RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

ENTIDAD DE CERTIFICACIÓN NACIONAL PARA EL ESTADO PERUANO
ECERNEP

Versión: 4.0	**Año: 2019**

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

Historial de Cambios				
Ver.	Fecha	Descripción	Responsable	Estado
1.0	04/12/2017	Elaboración y Aprobación	GRCD-SGREGD	Aprobado
2.0	29/10/2018	Actualización	GRCD-SGREGD	Aprobado
3.0	05/04/2019	Actualización	GRCD-SGREGD	Aprobado
4.0	17/07/2019	Actualización	GRCD-SGREGD	Aprobado

ÍNDICE

1. INTRODUCCIÓN

1.1. Visión general

El presente documento denominado Declaración de Prácticas de Certificación (en adelante CPS) establece de qué manera la ECERNEP implementa los procedimientos y controles para cumplir con los requerimientos establecidos en la Política General de Certificación Versión 3.0 (en adelante CP) en lo correspondiente a la jerarquía PKI denominada "ECERNEP PERU CA Root 3".

En tanto la ECERNEP, entidad a cargo de gestionar los certificados raíz de las jerarquías PKI del Estado Peruano, emite a su vez los certificados digitales a los prestadores de servicios de certificación, se incluyen también aquí los procedimientos y controles de registro correspondientes a la atención de sus solicitudes.

1.2. Nombre e identificación del documento

- **Nombre:** Declaración de Prácticas de Certificación de la ECERNEP PERÚ
- **Versión:** 4.0
- **OID:** 1.3.6.1.4.1.35300.2.1.3.1.0.102.1000
- **Website:** http://www.reniec.gob.pe/repository/
- **Fecha de elaboración:** 03/05/2017
- **Fecha de última modificación:** 17/07/2019
- **Lugar:** Lima, Peru

1.3. Participantes

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

La ECERNEP es la encargada de administrar el certificado digital raíz denominado "ECERNEP PERU CA Root 3". Asimismo, tiene como función emitir y cancelar los certificados digitales destinados a los prestadores de servicios de certificación acreditados o en proceso de acreditación bajo el marco de la Infraestructura Oficial de Firma Electrónica (en adelante IOFE) como entidades subordinadas o de nivel subsiguiente a la ECERNEP. 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. Asimismo, la ECERNEP administra el certificado digital denominado EC-PSVA, que ha sido emitido subordinado al mencionado certificado raíz de la ECERNEP y que es utilizado para emitir certificados digitales para los PSVA para el Estado Peruano en la modalidad de Autoridad de Sellado de Tiempo (TSA). En el siguiente diagrama se presenta una representación gráfica de lo mencionado.

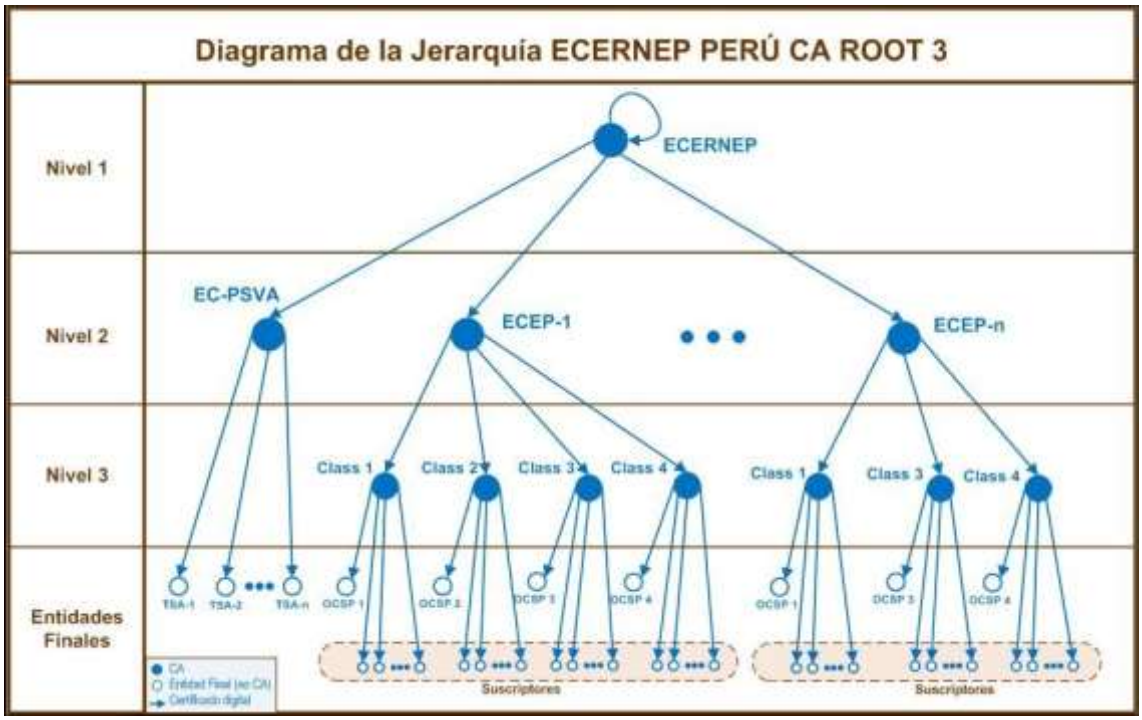

Figura 1. Diagrama de la jerarquía ECERNEP PERÚ CA Root 3

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

Las ECEP son Entidades de Certificación subordinadas a la ECERNEP que han sido acreditadas por la AAC y tienen como función principal gestionar el ciclo de vida de los certificados digitales de Entidades Finales.

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

La función principal de una EREP es la verificación de la identidad de los solicitantes que realizan solicitudes de emisión y cancelación (o cualquier otro servicio que brinde la ECEP asociada) de certificados digitales. La EREP debe realizar el levantamiento de datos y la comprobación de la información brindada por el solicitante. Asimismo, debe aprobar o rechazar la emisión, reemisión o cancelación de certificados digitales, comunicando a la respectiva Entidad de Certificación con la que se encuentra asociada, de acuerdo a lo estipulado en su correspondiente Declaración de Prácticas de Registro.

La ECERNEP emite los certificados digitales por medio de procedimientos de registro administrados por ella misma; no se encuentra asociada a una EREP.

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).

1.3.5. Titulares y suscriptores

Los titulares y a su vez suscriptores de los certificados emitidos por la ECERNEP son las ECEP y los PSVA-TSA (en adelante los Subordinados).

1.3.6. Terceros que confían

Los terceros que confían son las 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 en los mensajes cifrados correspondientes.

1.3.7. Otros participantes

Se considera como otro participante bajo el ámbito de la presente CPS a la AAC.

1.4. Uso de un certificado digital

1.4.1. Usos apropiados de los certificados digitales

El certificado digital raíz de la ECERNEP es utilizado para:

- La emisión de certificados digitales de Nivel 2 para los prestadores de servicios de certificación del Estado Peruano acreditados o en proceso de acreditación.
- Firmar la Lista de Certificados Cancelados (CRL) donde se encuentran los certificados cancelados de Nivel 2, tal como se indica en el numeral **4.9.7, Frecuencia de publicación de la Lista de Certificados Cancelados (CRL).**
- Emitir el certificado digital denominado “EC-PSVA”.

El certificado digital denominado “EC-PSVA” es utilizado para:

- Emitir certificados digitales para los prestadores de servicios de certificación como PSVA en la modalidad de Autoridad de Sellado de Tiempo (TSA) acreditados o en proceso de acreditación.
- Firmar la Lista de Certificados Cancelados (CRL) donde se encuentran los certificados cancelados de PSVA en la modalidad de TSA, tal como se indica en el numeral **4.9.7, Frecuencia de publicación de la Lista de Certificados Cancelados (CRL)**.

1.4.2. Usos prohibidos del certificado

Los certificados digitales administrados por la ECERNEP no son utilizados en situaciones diferentes a las descritas en el numeral **1.4.1, Usos apropiados de los certificados digitales**.

1.5. Administración de la CPS

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:** 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 de la CPS

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

1.5.4. Procedimiento de aprobación de la CPS

La presente CPS se propone a la AAC a quien corresponde aprobarla 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

2.1. Repositorio

La ECERNEP gestiona repositorios con la siguiente información:

- Directorio de certificados digitales emitidos
- Listas de certificados cancelados
- Política General de Certificación y Política de Prestador de Servicios de Valor Añadido para servicio de sellado de tiempo
- Declaraciones de Prácticas de Certificación
- Políticas de Privacidad
- Políticas de Seguridad
- Los instrumentos legales vinculantes con los PSC subordinados.

Los instrumentos legales vinculantes deben ser fácilmente identificables para cada certificado[1].

2.2. Publicación de información de certificación

La ECERNEP actualiza la información de sus repositorios en función a la frecuencia establecida en el numeral **2.3 Frecuencia de publicación**. Asimismo, los mantiene disponibles de forma pública en la Web en la dirección http://www.reniec.gob.pe/repository/ las veinticuatro (24) horas del día y los siete (07) días de la semana.

Los certificados digitales emitidos por la ECERNEP a los PSC se listan en el directorio de certificados digitales emitidos contando con el consentimiento de su suscriptor y de su titular. La AAC publica los certificados digitales de los PSC acreditados o en proceso de acreditación en el Registro Oficial de Prestadores de Servicio de Certificación Digital (ROPS), encontrándose disponibles para su descarga o recuperación.

2.3. Frecuencia de publicación

La ECERNEP gestiona y mantiene actualizado el repositorio 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: Actualizado cada vez que se cancela un certificado digital o con la emisión de una nueva CRL, según lo indicado en el numeral **4.9.7 Frecuencia de publicación de la Lista de Certificados Cancelados (CRL)**, del presente documento.
- Política General de Certificación (CP): Actualizado cada vez que la AAC aprueba una nueva versión de la misma.
- Declaración de Prácticas de Certificación (CPS): Actualizado cada vez que la AAC aprueba una nueva versión.
- Políticas de Privacidad: Actualizado cada vez que la AAC aprueba una nueva versión.
- Políticas de Seguridad: Actualizado cada vez que la AAC aprueba una nueva versión

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

2.4. Control de acceso al Repositorio

La ECERNEP no limita el acceso de lectura a la información de su repositorio, pero garantiza la existencia de controles físicos y lógicos para impedir que de forma no autorizada se puedan añadir, modificar o borrar registros, de modo tal que:

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

El repositorio de la ECERNEP es administrado y publicado por la propia organización.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Convención de nombres

3.1.1. Tipos de nombres

La estructura *DistinguishedName* (ITU-T X .501) en los campos *IssuerDN* y *SubjectDN* es utilizada por la ECERNEP para identificar de forma única y plena a los emisores, los titulares, y/o suscritores de los certificados digitales.

3.1.2. Necesidad de nombres significativos

El campo *SubjectDN* de los certificados digitales emitidos por la ECERNEP es significativo en la medida que registra el nombre oficial de los PSC, lo cual permite determinar sin ambigüedad la identidad de la organización que lo administra.

3.1.3. Anonimato o seudónimo de los suscriptores

La ECERNEP no emite ningún certificado digital anónimo ni con el uso de seudónimos.

3.1.4. Reglas de interpretación de diferentes modalidades de nombres

El certificado digital raíz de la ECERNEP utiliza el siguiente *SubjectDN*:

	Atributos	Valor
Subject Distinguished Name	**CN**	ECERNEP PERU CA ROOT 3
	SN	--
	GIVENNAME	--
	O	Entidad de Certificación Nacional para el Estado Peruano
	OU	--
	ST	--
	L	--
	C	PE
	SERIALNUMBER	--
SubjectAltName		- -

Tabla 1 – Valor de los campos del *SubjectDN* del certificado digital ECERNEP PERU CA Root 3

El certificado digital de Nivel 2 utilizado por la ECERNEP para la emisión de certificados de PSVA tiene el siguiente *SubjectDN*:

	Atributo	Valor
Subject Distinguished Name	**CN**	EC-PSVA
	SN	--
	GIVENNAME	--
	O	Entidad de Certificación Nacional para el Estado Peruano
	OU	--
	ST	--
	L	--
	C	PE
	OI	*NTRPE-<número de RUC de la Entidad>*
	SERIALNUMBER	--
SubjectAltName		--

Tabla 2 – Valor de los campos del *SubjectDN* del certificado digital de la EC-PSVA

Para la emisión de certificados digitales de una ECEP de Nivel 2 se utiliza el siguiente *SubjectDN*:

	Atributo	Valor
Subject Distinguished Name	**CN**	ECEP-*<Siglas de la Entidad>*
	SN	--
	GIVENNAME	--
	O	*<Nombre de la Entidad>*
	OU	--
	ST	--
	L	--
	C	PE
	OI	*NTRPE-<número de RUC de la Entidad>*
	SERIALNUMBER	--
SubjectAltName		--

Tabla 3 – Valor de los campos del *SubjectDN* del certificado digital emitido a una ECEP

Para la emisión de certificados digitales de una PSVA en modalidad de Autoridad de Sellado de Tiempo se utiliza el siguiente *SubjectDN*:

	Campo	Valor
Subject Distinguished Name	**CN**	PSVA-TSA-*<Siglas de la Entidad>*
	SN	--
	GIVENNAME	--
	O	*<Nombre de la Entidad>*
	OU	--
	ST	--
	L	--
	C	PE
	OI	*NTRPE-<número de RUC de la Entidad>*
	SERIALNUMBER	--
SubjectAltName		--

Tabla 4: Valor de los campos del *SubjectDN* del certificado digital emitido a una PSVA-TSA

3.1.5. Unicidad de Nombres

La ECERNEP garantiza que el *SubjectDN* de los certificados digitales que emite es único no sólo durante el periodo de vigencia del certificado, sino durante la entera existencia de la jerarquía de certificación digital.

3.1.6. Reconocimiento, autenticación y rol de las marcas registradas

No aplica.

3.2. Validación inicial de la identidad

3.2.1. Método para probar la posesión de la llave privada

La ECERNEP genera y administra sus propias llaves, según se indica en el numeral **6.1.1 Generación del par de llaves.**

Las entidades que soliciten un certificado para ECEP o PSVA, deben generar sus propias llaves y demostrar la posesión de su llave privada mediante el envío del *Certificate Signing Request* (CSR) en formato PKCS#10.

3.2.2. Autenticación de identidad de personas jurídicas

Las entidades solicitantes de la Administración Pública comprendidas en el Artículo I, del Título Preliminar de la Ley 27444 – Ley del Procedimiento Administrativo General, que requieran certificados digitales directamente subordinados a la ECERNEP deberán presentar una solicitud firmada por el titular o máximo reperesentante de la Entidad

adjuntando como requisitos los correspondientes[2].según sea el caso de una ECEP o un PSVA-TSA.

[2] PSC Acreditadas: la Resolución de Acreditación emitida por la AAC.
PSC en proceso de Acreditación: el Informe o Acta de evaluación favorable emitido por el Comité Evaluador como parte del procedimiento de acreditación seguido frente a la AAC de la IOFE.

3.2.3. Autenticación de identidad de personas naturales

No aplica.

3.2.4. Información no verificada del suscriptor

Ningún dato o información que no hayan sido verificados se incluirá en los certificados digitales emitidos por la ECERNEP.

3.2.5. Validación de autoridad para efectuar la solicitud

La ECERNEP valida el derecho que posee el solicitante de un certificado digital subordinado verificando la identidad y los poderes de representación correspondientes, así como la Resolución de acreditación o el Informe o Acta de Evaluación favorable emitido por el Comité Evaluador, según sea el caso, como parte del procedimiento de acreditación seguido frente a la AAC de la IOFE.

3.2.6. Criterios de interoperabilidad

La ECERNEP opera independientemente de otras PKI fuera del marco de la IOFE; sin embargo, garantiza la interoperabilidad con otras 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 de la Ley 27269 – Ley de Firmas y Certificados Digitales.

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

Este servicio no es brindado por la ECERNEP.

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 verifica y procesa las solicitudes de cancelación de los certificados digitales de los PSC directamente subordinados a ella.

4. CICLO DE VIDA DEL CERTIFICADO DIGITAL: REQUISITOS OPERACIONALES

4.1. Solicitud de certificado digital

4.1.1. Personas habilitadas para presentar una solicitud de certificado

La ECERNEP acepta únicamente solicitudes de emisión de certificados digitales a través del titular o máximo representante de la Entidad solicitante.

4.1.2. Proceso de registro de solicitud y responsabilidades

La ECERNEP recibe del solicitante:

- PSC en Proceso de Acreditación, el Informe o Acta de Evaluación favorable emitido por el Comité Evaluador como parte del procedimiento de acreditación seguido frente a la AAC de la IOFE.
- PSC acreditada, la Resolución de Acreditación emitida por la AAC.
- Evidencia de haber realizado una ceremonia de llaves para generar su par de llaves, incluyendo testimonio de asistentes, según lo indicado en el numeral **6.1.1 Generación del par de llaves**.
- Solicitud de emisión de certificado debidamente firmada por el titular o máximo representante de la Entidad. La entidad solicitante debe proveer los documentos que acrediten su constitución y las facultades del representante legal.
- En lo concerniente al aspecto técnico, se recibirá una solicitud compatible con el formato PKCS#10.

La ECERNEP informa a las entidades solicitantes sobre los términos de uso y las obligaciones que posee como titular y suscriptor.

4.2. Procesamiento de la solicitud del certificado

4.2.1. Identificación y autenticación

La ECERNEP realiza la identificación y autenticación de la entidad solicitante y de su representante legal, en concordancia con el tipo de certificado digital y con lo establecido en el numeral **3.2.2 Autenticación de identidad de personas jurídicas**, del presente documento.

4.2.2. Aprobación o rechazo de las solicitudes de certificados

La ECERNEP rechaza las solicitudes en los siguientes casos:

- Si las entidades solicitantes no presentan la Resolución de Acreditación, de encontrarse ya acreditadas, o el Informe o Acta de Evaluación favorable emitido por el Comité Evaluador como parte del procedimiento de acreditación que se encuentren siguiendo frente a la AAC de la IOFE.
- Si el resultado de la verificación de la identidad del representante legal fue negativo.
- Si el representante legal o su apoderado no cuentan con poder vigente o si no tienen plena capacidad de ejercicio de sus derechos civiles.

- Si la solicitud no es compatible con el formato PKCS#10, o los datos consignados no son correctos.

La ECERNEP comunica vía correo electrónico a la entidad solicitante sobre la aprobación de la solicitud para la emisión del certificado digital respectivo, requiriéndose la firma de un contrato de conformidad de responsabilidades por parte del representante legal del solicitante.

El contrato antes aludido contiene las obligaciones que debe cumplir la entidad solicitante en conformidad con la legislación vigente para garantizar el efecto legal de las transacciones realizadas empleando el certificado emitido por la ECERNEP. Entre estas obligaciones se tiene las siguientes:

- Emplear su certificado digital, según sea el caso:
  - ECEP: Emplear su certificado digital de Nivel 2 (ECEP *offline*) únicamente para emitir certificados de Nivel 3 (ECEP *online*) y emplear estos últimos para emitir únicamente certificados digitales de Entidad Final.
  - PSVA: En el caso de una TSA, emplear su certificado digital únicamente para generar sellos de tiempo.
- Ser diligente en la custodia de su llave privada, con el fin de evitar usos no autorizados.
- Notificar, sin retrasos injustificables, al Sub Gerente de Regulación Digital del RENIEC, persona de contacto de la ECERNEP conforme se señala en el numeral **1.5.2 Persona de contacto**, para que se proceda a la cancelación del certificado digital indicado, en los siguientes casos:
  - Pérdida, robo o extravío del módulo criptográfico que almacena su llave privada.
  - Compromiso potencial de su llave privada.
  - Pérdida de control sobre su llave privada, debido al compromiso de los datos de activación o por cualquier otra causa.
  - Ante 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 inversa 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, la ECERNEP proporciona la siguiente información incorporándola como parte del contrato:

- Referencia o enlace WEB a la Política General de Certificación Digital (CP) y a la Declaración de Prácticas de Certificación (CPS) de la ECERNEP aplicables, aprobadas por la AAC.
- Políticas de uso del certificado digital, limitaciones y prohibiciones.
- Las responsabilidades del titular frente a la actualización de sus datos, cancelación del certificado en caso que la llave privada se vea comprometida y la emisión de un nuevo certificado antes de la expiración del certificado actual.

- Información sobre cómo validar el certificado, incluyendo el requisito de comprobar el estado del mismo.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la ECERNEP acepta o excluye su responsabilidad.
- Ley aplicable y jurisdicción competente.

La firma del contrato puede realizarse de manera digital, si fuera el caso en que el representante legal del PSC posea un certificado digital de firma emitido dentro del marco de la IOFE, vigente y válido.

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

La ECERNEP procesa las solicitudes de emisión de certificados digitales dentro de un plazo máximo establecido en la Guia de Procedimiento " Emisión de Certificado Digital para Prestador de Servicios de Certificación" y en observancia de lo dispuesto en la Guía de Acreditación de Entidades de Certificación EC en su versión vigente, en la Política General de Certificación y en documentos mandatorios.

4.3. Emisión del certificado

4.3.1. Acciones durante la emisión del certificado

La ECERNEP emitirá un certificado digital siempre que reciba 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**, para lo cual se asegura 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

La ECERNEP notifica por correo electrónico al solicitante sobre la emisión y entrega del certificado digital. La entrega del certificado se realiza a través del envío del certificado a la persona jurídica que asume las facultades de su titular y suscriptor, acompañado para tales efectos de una declaración de emisión exitosa.

4.4. Aceptación del certificado

4.4.1. Conducta constitutiva de aceptación del certificado

Los PSC solicitantes aceptan un certificado digital de manera tácita mediante el empleo del certificado y de forma expresa a la firma del contrato respectivo.

4.4.2. Publicación del certificado por parte de la ECERNEP

Cada vez que la ECERNEP emite un certificado digital, se actualiza el repositorio correspondiente. Mayor información sobre la operatividad de los repositorios se encuentra en los numerales **2.1 Repositorio**, **2.2 Publicación de información de**

certificación, **2.3 Frecuencia de publicación** y **2.4 Control de acceso al Repositorio** del presente documento.

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

La ECERNEP no informa a terceros sobre la emisión de un certificado digital, lo que hace es actualizar el repositorio correspondiente a fin de que los interesados puedan tomar conocimiento del hecho.

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 solicitante haya aceptado los términos, el contrato, las condiciones y las políticas de la ECERNEP.

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 los certificados para realizar únicamente las validaciones indicadas 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 de certificados emitidos de acuerdo con el consentimiento de los suscriptores y titulares, como se expone en el numeral **2.1, Repositorio**, del presente documento.

El tercero que confía está obligado a:

- No monitorear, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de la Jerarquía ECERNEP PERÚ CA Root 3, sin autorización por escrito de la ECERNEP.
- No comprometer intencionadamente la seguridad de la Jerarquía ECERNEP PERÚ CA Root 3.
- 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 ECERNEP deba revocar el certificado de un PSC, siempre y cuando se tengan pruebas fehacientes del compromiso de la llave privada o de su uso ilegal. Dicha denuncia podrá realizarla directamente la persona de contacto, señalada en el numeral **1.5.2 Persona de contacto** del presente documento, pudiendo dirigirse formalmente o a través del correo electrónico ahí señalado.
- Solicitar a la ECERNEP para que se proceda a la cancelación del certificado digital en los siguientes casos:
  - ✓ Pérdida, robo o extravío del módulo criptográfico que almacena su llave privada.

- ✓ Compromiso potencial de su llave privada.
- ✓ Pérdida de control sobre su llave privada, debido al compromiso de los datos de activación o por cualquier otra causa.
- ✓ Ante inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

4.6. Renovación del certificado

La ECERNEP no brinda este servicio.

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

La ECERNEP no brinda este servicio.

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

La ECERNEP no brinda este servicio.

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 de certificados digitales

4.9.1. Motivos de cancelación

La ECERNEP cancelará un certificado digital por alguno de los siguientes motivos:

- 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.
- Cuando la información contenida en el certificado digital ya no resulte correcta.
- Pérdida, robo o extravío del módulo criptográfico que almacena su llave privada.
- Pérdida de control sobre su llave privada, debido al compromiso de los datos de activación o por cualquier otra causa.
- Ante inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

La revocación supone la cancelación de oficio de los certificados por parte de la ECERNEP. En este caso, las circunstancias bajo las cuales una ECERNEP puede revocar los certificados son:

- Cuando el PSC en proceso de acreditación, transcurrido el plazo que deberá establecer la ECERNEP, no ha cumplido con presentar la Resolución de Acreditación emitida por la AAC.
- Cuando el PSC titular de un certificado digital subordinado ha incumplido las obligaciones a las que se encuentra comprometido.
- Cuando se tenga evidencia de cualquiera de los motivos de cancelación expuestos líneas arriba.

4.9.2. Personas habilitadas para solicitar la cancelación de un certificado

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

- El representante legal de la entidad que solicitó el certificado.
- Un tercero que tenga 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.
- El juez a través de una resolución judicial o la autoridad administrativa competente a través de una resolución administrativa.

4.9.3. Procesamiento de la solicitud de cancelación de un certificado

Cuando la ECERNEP recibe una solicitud para la cancelación de un certificado, deja constancia de que la persona que efectúa la solicitud cumple con los requisitos solicitados en el numeral **4.9.2, Personas habilitadas para solicitar la cancelación de un certificado**, realiza la verificación de la identidad del solicitante y registra la fecha y hora de la cancelación. Todo lo anterior, se evidencia en un documento de aceptación de solicitud de cancelación firmado por el Sub Gerente de Regulación Digital del RENIEC en representantación de la ECERNEP.

Asimismo, en caso no se acepte la cancelación, se deja constancia de los hechos que motivaron dicha denegación mediante documento firmado por el Sub Gerente de Regulación Digital del RENIEC en representación de la ECERNEP.

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

La ECERNEP realiza la cancelación sin ser necesaria una confirmación del solicitante.

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

La solicitud de cancelación es procesada dentro de las 24 horas siguientes a la recepción de la solicitud por la ECERNEP, salvo aquellos casos en que se trate de una cancelación de oficio por parte de la ECERNEP, lo que supone revocar los certificados por los motivos

expuestos en los puntos 4 y 5 del numeral **4.9.1, Motivos de cancelación**, los que deberán considerarse como procedimiento de "evaluación previa" con "silencio negativo"[3]

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

Una vez realizada la cancelación de un certificado digital, la ECERNEP registra la cancelación en la CRL respectiva permitiendo, de esta manera, que todos los interesados puedan verificar el estado del certificado.

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

La ECERNEP emite la CRL donde se listan los certificados cancelados de Nivel 2 con una frecuencia de publicación de un (01) año (incluso si ningún certificado ha sido cancelado) o, ante la ocurrencia de una cancelación, dentro del periodo máximo de latencia establecido en 24 horas en el numeral **4.9.8 Periodo máximo de latencia para las** CRL.

Asimismo, la ECERNEP gestiona la CRL donde se listan los certificados cancelados de tipo PSVA que fuesen firmados por su certificado EC-PSVA, la que se actualiza con una frecuencia de seis (06) meses o, ante la ocurrencia de una cancelación, dentro del periodo máximo de latencia establecido 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 de las CRLs administradas por la ECERNEP se presenta en la siguiente tabla:

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

Tabla 5 - Niveles de CRL y máxima latencia

4.9.9. Disponibilidad del servicio online (en línea) para la verificación del estado de certificados

La ECERNEP no brinda el servicio OCSP de verificación en línea del estado de certificados.

4.9.10. Necesidad de verificación del estado del certificado mediante OCSP

No aplica.

[3] Ley Nº 27444, Ley de Procedimiento Administrativo General, Art. 30° Calificación de procedimientos administrativos.

4.9.11. Otras formas de publicar la cancelación

No aplica.

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

De darse el caso, la ECERNEP notificará, a la AAC, en un plazo máximo de 24 horas, el compromiso de las llaves que administra o su imposibilidad de uso. Además, en este caso realiza la cancelación de todos los certificados de la jerarquía según lo indicado en el numeral **5.7.3 Procedimiento en caso de compromiso de llave privada**.

4.9.13. Circunstancias para una suspensión

No aplica

4.9.14. Personas habilitadas para solicitar una suspensión

No aplica

4.9.15. Procedimiento para solicitar una suspensión

No aplica

4.9.16. Límite del periodo de suspensión

No aplica

4.10. Servicios de monitoreo de estado del certificado

4.10.1. Características operacionales

La ECERNEP brinda, de forma irrestricta, el servicio de verificación del estado de los certificados mediante la publicación de la Lista de Certificados Cancelados (CRL), la cual es firmada digitalmente y cuenta con registro de hora y fecha.

4.10.2. Disponibilidad del servicio

La ECERNEP brinda el servicio de 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 al servicio de certificación brindado por la ECERNEP se da por los siguientes motivos:

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

4.12. Custodia y recuperación de llaves

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

La ECERNEP almacena las llaves privadas que administra en módulos criptográficos que cumplen con las certificaciones indicadas en el numeral **6.2.11 Clasificación del módulo criptográfico**.

La ECERNEP no realiza almacenamiento del original, copia o *backup* de las llaves privadas de los certificados digitales de los PSC.

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

No aplica

5. CONTROLES DE LAS INSTALACIONES, DE GESTIÓN Y OPERACIONALES

La ECERNEP mantiene controles de seguridad físicos para impedir y prevenir el acceso a personas no autorizadas a sus instalaciones (área restringida y área operacional) mediante la aplicación de controles según los estándares NTP-ISO/IEC 27001 (ISO/IEC 27001) y NTP-ISO/IEC 17799 (ISO/IEC 27002) y conforme a la Política de Seguridad vigente.

5.1. Controles físicos

5.1.1. Ubicación y construcción del local

Las instalaciones de la ECERNEP cuentan con las siguientes características físicas:

- Perímetro cerrado con paredes de material noble, piso y techo de concreto y con puerta sólida. Las divisiones interiores, de tipo permanente, al igual que las puertas son de material aligerado.
- Medidas de prevención ante desastres naturales (inundación, terremoto, entre otros) y ante desastres accidentales creados por el hombre (incendios, explosiones, disturbios civiles).
- Área restringida con activos críticos protegida con acceso biométrico de dos personas, sin ventanas y con puerta sólida cortafuegos blindada.

Estas instalaciones se encuentran ubicadas en una edificación de concreto antisísmica en un piso mayor a ocho metros sobre el nivel del suelo.

5.1.2. Acceso físico

Las instalaciones de la ECERNEP se encuentran protegidas a través de procedimientos que permiten el ingreso solamente a personal autorizado contándose con controles de acceso ya sea a través de personal de seguridad o verificación biométrica y video vigilancia las 24 horas del día, los 7 días de la semana (24x7). Además, se dispone de verificación biométrica doble (dos personas) en sus áreas restringidas para la protección de activos críticos.

En las áreas restringidas, solo se permite el ingreso a personal ajeno a las instalaciones de la ECERNEP o visitas en casos de auditoría, soporte, mantenimiento o para su limpieza. El visitante pasa por un proceso de verificación de identidad mediante su documento oficial de identidad o fotocheck de la entidad a la que pertenece. Luego de la verificación de su identidad, ingresa escoltado y se registra la fecha, hora y motivo de la visita. Un visitante no puede ingresar solo bajo ninguna circunstancia.

5.1.3. Energía y aire acondicionado

El área restringida de la ECERNEP no cuenta con tomas de energía eléctrica y no requiere de aire acondicionado al no contar con equipos energizados que produzcan calor.

En caso se requiera activar o utilizar los componentes tecnológicos de la ECERNEP, estos son llevados a un área operacional con energía eléctrica, previa autorización. Las actividades realizadas se registran en un acta en la que firman todos los participantes.

5.1.4. Exposición al agua

El perímetro de las instalaciones de la ECERNEP es de material noble. En particular, el área restringida es de concreto y se encuentra protegida mediante piso a desnivel e impermeabilizantes para prevenir inundaciones y otros daños por exposición al agua.

5.1.5. Previsión y protección contra fuego

El área restringida de la ECERNEP cuenta con puerta sólida cortafuego blindada; además, el área operacional con detectores de humo y extintores.

5.1.6. Almacenamiento de material

Los activos críticos de la ECERNEP se almacenan dentro de una caja fuerte metálica, incluyendo:

- Los módulos criptográficos que contienen las llaves privadas de la ECERNEP y EC-PSVA.
- Las tarjetas inteligentes de activación de las claves privadas.
- Información crítica del sistema.

5.1.7. Eliminación de residuos

La información que se requiere eliminar contenida en formato papel, así como en soportes magnéticos u ópticos, es destruida tanto física como lógicamente a fin de reducir la posibilidad de recuperar dicha información desde los formatos que la contuvieron. La eliminación se realiza mediante un borrado seguro que minimiza la posibilidad de recuperación o restructuración de la información.

5.1.8. Copia de seguridad externa

Se dispone de copias externas de respaldo de la información crítica y sensible, incluyendo datos de auditoría.

5.2. Controles procedimentales

5.2.1. Roles de confianza

Los trabajadores designados para gestionar la plataforma de la ECERNEP son considerados como “personal de confianza”. Se designan de manera formal los roles correspondientes, incluyendo la descripción de sus funciones y responsabilidades mediante un contrato de trabajo o documento de gestión interna.

5.2.2. Número de personas requeridas por labor

Todas las tareas que se ejecuten con las llaves privadas de la ECERNEP requieren la presencia de, al menos, dos colaboradores.

5.2.3. Identificación y autenticación para cada rol

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

El control de acceso físico a las áreas restringidas de la ECERNEP está basado en el uso de biometría. El control de acceso lógico a los activos críticos está basado en el uso de tarjetas inteligentes.

5.2.4. Roles que requieren separación de funciones

Las actividades de la ECERNEP que requieren separación de funciones, sin que esto sea excluyente a otros casos, son:

- Generación, emisión o destrucción de llaves y certificados digitales.
- Acceso y gestión de los repositorios y bases de datos con información crítica.
- Auditoría interna.

En general, las personas que se encargan de la implementación de una función no tienen el rol de realización de la auditoría de conformidad, evaluación o revisión de dicha implementación.

5.3. Controles de personal

5.3.1. Requisitos de experiencia, capacidades y autorización

Los procedimientos dispuestos para la gestión del personal aseguran de manera suficiente su experiencia y capacidades, mediante la verificación curricular al momento de la contratación.

5.3.2. Procedimiento para verificación de antecedentes

Se verifica la documentación entregada por el personal aspirante, tomándose como referencia lo establecido en el Reglamento Interno de Trabajo del RENIEC. El área competente realiza las siguientes verificaciones:

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

5.3.3. Requisitos de capacitación

Se imparte una capacitación al inicio de funciones (inducción) y, al menos, una actualización anual, en los siguientes aspectos:

- Uso y operación del hardware y software de la ECERNEP.
- Aspectos relevantes de la Política General de Certificación, Declaración de Prácticas, Política de Seguridad, Plan de Privacidad, Política de Privacidad y otra documentación de la ECERNEP.
- 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.

Además, se imparten capacitaciones programadas sobre temas especializados, según se considere pertinente.

5.3.4. Requisitos y frecuencia de re-capacitación

Las capacitaciones especializadas se imparten al personal encargado cuando se realizan cambios significativos, por ejemplo, actualizaciones de hardware o software, cambio de los sistemas y/o procedimientos de seguridad.

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

5.3.5. Frecuencia y secuencia de rotación de las funciones

No aplica para la ECERNEP.

5.3.6. Sanciones por acciones no autorizadas

Se toman acciones administrativas y disciplinarias apropiadas contra el personal, independientemente de la modalidad de contratación, que ejecute acciones no autorizadas dentro de sus funciones o que viole las normas de seguridad, según lo establecido en el reglamento interno del RENIEC.

Se consideran acciones no autorizadas las que contravengan, de manera negligente o malintencionada a la Política General de Certificación de la ECERNEP, la Declaración de Prácticas de la ECERNEP, la Política de Seguridad y la Política de Privacidad, así como a los documentos normativos de alcance al personal de la entidad.

Por otro lado, la Ley N° 29622 “Ley que modifica la Ley N° 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.

En caso de una acción real o potencial no autorizada por parte una persona que desempeña un rol de confianza, dicha persona es inmediatamente removida de su rol y sometida a las sanciones correspondientes, según la gravedad y naturaleza de su accionar.

5.3.7. Requisitos para contratistas

En caso se estime conveniente el empleo de contratistas al interior de las instalaciones de la ECERNEP, éstos y sus empleados estarán 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 de la ECERNEP en cargos o roles similares. Los contratos especificarán las sanciones y reparaciones para las acciones llevadas a cabo por los contratistas y sus empleados.

5.3.8. Documentación suministrada al personal

La ECERNEP suministra al personal, de acuerdo a su cargo o rol, la documentación necesaria y suficiente para desempeñar sus funciones. Aquellos documentos confidenciales o con información crítica, son entregados considerando la clasificación de dicha información. Como mínimo, se suministra al personal, los siguientes documentos:

- Declaración de funciones y autorizaciones.
- Manuales para los equipos, hardware y software que deba operar.
- 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 situaciones de contingencia.

5.4. Procedimientos de registro de eventos

5.4.1. Tipos de eventos registrados

La ECERNEP mantiene un registro de auditoría de los siguientes eventos (incluyendo fecha y hora):

- Registro de eventos de los módulos criptográficos.
- Eventos relacionados con el ciclo de vida de sus certificados digitales.
- Modificaciones en la CP o CPS de la ECERNEP.
- Mantenimientos y cambios de configuración del sistema.
- Acceso físico al área restringida.
- Intentos de intrusión física a la infraestructura de la ECERNEP.
- Cambios en el personal.

5.4.2. Frecuencia de procesamiento del registro de eventos

Se realiza la revisión de registros de auditoría una vez al mes, como medida de prevención. Asimismo, los registros de auditoría son revisados ante la presencia de una alerta o incidente.

5.4.3. Periodo de conservación del registro de eventos

La conservación del registro de eventos es por un periodo mínimo de diez (10) años.

5.4.4. Protección del registro de eventos

Los registros de eventos, tanto físicos como electrónicos, son considerados activos de información por lo que se encuentran sujetos a controles físicos y lógicos, de manera que se previene el acceso no autorizado y se garantiza su conservación.

La destrucción de un archivo de eventos solo se realiza con la autorización de la AAC, siempre y cuando haya transcurrido un periodo mínimo de diez (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

La ECERNEP realiza copias mensuales de respaldo del registro de eventos, conforme lo especifica el documento “Copia de Respaldo de Información de la ECERNEP”. .

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

Las auditorías internas de la ECERNEP se llevan a cabo una vez cada tres (03) meses conforme al Plan Anual de Auditorías de la ECERNEP y las externas las realiza la AAC una vez al año o cuando así lo requiera conforme a los procedimientos establecidos en la *Guía de Acreditación de Entidades de Certificación EC.*

5.4.7. Notificación al causante del evento

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

En los casos en que se establece que el evento es de índole accidental y puede volver a ocurrir, se notifica formalmente al autor del evento (sujeto que causa el evento), para que tome las previsiones pertinentes.

5.4.8. Evaluación de la vulnerabilidad

La ECERNEP cuenta con módulos criptográficos HSM que cumplen con altos estándares de seguridad, tales como FIPS 140-2 nivel 3, los cuales han sido evaluados ante vulnerabilidades por los fabricantes. Es importante resaltar que ninguno de los equipos y

sistemas de la ECERNEP operan en modo online, lo que significa que ninguno de ellos está conectado a Internet.

5.5. Archivo

5.5.1. Tipos de información archivada

La ECERNEP gestiona el archivo de la siguiente información:

- Solicitudes, contratos y documentación de sustento presentada por los PSC, incluyendo información del titular del certificado digital o de su representante legal.
- CP y CPS
- Resolución de acreditación como ECERNEP ante la AAC.
- Modificación de cualquiera de los documentos anteriores
- Todos los certificados digitales emitidos (ECERNEP, EC-PSVA, PSVA-TSA y ECEP) cancelados o anulados
- Todas las CRL emitidas desde el inicio de sus operaciones
- Registros de eventos

5.5.2. Periodo de conservación del archivo

Los archivos, físicos y lógicos, son mantenidos como mínimo por un período de diez (10) años.

5.5.3. Protección del archivo

Los archivos son física y lógicamente protegidos y supervisados para evitar el empleo inadecuado, revelación o copia de información. Los archivos de mayor relevancia se guardan firmados digitalmente por la persona designada por el Oficial de Seguridad de Información. Los archivos físicos más importantes, como documentos de ceremonias de llaves y procedimientos confidenciales, se resguardan en una caja fuerte con llave física y contraseña. Esta caja fuerte se encuentra en un área restringida con control de acceso biométrico doble y se autoriza el ingreso de las personas designadas también por el Oficial de Seguridad de la Información.

5.5.4. Procedimientos para copia de seguridad del archivo

Se cuenta con procedimientos aprobados y compatibles con los establecidos por la AAC, para realizar las copias de seguridad de los archivos tanto físicos como electrónicos. Las copias se almacenan en un lugar físicamente separado de las instalaciones de la ECERNEP al que son trasladadas mediante un procedimiento seguro, siendo verificadas en su integridad y con regularidad por el personal autorizado.

5.5.5. Requisitos de fecha y hora de los registros

Todos los registros del archivo contienen información de fecha y hora del instante en que se generan.

5.5.6. Sistema de archivo (interno vs. externo)

La información del archivo de la ECERNEP se gestiona tanto internamente como externamente, en un lugar físicamente separado de las instalaciones principales.

5.5.7. Procedimientos para obtener y verificar la información archivada

La ECERNEP archiva la información clasificándola por su naturaleza y criticidad, indicando qué personas tienen acceso de acuerdo a los privilegios de su rol. En cualquier caso, para tener acceso a la información archivada, se debe solicitar autorización del Oficial de Seguridad de la Información y dejar constancia del hecho.

5.6. Cambio de llaves

El cambio de llaves de 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 en cuyo caso la ECERNEP procede a emitir el nuevo certificado.

Los PSVA-TSA pueden cambiar sus llaves periódicamente y solicitar un nuevo certificado digital 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.

Tanto en el caso de la ECEP como en el del PSVA-TSA, para el cambio de llaves se sigue el mismo procedimiento que para la emisión de su certificado digital por primera vez.

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

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

El Plan de Contingencias de la ECERNEP incluye un procedimiento documentado para la gestión de contingencias en caso de falla o interrupción de algún servicio, el cual es evaluado en cada auditoría interna y externa. En el procedimiento se establecen mecanismos de comunicación, registro y respuesta ante incidentes, indicando la acción que ha de emprenderse. Los incidentes son comunicados, tan pronto se haya tomado conocimiento, al Oficial de Seguridad de Información de la ECERNEP, para que se tomen las acciones para reducir el impacto de los mismos. Dichos procedimientos se encuentran alineados a lo indicado en el numeral **6. CONTROLES TÉCNICOS DE SEGURIDAD**.

De ser el caso, se generan reportes mensuales de incidentes que permiten 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), el

Oficial de Seguridad de la Información de la ECERNEP toma las previsiones y acciones que considere pertinentes contemplando lo establecido en la legislación vigente.

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

Se encuentran identificadas fuentes alternativas de recursos computacionales, software y datos para su uso en los casos de adulteraciones o fallas.

5.7.3. Procedimiento en caso de compromiso de llave privada

En caso que alguna llave privada que administra la ECERNEP resultase comprometida de manera real o potencial, el certificado digital será inmediatamente revocado, notificándose el hecho en un lapso máximo de 24 horas a la AAC. Todos los certificados digitales subordinados emitidos en el periodo comprendido entre el compromiso de la llave y la cancelación del certificado serán también cancelados, lo cual se comunicará a los suscriptores afectados.

5.7.4. Capacidad de continuidad de negocio luego de un desastre

La ECERNEP cuenta con un procedimiento de contingencia, conocido por su personal, probado y aprobado para garantizar la continuidad de sus operaciones en caso de desastres, priorizándose el servicio de verificación del estado de los certificados.

5.8. Terminación de un PSC

No aplica para la ECERNEP.

En caso que un PSC vaya a finalizar sus actividades, debe informar a la ECERNEP y a la AAC, así como a los titulares, suscriptores y terceros que confían sobre el cese de sus operaciones con un mínimo de treinta (30) días calendario de anticipación.

6. CONTROLES TÉCNICOS DE SEGURIDAD

6.1. Generación e instalación del par de llaves

6.1.1. Generación del par de llaves

La ECERNEP genera sus propios pares de llaves utilizando un módulo criptográfico HSM que cumple con los requisitos descritos en el numeral **6.2.1, Estándares y controles para el módulo criptográfico**. Este procedimiento se realiza mediante una ceremonia de generación de llaves.

El dispositivo criptográfico empleado para las llaves de firma del prestador únicamente genera llaves de firma del prestador bajo, al menos, control dual, requisito que se puede implementar en el propio dispositivo o en el software del sistema fiable[4].

El sistema fiable empleado para la generación de llaves de la ECERNEP, en su consideración de autoridad de certificación raíz y, por tanto, punto de confianza de la PKI, es operado en un sistema independiente y aislado que no tiene conexión con otros sistemas. El sistema está desconectado cuando no se precisa su uso[5].

La generación de llaves de la ECERNEP, y su subsiguiente certificación, se realiza en un entorno físicamente asegurado por personal en roles fiables bajo, como mínimo, control dual[6] y elementos de conocimiento dividido[7].

La ECERNEP dispone de un procedimiento documentado para la realización de sus ceremonias de llaves, el que indica, al menos, lo siguiente[8]:

- Los roles que participan en la ceremonia de llaves (internos y externos a la organización).
- Las funciones que asume cada rol y en qué fases.
- Las obligaciones de los roles antes y después de la ceremonia.
- La aprobación para la realización de la ceremonia.
- El hardware criptográfico y los materiales de activación necesarios para la ceremonia.
- Los pasos específicos que realizar durante la ceremonia.
- Los requisitos de seguridad física específicos para la localización de la ceremonia.
- Los procedimientos para el almacenamiento seguro del hardware criptográfico y los materiales de activación después de la ceremonia.
- Los requisitos de evidencias a recoger en relación con la ceremonia.
- Las desviaciones del guion de la ceremonia.

[4] CEN/TS 419 261:2015, sección 5.2.5.2.1 [KM1.3]; ETSI EN 319 411-1:2016, sección 6.5.4.a).
[5] CEN/TS 419 261:2015, sección 5.2.5.2.1 [KM1.6].
[6] ETSI EN 319 411-1:2016, sección 6.5.1.a); CICA WebTrust for CA 2.0, sección 4.1.
[7] CICA WebTrust for CA 2.0, sección 4.1; CA/Browser Forum Baseline Requirements 1.4.4, sección 6.1.1.1.
[8] ETSI EN 319 411-1:2016, sección 6.5.1.f); CICA WebTrust for CA 2.0, sección 4.1.

La ECERNEP produce un acta que demuestra que la ceremonia ha tenido lugar de acuerdo con el procedimiento establecido, y que se ha garantizado la integridad y confidencialidad del par de llaves. El acta es firmada[9]:

- En el caso de una Autoridad de Certificación raíz, por el rol fiable responsable de la seguridad de la ceremonia y una persona confiable independiente de la gerencia de RENIEC, como un Notario o Auditor, que testifica que el acta recoge de forma correcta cómo se realizó la ceremonia de llaves.

6.1.2. Entrega de la llave privada al suscriptor

Las llaves privadas de la ECERNEP son generadas y mantenidas bajo su control, por lo que no es necesaria su entrega.

Los PSC subordinados generan su propio par de llaves mediante una ceremonia de llaves, por lo tanto no es necesario realizar entrega alguna de llaves privadas. 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

En el caso de las llaves administradas por la ECERNEP, el titular, suscriptor y emisor es la misma ECERNEP, por lo que no es necesario el procedimiento de entrega de llave pública.

La ECERNEP recibe de los PSC subordinados la llave pública dentro de un CSR en formato PKCS#10.

6.1.4. Entrega de la llave pública al tercero que confía

La ECERNEP publica en los repositorios correspondientes, según lo indicado en el numeral **2.1 Repositorio**, todos los certificados digitales (que incluyen la llave pública) emitidos a fin de que estén accesibles para los terceros que confían.

[9] ETSI EN 319 411-1:2016, sección 6.5.1.g). CICA WebTrust for CA 2.0, sección 4.1.

6.1.5. Tamaño de llaves

Los tamaños de las llaves en uso en la Jerarquía ECERNEP PERÚ CA Root 3 son 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 6 - Algoritmo de firma y tamaño de llave de los certificados digitales

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

Las llaves de la ECERNEP se generan en un módulo criptográfico seguro y certificado con estándar FIPS 140-2 nivel 3, lo que garantiza la generación de llaves de calidad conforme a los parámetros establecidos en los numerales 6.1.1 Generación del par de llaves y **6.1.5 Tamaño de llaves**.

La verificación de calidad de las llaves de las PSC subordinadas, se realiza solicitando pruebas que indiquen que la generación se realizó en un módulo criptográfico acorde a las características indicadas en el numeral **6.2.1 Estándares y controles para el módulo criptográfico.**

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

Los valores de las extensiones *KeyUsage* y *ExtendedKeyUsage* de los certificados que emite la ECERNEP se puede consultar en el numeral7.1 **Perfil de los certificados**.

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 se encuentran certificados y operan conforme al estándar FIPS 140-2 nivel 3. Asimismo, se encuentran apagados, fuera de línea y debidamente resguardados en un área reservada con controles de acceso físico.

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

El acceso al módulo criptográfico que contiene las llaves de la ECERNEP se encuentra protegido por un algoritmo criptográfico que distribuye la credencial de acceso en cinco (05) partes y que requiere un quórum de tres (03) de ellas para poder realizar cualquier operación.

La ECERNEP distribuye cada parte en una smartcard protegida por PIN y se la entrega a una persona diferente, llamada "custodio", quien es responsable de su resguardo (junto con el PIN).

El acceso al módulo criptográfico de la EC-PSVA también se encuentra dividido en cinco (05) partes y se requiere un quórum de tres (03).

6.2.3. Custodia de la llave privada

La ECERNEP custodia sus propias llaves privadas y las de la EC-PSVA.

6.2.4. Respaldo de la llave privada

La ECERNEP realiza una copia de respaldo (*backup*) de sus llaves privadas, aplicando el mismo nivel de protección establecido para las llaves privadas originales. Esta copia es almacenada en un lugar físicamente separado al módulo criptográfico, garantizando así la posibilidad de realizar una restauración en caso de deterioro o destrucción del módulo criptográfico original.

6.2.5. Archivo de la llave privada

La ECERNEP archiva sus propias llaves privadas asegurando su confidencialidad e integridad; en ningún caso, archiva o respalda llaves privadas de los PSC subordinados.

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

La ECERNEP realiza al menos una copia de respaldo, de sus llaves privadas, como se indica en el numeral **6.2.4, Respaldo de la llave privada,** hacia otro módulo criptográfico HSM que cumple con las condiciones señaladas en el numeral **6.2.1, Estándares y controles para el módulo criptográfico**. En la migración, estas llaves son ilegibles fuera del HSM y se protegen por controles de seguridad de igual nivel que los establecidos en el módulo criptográfico HSM original y en conformidad con el estándar FIPS 140-2 nivel 3. Para esta actividad se requiere de la cantidad de personas necesarias para la activación del módulo criptográfico indicada en el numeral **6.2.2, Control multipersonal (k de m) de la llave privada,** y la presencia del Oficial de Seguridad de Información de la ECERNEP.

6.2.7. Almacenamiento de la llave privada en un módulo criptográfico

Las llaves privadas administradas por la ECERNEP han sido generadas y se mantienen en un módulo criptográfico HSM certificado y que opera bajo el estándar FIPS 140-2 nivel 3

6.2.8. Método de activación de la llave privada

La ECERNEP cuenta con métodos de activación según lo indicado en el numeral **6.2.2 Control multipersonal (k de m) de la llave privada**. Adicionalmente, al encontrarse en un área restringida, para realizar la activación se requiere primero acceder físicamente al módulo criptográfico que las contiene, el cual se encuentra protegido dentro de una caja

fuerte con llave física y contraseña dentro de un área con puerta blindada con control biométrico doble.

Las personas con autorización en el control biométrico no son las mismas que custodian las tarjetas de activación de la llave privada.

6.2.9. Método de desactivación de la llave privada

Las llaves privadas administradas por la ECERNEP, se encuentran en modo *offline*; por lo tanto, se encuentran desactivadas, ya que el módulo criptográfico que las contiene se encuentra apagado, fuera de línea y sin energía. De la misma manera, las copias de seguridad se encuentran en módulos criptográficos apagados como se indica en el numeral **6.2.4 Respaldo de la llave privada**.

6.2.10. Método de destrucción de la llave privada

En caso se requiera la destrucción de alguna llave privada de la ECERNEP, primero y de ser el caso se realiza el procedimiento de cancelación del certificado digital, según el numeral **3.4, Identificación y autenticación para solicitudes de cancelación,** y luego se elimina la llave privada de los módulos criptográficos que las contienen, incluyendo las copias de respaldo. El procedimiento se realiza según lo indicado por el fabricante del módulo criptográfico, de manera que copias recuperables no se mantengan en el dispositivo criptográfico o en zonas de memoria o de disco.

El Oficial de Seguridad de la Información de la ECERNEP registra el procedimiento de destrucción de cualquier llave privada.

6.2.11. Clasificación del módulo criptográfico

Los módulos criptográficos de la ECERNEP cuentan con la certificación de seguridad FIPS 140-2 nivel 3.

6.3. Otros aspectos de la gestión del par de llaves

6.3.1. Archivo de la llave pública

Las llaves públicas, o los certificados emitidos o administrados por la ECERNEP que las contienen, son archivados conforme se establece en el numeral **5.5**, **Archivo**, los mismos que a su vez se publican en los repositorios correspondientes como se muestra en los numerales **2.1, Repositorio**, y **2.2, Publicación de información de certificación**.

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 de certificados que emite la ECERNEP, se especifica en la siguiente tabla:

CN del certificado	Validez (años)

ECERNEP PERU CA Root 3	25
EC-PSVA y ECEP *offline*	16
PSVA-TSA	12

Tabla 7 - Tiempo de validez de los certificados digitales

6.4. Datos de activación

6.4.1. Generación e instalación de los datos de activación

La generación de los datos de activación se realiza utilizando módulos criptográficos que utilizan mecanismos se acceso multipersonal, 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 ECERNEP protege los datos de activación mediante lo indicado 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

Los datos de activación de los módulos criptográficos de la ECERNEP son cambiados una vez cada dos años o cuando se considere necesario.

6.5. Controles de seguridad computacional

6.5.1. Requisitos técnicos específicos de seguridad computacional

En relación a la implementación de controles de seguridad y los criterios para su evaluación, la ECERNEP cumple con lo estipulado en los siguientes estándares:

- 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

La ECERNEP mantiene sus equipos y sistemas críticos en un área restringida. Además, mantiene los equipos necesarios para el cumplimiento de sus funciones operativas (como gestión de repositorios de certificados emitidos o CRLs) en un área dedicada y aislada de otras actividades. Al respecto, se realizan pruebas de evaluación, clasificación y auditorías internas al menos una vez cada seis meses, según lo indicado en el numeral **6.5.1, Requisitos técnicos específicos de seguridad computacional**.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles para el desarrollo de sistemas

Los módulos criptográficos que utiliza la ECERNEP para la emisión y cancelación de certificados digitales cuentan con certificación de seguridad FIPS 140-2 nivel 3. La plataforma base de administración de los repositorios de la ECERNEP no recibe cambios ni actualizaciones que no provengan del fabricante.

6.6.2. Controles de gestión de seguridad

Los controles para prevenir o detectar la modificación no autorizada del software o hardware de la ECERNEP forman parte de los controles del sistema de gestión de la seguridad de la información bajo el que opera el proceso de certificación digital de la institución.

6.6.3. Controles de seguridad del ciclo de vida

Los controles de seguridad establecidos para la ECERNEP son revisados a través de auditorías externas y auditorías internas desarrolladas según lo señalado en el numeral **5.4.6, Sistema de realización de auditoría (Interna vs. Externa)**.

6.7. Controles de seguridad de red

Los módulos criptográficos de la ECERNEP se encuentran sin energía y, por lo tanto, fuera de la red y en modo *offline*. Asimismo, los equipos donde se despliegan los repositorios de la ECERNEP se encuentran protegidos contra ataques, accesos no autorizados o alteración de datos.

6.8. Fecha y Hora

La ECERNEP utiliza la fecha y hora UTC para firmar los certificados que emite, con un margen de error máximo del orden del minuto. Durante la Ceremonia de Llaves se establece esta hora y es certificada ante notario público. La sincronización horaria de los equipos *offline* de la ECERNEP es objeto de control de las auditorías periódicas.

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[10]. 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.

[10] Esta norma es la actualización del RFC 3628 y especificación ETSI TS 102 023.

7. PERFILES DE CERTIFICADOS, CRL y OCSP

7.1. Perfil de los certificados

Los certificados emitidos por la ECERNEP PERU CA ROOT 3 cumplen con el estándar ITU X.509 versión 3 y cuentan, 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 8 - Extensiones mínimas de un certificado digital de la Jerarquía ECERNEP PERU CA Root 3

El detalle de perfiles y extensiones de los certificados digitales emitidos por la ECERNEP PERU CA Root 3 se encuentra en el Anexo 2 del presente documento.

7.1.1. Versión

Los perfiles de los certificados digitales emitidos por la ECERNEP PERU CA Root 3 cumplen con el estándar x.509 versión 3.

7.1.2. Extensiones del certificado digital

Los campos y las extensiones mínimas que se utilizan en los certificados digitales emitidos por la ECERNEP PERU CA Root 3 se presentan en la Tabla 8 del presente documento. El detalle de sus perfiles y extensiones se encuentra en el Anexo 2 del presente documento.

7.1.3. Identificadores de objeto de algoritmos

Los certificados digitales emitidos por la ECERNEP usan los siguientes algoritmos de firma con los identificadores de objeto señalados:

- SHA512 con cifrado RSA para el certificado raíz de la ECERNEP PERU CA Root 3, para el certificado de la EC-PSVA y para los certificados de las ECEP de segundo nivel off line.

  - 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 para los certificados emitidos a través de la EC-PSVA a los PSVA-TSA.

  - 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 respeta 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 emitidos por la ECERNEP PERU CA Root 3, además de lo establecido en el artículo 7º de la Ley de Firmas y Certificados Digitales – Ley 27269, incluyen lo siguiente:

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

7.1.5. Restricciones de nombre

Los certificados digitales para PSC emitidos por la ECERNEP PERU CA Root 3 indican un nombre que permite el reconocimiento de la persona jurídica asociada y se cumple con lo establecido en el estándar RFC 5280.

7.1.6.Identificador de objeto de la política de certificados digitales

La ECERNEP consigna el identificador de objetos comodín "anyPolicy" en su certificado raíz y en los emitidos a la EC-PSVA y las ECEP de segundo nivel off line conforme se señala en el RFC 5280 para efectos de interoperabilidad.

Para los certificados emitidos por la EC-PSVA a las PSVA-TSA se incluye un OID identificador de objeto de la política de certificados digitales que proviene de un nodo o

arco asignado por la IANA (Autoridad de Números Asignados en Internet) al RENIEC, además del OID correspondiente a la política ETSI EN 319-411-1.[11]

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

La ECERNEP emite periódicamente sus CRL en el formato estipulado RFC 5280 "*PKIX Certificate and CRL Profile*" para el perfil de CRL en su versión 2 (X.509 v2).

7.3. Perfil de OCSP

La ECERNEP no implementa el servicio OCSP.

[11] De acuerdo con el Anexo 1 de la Guía de Acreditación para Entidades de Certificación Digital, corresponden al INDECOPI las funciones de Autoridad de Registro Nacional (ARN) para la asignación de los OID en el Perú, no obstante, ello no se ha llegado a implementar.

8. AUDITORÍAS DE CONFORMIDAD Y OTRAS EVALUACIONES

8.1. Frecuencia y circunstancias de evaluación

La ECERNEP está sujeta al menos a una auditoría externa anual y a una auditoría interna trimestral, en conformidad a lo regulado por la AAC.

8.2. Identidad/Calificaciones de auditores

Los auditores externos son designados por la AAC, de acuerdo a su normativa. Es potestad de la AAC evaluar y reconocer a un auditor como personal calificado.

8.3. Relación del auditor con la entidad auditada

La ECERNEP garantiza 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, sigue el procedimiento definido por la AAC para su designación y contempla además las restricciones establecidas a las Entidades Públicas bajo el marco legal vigente que son aplicables para su contratación.[12]

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

8.4. Elementos cubiertos por la evaluación

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

- Alineación de la CP y CPS de la ECERNEP a las Guías de Acreditación de la IOFE.
- Alineación de las medidas efectivas existentes.
- Evaluación y cumplimiento de los niveles de seguridad física.
- Revisión de los procedimientos de contingencia.
- Revisión de los controles de seguridad de la información.
- Revisión de los controles de acceso a la Base de Datos.

8.5. Acciones a ser tomadas frente a deficiencias

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

[12] Ley Nº 30225, Ley de contrataciones del Estado, modificatorias y su Reglamento.

Ley Nº 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.

8.6. Publicación de resultados

La AAC tiene la potestad de tomar acciones en relación a la publicación de resultados de auditoría.

9. OTRAS MATERIAS DE NEGOCIO Y LEGALES

9.1. Tarifas

Las tasas por la prestación de los servicios de certificación digital que brinda la ECERNEP se encuentran establecidas en el Texto Único de Procedimientos Administrativos del RENIEC (TUPA). Alternativamente, se puede dar la prestación de servicios a través de la suscripción de convenios donde se establecen las prestaciones y contraprestaciones del caso.

9.1.1. Tarifas para la emisión o renovación de certificados

La emisión de certificados digitales está supeditada al pago previo de la tasa respectiva establecida en el Texto Único de Procedimientos Administrativos (TUPA) del RENIEC. Esta tasa es un tributo que grava la emisión del certificado digital, en cumplimiento al Art. 36.1 de la Ley 27444, Ley del Procedimiento Administrativo General, siendo el trato a los administrados regulado por dicho texto sin requerirse que en el contrato de prestación se establezca costo o pago por la tarifa.

9.1.2. Tarifas de acceso a certificados

La ECERNEP brinda el servicio de acceso a certificados digitales considerando únicamente la tasa establecida en el Texto Único de Procedimientos Administrativos (TUPA) del RENIEC para la emisión de certificados. No aplica ninguna tasa por el empleo de los certificados digitales, ni por el acceso a los repositorios públicos donde se encuentran la CRL y los certificados digitales emitidos.

9.1.3. Tarifas para información sobre cancelación o estado

La ECERNEP brinda el servicio de información sobre cancelación del estado de los certificados digitales a través de la publicación de las CRL considerando únicamente la tasa establecida en el Texto Único de Procedimientos Administrativos (TUPA) del RENIEC para la emisión de certificados. No aplica ninguna tasa por el empleo de los certificados digitales, ni por el acceso a los repositorios públicos donde se encuentran la CRL y los certificados digitales emitidos.

9.1.4. Tarifas para otros servicios

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

9.1.5. Políticas de reembolso

Es política del RENIEC, en su calidad de Prestador de Servicios de Certificación Digital para el Estado Peruano, reembolsar al solicitante la tasa respectiva por la emisión del certificado digital, en caso su solicitud no hubiese sido atendida por responsabilidad atribuible a la ECERNEP.

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

9.2. Responsabilidad Financiera

9.2.1.Cobertura de seguro

La ECERNEP-RENIEC cuanta con una Póliza de Seguros de Responsabilidad Civil contra terceros, la que es de aplicación bajo todos los ámbitos de las operaciones que desarrolla la entidad en conformidad con los roles y funciones que le han sido atribuidos bajo el marco legal regulatorio vigente, cumpliéndose de este modo con la obligación señalada en el artículo 27° del Reglamento de la Ley de Firmas y Certificados Digitales.

9.2.2.Otros activos

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

9.2.3.Cobertura de seguro o garantía para entidades finales

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

9.3. Confidencialidad de información del negocio

9.3.1.Alcances de la información confidencial

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

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

9.3.2.Información no contenida dentro del rubro de información confidencial

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

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

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

9.3.3.Responsabilidad de protección de la información confidencial

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

9.4. Privacidad de la información personal

9.4.1.Plan de privacidad

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

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

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

El “Plan de Privacidad” es catalogado como información pública y es publicado en el repositorio de la ECERNEP.

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

9.4.2.Información tratada como privada

La ECERNEP declara expresamente como información personal de carácter privado, a toda aquella información que no se encuentre contenida en los certificados digitales ni en la lista CRL.

La información personal considerada como privada es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado.

9.4.3.Información no considerada privada

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

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

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

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

9.4.4.Responsabilidad de protección de la información privada

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

En tal sentido, ha implementado medidas de índole organizativo y técnico orientadas a garantizar la protección y privacidad de los datos personales, así como de la información confidencial que gestiona.

Las medidas implementadas por la ECERNEP se encuentran detalladas en la “Política de Seguridad”, en la “Política de Privacidad” y en el “Plan de Privacidad”.

9.4.5.Notificación y consentimiento para el uso de información

En los formatos de solicitud de emisión y cancelación de certificados digitales se especifican los datos personales de los titulares y/o suscriptores que son recolectados.

De conformidad con lo dispuesto en el numeral 1 del Artículo 14[13]de la Ley N° 29733, Ley de Protección de Datos Personales, la ECERNEP está exceptuada de solicitar el consentimiento al titular de los datos para el tratamiento de sus datos personales.

9.4.6.Divulgación con motivo de un proceso judicial o administrativo

Los datos personales de carácter privado o la información confidencial del titular y/o suscriptor de un certificado digital, serán revelados o comunicados cuando una orden judicial o 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 el titular y/o suscriptor.

9.4.7.Otras circunstancias para divulgación de información

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

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

En todo caso, la cesión o transferencia de datos personales se realizará de acuerdo a la Ley N° 29733, Ley de Protección de Datos Personales, y en lo que fuese aplicable, en el caso de las entidades de la Administración Pública, según lo señalado en el artículo 55 del Reglamento de la Ley de Firmas y Certificados Digitales.

En todos los casos, la entidad receptora debe garantizar a la ECERNEP la confidencialidad de la información transferida.

9.5. Derechos de propiedad intelectual

Todos los derechos de propiedad intelectual, incluyendo los referidos a certificados, repositorios de la ECERNEP, los OID, la Política General de Certificación, la presente Declaración de Prácticas de Certificación, la Política de Seguridad, la Política y el Plan de Privacidad, así como cualquier otro documento de gestión de la ECERNEP, corresponden al RENIEC.

Los documentos de la ECERNEP publicados en los repositorios correspondientes son de carácter público y por lo tanto se permite su reproducción, distribución y comunicación, más no su transformación o alteración. Se prohíbe la reproducción, distribución, comunicación,

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

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

transformación o alteración de los documentos de gestión de la ECERNEP que tienen el carácter de interno o reservado sin la autorización expresa del RENIEC.

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

9.6. Representaciones y garantías

9.6.1.Representaciones y garantías de la EC

Son obligaciones de la ECERNEP las siguientes:

1. Emitir y cancelar el certificado digital previa evaluación y aprobación de la solicitud.
2. Cancelar el certificado digital al suscitarse alguna de las causales señaladas en el contrato.
3. Incluir el certificado digital cancelado en la Lista de Certificados Digitales Cancelados (CRL).
4. Mantener la confidencialidad de la información relativa al titular y/o suscriptor, limitando su empleo a las necesidades propias del servicio de certificación, salvo por orden judicial o mandato de autoridad competente amparados por la Ley, o a pedido del titular y/o suscriptor.
5. Mantener actualizado el repositorio con los certificados digitales emitidos y la CRL.
6. Proceder a la entrega del certificado digital al titular y/o suscriptor conforme a las condiciones definidas en el presente documento.
7. En general, es obligación de la ECERNEP cumplir con todas las obligaciones establecidas en el artículo 26° del D.S N° 052-2008-PCM.

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

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

9.6.2.Representaciones y garantías de la ER

No aplica a la ECERNEP.

9.6.3.Representaciones y garantías de los suscriptores

Para la ECERNEP, la entidad solicitante (persona jurídica) se constituirá en el titular del certificado digital. Será su representante legal (persona natural) debidamente acreditado quien suscribirá la solicitud correspondiente, procediéndose al registro o verificación de su identidad, siendo quien asuma las obligaciones de suscriptor del certificado digital en aplicación del Art. 14° del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado por D.S 052-2008-PCM.

Conforme se encuentran detalladas en el correspondiente contrato de prestación de servicios, las obligaciones del Titular y Suscriptor son:

1. Entregar información veraz bajo su responsabilidad.
2. Actualizar la información proporcionada a la ECERNEP cuando estos ya no resulten exactos o son incorrectos.
3. Proporcionar evidencia de haber realizado una Ceremonia de Llaves para generar su par de llaves según lo indicado en el numeral 6.1.1 Generación del par de Llaves.
4. Utilizar para la activación de su clave privada los mecanismos previstos en el estándar FIPS 140-2 para dispositivos Hardware Security Module (HSM) de nivel 3 o equivalente para evitar su pérdida, revelación, modificación o uso no autorizado.
5. Observar las condiciones establecidas por la ECERNEP, para la utilización del certificado digital y la generación de firmas digitales.
6. Realizar un uso debido y correcto del certificado digital.
7. Notificar de inmediato a la ECERNEP en caso de que detecte que se ha incluido información incorrecta o inexacta en el certificado digital.
8. Solicitar inmediatamente a la ECERNEP la cancelación de su certificado digital en caso de tener conocimiento o sospecha de la ocurrencia de alguna de las siguientes circunstancias:
   a) Exposición, puesta en peligro o uso indebido de la clave privada o de los datos de activación de su clave privada . El compromiso de la clave privada puede darse, entre otras causas, por pérdida, robo del dispositivo HSM, de su Software de gestión y de los dispositivos criptográficos (tarjetas o tokens) que contienen sus datos de activación.
   b) Deterioro, alteración o cualquier otro hecho u acto que afecte el dispositivo HSM que contiene la clave y a los dispositivos criptográficos (tarjetas o tokens) que contiene sus datos de activación.
9. Solicitar de inmediato a la ECERNEP la cancelación del certificado cuando:
   a) La información contenida en el certificado digital ya no resulte correcta.
   b) El titular y suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la ECERNEP.

Asimismo, el titular y suscriptor del certificado asumirá las responsabilidades, a que hubiese lugar, por los daños y perjuicios que pudiese causar por aportar datos falsos, incompletos o inexactos, así como, es de su exclusiva responsabilidad el uso indebido, incorrecto o no acorde a los fines para el que fue extendido el certificado. A tal efecto, la ECERNEP está excluida de toda responsabilidad.

9.6.4.Representaciones y garantías de los terceros que confían

Es obligación de los Terceros que Confían en los certificados digitales emitidos por la ECERNEP:

1. Verificar la validez de los certificados digitales en el momento de realizar cualquier operación basada en los mismos mediante la comprobación de que el certificado es válido y no está caducado o ha sido cancelado.
2. No usar los certificados digitales fuera de los términos establecidos en el marco de la IOFE.
3. Limitar la fiabilidad de los certificados digitales a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados digitales y la Política de General de Certificación de la ECERNEP.
4. Dar lectura al presente documento.
5. Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados digitales en los que confía, y aceptar y sujetarse a las mismas.

9.6.5. Representaciones y garantías de otros participantes

Es responsabilidad de la ECERNEP la publicación de los certificados digitales emitidos en los repositorios institucionales del RENIEC puestos a su disposición.

9.7. Exención de garantías

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

9.8. Limitaciones a la responsabilidad

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

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

9.9. Indemnizaciones

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

9.10. Término y terminación

9.10.1. Término

El presente documento entra en vigencia desde el momento en que es aprobado por la AAC de la IOFE, y su periodo de vigencia es de 05 años al ser este el plazo de las acreditaciones otorgadas por la AAC de acuerdo a la legislación vigente. Esto sin perjuicio

que en el trascurso de este tiempo este documento pueda ser modificado por decisión propia del RENIEC o determinación de la AAC. Se contemplará que la validez de tal documentación estará sujeta a la continuidad de la acreditación.

9.10.2. Terminación

En caso de cese de actividades de la ECERNEP, ésta informará a la AAC, así como a los titulares, suscriptores y terceros que confían sobre el cese de sus operaciones con un mínimo de treinta (30) días calendario de anticipación.

9.10.3. Efecto de terminación y supervivencia

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

9.11. Notificaciones y comunicaciones individuales con los participantes

Toda notificación o comunicación con la ECERNEP se hará mediante correo electrónico o por escrito dirigido a la dirección señalada en el numeral **1.5.2, Persona de contacto,** del presente documento.

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

9.12. Enmendaduras

9.12.1. Procedimiento para enmendaduras

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

9.12.2. Mecanismos y periodos de notificación

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

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

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

9.12.3. Circunstancias bajo las cuales debe ser cambiado el OID

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

9.13. Procedimiento sobre resolución de disputas

En caso el reclamo esté directamente relacionado con el servicio de certificación digital brindado a las ECEP por la ECERNEP, éstas se deberán dirigir a la oficina con dirección indicada en el numeral **1.5.2, Persona de contacto** del presente documento para su atención.

El reclamo será resuelto por la ECERNEP en primera instancia dentro del plazo establecido en la ley N° 27444, Ley del Prodedimiento Administrativo General (30 dias hábiles), y de conformidad con lo establecido en la Segunda Disposición Complementaria Final del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo N° 052-2008-PCM, la AAC resolverá el recurso de apelación presentado por el titular y/o suscriptor.

9.14. Ley aplicable

Conforme al Artículo Nº47 del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado por D.S 052-2008-PCM, que designa al RENIEC como ECERNEP, ECEP y EREP, el funcionamiento y operaciones de la ECERNEP, así como el presente documento, estarán sujetos a la normatividad que resulte aplicable y en especial a las disposiciones siguientes:

- Ley N° 27444, Ley del Procedimiento Administrativo General.
- Ley N° 27269, Ley de Firmas y Certificados Digitales.
- Reglamento de la Ley de Firmas y Certificados aprobado mediante el Decreto Supremo Nº 052-2008-PCM y sus modificaciones.
- Guía de Acreditación de Entidades de Certificación EC.
- Ley N° 29733, Ley de Protección de Datos Personales.

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

9.15. Conformidad con la ley aplicable

Es responsabilidad de la ECERNEP en la prestación de sus servicios, velar por el cumplimiento de la legislación aplicable recogida en el numeral **9.14, Ley aplicable,** del presente documento.

9.16. Cláusulas misceláneas

9.16.1. Acuerdo Íntegro

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

9.16.2. Subrogación

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

9.16.3. Divisibilidad

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

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

No se aplica ninguna cláusula de ejecución a las operaciones de la ECERNEP .

9.16.5. Fuerza Mayor

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

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

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

9.17. Otras cláusulas

No se estipula.

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. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI.

- **Certificado de Autoridad:** Es un certificado digital de una entidad confiable y acreditada que emite certificados digitales subordinados.
- **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.
- **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 bajo la normatividad vigente.
- **Entidad final.** Es el suscriptor o propietario de un certificado digital.
- **Estándares Técnicos Internacionales.** Son los requisitos de orden técnico y de uso internacional que deben observarse en la emisión de certificados digitales y en las prácticas de certificación.
- **Estándares Técnicos Nacionales.** Son los estándares técnicos aprobados mediante Normas Técnicas Peruanas por el Instituto Nacional de Calidad (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, 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 llaves.** En un sistema de criptografía asimétrica comprende una llave 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 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:** 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
- **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 Entidad 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 emitidos por la ECERNEP

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	-	-	-	-

2. EC-PSVA

Además de emitir certificados para las ECEP, la ECERNEP emite certificados para los PSC como PSVA-TSA. 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 de la EC-PSVA con un certificado de nivel 2 cuya llave privada opera 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 Usage	-	Time Stamping (1.3.6.1.5.5.7.3.8)	Sí	No
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	-	-	-	-

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	cA	TRUE	Sí	Sí

Constraints	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	-	-	-	-

4. 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	-	-	-	-