Política General de Certificación y Declaración de Prácticas de la ECERNEP

Entidad de Certificación Nacional para el Estado Peruano - ECERNEP

Versión: 2.1	**Año:** 2017

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	22/06/2012	Elaboración y Aprobación	GCRD	Aprobado
2.0	05/12/2012	Se recoge observaciones del evaluador de INDECOPI.	GCRD	Aprobado
2.1	28/06/2017	Se excluye la emisión de certificados digitales SHA-1	GRCD	Aprobado

- Por resolución Jefatural N° 073-2016/JNAC/RENIEC se aprobó el ROF RENIEC 2016, modificándose la denominación de la unidad orgánica:
  Antes: GERENCIA DE CERTIFICACIÓN Y REGISTRO DIGITAL
  Ahora: GERENCIA DE REGISTROS DE CERTIFICACIÓN DIGITAL.

INDICE

1. Introducción

1.1. Visión general.

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

El presente documento rige el funcionamiento de la ECERNEP y da cumplimiento a los requerimientos exigidos por las Guías de Acreditación para Entidades de Certificación publicadas por la Autoridad Administrativa Competente (en adelante AAC). También describe la jerarquía que posee la ECERNEP sobre las demás Entidades de Certificación para el Estado Peruano.

La ECERNEP se encuentra alojada físicamente en las mismas instalaciones que la ECEP por lo cual muchos de los controles utilizados por esta última son aplicables a la ECERNEP.

La ECERNEP posee dos certificados digitales raíz autofirmados con un periodo de validez de 20 años a partir del 21 de Julio del 2010, los cuales vencen el 16 de Julio del 2030. La diferencia entre estos dos certificados digitales es únicamente el algoritmo de firma criptográfico utilizado (SHA-1 y SHA-256).

Por Resolución Nº 123-2016/CFE-INDECOPI de 9 de diciembre de 2016[1] la AAC de la Infraestructura Oficial de Firma Electrónica (en adelante IOFE) se establece:

> *"PRIMERO.- Las entidades de certificación pertenecientes a la Infraestructura Oficial de Firma Electrónica tienen plazo hasta el 30 de junio de 2017 para generar certificados digitales firmados con el algoritmo SHA-1. A partir del 1 de julio de 2017, dichas entidades de certificación quedarán obligadas a generar certificados digitales asociados al algoritmo SHA-256 u otro de mayor fortaleza criptográfica, sin necesidad de la emisión de una resolución administrativa adicional."*
>
> *"SEGUNDO.- Los certificados digitales generados con el algoritmo SHA_1 hasta el 30 de junio de 2017 sólo serán cancelados cuando se verifique alguna de las causales establecidas en el artículo 17 del Reglamento de la Ley de Firmas y Certificados Digitales."*

[1] La Resolución Nº 123-2016/CFE-INDECOPI de 9 de diciembre de 2016 otorga un plazo adicional hasta el 1 de julio de 2017 para la migración del algoritmo SHA-1 al algoritmo SHA-256 que fuese fijado inicialmente para el 1 de enero de 2017 en la Resolución Nº 073-2016/CFE-INDECOPI de 4 de agosto de 2016, precisando asimismo sus alcances.

> *"TERCERO.- La adecuación del software acreditado y de los servicios acreditados de valor añadido que actualmente utilizan el algoritmo SHA-1 en el proceso de firmado de documentos electrónicos, los cuales también deberán migrar al algoritmo SHA-256 u otro de mayor fortaleza criptográfica, se verificará en la primera evaluación anual de seguimiento que corresponda realizar después del 30 de junio de 2017."*

En concordancia con lo establecido por la AAC en la Resolución Nº 123-2016/CFE-INDECOPI, la ECERNEP emitirá certificados digitales firmados con el algoritmo SHA-1 solo hasta el 30 de junio de 2017 y a partir del 1 de julio de 2017 únicamente emitirá certificados con el algoritmo SHA-256. De igual manera deberán proceder las ECEP. Los SVA para el Estado Peruano cumplirán con lo señalado en el artículo tercero de la citada resolución.

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

1.1.1. Clases de Certificados

La infraestructura de clave pública del RENIEC emite y gestiona diferentes clases de certificados digitales según el tipo de suscriptor o entidad final, para ejecutar dicha tarea la Autoridad Raíz emite certificados digitales para Autoridades Intermedias quienes a su vez se encargarán de gestionar y emitir certificados digitales para suscriptores o entidades finales. Bajo esta premisa la clasificación es la siguiente:

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

Para mayor detalle de la clasificación puede recurrir a los perfiles de certificados digitales emitidos por la ECERNEP consignados en el documento "*Perfiles de Certificado Digital ECERNEP*".

1.2. Nombre e identificación del documento

Nombre: Política General de Certificación y Declaración de Prácticas

Nombre del documento	Política General de Certificación y Declaración de Prácticas de la ECERNEP Entidad de Certificación Nacional para el Estado Peruano - ECERNEP
Versión del documento	2.1
Estado del documento	Aprobado.
Fecha de emisión	28/06/2017
OID	1.3.6.1.4.1.35300.1.1.1.2
Publicación	http://www.reniec.gob.pe/repository/

1.3. Participantes de la PKI

1.3.1. Entidades de Certificación

La Entidad de Certificación Nacional para el Estado Peruano (ECERNEP) es la entidad encargada de emitir los certificados digitales destinados a Entidades de Certificación para el Estado Peruano de nivel intermedio, además de proponer a la Autoridad Administrativa Competente, las políticas y estándares de las Entidades de Certificación para el Estado Peruano (ECEP) y Entidades de Registro o Verificación para el Estado Peruano (EREP), según los requerimientos de la Autoridad Administrativa Competente[2].

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

1.3.2. Entidades de Registro

La ECERNEP se relaciona con las Entidades de Registro o Verificación a través de la ECEP, lo cual implica que los procesos descritos en la DPR de las EREP deben seguir las políticas y estándares de dicha ECEP y los propuestos por la ECERNEP.

1.3.3. Titulares de certificados

La persona jurídica RENIEC es la titular de los certificados digitales emitidos para las Autoridades Intermedias que conforman la ECEP, cuyos certificados digitales son firmados utilizando la clave privada de la ECERNEP.

[2] Reglamento de la Ley de Firmas y Certificados Digitales aprobado mediante el Decreto Supremo N° 052-2008-PCM

La persona jurídica RENIEC también es el titular de los certificados raíz de la ECERNEP.

1.3.4. Tercero que confía

Los terceros que confían o terceros usuarios son aquellas personas naturales o jurídicas, equipos, servicios o cualquier otro ente que decide aceptar y confiar en un certificado digital emitido por la ECERNEP, y actúa basado en la confianza sobre la validez de un certificado digital y/o verifica la firma digital.

1.3.5. Otros participantes

Todas las funciones, operaciones y actividades de la ECERNEP, dentro de los procesos de emisión y cancelación están a cargo del RENIEC en su calidad de Prestador de Servicios de Certificación Digital.

No obstante, en la eventualidad que el RENIEC requiera la tercerización de los servicios de directorio o repositorio y/o servicios de producción de certificados, entre otros, la ECERNEP se reserva el derecho de suscribir el acuerdo de tercerización respectivo, el mismo que contará con las cláusulas específicas relacionadas con la confidencialidad de la información y la protección de los datos personales, asimismo se informará de lo actuado a la AAC.

1.3.5.1. SVA

La ECERNEP emite los certificados digitales a los Prestadores de Servicios de Valor Añadido para el Estado Peruano bajo la modalidad de servicios de sellado de tiempo (TSA).

1.4. Uso del certificado

La ECERNEP emite certificados digitales de Autoridades Intermedias para las ECEP utilizados para la generación de certificados de entidad final y para los SVA TSA utilizados para la emisión de sellos de tiempo. Los certificados digitales para las ECEP son generados por la ECERNEP usando algoritmo SHA-256. Cada uno de estos certificados de Autoridades Intermedias tiene un periodo de vigencia de 10 años.

En concordancia con lo establecido por la AAC en la Resolución Nº 123-2016/CFE-INDECOPI, la ECERNEP emitirá certificados digitales firmados con el algoritmo SHA-1 solo hasta el 30 de junio de 2017 y a partir del 1 de julio de 2017 únicamente emitirá certificados con el algoritmo SHA-256. De igual manera deberán proceder las ECEP. Los SVA para el Estado Peruano cumplirán con lo señalado en el artículo tercero de la citada resolución.

Los certificados mencionados fueron emitidos con el siguiente fin:

- Dos clases para Persona Natural:

- Clase I con 1 año de duración.
- Clase II con 2 años de duración.

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

Lo antes descrito se resume en la siguiente tabla:

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

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

1.4.1. Uso apropiado del certificado

La ECERNEP emite únicamente certificados digitales para Autoridades Intermedias. Y ésta última está en facultad de definir el uso apropiado de los certificados digitales que emita por debajo de su infraestructura. Y deberá especificar las reglas de uso en su

Declaración de Prácticas de Certificación debidamente aprobada por la AAC.

1.4.2. Prohibiciones del uso del certificado

La ECERNEP entrega la responsabilidad de reglamentar el uso de los certificados digitales emitidos para entidades finales a las Autoridades Intermedias quienes informarán en su Declaración de Prácticas de Certificación y Política de Certificación, el uso adecuado de estos, teniendo como referencia la legislación de la materia y las Guías de Acreditación de la AAC.

1.5. Administración de políticas

1.5.1. Organización que administra los documentos de CPS o CP

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

Nombre: Registro Nacional de Identificación y Estado Civil - RENIEC.
Dirección de correo: identidaddigital@reniec.gob.pe
Dirección: Jr. Bolivia 109, Centro Cívico - Cercado de Lima.
Número de teléfono: 01-3152700 anexos3042

1.5.2. Persona de contacto

De parte del Registro Nacional de Identificación y Estado Civil:
Sub Gerente de Regulación Digital.
Dirección de correo electrónico: identidaddigital@reniec.gob.pe
Número de teléfono: 3152700 anexo3042
Dirección: Jr. Bolivia 109, Centro Cívico - Cercado de Lima.

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

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

1.5.4. Procedimiento de aprobación de CP

La AAC decidirá la aprobación de la Política General de Certificación de la ECERNEP mediante los procedimientos establecidos en la "Guía de Acreditación para Entidades de Certificación Digital EC".

1.6. Definiciones y acrónimos

DEFINICIONES:

Se ha tomado como referencia:

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

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

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

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

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

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

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

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

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

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

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

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

Canal seguro.- Es el conducto virtual o físicamente independiente a través del cual se pueden transferir datos garantizando una transmisión confidencial y confiable, protegiéndolos de ser interceptados o manipulados por terceros.

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

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

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

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

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

Código de verificación o resumen criptográfico (hash).- Es la secuencia de bits de longitud fija obtenida como resultado de procesar un documento electrónico con un algoritmo, de tal manera que:

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

(2) Sea improbable a través de medios técnicos, que el documento electrónico pueda ser derivado o reconstruido a partir del código de verificación (resumen) producido por el algoritmo.

(3) Sea improbable por medios técnicos, que se pueda encontrar dos documentos electrónicos que produzcan el mismo código de verificación (resumen) al usar el mismo algoritmo.

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

Criptografía Asimétrica.- Es la rama de las matemáticas aplicadas que se ocupa de transformar documentos electrónicos en formas aparentemente ininteligibles y devolverlas a su forma original, las cuales se basan en el empleo de funciones algorítmicas para generar dos "claves" diferentes pero matemáticamente relacionadas entre sí. Una de esas claves se utiliza para crear una firma numérica o transformar datos en una forma aparentemente ininteligible (clave privada), y la otra para verificar una firma numérica o devolver el documento electrónico a su forma original (clave pública). Las claves están matemáticamente relacionadas, de tal modo que cualquiera de ellas implica la existencia de la otra, pero la posibilidad de acceder a la clave privada a partir de la pública es técnicamente ínfima.

Declaración de Prácticas de Certificación (CPS).- Es el documento oficialmente presentado por una Entidad de Certificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Certificación.

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

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

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

Registro o Verificación acreditada por la AAC.

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

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

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

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

a) Documento Nacional de Identidad (DNI);
b) Carné de extranjería actualizado, para las personas naturales extranjeras domiciliadas en el país; o,
c) Pasaporte, si se trata de personas naturales extranjeras no residentes.

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

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

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

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

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

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

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

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

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

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

Equivalencia funcional.- Principio por el cual los actos jurídicos realizados por medios electrónicos que cumplan con las disposiciones legales vigentes poseen la misma validez y eficacia jurídica que los actos realizados por medios convencionales, pudiéndolos sustituir para todos los efectos legales. De conformidad con lo establecido en la Ley y su Reglamento, los documentos firmados digitalmente pueden ser presentados y admitidos como prueba en toda clase de procesos judiciales y procedimientos administrativos.

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

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

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

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

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

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

1) La integridad de los documentos electrónicos;

2) La identidad de su autor, lo que es regulado conforme a Ley.

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

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

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

- Interoperabilidad a nivel de componentes: consiste en la interacción entre sistemas que soportan o consumen directamente servicios relacionados con PKI.
- Interoperabilidad a nivel de aplicación: consiste en la compatibilidad entre aplicaciones que se comunican entre sí.
- Interoperabilidad entre dominios o infraestructuras PKI: consiste en la interacción de distintos sistemas de certificación PKI (dominios, infraestructuras), estableciendo relaciones de confianza que

permiten el reconocimiento indistinto de los certificados digitales por parte de los terceros que confían.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Políticas de Certificación.- Documento oficialmente presentado por una Entidad de Certificación a la Autoridad Administrativa Competente, mediante el cual se establece, entre otras cosas, los tipos de certificados digitales que podrán ser emitidos, cómo se deben emitir y gestionar los

certificados, y los respectivos derechos y responsabilidades de las Entidades de Certificación. Para el caso de una Entidad de Certificación Raíz, la Política de Certificación incluye las directrices para la gestión del Sistema de Certificación de las Entidades de Certificación vinculadas.

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

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

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

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

a. Prestadores de Servicio de Valor Añadido que realizan procedimientos sin firma digital de usuarios finales, los cuales se caracterizan por brindar servicios de valor añadido, como Sellado de Tiempo que no requieren en ninguna etapa de la firma digital del usuario final en documento alguno.

b. Prestadores de Servicio de Valor Añadido que realizan procedimientos con firma digital de usuarios finales, los cuales se caracterizan por brindar servicios de valor añadido como el sistema de intermediación electrónico, en donde se requiere en determinada etapa de operación del procedimiento la firma digital por parte del usuario final en algún tipo de documento.

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

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

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

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

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

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

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

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

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

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

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

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

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

ACRÓNIMOS:

Vocablo	Significado
AAC	Autoridad Administrativa Competente (en concreto la Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias (CNB) del INDECOPI)
CRL	Certicate Revocation List (Lista de certificados revocados o Lista de certificados cancelados)
CP	Certification Policy (Políticas de Certificación)
CPS	Certification Practice Statement (Declaración de Prácticas de Certificación)
DN	Distinguished Nane (Nombre distinguido o diferenciado)
DNIe	Documento Nacional de Identidad electrónico
DPC	Declaración de Prácticas de Certificación
DPR	Declaración de Prácticas de Registro o Verificación
EC	Entidad de Certificación

ECERNEP	Entidad de Certificación Nacional para el Estado Peruano
ECEP	Entidad de Certificación para el Estado Peruano
ER	Entidad de Registro o Verificación
EREP	Entidad de Registro o Verificación para el Estado Peruano
HSM	Hardware Security Module (Módulo de seguridad de hardware)
INDECOPI	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual
IOFE	Infraestructura Oficial de Firma Electrónica
ISP	Internet Service Provider *(*Proveedor de servicios de internet)
OCSP	Online Certificate Status Protocol (Protocolo del estado en línea del certificado)
PKI	Public Key Infrastructure (Infraestructura de Clave Pública)
PSC	Prestador de Servicios de Certificación Digital
RENIEC	Registro Nacional de Identificación y Estado Civil
SIE	Sistema de Intermediación Electrónico.
TSL	Trusted Services List (Lista de servicios de confianza)

2. Responsabilidades de publicación y repositorio

2.1. Repositorios

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

La ECERNEP comparte repositorios con la ECEP.

Los repositorios públicos son los siguientes:

i. Repositorios para la lista de certificados cancelados.
ii. Repositorio de certificados de Autoridades de la ECERNEP.
iii. Repositorio de la Política General de Certificación.

2.2. Publicación de información sobre certificación

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

i. Repositorios para la lista de certificados cancelados
Especificados en el campo **Punto de distribución de CRL** de los certificados digitales emitidos (Autoridades Intermedias), donde se indican las direcciones URL de descarga de la última CRL emitida.

Para la jerarquía *RENIEC Certification Authority:*
http://crl.reniec.gob.pe/arl/caservices01.crl
http://crl2.reniec.gob.pe/arl/caservices01.crl

Para la jerarquía *RENIEC High Grade Certification Authority:*
http://crl.reniec.gob.pe/arl/hgcaservices01.crl
http://crl2.reniec.gob.pe/arl/hgcaservices01.crl

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

iii. Repositorio de certificados emitidos para la ECERNEP
Los certificados digitales emitidos por la ECERNEP para las Autoridades Intermedias se encuentran publicados en la URL:
http://www.reniec.gob.pe/crt/

Los certificados digitales a publicarse serán únicamente de las Autoridades Intermedias que tengan un uso activo, omitiéndose aquellos certificados de Autoridades Intermedias que aún no sean utilizadas.

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

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

2.3. Tiempo o frecuencia de publicación

i. Repositorios para la lista de certificados cancelados.
La frecuencia de publicación de la CRL vigente se indica en el punto 4.9.7.

ii. Repositorio de certificados de Autoridades de la ECERNEP.
El repositorio de certificados de Autoridades es actualizado de acuerdo a los requerimientos de la ECERNEP, siendo algunos motivos para su modificación:
- Creación de una nueva Autoridad intermedia.
- Adicionar un nuevo formato de descarga para un certificado digital de una Autoridad ya existente.

Dichas actualizaciones son poco frecuentes.

iii. Repositorio de certificados emitidos por la ECERNEP.
Este repositorio es actualizado cada vez que se genera un nuevo certificado digital para alguna Autoridad Intermedia.

iv. Repositorio de la CP.
Los cambios en la Política General de Certificación y Declaración de Prácticas de la ECERNEP, están sujetos a la necesidad de modificación y a la aprobación de la AAC para su puesta en vigencia y publicación respectiva.

2.4. Controles de acceso a los repositorios

El acceso a los repositorios (indicados en los items 2.1 y 2.2 del presente documento) donde la ECERNEP almacena información de interés público, sólo permite la lectura y/o descarga, quedando restringidas las operaciones de actualización del contenido. A las operaciones de actualización sólo tienen acceso las aplicaciones internas con usuarios previamente autorizados y desde puntos de la red interna de la ECERNEP.

Cabe mencionar además, que los repositorios indicados están protegidos por equipos de seguridad de red (firewall), que impiden una manipulación no autorizada.

La ECERNEP gestiona sus repositorios conforme al Documento Técnico “Gestión de Repositorios de la ECERNEP”.

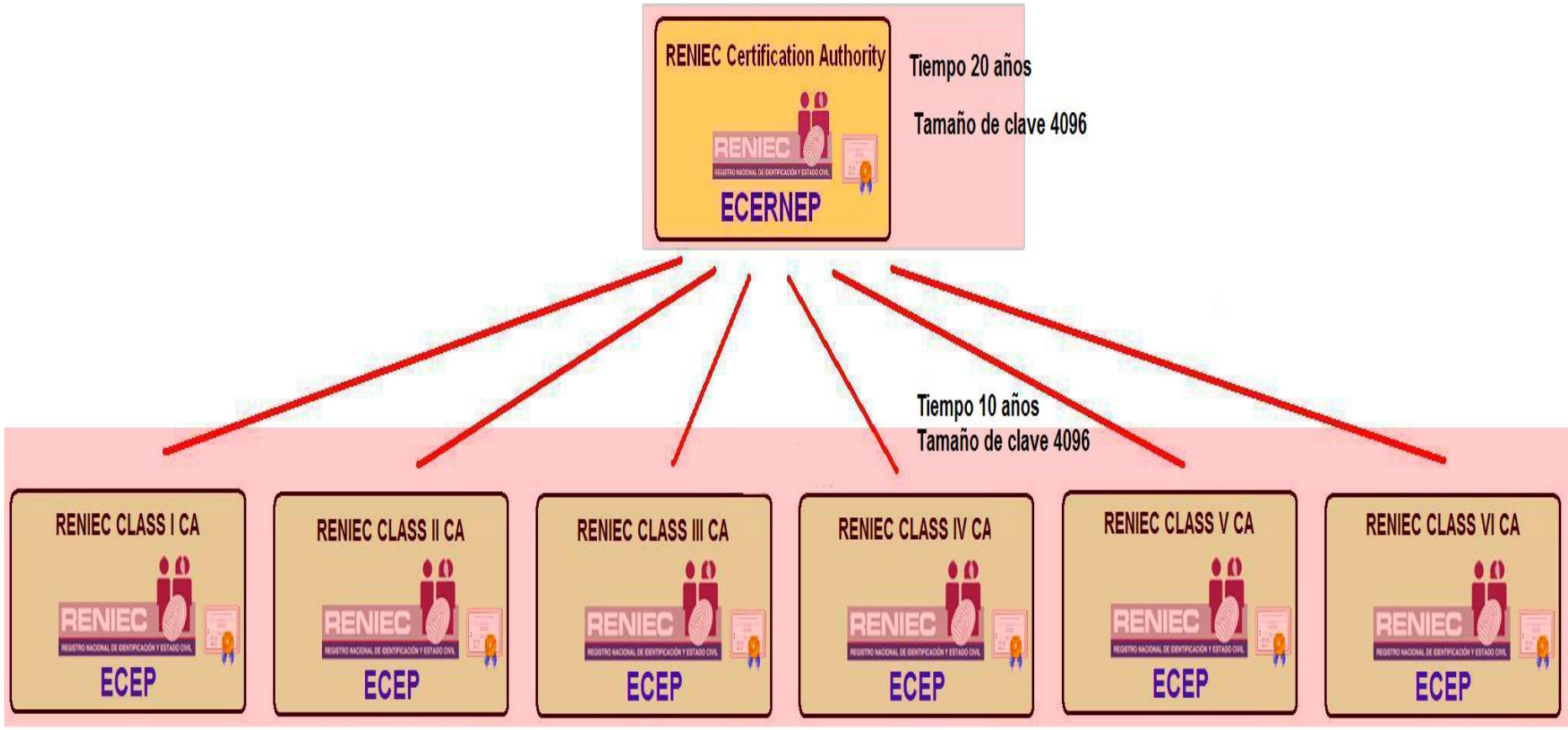
3. Identificación y autenticación

3.1. Nombre

3.1.1. Tipos de nombres

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

i. Nombre distinguido (Distinguished name - DN) X.509:


RENIEC Certification Authority
ECERNEP
Tiempo 20 años
Tamaño de clave 4096
Tiempo 10 años
Tamaño de clave 4096
RENIEC CLASS I CA
ECEP
RENIEC CLASS II CA
ECEP
RENIEC CLASS III CA
ECEP
RENIEC CLASS IV CA
ECEP
RENIEC CLASS V CA
ECEP
RENIEC CLASS VI CA
ECEP

- Tipo: Certificado de Autoridad Jerárquica

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

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

	(SHA-1)	Certification Authority organizationName = Registro Nacional de Identificación y Estado Civil countryName = PE
14	Clase VI Autoridad de Certificación Subordinada (SHA-256)	SerialNumber = <Número de Identificación Peruano registrado por RENIEC> commonName = RENIEC Class VI High Grade CA organizationalUnitName = RENIEC Certification Authority organizationName = Registro Nacional de Identificación y Estado Civil countryName = PE

El campo Nombre distinguido (Distinguished name - DN) debe identificar de forma única y plena a una autoridad raíz y a las intermedias.

En concordancia con lo establecido por la AAC en la Resolución Nº 123-2016/CFE-INDECOPI, la ECERNEP emitirá certificados digitales firmados con el algoritmo SHA-1 solo hasta el 30 de junio de 2017 y a partir del 1 de julio de 2017 únicamente emitirá certificados con el algoritmo SHA-256. De igual manera deberán proceder las ECEP. No obstante, los certificados generados con el algoritmo SHA-1 hasta el 30 de junio de 2017 mantendrán su validez dentro de su plazo de vigencia y solo serán cancelados bajo los supuestos contemplados en el Reglamento de la Ley de Firmas y Certificados Digitales. Los SVA para el Estado Peruano cumplirán a este respecto con lo señalado en el artículo tercero de la citada resolución.

3.1.2. Necesidad de que los nombres tengan un significado

Los campos del certificado mostrado en la tabla del ítem 3.1.1 para cada clase (Autoridades Intermedias) son "significativos" debido a que garantizan que se pueda determinar la identidad de la autoridad.

Este campo permitirá el reconocimiento del tipo de certificado de entidad final de acuerdo a la Autoridad Intermedia que la emitió cuando se construya la cadena de certificación (el Nombre Distinguido identificará que Autoridad intermedia lo emitió).

3.1.3. Anonimato o seudónimo de los suscriptores

No se permite el anonimato en los campos relacionados a la identidad de una Autoridad intermedia. Tampoco está contemplado el uso de seudónimos.

3.1.4. Reglas para interpretar las diferentes modalidades de nombres

La regla utilizada para interpretar los Nombre Distinguido (Distinguished Name - DN) de certificados que emite es la ISO/IEC 9595 (X.500) Distinguished Name.

3.1.5. Singularidad de los nombres

Los nombres de las Autoridades Intermedias son únicos para poder identificarlos plenamente, tal como está descrito en el cuadro del ítem 3.1.1.

3.1.6. Reconocimiento, autentificación y rol de marcas registradas

Tal como muestra el cuadro del ítem 3.1.1. no se hace uso de marcas registradas en los nombres de las Autoridades Intermedias. En los casos en que se requiera emitir un certificado de Autoridad Intermedia con una nomenclatura diferente el beneficiario deberá sustentar dicho nombre y el permiso de uso ante la ECERNEP.

3.2. Validación inicial de la identidad

Debido a que el RENIEC es una entidad constitucionalmente autónoma y pública a cargo de la ECERNEP y la ECEP, la validación inicial de la identidad es innecesaria. En caso de emitirse un certificado intermedio para otro ente diferente al mencionado deberá verificarse su constitución y aspectos en el marco de la Ley vigente de Firmas y Certificados Digitales.

3.2.1. Método para probar la posesión de la clave privada

La prueba de posesión de clave privada se realiza mediante la firma del pedido de certificado (request firmado). Este proceso es realizado por el RENIEC en una ceremonia de claves, tal como queda descrito en el acta correspondiente.

3.2.2. Autenticación de la identidad de la persona jurídica

Debido a que es el RENIEC una entidad pública reconocida en la Constitución Política del Perú como organismo autónomo quien se encuentra a cargo de la ECERNEP y la ECEP, la autenticación de su identidad es innecesaria.

En caso de emitirse un certificado intermedio para otro ente de la Administración Pública diferente al mencionado, deberá verificarse su constitución, la designación de su representante legal y otros aspectos bajo el marco de la Ley de Firmas y Certificados Digitales y su Reglamento.

Respecto a la determinación de las entidades de la Administración Pública hábiles para solicitar un certificado intermedio, se considerará para tal fin a aquellas comprendidas en el Artículo I del Título Preliminar de la Ley Nº 27444 – Ley del Procedimiento Administrativo General, las cuales deberán presentar una solicitud firmada por el máximo representante de la entidad, adjuntando la resolución de acreditación emitida por la AAC.

Para la emisión de certificados digitales de entidad final para persona jurídica las ECEP deberán proceder bajo las mismas consideraciones que se detalla en los párrafos precedentes del presente numeral.

3.2.3. Autenticación de la identidad individual

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

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

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

La ECERNEP no emite certificados digitales a personas naturales, no obstante, efectuará la autenticación de la identidad de los representantes legales de las entidades solicitantes de la administración pública conforme se describe en los numerales precedentes del presente numeral.

3.2.4. Información no verificada del suscriptor

No es necesaria en caso de la ECERNEP.

3.2.5. Validación de la Autoridad

No es necesaria en caso de la ECERNEP.

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

La ECERNEP acreditada, con su Política General de Certificación debidamente aprobada y conforme a las Guías y Reglamentos de Acreditación emitidos por el INDECOPI, está facultada para interactuar en el marco de la IOFE y realizar el reconocimiento cruzado.

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

La ECERNEP no brinda el servicio de re-emisión de certificados.

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

La ECERNEP no brinda el servicio de re-emisión de certificados.

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

La ECERNEP no brinda el servicio de re-emisión de certificados.

3.4. Identificación y autenticación de la solicitud de cancelación

La ECERNEP procesa todos los pedidos de cancelación de certificados digitales por escrito y requeridos por la ECEP, siendo esta última la responsable de administrar los certificados digitales de las Autoridades Intermedias.

4. Requisitos operacionales del ciclo de vida de los certificados

Los procesos del ciclo de vida de un certificado digital de Autoridades Intermedias, se definen como:

4.1. Solicitud del certificado

La ECERNEP procesa todos los pedidos de solicitud de certificado requeridos por la ECEP, conforme a lo indicado en sus procedimientos internos; siendo la ECEP la responsable de administrar los certificados digitales de las Autoridades Intermedias.

4.1.1. Habilitados para presentar la solicitud de un certificado.

La ECEP es un ente autorizado y válido para solicitar la emisión de un certificado digital para ser usado por una Autoridad intermedia. En caso de emitirse un certificado intermedio para otro ente diferente al mencionado deberá verificarse su constitución y aspectos en el marco de la Ley vigente de Firmas y Certificados Digitales.

4.1.2. Proceso de solicitud y responsabilidades

Es atribución de la ECERNEP aceptar una solicitud con datos correctos declarados por la ECEP según lo indicado en el ítem 3.1.6 del presente documento.

4.2. Procesamiento de la solicitud del certificado

4.2.1. Realización de las funciones de identificación y autenticación

Debido a que la ECERNEP y la ECEP es administrada por el mismo ente (RENIEC) la verificación de este punto es innecesario. En caso de emitirse un certificado intermedio para otro ente diferente al antes mencionado, la ECERNEP verificará su constitución y aspectos en el marco de la Ley vigente de Firmas y Certificados Digitales.

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

Es atribución de la ECERNEP aceptar una solicitud con datos correctos declarados por la ECEP según lo indicado en el ítem 3.1.6 del presente documento. En caso de emitirse un certificado intermedio para otro ente diferente al antes mencionado, la ECERNEP deberá verificar su constitución y aspectos en el marco de la Ley vigente de Firmas y Certificados Digitales.

4.2.3. Tiempo para el procesamiento de la solicitud del certificado

Una vez aprobada la solicitud por la ECERNEP, la Autoridad intermedia deberá establecer los detalles relevantes a una ceremonia de claves, en la cual se generará el par de claves utilizando un dispositivo criptográfico (HSM) que cumpla con el estándar FIPS 140-2 nivel 3 y el certificado digital respectivo, firmado por la Autoridad Raíz.

El tiempo de emisión de un certificado digital se precisa en el documento *"Gestión de la Emisión de los certificados digitales para usuarios de la ECERNEP"*.

4.3. Generación de claves y emisión del certificado

4.3.1. Acciones de la EC durante la emisión del certificado

Una vez autorizado el pedido de emisión de certificado digital para una Autoridad intermedia, la ECERNEP y la Autoridad intermedia deberán establecer los detalles relevantes a una ceremonia de claves en la cual se generará el par de claves utilizando un dispositivo criptográfico (HSM) que cumpla con el estándar FIPS 140-2 nivel 3 y el certificado digital respectivo, firmado por la Autoridad Raíz.

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

La Autoridad Intermedia participa de la ceremonia de claves por lo que tendrá permanentemente conocimiento del proceso de emisión del certificado digital, siendo innecesaria su notificación.

Además los certificados de autoridades generados serán publicados en la página web oficial del RENIEC y en los repositorios respectivos. Para mayor detalle respecto a los repositorios ver el ítem 2.1 del presente documento.

4.4. Aceptación del certificado

4.4.1. Conducta constitutiva de la aceptación de un certificado

Debido a que la ECERNEP y la ECEP son administradas por el mismo ente (RENIEC) la verificación de este punto es innecesario. En caso de emitirse un certificado digital intermedio para otro ente diferente al antes mencionado, deberá verificarse su constitución y aspectos en el marco de la Ley vigente de Firmas y Certificados Digitales.

4.4.2. Publicación del certificado por parte de la EC

La información concerniente al certificado digital emitido será publicada en el Repositorio de la ECERNEP indicado en el ítem 2.2 del presente documento.

La ECERNEP provee el servicio de consulta al Repositorio (para determinar la validez de los certificados digitales). La disponibilidad permanente de estos repositorios son soportados tecnológicamente por el RENIEC, acorde a lo mencionado por la AAC en el Anexo 1 "Marco de la política de emisión de certificados digitales" de su Guía de Acreditación para Entidades de Certificación, la cual indica que es conveniente una disponibilidad mínima de 99% anual, con un tiempo programado de inactividad máximo de 0.5% anual.

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

La ECERNEP, posterior la emisión del certificado digital procederá a publicar el mismo y comunicará a la AAC sobre la creación de esta nueva Autoridad Intermedia para su tratamiento correspondiente**.**

4.5. Par de claves y uso del certificado

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

La ECERNEP exige a la Autoridad intermedia, lo siguiente:

- Emplear el certificado digital de acuerdo con lo establecido en la Política General de Certificación de la ECERNEP u otro documento relevante dado por ésta.
- Ser diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados.
- En caso que la clave privada sea comprometida la Autoridad Intermedia deberá informar de manera inmediata a la ECERNEP para su cancelación.

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

La IOFE permite al tercero que confía tener acceso a los certificados digitales publicados en el Repositorio. La ECERNEP requiere del tercero que confía, como mínimo lo siguiente:

- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de la IOFE.

- No comprometer la seguridad de la Jerarquía de la IOFE.
- Aplicar los criterios de verificación adecuados para la validación de un certificado durante su uso en las transacciones electrónicas.
- Denunciar cualquier situación en la que la ECERNEP deba cancelar el certificado de la Autoridad Intermedia, siempre y cuando se tengan pruebas fehacientes del compromiso de la clave privada o de un uso ilegal en el manejo de la misma. 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.

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

4.6. Renovación del certificado

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

4.6.1. Circunstancias para la re-certificación de los certificados

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

4.6.2. Personas habilitadas para solicitar la renovación

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

4.6.3. Procesamiento de la solicitud de renovación de certificado.

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

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

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

4.6.5. Conducta constitutiva de aceptación de renovación de certificado

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

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

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

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

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

4.7. Re-emisión de certificado.

Este servicio no es brindado por la ECERNEP.
En caso de compromiso de las claves privadas de la ECEP se procederá de acuerdo a lo indicado en el ítem 4.9.12 del presente documento.

4.7.1. Circunstancias para la re-emisión de un certificado

Este servicio no es brindado por la ECERNEP.

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

Este servicio no es brindado por la ECERNEP.

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

Este servicio no es brindado por la ECERNEP.

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

Este servicio no es brindado por la ECERNEP.

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

Este servicio no es brindado por la ECERNEP.

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

Este servicio no es brindado por la ECERNEP.

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

Este servicio no es brindado por la ECERNEP.

4.8. Modificación del certificado

Este servicio no es brindado por la ECERNEP.

4.8.1. Circunstancias para la modificación de un certificado

Este servicio no es brindado por la ECERNEP.

4.8.2. Personas habilitadas para solicitar la modificación de un certificado

Este servicio no es brindado por la ECERNEP.

4.8.3. Circunstancias para la modificación de un certificado

Este servicio no es brindado por la ECERNEP.

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

Este servicio no es brindado por la ECERNEP.

4.8.5. Conducta constitutiva de la aceptación de un certificado modificado

Este servicio no es brindado por la ECERNEP

4.8.6. Publicación por parte de la EC del certificado modificado

Este servicio no es brindado por la ECERNEP.

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

Este servicio no es brindado por la ECERNEP.

4.9. Cancelación y suspensión del certificado

4.9.1. Circunstancias para la cancelación

La ECERNEP aceptará el pedido de cancelación de certificado de la Autoridad Intermedia y de los terceros que confían, debiendo sustentarse el motivo o razón de la cancelación. Adicionalmente la ECERNEP podrá realizar la cancelación del certificado digital en caso de extinción de la persona jurídica asociada a la Autoridad Intermedia.

La ECERNEP comunicará la cancelación a la AAC para las acciones pertinentes.

El detalle de lo indicado en el presente ítem se encuentra descrito en el documento "*Gestión de la cancelación de certificados digitales para usuarios de la ECERNEP"*.

4.9.2. Personas habilitadas para solicitar la cancelación

Únicamente se aceptarán los pedidos de cancelación de certificados digitales de las Autoridades Intermedias, a través de su

representante, el cual debe haber sido debidamente autorizado por ésta y de los terceros que confían.

El detalle de lo indicado en el presente ítem se encuentra descrito en el documento "*Gestión de la cancelación de certificados digitales para usuarios de la ECERNEP*".

4.9.3. Procedimiento para la solicitud de cancelación

Una vez enviado el pedido por parte de la Autoridad Intermedia o por el tercero que confía, la ECERNEP evaluará dicho pedido y procederá a la cancelación del certificado digital indicado, posterior a esto comunicará a la AAC y finalmente procederá a la generación y publicación de la CRL. El detalle está descrito en el documento "*Gestión de la cancelación de certificados digitales para usuarios de la ECERNEP*".

4.9.4. Período de gracia de la solicitud de cancelación

Una vez que existe la autorización por parte de la ECERNEP, se procederá de manera inmediata a cancelar el certificado digital, publicándose su estado en los repositorios respectivos, según lo indicado en el ítem 2.3 del presente documento.

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

La ECERNEP procesará de manera inmediata cualquier pedido de cancelación cursada por la Autoridad Intermedia o por el tercero que confía, cumpliendo con lo especificado en los ítems 4.9.2 y 4.9.3 del presente documento. El detalle está descrito en el documento "*Gestión de la cancelación de certificados digitales para usuarios de la ECERNEP*".

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

Una vez realizada la cancelación de un certificado digital por parte de la ECERNEP, ésta publicará su estado en los repositorios respectivos de acuerdo lo indicado en el ítem 2.3 del presente documento, notificando de esta manera a todos los interesados. El detalle de la publicación se encuentra descrito en el documento "*Gestión de Repositorios*".

4.9.7. Frecuencia de emisión de CRL

La ECERNEP actualiza su lista de certificados cancelados (CRL) por lo menos cada seis (6) meses o cuando se cancele algún certificado de Autoridad intermedia, publicándose en sus repositorios en un plazo máximo de 24 horas considerando el plazo de latencia así establecido y contemplando lo indicado en el ítem 2.1 del presente documento.

Además provee una disponibilidad para la CRL como mínimo de 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

4.9.8. Máxima Latencia para CRLs

La latencia entre la generación y la publicación de una CRL es como máximo de un día, debido a que la publicación se realiza de forma manual. El detalle de la publicación se encuentra descrito en el documento "*Gestión de Repositorios*".

4.9.9. Disponibilidad de la verificación en línea cancelación /estado

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

4.9.10. Requisitos para la verificación en línea de la cancelación

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

4.9.11. Otras formas disponibles de publicar la cancelación

La lista de certificados cancelados (CRL) emitidos por la ECERNEP son publicados en más de un repositorio, los cuales están indicados en cada uno de los certificados digitales que ésta emite.

Según refiere la Guía de Acreditación para Entidades de Certificación en el ítem 4.9.11 del Anexo I: "Cuando la publicación de una cancelación pueda reducir el daño potencial a los terceros que confían, INDECOPI permite que una EC o un suscriptor afectado puedan emplear diferentes formas para realizar dicha publicación.", por lo expuesto, de requerirlo la ECERNEP se permitirá publicar en algún otro repositorio adicional para satisfacer el requerimiento y necesidad.

El detalle de la publicación se encuentra descrito en el documento "*Gestión de Repositorios*".

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

La ECERNEP notificará en un lapso máximo de 24 horas a la AAC respecto a incidencias que produzcan el compromiso de sus claves privadas o su imposibilidad de uso.

En caso de compromiso de las claves privadas de la ECERNEP, ésta cancelará los certificados emitidos y notificará de forma inmediata a los entes afectados.

4.9.13. Circunstancias para la suspensión

La ECERNEP no brinda servicio de suspensión de certificados digitales.

4.9.14. Personas habilitadas para solicitar la suspensión

La ECERNEP no brinda servicio de suspensión de certificados digitales.

4.9.15. Procedimiento para solicitar la suspensión

La ECERNEP no brinda servicio de suspensión de certificados digitales.

4.9.16. Límite del periodo de suspensión

La ECERNEP no brinda servicio de suspensión de certificados digitales.

4.10. Servicios de estado de certificado

La ECERNEP mantiene una copia de la lista de entidades acreditadas (TSL), la cual es proporcionada por INDECOPI.

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

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

4.10.1. Características Operacionales

Cualquier información publicada por la ECERNEP respecto al estado de uno de sus certificados (a través de la CRL) es firmada digitalmente por la ECERNEP. La hora y fecha son consignadas por la ECERNEP ejecutando la sincronización correspondiente como parte del procedimiento de emisión de CRL.

4.10.2. Disponibilidad del servicio

La ECERNEP brinda el servicio de información sobre el estado del certificado a través de sus CRLs con un mínimo de 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

4.10.3. Rasgos Operacionales

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

4.11. Finalización de la suscripción

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

- Caducidad de la vigencia del certificado digital.
- Por cancelación del certificado digital por cualquiera de las circunstancias señaladas en el ítem 4.9.1 del presente documento.

4.12. Depósito y recuperación de claves

4.12.1. Políticas y prácticas de recuperación de Depósito de claves

No está permitido para la ECERNEP el almacenamiento del original, copia o backup alguna de las claves privadas de certificados digitales emitidos por ésta.

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

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

No es parte del alcance que ofrece la ECERNEP.

5. Controles de las instalaciones, de la gestión y controles operacionales

5.1. Controles físicos

5.1.1. Ubicación y construcción del local

Las características de las instalaciones de la ECERNEP son:

- Puertas cortafuego blindadas para el acceso del personal autorizado.
- La puerta de acceso principal cuenta con personal de seguridad que verifica que sólo personas autorizadas puedan acceder a la misma.
- El acceso a zonas de alta seguridad está restringida por controles biométricos.
- Los ambientes que constituyen las instalaciones de la ECERNEP, cuentan con las estructuras y secciones necesarias, que garantizan que sólo el personal autorizado los pueda acceder.

Para el acceso del personal a los ambientes de la ECERNEP, se realiza una identificación previa y registro del mismo en el sistema de control de acceso. El ingreso de visitas y proveedores se efectúa

previo permiso y conforme a lo establecido en el documento "*Control de acceso físico*".

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

i. Ante desastres naturales:
- Inundación.- Protección mediante tarrajeo impermeabilizado y hermetizado y detectores de aniego debajo del piso técnico.
- Terremoto.- Los equipos y documentación utilizados por la ECERNEP se encuentran resguardados en una caja fuerte.

ii. Desastres accidentales creados por el hombre:
- Incendios.- Se cuenta con extintores y puertas corta fuego con barra anti-pánico desde el interior.
- Explosiones.- Se cuenta con extintores, cerramiento del perímetro mediante paredes, piso, techo de concreto y puerta cortafuego.
- Disturbios civiles.- Los ambientes cuentan con un sistema de puertas blindadas, sistema de cámaras que graban las actividades tanto al personal como a los invitados desde su ingreso a las instalaciones de la ECERNEP, además se cuenta con un sistema de control de acceso biométrico, que garantiza que sólo el personal autorizado pueda ingresar a las instalaciones de la ECERNEP.

5.1.2. Acceso físico

Perímetros de seguridad física:
Cerramiento del perímetro mediante paredes, piso y techo de concreto, y puerta cortafuego.

Controles físicos de entrada:
Se dispone de un sistema de control de acceso físico a la entrada y a la salida que conforman varios niveles de control, lo cual se encuentra detallado en el documento "*Control de acceso físico*".
En áreas donde se guardan componentes de la ECERNEP no se permiten visitas.

5.1.3. Energía y aire acondicionado

Los equipos que almacenan información relevante a la ECERNEP se encuentran apagados y sin alimentación de energía eléctrica, por lo cual, tanto la energía como aire acondicionado son innecesarios.

En caso se requiera activar o utilizar los componentes tecnológicos de la ECERNEP, estos son llevados a un área segura con energía eléctrica, previa autorización y conforme a los procedimientos correspondientes para la emisión y cancelación de certificados digitales para usuarios de la ECERNEP..

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. Prevención y protección contra fuego

En los ambientes de la ECERNEP se cuenta con sensores de humo y con extintores en ubicaciones señalizadas.

5.1.6. Archivo de material

Los componentes tecnológicos y documentos que pertenecen a la ECERNEP cuentan con:

- Protección de acceso físico: más de 03 niveles de puertas desde el exterior, más de 2 de estos niveles protegidos por acceso biométrico y el último de ellos es protegido por doble acceso biométrico.
- Protección en caja de seguridad: caja fuerte cuya apertura se efectúa únicamente por un personal autorizado.

5.1.7. Gestión de residuos

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

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

5.1.8. Copia de seguridad externa

Por la naturaleza de su información la ECERNEP no maneja copias de seguridad externa para su información crítica.

5.2. Controles procesales.

5.2.1. Roles de confianza

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

Dichos roles se encuentran descritos en la "Memoria Descriptiva y organigrama funcional de la ECERNEP".

5.2.2. Número de personas requeridas por labor

La asignación de roles en la ECERNEP ha sido aprobado, documentada y estandarizada de acuerdo al documento "Memoria Descriptiva y organigrama funcional de la ECERNEP".

5.2.3. Identificación y autenticación para cada rol

Los requerimientos de cada rol, competencias y el detalle de sus actividades se encuentran descritos en el documento denominado "Memoria Descriptiva y organigrama funcional de la ECERNEP".

5.2.4. Roles que requieren funciones por separado

Con el fin de mantener una adecuada separación de funciones, se han definido diferentes roles, los cuales se detallan en el documento "Memoria Descriptiva y organigrama funcional de la ECERNEP".

5.3. Controles de personal

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

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

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

5.3.1. Cualidades y requisitos, experiencia y certificados

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

Las prácticas de selección y reclutamiento de personal se llevan a cabo en la Gerencia de Recursos Humanos del RENIEC tomándose como referencia lo establecido en el *"Reglamento Interno de Trabajo"*, y lo requerido en los perfiles fijados por la ECERNEP, donde se considera

requisitos de experiencia y cualificación para cada personal, además del rol que desempeñará.

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

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

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

5.3.2. Procedimiento para verificación de antecedentes

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

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

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

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

5.3.3. Requisitos de capacitación

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

El contenido de los programas de capacitación se controla y refuerza periódicamente, llevándose un registro y archivo de las materias

impartidas para los efectos de las re-capacitaciones a las que se alude en la sub sección 5.3.4 del presente documento.

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

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

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

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

5.3.4. Frecuencia y requisitos de las re-capacitaciones

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

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

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

5.3.5. Frecuencia y secuencia de la rotación en el trabajo

La ECERNEP, en caso lo determine conveniente, podrá establecer métodos de rotación laboral para la prestación del servicio.

5.3.6. Sanciones por acciones no autorizadas

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

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

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

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

5.3.7. Requerimientos de los contratistas

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

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

5.3.8. Documentación suministrada al personal

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

- Reglamento de Organizaciones y Funciones (ROF) y Manual de Organizaciones y Funciones (MOF).
- Política General de Certificación y Declaración de Prácticas.
- La documentación que define las obligaciones y procedimientos de cada rol.
- Manual de funcionamiento de equipos y software que debe operar en la ECERNEP.
- Normas Legales y marco regulatorio aplicables a sus funciones en la ECERNEP.
- Documento relativo al ciclo de vida de los certificados digitales e instructivos o procedimientos de trabajo.
- Documentación aplicable respecto a su rol dentro del "*Plan de Recuperación y Continuidad de la Planta de Certificación Digital*".

5.4. Procedimiento de registro de auditorías

5.4.1. Tipos de eventos registrados

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

- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios (registro de eventos en equipos que manejen información de la ECERNEP).
- Intentos de entrada y salida (registro de eventos en equipos que manejen información de la ECERNEP).
- Generación de claves de la ECERNEP (registro de eventos de módulo criptográfico).
- Los registros de auditoría de eventos registran la fecha, hora e identificadores software/hardware.
- La ECERNEP registra de manera manual o electrónica, como mínimo, la siguiente información:
  - Acceso físico a las áreas sensibles según **"***Control de acceso físico***".**
  - Cambios en el personal.

5.4.2. Frecuencia del procesamiento del registro

Se tiene establecido las fechas, frecuencias, objetivos, estándares, guías, procedimientos y documentación pertinente, para lograr evidencia suficiente y competente para obtener y sustentar las conclusiones y opiniones de auditoría.

Los registros de auditoría deben ser procesados y revisados una vez al mes como mínimo según el documento de "Gestión de registros de auditoría de la ECERNEP" y el "*Plan anual de auditorías internas de la ECERNEP*"**.**

5.4.3. Periodo de conservación del registro de auditorías

En cumplimiento de lo establecido por la AAC, la conservación del registro de auditorías será como máximo por un periodo de diez (10) años, tal como lo indica la **"***Gestión de registros de auditoría de la ECERNEP***"**.

5.4.4. Protección del registro de auditoría

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

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

5.4.5. Procedimiento de copia de seguridad del registro de auditorías

En la ECERNEP, se realizan copias de seguridad completas de los registros de auditoría, conforme a lo especificado en el documento "Procedimiento de copia de seguridad de la ECERNEP".

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

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

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

5.4.7. Notificación al titular que causa un evento

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

5.4.8. Valoración de vulnerabilidad

La ECERNEP cuenta con hardware y software que cumplen con altos estándares de seguridad, tales como Common Criteria EAL4+ y FIPS 140-2 nivel 3. El análisis de las vulnerabilidades es efectuado por los fabricantes, quienes al identificarlas efectúan los ajustes

necesarios para ser puestas a disposición del usuario del hardware o software.

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

5.5. Archivo de registro

5.5.1. Tipos de eventos registrados

Los eventos que la ECERNEP mantendrá serán:

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

La ECERNEP es responsable del correcto archivamiento de estos registros. Para ello se guiará de lo indicado en el documento "*Gestión de registros de auditoría de la ECERNEP*" y "*Gestión de archivo de la ECERNEP*".

5.5.2. Periodo de conservación del archivo

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

5.5.3. Protección del archivo

Los archivos de registro son:
i. Físicamente protegidos.
ii. Lógicamente protegidos.
iii. Supervisados para evitar el empleo inadecuado.

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

5.5.4. Procedimientos para copia de seguridad del archivo

La ECERNEP realiza copias de seguridad completas, tanto de la información como del software (primordial para el funcionamiento de la ECERNEP). Estas copias son probadas en su integridad con regularidad por el personal autorizado.

5.5.5. Requisitos para los archivos de sellado de tiempo

Los sistemas de la ECERNEP para proteger los archivos de registro realizan una marca de fecha y hora en el instante en que se genera el registro.

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

Las copias de seguridad de la ECERNEP, se mantienen de forma interna (almacenada en dispositivos al interior de la Planta de Certificación Digital – PKI). El detalle es especificado en el DT " Copia de seguridad de la ECERNEP".

5.5.7. Procedimiento para obtener y verificar la información del archivo

Dependiendo de la naturaleza de la información contenida en el archivo, el acceso a ésta se efectuará de acuerdo a los privilegios asignados a los usuarios autorizados y conforme a la clasificación de la información establecida en el documento "Gestión de archivo de la ECERNEP".

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

5.6. Cambio de clave

Bajo la jerarquía RENIEC High Grade Certification Authority la ECERNEP no brinda el servicio de cambio de clave.

5.7. Recuperación frente al compromiso y desastre

El Plan de Contingencias de la ECERNEP incluye un procedimiento documentado para la gestión de contingencias en caso de falla o interrupción, 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.

5.7.1. Procedimiento de manejo de incidentes y compromisos

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

Dichos mecanismos contemplan que ante la detección de un supuesto incidente o violación de la seguridad de información,

deberán ser comunicados a través de canales pre-establecidos tan pronto como se haya tomado conocimiento, al Oficial de Seguridad de Información para las acciones correspondientes.

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

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

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

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

En caso, la clave de la ECERNEP fuera comprometida de manera real o potencial, ésta deberá ser inmediatamente cancelada, notificándose el hecho en un lapso máximo de 24 horas a la AAC y comunicará también el hecho a las Entidades Intermedias afectadas.

Asimismo, las Entidades de Certificación afectadas comunicarán a sus respectivas Entidades de Registro, para que informen a los suscriptores afectados, que los certificados suministrados que tienen como raíz a la ECERNEP, han dejado de ser válidos; estando los usuarios en la facultad de apersonarse a las oficinas de la correspondiente EREP para solicitar la emisión de un nuevo certificado digital.

5.7.4. Capacidad de continuidad del negocio luego de un desastre

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

- Recepción de solicitudes de emisión de certificados digitales, encaminadas por la ECEP.
- Emisión de certificados digitales.
- Recepción de solicitudes de cancelación de certificados digitales, encaminadas por la ECEP.
- Cancelación de certificados digitales.
- Generación y publicación de la lista de certificados cancelados.

5.8. Finalización de la EC o ER

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

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

6. Controles de seguridad técnica

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

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

Para la generación de claves de Autoridades Intermedias, se requiere que el proceso se desarrolle en medios criptográficos que cuenten con las certificaciones FIPS 140-2 nivel 3 y Common Criteria EAL4+.

6.1.2. Entrega al suscriptor de la clave privada

La clave privada es generada por la ECEP y siempre se encuentra bajo su control. Dicha clave será generada en una ceremonia de claves organizada por la ECEP en la cual la ECERNEP será una participante activa al firmar los pedidos de certificado para las Autoridades Intermedias.

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

Cuando la ECEP genere su par de claves de Autoridad Intermedia, el pedido de certificado (incluida la clave pública) es entregado a la ECERNEP, para la generación del certificado y su posterior publicación.

El detalle de lo indicado en este ítem se encuentra descrito en el documento "*Gestión de la emisión de certificados digitales para usuarios de la ECERNEP".*

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

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

6.1.5. Tamaño de claves

La ECERNEP mantiene el siguiente tamaño de claves:

Certificados de la ECERNEP	
Algoritmo de Firma	SHA-256
Nombre del Certificado	Reniecrootca1HG
Tamaño de clave	4096

Nota: En concordancia con lo establecido por la AAC en la Resolución Nº 123-2016/CFE-INDECOPI, la ECERNEP emitirá certificados digitales firmados con el algoritmo SHA-1 solo hasta el 30 de junio de 2017 y a partir del 1 de julio de 2017 únicamente emitirá certificados con el algoritmo SHA-256.

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

La ECERNEP valida la clave pública de la ECEP y se asegura de que no pertenezca a otra Autoridad Intermedia. Este proceso se realiza para todo ámbito de la Autoridad Raíz o Certificado Raíz y es parte del procedimiento de emisión de certificados digitales.

6.1.7. Propósitos del uso de las claves

Los propósitos de claves permitidas y establecidas por la ECERNEP para las Autoridades Intermedias son determinados de acuerdo a lo descrito en el documento **"***Perfiles de Certificado Digital ECERNEP***"** y a lo indicado en el ítem 1.4 del presente documento.

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

6.2.1. Estándares y controles para el módulo criptográfico

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

- FIPS 140-2 nivel 3.
- Common Criteria EAL4+.

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

- Para la generación y uso de las claves privadas se requiere de la concurrencia de 3 personas de un conjunto de 6 autorizadas.
- Para el acceso físico a las claves privadas se requiere de la concurrencia de 2 persona de un conjunto de 3 autorizadas.

Nota: k de m, donde:

k = número de personas concurrentes.
m = total de personas autorizadas.

6.2.3. Depósito de clave privada

La ECERNEP no admite el depósito, almacenamiento o copia de claves privadas de ningún tipo.

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

Bajo la jerarquía *RENIEC High Grade Certification Authority* no está permitida la copia de seguridad de la clave privada de la ECERNEP.

Existe un único dispositivo criptográfico que contiene las claves privadas de la ECERNEP, pero de requerirse, la ECERNEP está en facultad de migrar a un dispositivo criptográfico adicional, lo cual es permitido por motivos de operatividad; estás claves son ilegibles fuera del HSM y están protegidas por los estándares de seguridad FIPS 140-2 nivel 3 y Common Criterian EAL4+.

6.2.5. Archivo de la clave privada

La ECERNEP no archiva la clave privada de ninguna Autoridad Intermedia.

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

La clave privada de la ECERNEP ha sido generada y es mantenida en el módulo criptográfico (HSM) que se encuentra almacenada en un ambiente seguro.

En caso de transferencia hacia otro equipo HSM, se seguirá lo indicado en el ítem 6.2.4 del presente documento.

6.2.7. Almacenamiento de la clave privada en un módulo criptográfico

La clave privada de la ECERNEP es generada y mantenida en el módulo criptográfico (HSM) de la Planta de Certificación Digital.
Los módulos criptográficos usados por la ECERNEP están certificados bajo los estándares FIPS 140-2 nivel 3 y Common Criteria EAL4+.

6.2.8. Método de activación de la clave privada

Para el uso de la clave privada de la ECERNEP se requiere de por lo menos tres personas autorizadas con las tarjetas de acceso y las claves pertinentes para su uso. La activación de la clave privada es parte de los procedimientos de emisión de certificados digitales y de listas CRL de la ECERNEP.

6.2.9. Método de desactivación de la clave privada

Las claves privadas de la ECERNEP se encuentran en un equipo HSM que se encuentra desconectado, por lo cual éstas se encuentran inactivas, requiriéndose de las tarjetas de acceso y contraseñas respectivas para su uso.

En cuanto a las claves privadas de la ECEP, éstas deben asegurarse de que se encuentran en un HSM con acceso restringido; para la activación del uso de las mismas se debe contar con controles de acceso lógico y físico adecuados.

6.2.10. Método de destrucción de la clave privada

En caso se requiera la destrucción de la clave privada por parte de la ECEP, primero deberá realizarse el procedimiento de cancelación del certificado (ver ítem 3.4 del presente documento), y luego debe eliminar su clave privada del equipo que almacena dicha clave.

6.2.11. Clasificación del módulo criptográfico

- Para la ECERNEP:
  Los módulos criptográficos usados cumplen los siguientes requerimientos:
  - FIPS 140-2 nivel 3
  - Common Criteria EAL4+
- Para la Autoridad Intermedia:
  Los módulos criptográficos usados por la Autoridad Intermedia para almacenar sus certificados digitales deben cumplir con al menos uno de los siguientes estándares:
  - FIPS 140-2 nivel de seguridad 3 como mínimo
  - Common Criteria EAL4+.

6.3. Otros aspectos de la gestión del par de claves

6.3.1. Archivo de la clave publica

Las claves públicas o los certificados que las contengan, son almacenados en los repositorios de certificados de la ECERNEP y son custodiadas según lo establecido en el documento **"***Gestión de Repositorios de la ECERNEP***"**.

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

A continuación se muestra los periodos operacionales de los certificados de la ECEP emitidos por la ECERNEP:

Clase	Tipo de persona	Tiempo	Tamaño de clave

Clase I	Persona Natural	1 año	2048
Clase II	Persona Natural	2 años	2048
Clase III	Persona Jurídica	1 año	2048
		2 años	2048
Clase IV	Persona Jurídica (Servidor SSL)	2 años	2048
Clase V	Persona Jurídica (Sistema de Intermediación Electrónico)	2 años	2048
Clase VI	Persona Jurídica (Entidad de Certificación)	Depende del tamaño de la clave y del periodo autorizado*	Mínimo 2048

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

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Las claves privadas de la ECERNEP se encuentran en un equipo HSM que se encuentra desconectado, por lo cual éstas se encuentran inactivas, requiriéndose de las tarjetas de acceso y contraseñas respectivas para su uso.

En cuanto a las claves privadas de la ECEP, éstas deben asegurarse de que se encuentran en un HSM con acceso restringido; para la activación del uso de las mismas se debe contar con controles de acceso lógico y físico adecuados.

La participación de los custodios con las tarjetas de acceso correspondientes al momento de activar las claves privadas es parte de los procedimientos de emisión de certificados y listas CRL de la ECERNEP.

6.4.2. Protección de los datos de activación

La protección que debe ser utilizada es la ofrecida por un equipo criptográfico que cuenta con niveles altos de seguridad tales como FIPS 140-2 nivel 3 y Common Criteria EAL4+.

6.4.3. Otros aspectos de los datos de activación

No son contemplados otros aspectos de activación por la ECERNEP.

6.5. Controles de seguridad computacional

6.5.1. Requisitos técnicos específicos para seguridad computacional

La ECERNEP cumple los controles establecidos en:

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

El cumplimiento de los estándares antes mencionados se da de acuerdo al nivel de acreditación de la ECERNEP.

6.5.2. Evaluación de la seguridad computacional

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

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

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

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo del sistema

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

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

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

El software y hardware que utiliza la ECERNEP, fueron probados antes de ponerse en producción.

6.6.2. Controles de gestión de la seguridad

Los componentes de la ECERNEP se encuentran protegidos en zonas seguras, contándose con los controles indicados en el ítem 6.2.2 del presente documento.

6.6.3. Evaluación de seguridad del ciclo de vida

Los controles de seguridad establecidos para la ECERNEP serán revisados a través de las auditorías o evaluación de compatibilidad con la IOFE.

6.7. Controles de seguridad de la red

Los equipos de la ECERNEP cuentan con mecanismos de control de acceso para prevenir el acceso no autorizado o el cambio de datos, conforme al documento "Controles para la seguridad de la información"

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

Los equipos de la ECERNEP que contienen información sensible se encuentran:

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

6.8. Sello de tiempo

La información publicada en los repositorios (directorios, CRLs, copias archivadas y otros) indica la fecha y hora de su generación, las cuales se obtienen del equipo off line (sin acceso a Internet) en que se generaron y se verifican previamente confrontándolas con una fuente confiable del UTC (Tiempo Universal Coordinado).

7. Perfiles del certificado

7.1. Perfil del certificado

7.1.1. Número(s) de versión(es)

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

- Número de serie, que será un código único con respecto al nombre distinguido del emisor.
- Algoritmo de firma.

- El nombre distinguido del emisor.
- Inicio de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 3280.
- Fin de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 3280.
- Nombre distinguido de la Autoridad propietaria del certificado digital.
- Clave pública de la Autoridad propietaria del certificado digital, codificada de acuerdo con RFC 3280.
- Firma, generada y codificada de acuerdo con RFC 3280.
- Uso autorizado del certificado digital.

7.1.2. Extensiones del certificado

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

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

7.1.3. Identificadores de objeto de algoritmo

Los algoritmos OIDs están de conformidad con el RFC 3279 y RFC 3280.

7.1.4. Forma de nombres

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

7.1.5. Restricciones de Nombre

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

Los nombres contenidos en los certificados están restringidos a nombres distinguidos (Distinguished name - DN) X.500, únicos y no ambiguos.

Los atributos de un nombre distinguido (Distinguished name - DN) serán los que lo distingan de otros.

7.1.6. Identificador de objeto de la política de certificados

La Política General de Certificación de la ECERNEP tiene un identificador de objeto (OID), el cual es: 1.3.6.1.4.1.35300.1.1.1.2

7.1.7. Extensión de restricciones de uso de la política

Las restricciones de políticas están establecidas conforme al RFC 3280.

7.1.8. Sintaxis y semántica de los calificadores de la política

Los calificadores de políticas son soportados tal como se encuentran definidos en el RFC 3280.

La extensión "CERTIFICATE POLICIES" contiene el siguiente calificador de política ("Policy Qualifiers"):

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

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

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

7.2. Perfil CRL

7.2.1. Número(s) de versión(es)

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

7.2.2. CRL y extensiones de entrada CRL

Se soportan las extensiones CRL definidas en el RFC 3280.

7.3. OCSP Profile

7.3.1. Version number(s)

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

7.3.2. OCSP extensions

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

8. Auditorias de conformidad y otras evaluaciones

8.1. Frecuencia y circunstancias de la evaluación

La ECERNEP se someterá a una auditoría anual por parte de la AAC; en caso esta autoridad comunique que no desarrollará la mencionada

auditoría, la ECEP podrá realizarla convocando a un tercero independiente.

8.2. Identidad/Calificaciones de asesores

El auditor es independiente a la ECERNEP.

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

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

Las auditorías efectuadas a la ECERNEP pueden realizarse en forma conjunta con la ECEP del RENIEC.

8.3. Relación del auditor con la entidad auditada

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

Si durante el desarrollo de las labores de auditoría, el auditor requiera contar con acceso a los componentes de la ECERNEP, se le otorgará el acceso de forma restringida y previa evaluación.

En las labores de auditoría que quiera llevar a cabo en relación a los módulos criptográficos HSM, estos serán siempre operados por el personal de la ECERNEP, proporcionando al auditor la información requerida. El auditor no estará en ningún caso autorizado a la manipulación física de los HSM.

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

8.4. Elementos cubiertos por la evaluación

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

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

- Alineación del presente documento a las Guías de Acreditación de la EC.

- Alineación de las medidas efectivas existentes en la ECERNEP con los procedimientos marcados en el presente documento.
- Evaluación y cumplimiento de los niveles de seguridad física.
- Revisión de los procedimientos de contingencia.
- Validez de alta y accesos del personal que labora en la ECERNEP.

8.5. Acciones a ser tomadas frente a resultados deficientes

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

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

- El auditor realizará un informe con los resultados de su auditoria.
- El auditor notificará la deficiencia al RENIEC y a la AAC.
- La AAC evaluará los resultados y en caso de una:

a. No conformidad leve
Indicará las irregularidades (no conformidad), pero permitirá que la ECERNEP continúe con sus operaciones hasta la próxima auditoría programada.

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

c. No conformidad grave
Suspender la operación de la ECERNEP.

En este caso todos los certificados emitidos por la ECEP serán cancelados antes de la suspensión del servicio.

En los casos del literal a y b, la ECERNEP:

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

8.6. Publicaciones de resultados

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