4.1.Plan de privacidad

Se requiere de los PSCs la preparación de un Plan de Privacidad en conformidad con la Norma Marco sobre Privacidad del APEC, con la Ley Nº29733, Ley de Protección de Datos Personales y su reglamento, como parte de la documentación a ser presentada y evaluada para su acreditación ante la AAC de la IOFE.

El plan debe establecer el tipo de datos personales que pueden ser recolectados y cómo serán utilizados, protegidos, recuperados/corregidos, las circunstancias en que estos serán revelados y las sanciones en caso de incumplimiento del plan.

9.4.2.Información tratada como privada

Los PSC deben mantener de manera confidencial la siguiente información:

- Información personal provista por los suscriptores, titulares y terceros que confían que no sea la autorizada para estar contenida en certificados y repositorios;
- Información que pueda permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre suscriptores, titulares y terceros que confían; e
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían.

No obstante, de acuerdo al Artículo 14 de la Ley Nº 29733, Ley de Protección de Datos Personales, no se requiere del consentimiento del titular de datos personales para los efectos de su tratamiento, cuando tales datos se recopilen o transfieran para el ejercicio de las funciones de las entidades de la administración pública en el ámbito de sus competencias.

Se debe permitir la publicación de información respecto a la cancelación o suspensión de un certificado, sin revelar la causal que motivó dicha cancelación o suspensión.

9.4.3.Información no considerada privada

Se permite la divulgación de información personal sólo en los casos en que exista consentimiento expreso del individuo cuya información corresponde. No obstante, de acuerdo al Artículo 14 de la Ley Nº 29733, Ley de Protección de Datos Personales, no se

requiere del consentimiento del titular de datos personales para los efectos de su tratamiento, cuando tales datos se recopilen o transfieran para el ejercicio de las funciones de las entidades de la administración pública en el ámbito de sus competencias.

Se permite la publicación de certificados e información de estado de certificado y la publicación de información en relación a si un certificado ha sido suspendido o cancelado, sin revelar la causal que motivó dicha suspensión o cancelación.

9.4.4. Responsabilidad de protección de la información privada

Los PSC acreditados deben cumplir con sus requerimientos de confidencialidad y con la Ley Nº 29733, Ley de Protección de Datos Personales en conformidad con su Plan de Privacidad y la Norma Marco sobre Privacidad del APEC.

9.4.5.Notificación y consentimiento para el uso de información

No obstante lo establecido en el Artículo 14, numeral 1, de la Ley Nº 29733, Ley de Protección de Datos Personales, en el sentido que no se requiere del consentimiento del titular de datos personales para los efectos de su tratamiento, cuando tales datos se recopilen o transfieran para el ejercicio de las funciones de las entidades de la administración pública en el ámbito de sus competencias, en los contratos que serán firmados por los suscriptores se deberá contemplar tal consentimiento conforme se establece en el numeral 9.4.5 del Anexo 1 de la Guía de Acreditación de Entidades de Certificación EC, lo cual guarda concordancia con estándares internacionales reconocidos[16].

9.4.6. Divulgación con motivo de un proceso judicial o administrativo

Los datos personales de carácter privado o la información confidencial los usuarios de los servicios de certificación digital podrán ser revelados o comunicados cuando una orden judicial o una resolución administrativa emitida por la autoridad competente y de acuerdo a ley así lo exijan. De igual manera, cuando ésto sea autorizado de manera expresa por tales usuarios.

9.4.7.Otras circunstancias para divulgación de información

Se debe permitir a los usuarios de los servicios de certificación digital, en particular suscriptores y titulares de certificados digitales o terceros que confían, solicitar la divulgación de la información que han provisto a los PSC.

Bajo otras circunstancias, se debe requerir que la divulgación de la información se realice de conformidad con las declaraciones de prácticas u otra documentación relevante, cumpliendo con lo establecido en la Ley Nº 29733, Ley de Protección de Datos Personales y su reglamento, en el Artículo 55 del Reglamento de la Ley de Firmas y Certificados Digitales y en la Norma Marco sobre Privacidad del APEC.

[16] Cfr. la sección 6.1.b) de ETSI EN 319 411-1, en la que se establece que solo se podrá poner a disposición certificados digitales para su descarga o recuperación contando con el consentimiento de su suscriptor y de su titular.

9.5. Derechos de propiedad intelectual

Se permite a los PSC acreditados, la protección de los derechos de propiedad intelectual respecto de sus propias tecnologías y procesos.

Los PSC acreditados deben mantener los derechos de propiedad intelectual necesarios para el material y los procesos que utilizan para las operaciones dentro del marco de la IOFE.

9.6. Representaciones y garantías

9.6.1. Representaciones y garantías de la EC

Los PSC y las ECEP en particular deben establecer en su CPS provisiones de garantía y responsabilidad, incluyendo limitaciones y exenciones. Debe asimismo asegurar que dichas cláusulas se encuentren establecidas en los contratos de suscriptor y tercero que confía.

Cuando las ECEP tercerizan las funciones repositorio, debe establecerse la responsabilidad de las ECEP y de aquellas organizaciones que realizan las actividades tercerizadas. Las ECEP deben asegurarse que las organizaciones realizando las actividades tercerizadas, realizan dichas funciones de conformidad con la CP, CPS y otra documentación de la ECEP, estableciendo provisiones de responsabilidad respecto a los eventuales errores y omisiones que pudieran generarse.

En particular, las ECEP deben establecer responsabilidades en relación a errores u omisiones en la producción y distribución de certificados, directorios y listas de revocación de certificados, incluyendo la disponibilidad de dichos directorios y listas CRL.

9.6.2. Representaciones y garantías de la ER

Los PSC y las EREP en particular deben establecer en su CPS provisiones de garantía y responsabilidad, incluyendo limitaciones y exenciones. Debe asimismo asegurar que dichas cláusulas se encuentren establecidas en los contratos de suscriptor y tercero que confía.

En particular, las EREP deben establecer responsabilidades en relación a errores u omisiones en la identificación del suscriptor, procesamiento de las solicitudes de certificado o de revocación y protección de datos personales provistos.

9.6.3. Representaciones y garantías de los suscriptores

El suscriptor y el titular de un certificado digital, o los usuarios de servicios de certificación digital, están obligados a cumplir lo establecido en la políticas y declaraciones de prácticas de los PSC. Se les debe requerir la firma de un contrato donde consten sus obligaciones. El acuerdo debe incluir las consecuencias de eventuales incumplimientos.

El contrato debe contemplar las obligaciones cuando la legislación las establezca para los suscriptores o titulares de certificados digitales a fin de asegurar los efectos legales de las transacciones realizadas utilizando certificados emitidos por las ECEP.

Las obligaciones del suscriptor o titular de un certificado digital pueden incluir la garantía de la exactitud de la información provista en las solicitudes de prestación de servicios, la

protección de las llaves y certificados digitales frente a malos usos y el acuerdo de no emplearlos fuera de los alcances de la IOFE.

9.6.4. Representaciones y garantías de los terceros que confían

Un tercero que confía puede ser requerido a cumplir con las obligaciones establecidas para él en las declaraciones de prácticas de los PSC. Se le debe notificar al tercero que confía dichas obligaciones por intermedio de la publicación de un documento accesible. La declaración o documento, debe incluir las consecuencias derivadas de su incumplimiento.

Cuando la legislación establezca determinadas obligaciones al tercero que confía para asegurar efecto legal a las transacciones realizadas utilizando certificados en los cuales esta parte confía, la documentación debe de establecer dichas obligaciones.

Las obligaciones del tercero que confía pueden incluir la necesidad de verificación del estado de los certificados y el acuerdo de no usar los certificados fuera de los términos establecidos en el marco de la IOFE.

9.6.5. Representaciones y garantías de otros participantes

Los PSC bajo la jerarquía ECERNEP PERU CA Root 3 en general, deben establecer en sus políticas, declaraciones de prácticas u otra documentación relevante provisiones sobre garantías y responsabilidades, incluyendo limitaciones y exclusiones de las mismas en relación a cualquier otro participante no mencionado anteriormente. Asimismo, deben asegurarse que dichas provisiones se incluyan en todo contrato para los usuarios de sus servicios o terceros que confían.

Las ECEP deben establecer, de igual manera, la responsabilidad que les toca en relación a la gestión del repositorio, en particular respecto a errores u omisiones en el procesamiento y mantenimiento de directorios y listas CRL y su disponibilidad.

9.7. Exención de garantías

Los PSC deben establecer en sus políticas, declaraciones de prácticas o en otra documentación relevante, cualquier exención de responsabilidad que pudiera aplicárseles. Asimismo deben asegurarse que estas provisiones sean incluidas en cualquier contrato de suscriptor o tercero que confía.

No cabe exención de responsabilidad para aquellas garantías establecidas por la legislación vigente (Ley Nº27269, Ley de Firmas y Certificados Digitales y normas complementarias).

9.8. Limitaciones a la responsabilidad

Los PSC deben establecer en sus políticas, declaraciones de prácticas o en otra documentación relevante, cualquier limitación de responsabilidad que pudiera aplicárseles, considerando las responsabilidades de privacidad, seguridad y diligencia en los procesos de certificación que la AAC establece en las guías de acreditación correspondientes. Asimismo, deben asegurarse que estas provisiones sean incluidas en cualquier contrato de suscriptor o tercero que confía.

9.9. Indemnizaciones

Los PSC deben establecer en sus políticas, declaraciones de prácticas o en otra documentación relevante, lo relativo a las indemnizaciones a las que pudieran estar sujetos.

Asimismo, deben asegurarse que estas provisiones sean incluidas en cualquier contrato de suscriptor o tercero que confía.

9.10. Término y terminación

9.10.1. Término

Cuando caduca la acreditación de un PSC, su documentación también debe de caducar. En consecuencia, el periodo de validez o plazo máximo de la documentación relativa a los PSC acreditados es de cinco (5) años de acuerdo a la normativa vigente. Se contemplará que la validez de tal documentación estará sujeta a la continuidad de la acreditación.

Se permite que los contratos de prestación de servicios de certificación digital sean resueltos cuando las partes del acuerdo incumplen las obligaciones que les tocan dentro del marco de la IOFE.

Se incluirá las provisiones del caso sobre la vigencia de la documentación en los contratos de prestación de servicios de certificación digital. Los PSC modificarán dicha documentación cada vez que la AAC de la IOFE y/o el propio PSC lo determinen. Las modificaciones realizadas deben ser comunicadas a los involucrados: usuarios, suscriptores, titulares y/o terceros que confían, según el caso.

9.10.2. Terminación

En caso de cese de actividades de los PSC, estos informarán a la ECERNEP y a la AAC de la IOFE, así como a los titulares, suscriptores y terceros que confían con un mínimo de treinta (30) días calendario de anticipación.

Los procedimientos necesarios para el cese de las operaciones de un PSC, serán establecidos por la AAC de la IOFE en conformidad con la legislación vigente.

9.10.3. Efecto de terminación y supervivencia

Los PSC deben establecer en sus políticas, declaraciones de prácticas u otra documentación relevante las provisiones de divisibilidad, supervivencia y fusión que resulten aplicables de acuerdo a su naturaleza jurídica, incluyendo las mismas en los contratos de suscriptor y tercero que confía. En el caso de las entidades de la administración pública cuyas funciones sean transferidas o fusionadas, tales provisiones se encuentran señaladas en las normas emitidas para tal fin.

Las EREP en sus modelos de contratos de suscriptor y terceros que confían deberán establecer, en lo que les resulte aplicable, cláusulas de supervivencia, de modo que ciertas reglas continúen vigentes después del término de validez de las declaraciones de prácticas y de los contratos de los suscriptores y terceros que confían.

9.11. Notificaciones y comunicaciones individuales con los participantes

Los PSC deben establecer en sus políticas, declaraciones de prácticas, contratos u otra documentación relevante, provisiones sobre notificación que regulen los procedimientos por los que las partes se notifiquen hechos mutuamente.

9.12. Enmendaduras

9.12.1. Procedimiento para enmendaduras

Los participantes de la IOFE serán consultados antes de efectuar cualquier tipo de cambio en los documentos que la regulan. Esta provisión no se aplica a cambios de las políticas y prácticas de los PSCs acreditados, cuando dichos cambios son consistentes con las exigencias documentadas de la propia IOFE.

Los cambios efectuados a las políticas y prácticas documentadas por los PSC acreditados deben ser revisados por la AAC de la IOFE antes que estos puedan implementarse. La documentación puede requerir una revisión.

9.12.2. Mecanismos y periodos de notificación

Los cambios en las políticas y prácticas de los PSC acreditados deben ser notificados a los suscriptores, terceros que confían y otras partes involucradas, cuando dichos cambios puedan afectarles.

Cualquier cambio en los términos y condiciones básicas de operación como: identificadores de políticas, limitaciones de uso, obligaciones de suscriptor, forma de validación de un certificado, limitaciones a responsabilidad, procedimiento de resolución de disputas, periodo dentro del cual los registros de auditoría serán conservados, sistema legal aplicable y conformidad según el marco de la IOFE, deberá ser notificado a los usuarios de los servicios de certificación digital y terceros que confían.

Los PSC acreditados, deben advertir a los suscriptores y potenciales terceros que confían la forma de notificación de esta información y las implicancias de dicha notificación.

9.12.3. Circunstancias bajo las cuales debe ser cambiado el OID

Para mantener la acreditación del PSC será necesario que cualquier cambio en el OID de cualquiera de los certificados y políticas o declaraciones de prácticas sea aprobado previamente por la AAC de la IOFE.

Debe llevarse control de versiones para asegurar el que se pueda determinar las políticas y declaraciones de prácticas vigentes al momento de archivar una transacción.

9.13. Procedimiento sobre resolución de disputas

Un PSC acreditado debe establecer procedimientos de resolución de disputas en su CPS u otra documentación relevante.

Se pueden establecer diferentes leyes aplicables para diferentes tipos de procesos de resolución de disputas.

De ser posible y estar permitido por las leyes correspondientes, debe considerarse el empleo de resolución de disputas en línea.

9.14. Ley aplicable

Los PSC deben identificar en sus declaraciones de prácticas y otra documentación relevante, la ley aplicable a sus operaciones, en particular la Ley N° 27269, Ley de Firmas y Certificados Digitales y su reglamento.

Los requerimientos legalmente significativos deben de estar establecidos o referenciados en los contratos pertinentes.

9.15. Conformidad con la ley aplicable

Los PSC deben identificar en sus declaraciones de prácticas y otra documentación relevante, la ley aplicable a sus operaciones, en particular la Ley N° 27269, Ley de Firmas y Certificados Digitales y su reglamento.

Los requerimientos legalmente significativos deben de estar establecidos o referenciados en los contratos pertinentes.

9.16. Cláusulas misceláneas

Los PSC deben incluir en sus declaraciones de prácticas y otra documentación toda cláusula miscelánea que se aplique a las operaciones que realiza bajo la IOFE.

De ser apropiado, estas provisiones deben ser establecidas o referenciadas en los contratos pertinentes.

9.16.1. Acuerdo Íntegro

Se debe hacer referencia en cada acuerdo que celebren los PSC acreditados de cualquier otra documentación que pueda ser incorporada en el acuerdo.

Los PSC deben establecer en sus contratos cláusulas de acuerdo íntegro en virtud de las cuales se entenderá que el instrumento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.

9.16.2. Subrogación

Los derechos y los deberes asociados a la condición de PSC no podrán ser objeto de cesión a terceros de ningún tipo, ni ninguna tercera entidad podrá subrogarse en la posición jurídica de dichas entidades.

Los PSC acreditados deben establecer en su documentación cualquier limitación en la subrogación de derechos o delegación de obligaciones.

9.16.3. Divisibilidad

Los PSC deberán establecer en sus declaraciones de prácticas o en sus contratos cláusulas de divisibilidad, por las cuales la invalidez de una cláusula no afectará al resto del contrato.

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

El PSC acreditado debe establecer en su CPS y otra documentación relevante toda cláusula de ejecución que se aplique a las operaciones que realiza. Estas cláusulas deben estar establecidas o referenciadas en los contratos de suscriptor y tercero que confía.

9.16.5. Fuerza Mayor

Los PSC deben garantizar que se establezcan explícitamente clásulas de “fuerza mayor” en los contratos correspondientes.

9.17. Otras cláusulas

El PSC acreditado debe establecer en su declaración de prácticas y otra documentación relevante cualquier otra cláusula que se aplique a las operaciones que realiza bajo la IOFE. Cuando fuere apropiado, estas cláusulas deben establecerse o referenciarse en los contratos correspondientes.

Anexo 1: Definiciones, abreviaturas y acrónimos

A. Acrónimos:

- APEC: Foro de Cooperación Económica Asia-Pacífico
- CP: Política de Certificación
- CPS: Declaración de Prácticas de Certificación
- ECEP: Entidad de Certificación para el Estado Peruano
- ECERNEP: Entidad de Certificación Nacional para el Estado Peruano
- EREP: Entidad de Registro para el Estado Peruano
- INACAL: Instituto Nacional de Calidad
- INDECOPI: Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual
- PSC: Prestador de Servicios de Certificación Digital
- PSVA: Prestador de Servicios de Valor Añadido
- RENIEC: Registro Nacional de Identificación y Estado Civil
- RPS: Declaración de Prácticas de Registro
- SID: Sistema de Intermediación Digital
- TSA: Autoridad de Sellado de Tiempo

B. Definiciones:

Se ha tomado como referencia las definiciones establecidas en el D.S. N° 052-2008-PCM "Reglamento de la Ley de Firmas y Certificados Digitales".

- **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 requisitos predefinidos y dar una respuesta automática sin intervención humana, en dicha fase.
- **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.
- **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.
- **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:

    - El documento electrónico produzca siempre el mismo código de verificación (resumen) cada vez que se le aplique dicho algoritmo.
    - 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.
    - 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.

- **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 (RPS).-** 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.
- **Declaración de Prácticas de Prestador de Servicios de Valor Añadido (PSVA).-** Documento oficialmente presentado por un Prestador de Servicios de Valor Añadido a la Autoridad Administrativa Competente, mediante el cual define las prácticas para la prestación de su servicio.
- **Documento oficial de identidad.-** Es el documento oficial que sirve para acreditar la identidad de una persona natural, que puede ser:

    - Documento Nacional de Identidad (DNI);
    - Carné de extranjería actualizado, para las personas naturales extranjeras domiciliadas en el país; o,
    - 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 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 deberán contar con acreditación o reconocimiento dentro de la IOFE y serán supervisadas y reguladas lavajo el marco 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 el INACAL, 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 significa módulo de seguridad de hardware. Es un módulo 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, CP, 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:

    - La integridad de los documentos electrónicos;
    - 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 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.
- Modificación del certificado: La modificación de un certificado digital consiste en cambiar los datos contenidos en él sin efectuar una renovación de llaves.
- **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.
- **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 requisitos 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:
    - 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 el Sellado de Tiempo que no requieren en ninguna etapa de la firma digital del usuario final en documento alguno.
    - 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.
- Reemisión del certificado: En la reemisión de un certificado digital se genera un nuevo par de llaves y se emite un nuevo certificado al suscriptor utilizando su información previamente presentada.
- **Reglamento.-** Reglamento de la Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley Nº 27310.
- **Renovación del certificado:** La renovación de un certificado digital es el procedimiento por el cual un suscriptor que ya cuenta con un certificado digital solicita la generación de uno nuevo con la información previa del suscriptor y utilizando el mismo par de llaves
- **Revocación de un certificado digital:** Cancelación de oficio de un certificado digital efectuada por una entidad de certificación.
- **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 (online) 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.
- **Suspensión:** La suspensión es el proceso por el cuál una ECEP, remueve temporalmente un certificado del directorio de certificados válidos o cambia su estado a "suspendido".
- **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.

Anexo 2 – Detalle de Perfiles y Extensiones de Certificados Digitales de la Jerarquía ECERNEP PERU CA Root 3

1. Perfiles y extensiones de certificados digitales emitidos por la ECERNEP

1.1. ECERNEP Root CA

Perfil de Certificado ECERNEP				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 20 bytes>*	Sí	-
Signature	algorithm	Sha512WithRSAEncryption	Sí	-
Issuer	CN	ECERNEP PERU CA ROOT 3	Sí	-
	O	Entidad de Certificación Nacional para el Estado Peruano		
	C	PE		
Validity	(Not After - Not Before)	25 años	Sí	-
Subject	CN	ECERNEP PERU CA ROOT 3	Sí	-
	O	Entidad de Certificación Nacional para el Estado Peruano		
	C	PE		
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	4096 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	keyCertSign, cRLSign	Sí	Sí
Certificate Policies	policyIdentifier (OID)	2.5.29.32.0	Sí	No
	cPSuri	-		
	explicitText	Any Policy		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	TRUE	Sí	Sí
	Path Length Constraint	2		
Extended Key Usage	-	-	-	-
CRL Distribution Points	-	-	-	-
Authority Information Access	calssuers (URI)	http://www.reniec.gob.pe/crt/sha2/ecernep.crt	Sí	No

	ocsp (URI)	-	-	-
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

1.2. EC-PSVA

Además de emitir certificados para las ECEP, la ECERNEP tiene la responsabilidad de emitir certificados para los PSC acreditados como PSVA. Por cuestiones de seguridad, la ECERNEP no puede emitir tales certificados directamente subordinados a la raíz. Por lo tanto, para estos casos se hace por intermedio de un certificado de nivel 2 cuyas llaves privadas operan en modo offline. En la siguiente Tabla se presenta el perfil del referido certificado

Perfil de Certificado EC-PSVA				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de 20 bytes>*	Sí	-
Signature	algorithm	Sha512WithRSAEncryption	Sí	-
Issuer	CN	ECERNEP PERU CA ROOT 3	Sí	-
	O	Entidad de Certificación Nacional para el Estado Peruano		
	C	PE		
Validity	(Not After - Not Before)	16 años	Sí	-
Subject	CN	EC-PSVA	Sí	-
	O	Entidad de Certificación Nacional para el Estado Peruano		
	C	PE		
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	4096 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	keyCertSign, cRLSign	Sí	Sí
Certificate Policies	policyIdentifier (OID)	2.5.29.32.0	Sí	No
	cPSuri	-		
	explicitText	Any Policy		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	TRUE	Sí	Sí
	Path Length Constraint	0		
Extended Key	-	Time Stamping (1.3.6.1.5.5.7.3.8)	Sí	No

Usage				
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/arl/sha2/ecernep.crl	Sí	No
	DistributionPointName (URI)	http://crl2.reniec.gob.pe/arl/sha2/ecernep.crl	Sí	No
Authority Information Access	cAIssuers	http://www.reniec.gob.pe/crt/sha2/ecernep.crt	Sí	No
	ocsp (URI)	-	-	-
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

1.3. ECEP off line

Perfil de Certificado ECEP-XX				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha512WithRSAEncryption	Sí	-
Issuer	CN	ECERNEP PERU CA ROOT 3	Sí	-
	O	Entidad de Certificación Nacional para el Estado Peruano		
	C	PE		
Validity	(Not After - Not Before)	16 años	Sí	-
Subject	CN	ECEP-*<Siglas de la Entidad>*	Sí	-
	O	<Nombre de la Entidad>		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad>	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	4096 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	keyCertSign, cRLSign	Sí	Sí
Certificate Policies	policyIdentifier (OID)	2.5.29.32.0	Sí	No
	cPSuri	-		
	explicitText	Any Policy		
Subject Alternative Name	-	-	-	-

Basic Constraints	cA	TRUE	Sí	Sí
	Path Length Constraint	1		
Extended Key Usage	-	ClientAuth (1.3.6.1.5.5.7.3.2)	No	No
	-	EmailProtection (1.3.6.1.5.5.7.3.4)	No	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	No	No
	-	OcspSigning (1.3.6.1.5.5.7.3.9)	No	No
	-	ServerAuth (1.3.6.1.5.5.7.3.1)	No	No
CRL Distribution Points	DistributionPointName (URI)	http://crl.reniec.gob.pe/arl/sha2/ecernep.crl	Sí	No
Authority Information Access	cAIssuers	http://crl.reniec.gob.pe/crt/sha2/ecernep.crt	Sí	No
	ocsp (URI)	-	-	-
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

1.4. ECEP on line

Perfil de Certificado ECEP-XX CA Class X				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha512WithRSAEncryption	Sí	-
Issuer	CN	ECEP-*<Siglas de la Entidad>*	Sí	-
	O	<Nombre de la Entidad>		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	8 años	Sí	-
Subject	CN	ECEP-*<Siglas de la Entidad>* CA Class {1,2,3,4}	Sí	-
	O	<Nombre de la Entidad>		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad>	Sí	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	4096 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	keyCertSign, cRLSign	Sí	Sí

Certificate Policies	policyIdentifier (OID)	2.5.29.32.0	Sí	No
	cPSuri	-		
	explicitText	Any Policy		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	TRUE	Sí	Sí
	Path Length Constraint	0		
Extended Key Usage	-	ClientAuth (1.3.6.1.5.5.7.3.2)	No	No
	-	EmailProtection (1.3.6.1.5.5.7.3.4)	No	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	No	No
	-	OcspSigning (1.3.6.1.5.5.7.3.9)	No	No
	-	ServerAuth (1.3.6.1.5.5.7.3.1)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	No	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

2. Perfil de certificado digital de entidad final PSVA – TSA emitido por la ECERNEP a través de la EC-PSVA

Perfil de Certificado PSVA-TSA				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	EC-PSVA	Sí	-
	O	Entidad de Certificación Nacional para el Estado Peruano		
	C	PE		
Validity	(Not After - Not Before)	min 8 años, máx 12 años	Sí	-
Subject	CN	PSVA-TSA-*<Siglas de la Entidad>*	-	-
	SERIALNUMBER	*<Información adicional>*	No	
	O	*<Nombre de la Entidad>*	Sí	
	C	PE	Sí	
Subject Public Key Info	algorithm	RSA	-	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No

Key Usage	-	digitalSignature, nonRepudiation	Sí	No
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://www.reniec.gob.pe/repository/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	Time Stamping (1.3.6.1.5.5.7.3.8)	Sí	Sí
CRL Distribution Points	DistributionPoint Name (URI)	http://crl.reniec.gob.pe/arl/sha2/ecpsva.crl	Sí	No
	DistributionPoint Name (URI)	http://crl2.reniec.gob.pe/arl/sha2/ecpsva.crl	Sí	No
Authority Information Access	cAIssuers	http://www.reniec.gob.pe/crt/sha2/ecpsva.crt	Sí	No
	ocsp (URI)	-	-	-
Subject Information Access	timeStamping (URI)	-	Sí	No
OCSP no check	-	-	-	-

3. Perfiles y extensiones de certificados digitales de entidad final que pueden ser emitidos por las ECEP

La ECERNEP define a continuación todos los posibles tipos de certificado que las ECEP pueden emitir. Sin embargo, es potestad de las ECEP delimitar y declarar la versión final de los perfiles de certificado digital que emiten. Cabe resaltar que la Class 2 está reservada únicamente para el Registro Nacional de Identificación y Estado Civil, en conformidad con lo establecido en el Reglamento de la Ley de Firmas y Certificados Digitales y en la Ley N° 26497 – Ley Orgánica del Registro Nacional de Identificación y Estado Civil.

El tipo de certificado indica el fin para el cual se utilizará dicho certificado y los valores que deben contener en sus perfiles. La siguiente tabla indica los tipos de certificado que pueden ser emitidos por las ECEP bajo cada clase, se añade además el que puede emitir la EC-PSVA:

SUSCRIPTORES						
	Class 1	Class 2	Class 3	Class 4	EC-PSVA	Totales
AUT Software	X		X			2
AUT Hardware	X	X	X			3
FIR Software	X		X			2
FIR Hardware	X	X	X			3
FAU Software	X		X			2
FAU Hardware	X		X			2
CIF Software	X		X			2
CIF Hardware	X	X	X			3
SSL/TLS				X		1
SSL/TLS EV				X		1
DC				X		1
AA				X		1
TSA					X	1
TOTAL	8	3	8	4	1	24

Leyenda: AUT (Autenticación), FIR (Firma), FAU (Firma y autenticación), CIF (Cifrado), SSL/TLS (Secure Sockets Layer/Transport Layer Security), SSL/TLS EV (Secure Sockets Layer/Transport Layer Security Extended Validation), DC (Domain Controller), AA (Agente Automatizado), TSA (Time Stamp Authority).

Como se observa, la ECERNEP permite a la EC-PSVA emitir un (01) tipo de certificado, solamente a los PSVA acreditados como TSA. Además, permite a la ECEP-RENIEC emitir veinticuatro (24) tipos de certificados para suscriptores, repartidos en las cuatro (04) Clases. Las otras ECEP, pueden emitir veinte (20) tipos de certificados, repartidos en la Class 1, Class 3 y Class 4.

Las ECEP deben indicar en su CPS los tipos de certificados que emiten y detallar cada perfil, ya sea para producción o para pruebas.

En todos los casos, el texto contenido entre los símbolos “<>”, indica que se debe reemplazar por la información del suscriptor. Ejemplo: En un certificado emitido para el Sr. Juan Alberto Perez Gonzales el texto **CN=<APELLIDOS Nombres> tomará el valor CN=PEREZ GONZALES Juan Alberto**. Asimismo, el texto contenido entre los símbolos {} y entre comas, indica que se debe elegir uno y sólo uno de los valores, según el tipo de certificado. Ejemplo: En un certificado de OCSP responder emitido para la Class 4, el texto **CN=OCSP Responder Class {1, 2, 3, 4} tomará el valor CN= OCSP Responder Class 4.**

3.1. Class 1

La Class 1 se encuentra reservada para emitir certificados que no estén contenidos dentro del DNIe a personas naturales.

3.1.1. Autenticación en Software

Perfil de Certificado Class 1 AUT MEDIO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 1	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	O	*<Nombre del Colegio Profesional>*	No	
	OI	NTRPE-<número de RUC del Colegio>	No	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		

	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.1*	Sí	
	explicitText	*Política de Certificado Normalizado NCP de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	ClientAuth (1.3.6.1.5.5.7.3.2)	No	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

3.1.2. Autenticación en Hardware

Perfil de Certificado Class 1 AUT ALTO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 1	Sí	-
	O	*<Nombre de la Entidad>*		

	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	O	*<Nombre del Colegio Profesional>*	No	
	OI	NTRPE-<número de RUC del Colegio>	No	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.2*	Sí	
	explicitText	*Política de Certificado NCP+ con QSCD de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	-	-	-	-

Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	ClientAuth (1.3.6.1.5.5.7.3.2)	No	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

3.1.3. Firma en Software

Perfil de Certificado Class 1 FIR MEDIO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 1	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	O	*<Nombre del Colegio Profesional>*	No	
	OI	NTRPE-<número de RUC del Colegio>	No	

	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	nonRepudiation	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.1*	Sí	
	explicitText	*Política de Certificado Normalizado NCP de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

Qualified Certificate Statements	QcRetentionPeriod	10	Sí	
	QcLimitValue		No	
	QcPDS	*{https://pki.reniec.gob.pe/repositorio/,es}*	Sí	

3.1.4. Firma en Hardware

Perfil de Certificado Class 1 FIR ALTO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 1	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	O	*<Nombre del Colegio Profesional>*	No	
	OI	NTRPE-<número de RUC del Colegio>	No	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject*	Sí	No

		Public Key Info del emisor>		
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	nonRepudiation	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.2*	Sí	
	explicitText	*Política de Certificado NCP+ con QSCD de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-
Qualified Certificate Statements	QcRetentionPeriod	10	Sí	
	QcLimitValue		No	
	QcPDS	*{https://pki.reniec.gob.pe/repositorio/,es}*	Sí	

3.1.5. Firma y Autenticación en Software

Perfil de Certificado Class 1 FAU MEDIO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 1	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	O	*<Nombre del Colegio Profesional>*	No	
	OI	NTRPE-<número de RUC del Colegio>	No	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature, nonRepudiation	Sí	Sí
Certificate	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No

Policies	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.1*	Sí	
	explicitText	*Política de Certificado Normalizado NCP de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	No	No
	-	ClientAuth (1.3.6.1.5.5.7.3.2)	No	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-
Qualified Certificate Statements	QcRetentionPeriod	10	Sí	
	QcLimitValue		No	
	QcPDS	*{https://pki.reniec.gob.pe/repositorio/,es}*	Sí	

3.1.6. Firma y Autenticación en Hardware

Perfil de Certificado Class 1 FAU ALTO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 1	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	O	*<Nombre del Colegio Profesional>*	No	
	OI	NTRPE-<número de RUC del Colegio>	No	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature, nonRepudiation	Sí	Sí
Certificate	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No

Policies	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.2*	Sí	
	explicitText	*Política de Certificado NCP+ con QSCD de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	No	No
	-	ClientAuth (1.3.6.1.5.5.7.3.2)	No	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-
Qualified Certificate Statements	QcRetentionPeriod	*10*	Sí	
	QcLimitValue		No	
	QcPDS	*{https://pki.reniec.gob.pe/repositorio/,es}*	Sí	

3.1.7. Cifrado en Software

Perfil de Certificado Class 1 CIF MEDIO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 1	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	O	*<Nombre del Colegio Profesional>*	No	
	OI	NTRPE-<número de RUC del Colegio>	No	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	dataEncipherment	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.1*	Sí	
	explicitText	*Política de Certificado Normalizado NCP de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No

	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

3.1.8. Cifrado en Hardware

Perfil de Certificado Class 1 CIF ALTO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 1	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	

	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	O	*<Nombre del Colegio Profesional>*	No	
	OI	NTRPE-<número de RUC del Colegio>	No	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	dataEncipherment	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.2*	Sí	
	explicitText	*Política de Certificado NCP+ con QSCD de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

3.2. Class 2

La Class 2 se encuentra reservada para emitir certificados a personas naturales dentro del DNIe. La ECEP-RENIEC, es la única que puede emitir certificados de Class 2.[17]

3.2.1. Autenticación en Hardware

Perfil de Certificado Class 2 AUT ALTO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 2	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	4 años	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No

[17] Mediante Resolución Nº 042-2016/CFE-INDECOPI de 7 de abril de 2016, la AAC establece:
"Se aceptará en la IOFE un plazo de vigencia de cuatro años para los certificados digitales que cuenten con claves de 2048 bits de longitud, siempre que en el proceso de cifrado se utilice el algoritmo de encriptación SHA-256."

Key Usage	-	digitalSignature	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.2*	Sí	
	explicitText	*Política de Certificado NCP+ con QSCD de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	ClientAuth (1.3.6.1.5.5.7.3.2)	Sí	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	Sí	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

3.2.2. Firma en Hardware

Perfil de Certificado Class 2 FIR ALTO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 2	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		

	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	4 años	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	nonRepudiation	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.2*	Sí	
	explicitText	*Política de Certificado NCP+ con QSCD de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic	cA	FALSE	Sí	Sí

Constraints	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-
Qualified Certificate Statements	QcRetentionPeriod	*10*	Sí	
	QcLimitValue		No	
	QcPDS	*{https://pki.reniec.gob.pe/repositorio/,es}*	Sí	

3.2.3. Cifrado en Hardware

Perfil de Certificado Class 2 CIF ALTO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-RENIEC CA Class 2	Sí	-
	O	Registro Nacional de Identificación y Estado Civil		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	

Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	dataEncipherment	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.2*	Sí	
	explicitText	*Política de Certificado NCP+ con QSCD de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	:			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

3.3. Class 3

La Class 3 se encuentra reservada para emitir certificados a personas físicas (suscriptor), en su calidad de trabajadores de las Entidades Públicas. El titular de los certificados digitales Class 3, será el representante legal de la Entidad o la persona que se designe como tal.

3.3.1. Autenticación en Software

Perfil de Certificado Class 3 AUT MEDIO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha512WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 3	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	O	*<Nombre de la Entidad del suscriptor>*	Sí	
	OU	*<RUC de la entidad>*	No	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OI	*NTRPE-<número de RUC de la Entidad del suscriptor>*	Sí	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.1*	Sí	
	explicitText	*Política de Certificado Normalizado*	Sí	

		NCP de acuerdo con ETSI EN 319411-1		
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	•			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	ClientAuth (1.3.6.1.5.5.7.3.2)	No	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

3.3.2. Autenticación en Hardware

Perfil de Certificado Class 3 AUT ALTO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha512WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 3	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	O	*<Nombre de la Entidad del*	Sí	

		suscriptor>		
	OU	*<RUC de la entidad>*	No	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OI	*NTRPE-<número de RUC de la Entidad del suscriptor>*	Sí	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.2*	Sí	
	explicitText	*Política de Certificado NCP+ con QSCD de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	•			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	ClientAuth (1.3.6.1.5.5.7.3.2)	No	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No

Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

3.3.3. Firma en Software

Perfil de Certificado Class 3 FIR MEDIO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 3	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	O	*<Nombre de la Entidad del suscriptor>*	Sí	
	OU	*<RUC de la entidad>*	No	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OI	*NTRPE-<número de RUC de la Entidad del suscriptor>*	Sí	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No

Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	nonRepudiation	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.1*	Sí	
	explicitText	*Política de Certificado Normalizado NCP de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-
Qualified Certificate Statements	QcRetentionPeriod	*10*	Sí	
	QcLimitValue		No	
	QcPDS	*{https://pki.reniec.gob.pe/repositorio/,es}*	Sí	

3.3.4. Firma en Hardware

Perfil de Certificado Class 3 FIR ALTO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 3	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	O	*<Nombre de la Entidad del suscriptor>*	Sí	
	OU	*<RUC de la entidad>*	No	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OI	*NTRPE-<número de RUC de la Entidad del suscriptor>*	Sí	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	nonRepudiation	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No

	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.2*	Sí	
	explicitText	*Política de Certificado NCP+ con QSCD de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-
Qualified Certificate Statements	QcRetentionPeriod	*10*	Sí	
	QcLimitValue		No	
	QcPDS	*{https://pki.reniec.gob.pe/repositorio/,es}*	Sí	

3.3.5. Firma y autenticación en Software

Perfil de Certificado Class 3 FAU MEDIO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-

Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 3	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	O	*<Nombre de la Entidad del suscriptor>*	Sí	
	OU	*<RUC de la entidad>*	No	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OI	*NTRPE-<número de RUC de la Entidad del suscriptor>*	Sí	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature, nonRepudiation	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.1*	Sí	
	explicitText	*Política de Certificado Normalizado NCP de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		

	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	No	No
	-	ClientAuth (1.3.6.1.5.5.7.3.2)	No	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-
Qualified Certificate Statements	QcRetentionPeriod	*10*	Sí	
	QcLimitValue		No	
	QcPDS	*{https://pki.reniec.gob.pe/repositorio/,es}*	Sí	

3.3.6. Firma y autenticación en Hardware

Perfil de Certificado Class 3 FAU ALTO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 3	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	

Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	O	*<Nombre de la Entidad del suscriptor>*	Sí	
	OU	*<RUC de la entidad>*	No	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OI	*NTRPE-<número de RUC de la Entidad del suscriptor>*	Sí	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature, nonRepudiation	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.2*	Sí	
	explicitText	*Política de Certificado NCP+ con QSCD de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-

Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	No	No
	-	ClientAuth (1.3.6.1.5.5.7.3.2)	No	No
	-	SmartcardLogon (1.3.6.1.4.1.311.20.2.2)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-
Qualified Certificate Statements	QcRetentionPeriod	*10*	Sí	
	QcLimitValue		No	
	QcPDS	*{https://pki.reniec.gob.pe/repositorio/,es}*	Sí	

3.3.7. Cifrado nivel en Software

Perfil de Certificado Class 3 CIF MEDIO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	SÍ	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 3	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	O	*<Nombre de la Entidad del suscriptor>*	Sí	
	OU	*<RUC de la entidad>*	No	
	ST	*<Provincia-Departamento>*	Sí	

	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OI	*NTRPE-<número de RUC de la Entidad del suscriptor>*	Sí	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	dataEncipherment	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.1*	Sí	
	explicitText	*Política de Certificado Normalizado NCP de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No

Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

3.3.8. Cifrado en Hardware

Perfil de Certificado Class 3 CIF ALTO				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 3	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<CN del suscriptor>*	Sí	-
	SN	*<Apellidos>*	Sí	
	GIVENNAME	*<Nombres>*	Sí	
	O	*<Nombre de la Entidad del suscriptor>*	Sí	
	OU	*<RUC de la entidad>*	No	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*PNOPE-<número de DNI>*	No	
	OI	*NTRPE-<número de RUC de la Entidad del suscriptor>*	Sí	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key*	Sí	No

Identifier		*Info del emisor>*		
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	dataEncipherment	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*0.4.0.2042.1.2*	Sí	
	explicitText	*Política de Certificado NCP+ con QSCD de acuerdo con ETSI EN 319411-1*	Sí	
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	rfc822Name	*<email del suscriptor>*	No	No
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	EmailProtection (1.3.6.1.5.5.7.3.4)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

3.4. Class 4

La Class 4 se encuentra reservada para emitir certificados a sistemas de información (equipos, servidores, dominios) de las Entidades Públicas. El titular de los certificados digitales de Class 4, será el representante legal de la Entidad Pública o la persona que se designe como tal.

3.4.1. Agente Automatizado

Perfil de Certificado Class 4 AA

Nombre	Atributo	Valor	Obligatorio	Crítica
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 4	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<Nombre del Agente Automatizado>*	Sí	-
	O	*<Nombre de la Entidad>*	Sí	
	OU	*<RUC de la entidad>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	OI	*NTRPE-<número de RUC de la Entidad>*	Sí	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	nonRepudiation	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		

	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	-	-	-	-
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	-	-	-
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

3.4.2. Controlador de Dominio

Perfil de Certificado Class 4 DC				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 4	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad emisora del certificado>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<Nombre del servidor Active Directory>*	Sí	-

	O	*<Nombre de la Entidad>*	Sí	
	OU	-	-	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	OI	*NTRPE-<número de RUC de la Entidad>*	Sí	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature, keyEncipherment	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	⋮			
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject Alternative Name	dNSName	*<Nombre DNS principal>*	Sí	No
	otherName	*<MS GUID = Globally Unique Identifier del Servidor Active Directory>*	Sí	
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	ServerAuth (1.3.6.1.5.5.7.3.1)	Sí	No
	-	ClientAuth (1.3.6.1.5.5.7.3.2)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No

Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

3.4.3. SSL/TLS

Perfil de Certificado Class 4 SSL/TLS				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Campos				
Version	-	3	Sí	-
Serial Number	-	*<Número entero, mayor a cero (0) y aleatorio de al menos 8 bytes y máximo 20 bytes>*	Sí	-
Signature	algorithm	Sha256WithRSAEncryption	Sí	-
Issuer	CN	ECEP-<Siglas de la Entidad> CA Class 4	Sí	-
	O	*<Nombre de la Entidad>*		
	C	PE		
	OI	NTRPE-<número de RUC de la Entidad>	Sí	
Validity	(Not After - Not Before)	1 año	Sí	-
Subject	CN	*<DNS, nombre FQDN o número de IP>*	Sí	-
	O	*<Nombre de la Entidad>*	Sí	
	ST	*<Provincia-Departamento>*	Sí	
	L	*<Distrito>*	Sí	
	C	PE	Sí	
	SERIALNUMBER	*<RUC de la Entidad>*	Sí	
	OI	*NTRPE-<número de RUC de la Entidad>*	Sí	
	OU	*EREP_{PJ/PN}_<siglas de la Entidad>_<código identificador de la transacción>*	No	
Subject Public Key Info	algorithm	RSA	Sí	-
	KeyLength	2048 bits		
Extensiones				
Authority Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>*	Sí	No
Subject Key Identifier	-	*<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info>*	Sí	No
Key Usage	-	digitalSignature, keyEncipherment	Sí	Sí
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.35300.2.1.3.1.0.101.1000.0	Sí	No
	cPSuri	https://pki.reniec.gob.pe/repositorio/		
	explicitText	Política General de Certificación		
	policyIdentifier (OID)	*<OID "1">*	No	No
	cPSuri	*<URI "1">*		
	explicitText	*<Texto explicativo "1">*		
	policyIdentifier (OID)	*<OID "n">*		
	cPSuri	*<URI "n">*		
	explicitText	*<Texto explicativo "n">*		
Subject	dNSName	*<Nombre DNS principal>*	Sí	No

Alternative Name	dNSName	*<Nombre DNS adicional>*	No	
Basic Constraints	cA	FALSE	Sí	Sí
	Path Length Constraint	-	-	-
Extended Key Usage	-	ServerAuth (1.3.6.1.5.5.7.3.1)	Sí	No
	-	ClientAuth (1.3.6.1.5.5.7.3.2)	No	No
CRL Distribution Points	DistributionPointName (URI)	*<URL de la CRL firmada por el emisor>*	Sí	No
Authority Information Access	cAIssuers	*<URL de ubicación del certificado digital del emisor>*	Sí	No
	ocsp (URI)	*<URL de servicio OCSP implementado por el emisor>*	Sí	No
Subject Information Access	timeStamping (URI)	-	-	-
OCSP no check	-	-	-	-

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 sus modificatorias.
- 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).