RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Declaración de Prácticas de Registro

Entidad de Registro o Verificación para el Estado Peruano Persona Jurídica

EREP – RENIEC – PJ

Código: DA-DCSD/SDSCD-003		
OID: 1.3.6.4.1.35300.1.2.1.1		
Versión: 5.0	**Año: 2022**	
Elaborado por: Sub Dirección de Servicios de Certificación Digital	**Revisado por:** Sub Director(a) de Servicios de Certificación Digital	**Aprobado por:** Director(a) de Certificación y Servicios Digitales

Historial de Cambios				
Ver.	**Fecha**	**Descripción**	**Responsable**	**Estado**
1.0	22/06/2012	Elaboración y aprobación	SGRD	Aprobado
2.0	10/12/2012	Actualización y aprobación	SGRD	Aprobado
3.0	01/10/2014	Actualización y aprobación	SGRD	Aprobado
4.0	12/02/2018	Actualización y aprobación	SGRD	Aprobado
5.0	09/06/2022	Actualización y aprobación	SDSCD	Aprobado

INDICE

1. INTRODUCCIÓN

El Registro Nacional de Identificación y Estado Civil (en adelante el RENIEC) es un organismo constitucional y autónomo con personería jurídica de derecho público interno, creado por mandato de la Constitución Política del Perú mediante la Ley Orgánica N° 26497, goza de atribuciones en materia registral, técnica, administrativa, económica y financiera. Está encargado de registrar la identidad, los hechos vitales y los cambios de estado civil de las personas; participar del Sistema Electoral; y promover el uso de la identificación y certificación digital.

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

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

El artículo 47º del Reglamento de la Ley de Firmas y Certificados Digitales designó al RENIEC como Entidad de Certificación para el Estado Peruano (en adelante ECEP) y Entidad de Registro o Verificación para el Estado Peruano (en adelante EREP), disponiendo se realicen los trámites correspondientes ante la AAC, con el fin de acreditarse como Prestador de Servicios de Certificación Digital y formar parte de la IOFE. Mediante el Artículo 57° del Reglamento acotado se designó al Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI como AAC.

Además, de conformidad con lo dispuesto por el Artículo 47º del vigente Reglamento, los servicios a ser prestados por El RENIEC, en su calidad de Entidad de Registro para el Estado Peruano, "…*estarán a disposición de todas las Entidades Públicas del Estado Peruano y de todas las personas naturales y jurídicas que mantengan vínculos con él*…"

En dicho orden de ideas, y con la finalidad de dar cumplimiento a lo dispuesto por el Reglamento de la Ley de Firmas y Certificados Digitales, la presente Declaración de

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

Prácticas de Registro describe las prácticas y funciones del RENIEC en su calidad de EREP-RENIEC para Persona Jurídica.

La presente Declaración de Prácticas de Registro (conocida también por su acrónimo en Inglés como RPS[4]) ha sido redactada acogiendo los criterios señalados en la norma RFC 3647 "*Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framewortk*" del *Internet Engineering Task Force* (IETF)(que sustituye a la RFC 2527).

Así mismo, con el propósito de conservar la correspondencia con el documento técnico antes citado y a fin de otorgarle uniformidad al presente documento, facilitando su posterior revisión y análisis, se incluyen todas las secciones allí establecidas, indicándose en aquello que no resulta de aplicación la frase "No aplica a la EREP–RENIEC–PJ".

Finalmente, con relación a la prestación de servicios de certificación digital la EREP–RENIEC–PJ se encuentra vinculada con la ECEP-RENIEC. A tal efecto, los certificados digitales gestionados por la EREP-RENIEC-PJ y emitidos por la ECEP-RENIEC gozan de las presunciones legales establecidas en el Reglamento de la Ley de Firmas y Certificados Digitales[5].

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

1.1. Visión General

El RENIEC, en su calidad de EREP-RENIEC-PJ, y de conformidad con lo dispuesto por el artículo 46º, inciso c) del vigente Reglamento de la Ley de Firmas y Certificados Digitales, cumplirá las funciones de "…*levantamiento de datos, comprobación de la información del solicitante, identificación y autenticación de los titulares y suscriptores, aceptación y autorización de solicitudes de emisión, cancelación, modificación, re-emisión y suspensión si fuera el caso, de certificados digitales, además de su gestión ante las Entidades de Certificación; para los fines previstos en el inciso b) del presente artículo*".

[4] Corresponde con el término en inglés *Registration Authority Practice Statement* (RPS). Se entiende por Declaración Prácticas de Registro al conjunto de procedimientos, estándares o normas técnicas y/o disposiciones legales definidos y aplicados por la EREP–RENIEC en el marco de sus funciones dentro de la IOFE.

[5] **Artículo 3º.- De la validez y eficacia de la firma digital**
La firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita. En tal sentido, cuando la ley exija la firma de una persona, ese requisito se entenderá cumplido en relación con un documento electrónico si se utiliza una firma digital generada en el marco de la Infraestructura Oficial de la Firma Electrónica.

Artículo 8º.- De las presunciones
Tratándose de documentos electrónicos firmados digitalmente a partir de certificados digitales generados dentro de la Infraestructura Oficial de Firma Electrónica, se aplican las siguientes presunciones:
a) Que el suscriptor del certificado digital tiene el control exclusivo de la clave privada asociada.
b) Que el documento electrónico fue firmado empleando la clave privada del suscriptor del certificado digital.
c) Que el documento electrónico no ha sido alterado con posterioridad al momento de la firma.
Como consecuencia de los literales previos, el suscriptor no podrá repudiar o desconocer un documento electrónico que ha sido firmado digitalmente usando su clave privada siempre que no medie ninguno de los vicios de la voluntad previstos en el Título VIII del Libro II del Código Civil.

Las referidas funciones se encuentran organizadas dentro de los procesos: *"Identificación y Registro"* y "*Entrega y Actualización"* correspondientes a la EREP-RENIEC-PJ.

1.2. Nombre e identificación del documento

Nombre del documento	Declaración de Prácticas de Registro Entidad de Registro o Verificación para el Estado Peruano – Persona Jurídica (EREP-RENIEC-PJ)
OID	1.3.6.4.1.35300.1.2.1.1
Versión del documento	5.0
Estado del documento	Aprobado
Fecha de emisión	09/06/2022
Publicación de la DPR	https://pki.reniec.gob.pe/repositorio/

1.3. Participantes

Son considerados como participantes, para efectos del presente documento, la entidad de certificación, la entidad de registro, los titulares y/o suscriptores, los terceros que confían y los proveedores de servicios de valor añadido.

1.3.1 Entidad de Certificación para el Estado Peruano (ECEP-RENIEC).

La ECEP-RENIEC emite o cancela certificados digitales en atención a los pedidos efectuados por la EREP-RENIEC. Los servicios ofrecidos por la ECEP-RENIEC comprenden aquellos orientados a la gestión del ciclo de vida de los certificados digitales, de acuerdo con lo especificado en la correspondiente DPC de la ECEP-RENIEC. La vinculación de la EREP-RENIEC con la ECEP-RENIEC implica necesariamente que la correspondiente DPC es compatible con la presente DPR, delimitándose expresamente en los referidos documentos los procedimientos que corresponden a cada entidad.

1.3.2 Entidad de Registro o Verificación para el Estado Peruano – Persona Jurídica (EREP-RENIEC-PJ).

La EREP-RENIEC-PJ es la entidad encargada del levantamiento de datos, comprobación de la información del solicitante, identificación y autenticación de los titulares y/o suscriptores, aceptación y autorización de solicitudes de emisión y cancelación de certificados digitales, y su respectiva gestión ante la ECEP-RENIEC a fin de que aquella genere o cancele el certificado digital emitido a nombre de los solicitantes (servidores de la Administración Pública; entidades de la Administración Pública y personas jurídicas).

1.3.3 Titulares de certificados

La EREP-RENIEC-PJ declara que las entidades de la Administración Pública y Personas Jurídicas son titulares del certificado digital; y sus funcionarios, empleados o servidores son los suscriptores.

1.3.4 Terceros que Confían

La EREP-RENIEC declara que la comunidad de usuarios definidos como Terceros que Confían son las personas naturales o jurídicas (diferentes al titular o suscriptor del certificado digital), equipos, servicios o cualquier otro ente que decide aceptar y confiar en un certificado digital emitido por la ECEP-RENIEC, y actúa basado en la confianza sobre la validez de un certificado digital y/o verifica la firma digital en la que se utilizó dicho certificado.

Lo aquí expresado concuerda con lo establecido en la DPC de la ECEP-RENIEC.

1.3.5 Otros participantes

Todas las funciones, operaciones y actividades a cargo de la EREP-RENIEC-PJ serán desarrolladas y estarán a cargo del RENIEC en su calidad de Prestador de Servicios de Certificación Digital. No obstante, en la eventualidad que el RENIEC requiera contratar los servicios de un tercero para realizar algún servicio de la EREP–RENIEC–PJ, ésta se reserva el derecho de suscribir el acuerdo de tercerización respectivo, el mismo que contará con cláusulas específicas relacionadas con la confidencialidad de la información del negocio y la protección de los datos personales.

1.3.5.1 SVAs

No aplica a la EREP-RENIEC-PJ.

1.4. Uso del certificado

El uso de los certificados digitales depende de lo establecido en la DPC de la ECEP–RENIEC.

1.4.1 Uso apropiado del certificado

No aplica a la EREP-RENIEC-PJ.

1.4.2 Uso prohibido del certificado

No aplica a la EREP-RENIEC-PJ.

1.5. Administración de Políticas

1.5.1 Organización que administra los documentos de la Declaración de Prácticas de Registro

Los documentos relacionados con la presente DPR son administrados por la Sub Dirección de Servicios de Certificación Digital de la Dirección de Certificación y Servicios Digitales del RENIEC.

RENIEC
Sub Dirección de Servicios de Certificación Digital
Jr. Bolivia No. 109, Tercer Piso - Lima 01
Lima - Perú.
Teléfono: (51 1) 315-2700, anexo 1194
Correo: identidaddigital@reniec.gob.pe

1.5.2 Persona de Contacto

Las consultas relacionadas con la presente DPR de la EREP-RENIEC las puede realizar vía correo electrónico identidaddigital@reniec.gob.pe, o a la siguiente dirección:

RENIEC
Sub Director(a) de Servicios de Certificación Digital
Jr. Bolivia No. 109, tercer piso - Lima 01
Lima - Perú.
Teléfono: (51 1) 315-2700, anexo 1194

1.5.3 Persona que determina la conformidad de la DPR con las políticas

Según lo dispuesto en el Reglamento de la Ley de Firmas y Certificados Digitales, la AAC es la responsable de aprobar la presente Declaración de Prácticas de Registro, asimismo es responsable de acreditar y determinar si una entidad de Registro será parte de la Infraestructura Oficial de Firma Electrónica (IOFE).

1.5.4 Procedimiento de aprobación de DPR

El presente documento, así como sus actualizaciones son propuestos por la EREP–RENIEC–PJ a la AAC–INDECOPI, a quien corresponde su aprobación, de conformidad con lo establecido en la Guía de Acreditación de Entidades de Registro ER y sus procedimientos, según lo dispuesto en el Reglamento de la Ley de Firmas y Certificados Digitales.

1.6. Definiciones y acrónimos

Las definiciones y acrónimos se desarrollan en la sección 11 del presente documento.

2. PUBLICACIÓN Y REGISTRO

2.1. Repositorios

No aplica a la EREP-RENIEC-PJ.

2.2. Publicación de la información sobre certificación

La presente DPR, así como toda la información relevante vigente y de conocimiento público, se encuentra disponible en la página web: https://pki.reniec.gob.pe/repositorio/

La EREP–RENIEC–PJ asegura que los datos personales de los titulares y/o suscriptores se encuentran debidamente protegidos de conformidad con lo dispuesto por la Ley N° 29733 – Ley de Protección de Datos Personales y su Reglamento, así como la norma Marco sobre Privacidad del APEC.

2.3. Tiempo o frecuencia de la publicación

La DPR se publicará cada vez que ésta sea modificada y presentada ante la AAC; y estará disponible en la página web: https://pki.reniec.gob.pe/repositorio/

2.4. Controles de acceso a los registros

El acceso para la lectura de los documentos referidos (*"Declaración de Prácticas de Registro"*, *"Política de Seguridad"*, "*Política de Privacidad"*) a la EREP–RENIEC–PJ es de carácter público; no obstante, sólo el personal autorizado podrá realizar las modificaciones o actualizaciones respectivas que concierne a cada una de ellas.

El acceso a los registros de los servicios prestados por la EREP– RENIEC-PJ está restringido únicamente al personal expresamente autorizado.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

Dentro del marco de aplicación de la presente DPR, en esta sección se describe cómo la EREP-RENIEC-PJ realiza la comprobación de la identidad del solicitante.

3.1. Nombre

No aplica a la EREP-RENIEC-PJ.

3.1.1 Tipos de nombres

No aplica a la EREP-RENIEC-PJ.

3.1.2 Necesidad que los nombres tengan un significado

No aplica a la EREP-RENIEC-PJ.

3.1.3 Anonimato o seudónimo de los suscriptores

No aplica a la EREP-RENIEC-PJ.

3.1.4 Reglas para interpretar las diferentes modalidades de nombres

No aplica a la EREP-RENIEC-PJ.

3.1.5 Singularidad de los nombres

No aplica a la EREP-RENIEC-PJ.

3.1.6 Reconocimiento, autenticación y rol de las marcas registradas

Las entidades de la Administración Pública y Personas Jurídicas solicitantes de certificados digitales se encuentran prohibidas de utilizar en sus solicitudes nombres que contravengan el mejor derecho que pudieran ostentar terceros. La EREP-RENIEC-PJ no asignará un nombre de titular igual al que ya haya sido asignado a un titular diferente.

En cualquier caso, no corresponde a la EREP-RENIEC-PJ determinar si un solicitante posee o le asiste algún tipo de derecho sobre el nombre que consigna en su solicitud de un certificado digital, sea cual sea el fin que se dé, así como no es su función resolver controversias relativas a la propiedad de nombres de personas, naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.

No obstante, en el marco de las funciones de la EREP-RENIEC-PJ se comprobará que los nombres de titular y/o suscriptor correspondan con la documentación que presenten los solicitantes.

La EREP-RENIEC-PJ se reserva el derecho de denegar una solicitud de certificado digital a causa de conflicto de nombres.

3.2. Validación inicial de la identidad

3.2.1. Método para probar la posesión de la clave privada

En concordancia con lo señalado en la DPC de la ECEP-RENIEC, la clave privada correspondiente a la clave pública para la que se solicita que se emita un certificado digital, se genera utilizando un módulo criptográfico de creación de firma que cumpla con la certificación FIPS 140-2 nivel de seguridad 1 o la Common Criteria EAL4, como mínimo. De esta forma, la posesión de la clave privada quedará probada mediante el envío de la petición de certificado Certificate Signing Request (CSR) en formato PKCS#10, en la cual se incluye la clave pública firmada mediante la clave privada asociada. Esta petición de certificado será enviada a la ECEP-RENIEC para su procesamiento, lo que posibilita la detección de errores en la generación del certificado; probando así, que el solicitante ya tiene en su posesión el par de claves y cuenta con la capacidad de hacer uso de ellas.

3.2.2. Autenticación de Identidad de una persona jurídica

La EREP-RENIEC-PJ verificará la existencia de una entidad de la Administración Pública, a través de la norma legal de creación correspondiente. Asimismo, su vigencia será verificada consultando que, en la base de datos de la SUNAT, la entidad se encuentre en estado “activo” y que la condición de su domicilio sea “habido”.

La autenticación de la identidad del representante del titular o entidad de la Administración Pública, quien a la vez es suscriptor, se realizará de acuerdo a lo especificado en la subsección 3.2.3 del presente documento.

3.2.3. Autenticación de Identidad de la persona natural.

La validación de la identidad de los suscriptores, según el procedimiento de trámite de emisión y entrega del certificado digital[6], se podrá realizar de la siguiente manera:

- Para el caso de los ciudadanos peruanos, la validación de la identidad del solicitante consiste en verificar y/o autenticar su identidad empleando la “*Base de Datos del RENIEC”* y mecanismos tecnológicos seguros aprobados por la AAC.

- Para el caso de los extranjeros, la comprobación de la identidad del solicitante se realiza mediante la consulta a la “*Base de Datos de la Superintendencia Nacional de Migraciones*”, disponible a través de su página web, caso contrario deberá presentar la copia autenticada, por Fedatario Institucional o Notario, de su Carné de Extranjería vigente.

[6] GP-430-GRCD/SGRD/002 Trámite de emisión y entrega del certificado digital

3.2.4. Información no verificada del suscriptor

La EREP-RENIEC-PJ no aceptará información que no pueda ser objeto de comprobación. En ese sentido, la EREP-RENIEC-PJ verificará la información recabada del solicitante, según lo descrito en las sub secciones 3.2.2 y 3.2.3 del presente documento.

Se exceptúa la verificación de la cuenta de correo electrónico proporcionada por el solicitante.

3.2.5. Validación de la autoridad

Los solicitantes pertenecientes a las entidades de la Administración Pública y personas jurídicas, que requieran de la emisión de un certificado digital para acreditar el ejercicio de un cargo en concreto, deberán presentar ante la EREP-RENIEC-PJ la documentación sustentatoria, incluyendo la facultad de actuar en nombre de la entidad de la Administración Pública o de la persona jurídica.

3.2.6. Criterios para la interoperabilidad

La EREP–RENIEC–PJ se encuentra vinculada a la ECEP-RENIEC. Ambas entidades prestan sus servicios de certificación digital dentro del marco de la IOFE, por tanto, las firmas digitales realizadas con los certificados digitales emitidos por la ECEP-RENIEC, tienen la misma validez y eficacia jurídica que el uso de una firma manuscrita (principio de equivalencia funcional). La EREP–RENIEC–PJ no contempla el establecimiento de relaciones de confianza con otra Entidad de Certificación.

La DPC, así como la presente DPR, se encuentran disponibles en https://pki.reniec.gob.pe/repositorio/.

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

La re-reemisión implica la generación de un nuevo par de llaves y la emisión de un nuevo certificado mediante un procedimiento especial antes del vencimiento del certificado emitido con anterioridad al solicitante.

El suscriptor firmará digitalmente los documentos relacionados al trámite de re-emisión con el certificado digital de persona jurídica que está por caducar y que no fue brindado por re-emisión.

La identificación y autenticación del suscriptor se dará al momento de firmar digitalmente los documentos relaciones al trámite de la re-emisión.

Una vez aprobado el flujo de re-emisión, se brindarán nuevos accesos para la generación y descarga de un nuevo certificado digital para el suscriptor que lo solicitó.

3.4. Identificación y autenticación de la solicitud de cancelación

De acuerdo con la competencia de la EREP-RENIEC-PJ, así como a los procedimientos establecidos[7], la solicitud de cancelación de un certificado digital puede ser realizada por el representante del titular, el propio suscriptor o un tercero. La verificación y/o autenticación de la identidad de éstos, se realizará según lo descrito en la subsección 3.2.3 del presente documento.
Todo suscriptor dispone, asimismo, de un acceso habilitado a la Plataforma Integrada de la Entidad de Registro (PIER) a través de la cual puede consultar sus certificados digitales y, de ser necesario, efectuar su cancelación, conforme consta en el contrato del suscriptor. El acceso a la plataforma y a los instructivos y manuales correspondientes se encuentran en la página web https://pki.reniec.gob.pe/pier/.

[7] GP-413-GRCD/SGRD/001 Cancelación del certificado digital

4. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS

Dentro del marco de aplicación de la presente DPR, y de acuerdo con los lineamientos establecidos por la AAC, en la presente sección, se describen los requisitos operacionales que aplicará el RENIEC en su calidad de EREP- RENIEC-PJ, respecto a las solicitudes de emisión y cancelación de certificados digitales y conforme a procedimientos que establezca la ECEP-RENIEC en su DPC.

El ciclo de vida de los certificados digitales se encuentra determinado por el periodo de vigencia de este, el cual inicia y finaliza en las fechas indicadas en él, salvo en los supuestos de cancelación o de revocación de oficio conforme lo señalado en el respectivo contrato.

4.1. Solicitud del certificado

4.1.1. Habilitados para presentar la solicitud de un certificado

A solicitud del interesado, la EREP-RENIEC-PJ gestionará ante la ECEP-RENIEC la emisión de un certificado digital. En tal sentido, se encontrarán habilitados para solicitar un certificado digital las entidades de la Administración Pública y personas jurídicas. El trámite será realizado por la máxima autoridad administrativa o por el representante legal o una persona designada, quienes deberán contar con las respectivas facultades debidamente acreditadas para realizar los trámites respectivos ante la EREP-RENIEC-PJ, convirtiéndose en representantes del titular. La entidad de la Administración Pública o la persona jurídica es el titular del certificado digital, y los suscriptores son las personas naturales autorizadas por el representante del titular para solicitar un certificado digital.

4.1.2. Proceso de solicitud y responsabilidades

Los solicitantes que deseen gestionar la emisión de un certificado digital[8].

En caso sea la atención presencial: Deberán apersonarse a una oficina autorizada de la EREP-RENIEC-PJ, debiendo cumplir con los requisitos señalados en el TUPA, y de acuerdo con los procedimientos establecidos, a fin de que la EREP-RENIEC-PJ pueda tramitar sus solicitudes.

En caso sea la atención remota: Deberán proporcionar información fidedigna a través de mecanismos tecnológicos seguros alternativos a la comparecencia física aprobados por la AAC.

El trámite de emisión de un certificado digital es estrictamente personal e indelegable.

El solicitante asume responsabilidad por la veracidad y exactitud de la información proporcionada, sin perjuicio de la respectiva comprobación de la información por parte de la EREP-RENIEC-PJ.

[8] GP-430-GRCD/SGRD/002 Trámite de emisión y entrega del certificado digital

Las obligaciones y responsabilidades de los titulares y/o suscriptores se encuentran contenidas en el contrato correspondiente, el cual ha sido elaborado junto con la ECEP-RENIEC.

4.2. Procesamiento de la solicitud de un certificado

4.2.1. Realización de las funciones de identificación y autenticación

Se realizan de acuerdo a lo señalado en la subsección 3.2.3 del presente documento.

4.2.2. Aprobación o rechazo de la solicitud de un certificado

De conformidad con la legislación vigente[9], la EREP-RENIEC-PJ tiene como función aprobar o denegar una solicitud relacionada con el ciclo de vida del certificado digital.

En el caso de los servidores públicos, la EREP-RENIEC-PJ aprobará la solicitud luego de haberse verificado y autenticado la identidad del solicitante conforme a lo descrito en la subsección 3.2.3 del presente documento; y haber cumplido con los requisitos señalados en el TUPA vigente.

La EREP-RENIEC-PJ no aceptará o aprobará una solicitud en los siguientes supuestos:

- Suplantación de identidad.
- En caso no se hubiese podido comprobar la identidad del solicitante.
- Si en la base de datos del RENIEC hubiese alguna observación de interdicción judicial o declaración de incapacidad que lo limite en el pleno ejercicio de sus derechos civiles, conforme a lo dispuesto en los artículos 43°, 44° y 585° del Código Civil.

En el caso de uno de estos supuestos, el Operador de Registro Digital comunicará al solicitante los motivos que originaron la no aceptación o la denegación de la solicitud.

4.2.3. Tiempo para el procesamiento de la solicitud de un certificado

Aprobada la solicitud respectiva, la EREP-RENIEC-PJ comunicará en forma inmediata a la ECEP-RENIEC la aprobación de la emisión del certificado digital, quien deberá generar el certificado digital.

4.3. Generación de claves y emisión del certificado

No aplica a la EREP-RENIEC-PJ.

4.3.1. Acciones de la EC durante la emisión del certificado

No aplica a la EREP-RENIEC-PJ.

[9] Artículo 29º, inciso b), del Reglamento de la Ley de Firmas y Certificados Digitales aprobado mediante el Decreto Supremo Nº 052-2008-PCM.

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

No aplica a la EREP-RENIEC-PJ.

4.4. Aceptación del certificado

No aplica a la EREP-RENIEC-PJ.

4.4.1. Conducta constitutiva de la aceptación de un certificado

No aplica a la EREP-RENIEC-PJ.

4.4.2. Publicación del certificado por parte de la EC

No aplica a la EREP-RENIEC-PJ.

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

No aplica a la EREP-RENIEC.

4.5. Par de claves y uso del certificado

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

No aplica a la EREP-RENIEC-PJ.

4.5.2. Uso de la clave pública y certificado por el Tercero que Confía

No aplica a la EREP-RENIEC-PJ.

4.6. Renovación del certificado

No aplica a la EREP-RENIEC-PJ.

4.6.1. Circunstancias para la re-certificación (renovación de certificados con el mismo par de claves)

No aplica a la EREP-RENIEC-PJ.

4.6.2. Personas habilitadas para solicitar la renovación

No aplica a la EREP-RENIEC-PJ.

4.6.3. Procesamiento de la solicitud de renovación de certificado

No aplica a la EREP-RENIEC-PJ.

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

No aplica a la EREP-RENIEC-PJ.

4.6.5. Conducta constitutiva de aceptación de renovación de certificado

No aplica a la EREP-RENIEC-PJ.

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

No aplica a la EREP-RENIEC-PJ.

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

No aplica a la EREP-RENIEC-PJ.

4.7. Re-emisión de certificado

La ECEP-RENIEC brinda nuevos certificados digitales a solicitud de la EREP-RENIEC-PJ.

La re-emisión de un certificado digital de persona jurídica, consiste en brindar un nuevo certificado digital en base a un certificado digital anteriormente brindado sin re-emisión. Por lo tanto, el suscriptor firmará los documentos relacionados al trámite de re-emisión con el certificado digital de persona jurídica que está por caducar y al cual se le aplicará el flujo de re-emisión. La identificación y autenticación del suscriptor se dará al momento de firmar digitalmente los documentos relaciones al trámite de la re-emisión.

4.8. Modificación del certificado

Este servicio no es brindado por la ECEP-RENIEC, por lo tanto, la EREP-RENIEC-PJ no brindará el mismo.

4.9. Cancelación y suspensión del certificado

La cancelación del certificado digital es el acto por el cual se deja sin efecto la validez del mismo, antes de su fecha de expiración. El efecto de la cancelación de un certificado es la pérdida de la validez del mismo, originando el cese permanente de su operatividad conforme a los usos que le son propios. En consecuencia, la cancelación inhabilita el uso legítimo del certificado por parte del titular y/o suscriptor.

La cancelación de los certificados digitales emitidos por la ECEP-RENIEC es un mecanismo a utilizarse en el supuesto de que por alguna de las causas establecidas en el artículo 17 del Reglamento de la Ley de Firmas y

Certificados Digitales[10], y por ende en el respectivo contrato, se deje de confiar en dichos certificados antes de la fecha de expiración indicada en el mismo certificado.

La ECEP-RENIEC podrá de oficio cancelar el certificado digital, cuando tenga conocimiento de alguna de las circunstancias señaladas en la subsección 4.9.1 del presente documento.

Por ende, es obligación de los Terceros que Confían verificar el estado del certificado digital en el repositorio de la ECEP-RENIEC.

El servicio de suspensión de certificados digitales no es brindado por la ECEP-RENIEC, por lo tanto, la EREP-RENIEC-PJ no brindará el mismo.

4.9.1. Circunstancias para la cancelación

Los certificados digitales pueden ser cancelados por las causas siguientes:

a. Por circunstancias que afecten la clave privada o la clave personal de acceso (PIN):
   - Exposición, puesta en peligro o uso indebido de la clave privada o de la clave personal de acceso o contraseña (PIN) que permite la activación de dichas claves.
   - Deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
   - Por compromiso de las claves privadas, bien porque concurran las causas de pérdida, robo, hurto, divulgación o revelación de la clave personal de acceso o contraseña (PIN) que permite la activación de dichas claves.

b. Por circunstancias que afecten el certificado digital:
   - La información contenida en el certificado digital ya no resulta correcta o es inexacta.
   - Resolución administrativa o judicial que ordene la cancelación del certificado digital.
   - Incumplimiento derivado de la relación contractual o inobservancia de las obligaciones comprometidas dentro de la IOFE contenidas en el respectivo contrato.
   - Expiración del plazo de vigencia.
   - Cese de operaciones de la ECEP-RENIEC.

c. Por circunstancias que afectan a la persona natural, titular y suscriptor del certificado digital:
   - Interdicción civil declarada judicialmente.
   - Por declaración judicial de ausencia o de muerte.
   - Muerte o por inhabilitación o incapacidad declarada judicialmente.

[10] Aprobado por el D.S N° 052-2008-PCM.

d. Por circunstancias que afectan a la entidad de la Administración Pública o Persona jurídica, titular y/o suscriptor del certificado digital:
   - Extinción de la entidad.
   - Revocación de las facultades del representante del titular.

e. Por otras circunstancias que afectan a titulares y/o suscriptores del certificado digital:
   - A pedido del titular y/o suscriptor sin previa justificación.
   - Cuando el titular y/o suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la ECEP-RENIEC.
   - Por otras circunstancias que establezca la AAC, según lo señalado en el Reglamento de la Ley de Firmas y Certificados Digitales, Artículo 17 inciso j).

4.9.2. Personas habilitadas para solicitar la cancelación

Se encontrarán habilitadas para solicitar la cancelación de un certificado digital, en las circunstancias señaladas en la subsección 4.9.1 del presente documento, las personas siguientes:

- En caso de certificados para entidades de la Administración Pública y personas jurídicas, el trámite es solicitado por el representante del titular. Los suscriptores distintos al representante del titular (funcionarios, empleados o servidores) podrán solicitar la cancelación de su certificado digital cuando medien las circunstancias que se describen a continuación:

  a) Por exposición, puesta en peligro o uso indebido de la clave privada o de la clave personal de acceso o contraseña (PIN) que permite la activación de dichas claves.
  b) Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
  c) Por compromiso de las claves privadas, bien porque concurran las causas de pérdida, robo, hurto, divulgación o revelación de la clave personal de acceso o contraseña (PIN) que permite la activación de dichas claves.

- Un tercero, en caso tenga conocimiento de alguna de las circunstancias siguientes:

  a) Muerte o declaración judicial de ausencia o muerte presunta del suscriptor del certificado.
  b) Interdicción civil judicialmente declarada.
  c) Extinción de la personería jurídica o declaración de quiebra.
  d) Inhabilitación o incapacidad declarada judicialmente.
  e) Cuando la información contenida en el certificado digital es inexacta o ha sido modificada.

- Un juez que de acuerdo con la Ley decida revocar el certificado digital.

4.9.3. Procedimiento para la solicitud de cancelación

La EREP-RENIEC-PJ verificará y/o autenticará la identidad del solicitante según el procedimiento señalado en la subsección 3.4 del presente documento.

La solicitud de cancelación de un certificado digital realizada por el titular y/o suscriptor puede ser de manera presencial, apersonándose a una oficina de la EREP-RENIEC-PJ; o de manera virtual a través de la web para que, de manera remota, el solicitante pueda realizar la cancelación de los certificados digitales correspondientes.

La solicitud de cancelación de un certificado digital realizada por un tercero debe ser de manera presencial, apersonándose a una oficina de la EREP–RENIEC–PJ, presentando su documento de identidad vigente y los documentos de sustento, debiendo probar de manera fehaciente, alguna de las circunstancias señaladas en la subsección 4.9.1 del presente documento, y de acuerdo al procedimiento establecido[11].

Una vez aprobada la solicitud de cancelación de un certificado digital, la EREP-RENIEC-PJ deberá comunicarlo a la ECEP-RENIEC, de acuerdo con los procedimientos establecidos. En caso de que ocurra denegación, deberá registrarse el motivo.

La EREP–RENIEC–PJ registrará toda la información respecto a la aprobación o denegación de la solicitud de cancelación de un certificado digital, así como toda la información relacionada con la persona que efectúa la solicitud, las circunstancias de la cancelación, y la fecha y hora relacionada a ésta.

4.9.4. Periodo de gracia de la solicitud de cancelación

No aplica a la EREP-RENIEC-PJ.

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

No aplica a la EREP-RENIEC-PJ.

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

No aplica a la EREP-RENIEC-PJ.

4.9.7. Frecuencia de emisión de CRL

No aplica a la EREP-RENIEC-PJ.

4.9.8. Máxima latencia para CRLs

No aplica a la EREP-RENIEC-PJ.

[11] GP-413-GRCD/SGRD/001 Cancelación del certificado digital

4.9.9. Disponibilidad de la verificación en línea de la cancelación /estado

No aplica a la EREP-RENIEC-PJ.

4.9.10. Requisitos para la verificación en línea de la cancelación

No aplica a la EREP-RENIEC-PJ.

4.9.11. Otras formas disponibles de publicar la cancelación

No aplica a la EREP-RENIEC-PJ.

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

No aplica a la EREP-RENIEC-PJ.

4.9.13. Circunstancias para la suspensión

No aplica a la EREP-RENIEC.

4.9.14. Personas habilitadas para solicitar la suspensión

No aplica a la EREP-RENIEC-PJ.

4.9.15. Procedimiento para la solicitud de la suspensión

No aplica a la EREP-RENIEC-PJ.

4.9.16. Límite del periodo de suspensión

No aplica a la EREP-RENIEC-PJ.

4.10. Servicios de estado de certificado

No aplica a la EREP-RENIEC-PJ.

4.10.1. Características operacionales

No aplica a la EREP-RENIEC-PJ.

4.10.2. Disponibilidad del servicio

No aplica a la EREP-RENIEC-PJ.

4.10.3. Rasgos operacionales

No aplica a la EREP-RENIEC-PJ.

4.11. Finalización de la suscripción

No aplica a la EREP-RENIEC-PJ.

4.12. Depósito y recuperación de claves

No aplica a la EREP-RENIEC-PJ.

4.12.1. Políticas y prácticas de recuperación de Depósito de claves

No aplica a la EREP-RENIEC-PJ.

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

No aplica a la EREP-RENIEC-PJ.

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

De acuerdo con los lineamientos establecidos por la AAC, la presente sección describe las medidas que ha implementado el RENIEC, en su calidad de EREP-RENIEC-PJ, con la finalidad de garantizar los requerimientos que en materia de seguridad se encuentran asociados al proceso: "*Gestión de Solicitud de Certificado Digital de Persona Jurídica"* correspondientes a la EREP-RENIEC-PJ. En las subsecciones siguientes se reseña las medidas adoptadas más relevantes.

5.1. Controles físicos

En esta subsección se describen los controles que se aplicarán a los recursos físicos que comprenden las instalaciones de la EREP- RENIEC-PJ, lo cual incluye la infraestructura física y su acondicionamiento, el acceso físico a ésta, así como su protección y seguridad.

5.1.1. Ubicación y construcción del local

Las instalaciones de las agencias sucursales de la EREP-RENIEC-PJ se encuentran resguardadas físicamente con las medidas de protección necesarias, según los procedimientos definidos por los órganos competentes del RENIEC, a fin de salvaguardar el desarrollo de las actividades de prestación de los servicios del RENIEC.[12]

5.1.2. Acceso físico

En los ambientes donde se desarrollan las actividades y operaciones de la EREP-RENIEC-PJ se han establecido perímetros de seguridad e implementado controles de acceso, de modo que sólo el personal autorizado y acreditado puede acceder a los mismos. Esto controles de acceso aplican para el personal de la EREP-RENIEC-PJ, visitantes o proveedores.[13]

5.1.3. Energía y aire acondicionado

Las instalaciones de las agencias sucursales de la EREP-RENIEC-PJ, se han implementado medidas adecuadas a fin de suministrar energía temporal en caso de caídas del sistema eléctrico principal, protegiendo a los equipos frente a fluctuaciones eléctricas que los pudieran dañar.

El ambiente donde se encuentran situados los servidores y equipos de tratamiento y almacenamiento de la información dispone de equipos (aire acondicionado o equipos de enfriamiento o ventiladores, etc.) que dotan al entorno de operaciones de una humedad y temperatura adecuada y constante, consiguiendo la

[12] DI-206-OSDN/001 "Seguridad de las Instalaciones en Sedes, Oficinas Registrales, Agencias, Locales y/o Puntos de Atención", Séptima Versión.
[13] DI-206-OSDN/001 "Seguridad de las Instalaciones en Sedes, Oficinas Registrales, Agencias, Locales y/o Puntos de Atención", Séptima Versión.
NAI-386-OSDN/005 "Normas y Obligaciones del Personal de Vigilancia Privada", Segunda Versión.

protección de los equipos y un óptimo funcionamiento de los mismos, logrando un entorno de operaciones fiable

Los equipos de apoyo que suministran energía eléctrica, así como los equipos de aire acondicionado, cuentan con mantenimientos preventivos periódicos a fin de garantizar su correcto funcionamiento, los mismos que son realizados por los órganos encargados en RENIEC

5.1.4. Exposición al agua

En las instalaciones donde se desarrollan las actividades y operaciones de la EREP-RENIEC-PJ, según corresponda, se han implementado medidas adecuadas para prevenir la exposición al agua, disponiendo de controles que previenen o protegen en lo razonablemente posible contra posibles aniegos o inundaciones.[14]

5.1.5. Prevención y protección contra fuego

En las instalaciones donde se desarrollan las actividades y operaciones de la EREP-RENIEC-PJ, se han implementado medidas que permiten prevenir y extinguir incendios u otras exposiciones dañinas como llamas o humo; en tal sentido, en dichos ambientes de la EREP–RENIEC-PJ se cuentan con equipos adecuados como extintores que permiten detectar y sofocar un eventual siniestro, según las recomendaciones del órgano competente del RENIEC.[15]

5.1.6. Archivo de material

El RENIEC ha establecido lineamientos para la clasificación de la información[16], así como su tratamiento y condiciones de almacenamiento de acuerdo a la criticidad de esta información y en concordancia con el proceso de certificación digital, las leyes y regulaciones vigentes.

Toda información contenida en formato papel, relacionada con una solicitud de un certificado digital, se almacena en las instalaciones del RENIEC, las cuales cuentan con adecuados controles de acceso físico para limitar el acceso sólo al personal autorizado, así como proteger dicha información de algún deterioro o daño accidental (ej. agua, incendio, etc.).

Respecto a la información que ingresa en formato electrónico, ésta es almacenada en los equipos (servidores) ubicados en las instalaciones del RENIEC, en un ambiente que cuenta con controles de acceso físico y lógico para limitar el acceso sólo al personal autorizado. Así también, se protege dicha información de algún daño

[14] NAI-368-OSDN/003 "Indicaciones a Seguir Ante Señales de Alerta del Sistema de Alarma de Incendio y Aniego", Tercera Versión.
[15] NAI-368-OSDN/003 "Indicaciones a Seguir Ante Señales de Alerta del Sistema de Alarma de Incendio y Aniego", Tercera Versión.
[16] DI-373-OSDN/007 "Clasificación de la Información del Sistema de Gestión de Seguridad de la Información", Segunda Versión; DI-434-SGEN-OAA" Sistema de Archivo Institucional del RENIEC", Primera Versión.

o destrucción deliberada o accidental (ej. robo, alteración no autorizada, agua, incendio y electromagnetismo).

Adicionalmente, las copias de seguridad se encuentran en ambientes diferentes que cuentan con controles de protección contra fuego, humedad, electromagnetismo y acceso no autorizado.

5.1.7. Gestión de residuos

La información contenida en formato papel, así como en soportes magnéticos u ópticos, antes de ser eliminada, es destruida tanto física como lógicamente a fin de evitar la posibilidad de recuperación de dicha información desde los formatos que la contuvieren.

Este procedimiento es efectuado de acuerdo con la legislación vigente y los procedimientos establecidos por RENIEC.[17]

5.1.8. Copia de seguridad externa

En general, para las copias de seguridad de la información correspondiente a la EREP-RENIEC-PJ, resulta de aplicación lo dispuesto en la subsección 5.1.6 del presente documento.

5.2. Controles procesales

5.2.1. Roles de confianza

La EREP-RENIEC-PJ ha definido y comunicado las funciones a su personal, así mismo se ha determinado los roles de confianza y los procedimientos de control adecuados para el cumplimiento de las obligaciones establecidas en el presente documento. Estos roles son los siguientes:

- **Administrador de la Oficina EREP:** Encargado de asegurar el cumplimiento de la calidad de servicio de la oficina EREP a su cargo; cautelar el cumplimiento del TUPA, cumplir y hacer cumplir los plazos establecidos para los trámites realizados; controlar el cumplimiento de las disposiciones legales, normas internas, DPR y otras que correspondan a las actividades dentro de la Infraestructura Oficial de Firma Electrónica y; administrar los recursos y bienes que le han sido asignados.

- **Supervisor de Registro Digital EREP:** Encargado de velar por el cumplimiento de las funciones de los Operadores de Registro Digital a su cargo; distribuir la carga de trabajo entre los Operadores de Registro Digital a su cargo; cumplir y hacer cumplir los plazos establecidos para los trámites realizados; controlar el cumplimiento de las disposiciones legales, normas internas, DPR, y otras que correspondan a las actividades dentro de la Infraestructura Oficial de Firma Electrónica; supervisar el cumplimiento de normas, procedimientos y directivas de las oficinas EREP a su cargo; promover la calidad, eficiencia y eficacia de la operación de las oficinas a su cargo; velar por el

[17] NAI-476-GRCD/013 “Gestión de Eliminación de Residuos”, Primera Versión.

cumplimiento de la aplicación de encuestas de satisfacción al cliente; reportar las fallas e interrupciones de los sistemas y servicios de las oficinas a su cargo; proveer los recursos para la correcta operación de las oficinas a su cargo; supervisar y apoyar el cumplimiento de las metas de las oficinas a su cargo y; elaborar cuadros estadísticos de información de las oficinas a su cargo.

5.2.2. Número de personas requeridas por labor

La EREP-RENIEC-PJ mantiene una política rigurosa para asegurar la separación de funciones basado en responsabilidades de trabajo.

Primero el Operador de Registro Digital quien verificará y/o autenticará la identidad del solicitante, podrá aprobar o denegar la solicitud correspondiente. En el caso, que no se realice la verificación de la identidad del solicitante a través de la biometría, deberá realizarlo a través de una consulta al RUIPN, de esta manera el operador realizara una pre-aprobación y luego el Supervisor de Registro Digital será el responsable de realizar la aprobación de la solicitud para la emisión del certificado comunicándolo a la ECEP-RENIEC, según lo señalado en el procedimiento de trámite de emisión y entrega del certificado digital.

5.2.3. Identificación y autenticación para cada rol

La EREP-RENIEC-PJ, ha definido controles de acceso físico y lógico para su personal, de acuerdo con el rol que desempeñan dentro de las actividades y operaciones de la EREP-RENIEC-PJ.

El personal que opera la Plataforma Integrada de la Entidad de Registro PIER está autorizado para acceder a la misma previa autenticación de su identidad mediante el uso de biometría dactilar o a través de su certificado digital.

5.2.4. Roles que requieren funciones por separado

Con el fin de mantener una adecuada separación de funciones, en cada uno de los roles definidos por la EREP-RENIEC-PJ se desempeñarán diferentes responsables.

5.3. Controles de personal

En esta subsección se establecen los controles implementados por el RENIEC en relación con el personal que desempeña funciones en la EREP-RENIEC-PJ; 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, la presente subsección alcanza al personal a cargo de terceros y contratistas que realicen labores por tiempo determinado en las instalaciones de la EREP-RENIEC-PJ.

En ambos casos, para el personal que ejerza labores en la EREP-RENIEC-PJ y tenga acceso a la información clasificada como “confidencial” o

"reservada", los acuerdos se encuentran en el contrato y/o términos de referencia.

5.3.1. Cualidades y requisitos, experiencia y certificados

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

En tal sentido, las prácticas de selección y reclutamiento del personal se llevan a cabo en la Oficina de Potencial Humano del RENIEC tomando en cuenta los perfiles fijados por la EREP-RENIEC-PJ, donde se consideran requisitos de experiencia y calificación para cada rol de confianza.

La definición de los puestos de trabajo y sus funciones se encuentran delineadas en los correspondientes procedimientos. El contrato de trabajo respectivo regulará las relaciones de trabajo entre el RENIEC y su personal.

En caso del personal a cargo de terceros, será responsabilidad del contratista acreditar la formación y experiencia de aquellos, de acuerdo con los requerimientos de la EREP-RENIEC, debiendo presentar la documentación que evidencie el cumplimiento de dicho aspecto.

5.3.2. Procedimiento para verificación de antecedentes

Es política del RENIEC verificar la documentación aportada por el personal aspirante a realizar labores al interior de la entidad. A tal efecto, la Oficina de Potencial Humano ejecuta los siguientes controles mínimos:[18]

- 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, entre otros.

En caso de personal a cargo de terceros, corresponde al contratista realizar la verificación de los antecedentes respectivos de sus empleados.

5.3.3. Requisitos de capacitación

Es política del RENIEC que toda persona que desarrolla funciones al interior de la EREP-RENIEC-PJ reciba desde su ingreso una instrucción – inducción – acorde con la función a desempeñar. Dicho personal se encontrará sujeto al plan de capacitación continuo, a fin

[18] DI-346-GTH/001 "Proceso de Evaluación y Selección para Cubrir Plazas Vacantes del Cuadro para Asignación del Personal(CAP) del RENIEC", Primera Versión
GP-461-GTH/SGPS/001 "Selección De Personal Bajo el Régimen Especial de Contratación Administrativa de Servicios", Primera Versión.

que las responsabilidades asumidas como parte de los servicios de certificación digital se desarrollen en forma competente.

El contenido de los programas de capacitación se controla y refuerza periódicamente por la Sub Dirección de Servicios de Certificación Digital, en coordinación con la Dirección de Certificación y Servicios Digitales y la Oficina de Formación Ciudadana e Identidad, llevándose un registro y archivo de las materias impartidas para los efectos de las re-capacitaciones a las que se alude en la subsección 5.3.4 del presente documento.

El plan de capacitación, adecuado a las funciones a desempeñar en la EREP-RENIEC-PJ, contiene como mínimo los siguientes conceptos básicos y se aprueba anualmente:

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

La Sub Dirección de Servicios de Certificación Digital, en coordinación con la Dirección de Certificación y Servicios Digitales y la Oficina de Formación Ciudadana e Identidad, cuando lo 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 de la capacitación del personal.

En lo que corresponda, los contratistas que realicen labores por tiempo determinado en las instalaciones de la EREP-RENIEC-PJ, tienen la obligación de capacitar de manera continua a su personal.

5.3.4. Frecuencia y requisitos de las re-capacitaciones

La re-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 "*Declaración de Prácticas de Registro*", "*Política de Seguridad*", *"Política de Privacidad*" y "*Plan de Privacidad"* o en cualquier otro documento que resulte relevante para la EREP-RENIEC-PJ y que comprometa los aspectos funcionales de las labores del personal.

Sin perjuicio de lo antes expuesto, el Plan de Capacitación resulta ser un proceso de formación continua del personal, encontrándose sus requisitos dispuestos en la subsección 5.3.3 del presente documento.

5.3.5. Frecuencia y secuencia de la rotación en el trabajo

La EREP-RENIEC-PJ, en caso determine la conveniencia, podrá implementar rotaciones de trabajo entre los distintos roles, con el objeto de incrementar la seguridad y asegurar la continuidad de las actividades. La rotación es comunicada al personal con el documento pertinente.

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 EREP-RENIEC-PJ, se considerarán acciones no autorizadas, aquellas realizadas por el personal de manera negligente o malintencionada y que contravengan la presente "*Declaración de Prácticas de Registro*", "*Política de Seguridad*", *"Política de Privacidad*" y "*Plan de Privacidad"*, así como, las directivas, guías de procedimientos, normas administrativas internas y otras normas que emita el RENIEC.

La EREP-RENIEC-PJ apenas tome conocimiento de la acción no autorizada o de su potencial ejecución, suspenderá el acceso a todos los sistemas de información a aquel personal que se encuentre involucrado en el hecho.

Con la confirmación del hecho, la EREP-RENIEC-PJ informará a la Oficina de Potencial Humano a fin de que por su intermedio se inicie el procedimiento sancionador correspondiente, y de ser el caso, se inicien las acciones legales para el resarcimiento por los daños y perjuicios en lo que pudiera verse afectado el RENIEC.

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 y, de igual manera, el Reglamento Interno de los Servidores Civiles – RIS del RENIEC.

5.3.7. Requerimientos de los contratistas

En caso de que el RENIEC, en su calidad de EREP-RENIEC-PJ, 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 subsección 5.3 del presente documento en lo que resulte aplicable, en los mismos criterios de funciones y seguridad aplicados a empleados de la EREP-RENIEC-PJ en posición similar.

5.3.8. Documentación suministrada al personal

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

- Manual de funcionamiento de equipos y software que debe operar en la EREP-RENIEC-PJ.
- La presente "*Declaración de Prácticas de Registro*", "*Política de Seguridad*", *"Política de Privacidad*" y "*Plan de Privacidad"*.[19]
- Normas Legales y marco regulatorio aplicables a sus funciones en la EREP-RENIEC-PJ.
- Documentación aplicable en caso de contingencias.
- Otra documentación relevante en relación con sus funciones en la EREP-RENIEC-PJ.

5.4. Procedimiento de registro de auditorías

En esta subsección se establecen y describen los controles implementados por la EREP-RENIEC-PJ, respecto a los hechos o eventos relevantes del proceso de identificación y su conservación en el registro de auditorías establecidos con el propósito de conservar un entorno de operaciones seguro.

5.4.1. Tipos de eventos registrados

La EREP-RENIEC-PJ registrará y conservará todos aquellos hechos o eventos que resulten relevantes para el desarrollo de las operaciones del proceso a su cargo, con la finalidad de acreditar que éste se efectúa conforme a los procedimientos internos, a la normatividad legal aplicable y según lo establecido en la "*Política de Seguridad*", permitiendo detectar causas de posibles anomalías e implementar las soluciones correspondientes.

En ese sentido, se registrarán todos los eventos relacionados con la operación y gestión del sistema, así como los relacionados con la seguridad del mismo, señalándose a continuación los eventos que se registrará como mínimo:

- Intentos no autorizados de acceso a los registros o bases de datos del sistema.
- Intentos de entrada y salida del sistema que procesa información sensible.
- Intentos de crear, borrar, cambiar PIN o permisos de los usuarios de base de datos.

Adicionalmente, la EREP-RENIEC-PJ registrará en el formato que corresponda (manual o electrónico), la información de los hechos siguientes:

- Mantenimientos y cambios de configuración del sistema que procesa información sensible.
- Acceso físico a las áreas sensibles.
- Cambios en el personal.
- Informes de los intentos de intrusión a las instalaciones de la EREP-RENIEC-PJ o faltas a la seguridad de la información.

[19] https://pki.reniec.gob.pe/repositorio/

El registro de auditorías incluirá la hora y fecha del evento, así como los identificadores del software y hardware, de ser el caso.

5.4.2. Frecuencia del procesamiento del registro

Los registros de auditoría serán objeto de un proceso de revisión, al menos mensualmente, ante alertas o alarmas que reporten algún tipo de actividad sospechosa o inusual.

El proceso de revisión de los registros de auditoría consiste en el escrutinio de dichos registros, así como la documentación de todos los eventos o hechos relevantes en el desarrollo de las operaciones, los cuales se hallan incluidos en un resumen del registro de auditoría. Las revisiones de los registros de auditoría incluyen una verificación que los mismos no han sido manipulados, una inspección de todas las entradas, y una investigación de todas las alertas o irregularidades del registro.

5.4.3. Periodo de conservación del registro de auditorías

La EREP-RENIEC-PJ conservará todos los registros de auditoría y su correspondiente documentación por un periodo mínimo de diez (10) años, conforme lo dispone la AAC.

5.4.4. Protección del registro de auditoría

La EREP-RENIEC-PJ dispone de medidas de seguridad destinadas a proteger los archivos, tanto en formato papel como electrónico o digital, que contienen los registros de auditoría de accesos no autorizados, sean internos o externos, de modo que sólo las personas debidamente designadas y con los permisos adecuados, puedan acceder a realizar la lectura y/o escritura de dichos registros.

La destrucción de los archivos que contienen registros de auditoría solo se puede llevar a cabo con la autorización de la AAC, y siempre que haya transcurrido el periodo mínimo de conservación de diez (10) años, sin perjuicio que deba observarse la normativa y procedimientos que sobre la materia dispone el RENIEC, en aplicación del procedimiento legal establecido para las eliminaciones de documentos en general previstos en las leyes especiales aplicables al sector público.

5.4.5. Procedimiento de copia de seguridad del registro de auditorías

Los registros de auditoría serán objeto de un proceso de respaldo o copia de seguridad, el cual se realiza de acuerdo con el procedimiento establecido por la EREP-RENIEC-PJ, por lo menos una vez al mes. Adicionalmente, se almacenará una copia adicional en un lugar seguro fuera de las instalaciones de la EREP-RENIEC-PJ, conforme a lo dispuesto en la subsección 5.5.6 del presente documento.

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

La EREP-RENIEC-PJ realiza, como mínimo una vez al año, una auditoría interna a los archivos que contienen los registros de auditoría. Las auditorías externas corresponden a INDECOPI en su calidad de AAC, y se efectuarán en forma periódica una vez al año.

5.4.7. Notificación al titular que causa un evento

La persona designada para realizar una auditoría a un evento de seguridad no informará previamente al autor del mismo.

Sin embargo, cuando alguna persona que efectúa funciones en la EREP-RENIEC-PJ, bajo cualquier modalidad, conoce algún evento susceptible de auditoría, debe informar inmediatamente al Oficial de Seguridad de Información y al Oficial de Privacidad de Datos para que proceda en función de la gravedad del evento o hecho.

Tratándose de eventos o hechos de índole accidental o cuya ocurrencia es susceptible que vuelva a ocurrir, se notificará también al autor a fin de que tome la acción que corresponda.

5.4.8. Valoración de la vulnerabilidad

La EREP-RENIEC-PJ dispone en la *"Política de Seguridad"* la evaluación periódica de los riesgos y vulnerabilidades detectadas.

5.5. Archivo de registros

En esta subsección se fija y describe la política de archivo de los registros en general que son objeto de las operaciones del proceso de identificación a cargo de la EREP-RENIEC-PJ.

5.5.1. Tipos de eventos registrados

La EREP-RENIEC-PJ realiza, como mínimo, el registro y archivo respectivo de los eventos o hechos siguientes:

a. Respecto de los solicitantes
- Solicitudes de emisión y cancelación.
- Documentación entregada por el solicitante.
- Datos personales de los suscriptores.
- Contrato para la prestación del servicio de certificación digital debidamente rubricado por el solicitante.

b. Respecto del proceso de identificación y registro a cargo de la EREP-RENIEC-PJ
- Oficina EREP-RENIEC donde se tramitó la solicitud.
- Autorizaciones de acceso del Operador de Registro Digital a los sistemas de información de la EREP-RENIEC-PJ.
- Operador de Registro Digital que realiza el proceso de identificación y autenticación del solicitante.
- Fecha y hora de la comunicación enviada a la ECEP-RENIEC.

c. Respecto de la EREP-RENIEC

- Los registros de auditoría especificados en la sub sección 5.4.1 del presente documento.
- Nombres de los operadores y administradores del sistema de administración de la EREP-RENIEC-PJ.
- Los registros de las auditorías internas y externas, así como de las visitas comprobatorias de la AAC y, de corresponder, las acciones de cumplimiento efectuadas.
- Versiones de la "*Declaración de Prácticas [y Políticas] de Registro*".
- Versiones de la "*Política de Seguridad*".
- Versiones de la *"Política de Privacidad*".
- Versiones del "*Plan de Privacidad"*.

5.5.2. Periodo de conservación del archivo

La EREP-RENIEC-PJ conservará todos los archivos que contienen eventos por un periodo mínimo de diez (10) años, conforme lo dispone la AAC – INDECOPI y el Archivo General de la Nación. Igual disposición se aplica para la conservación de las aplicaciones o sistemas requeridos para tener acceso a dichos archivos.

5.5.3. Protección del archivo

La EREP-RENIEC-PJ dispone de medidas de seguridad destinadas a proteger la información archivada de accesos no autorizados, sean internos o externos, así como asegurar su confidencialidad, de modo que sólo personas autorizadas puedan acceder a ella. Estas medidas de seguridad se señalan en la *"Política de Seguridad".*[20]

5.5.4. Procedimientos para copia de seguridad del archivo

Los archivos a los que se aluden en la subsección 5.5.1 del presente documento, así como el software esencial de uso exclusivo de la EREP-RENIEC-PJ, serán realizados de acuerdo con el procedimiento de respaldo o copia de seguridad establecido por el RENIEC. Adicionalmente los dispositivos que contengan dichas copias de seguridad se almacenarán en un lugar seguro fuera de las instalaciones de la EREP-RENIEC-PJ, conforme a lo dispuesto en la subsección 5.5.6 del presente documento.

Las copias de seguridad serán objeto de un procedimiento de pruebas regulares con el fin de asegurar el adecuado respaldo de la información.

5.5.5. Requisitos para los archivos de sellado de tiempo

Los datos archivados por la EREP-RENIEC-PJ consignan la fecha y hora en la que fueron generados.

[20] https://pki.reniec.gob.pe/repositorio/

5.5.6. Sistema de recolección del archivo (Interna o Externa)

El sistema de recolección y almacenamiento de los archivos es realizado en forma interna por personal calificado autorizado por la EREP-RENIEC-PJ.[21]

La copia controlada de los respaldos realizados se almacena en forma externa en un lugar seguro fuera de las instalaciones de la EREP-RENIEC-PJ.

5.5.7. Procedimiento para obtener y verificar la información del archivo

Sólo el personal autorizado tiene acceso a los elementos materiales de soporte que contienen información de respaldo con la finalidad de llevar a cabo verificaciones de integridad.

5.6. Cambio de clave

No aplica a la EREP-RENIEC-PJ.

5.7. Recuperación frente al compromiso y desastre

En esta subsección se describe la política de la EREP-RENIEC-PJ, frente a la posibilidad de desastres, producidos de forma intencional o accidental, y la garantía de la continuidad de las operaciones.

5.7.1. Procedimiento de manejo de incidentes y compromisos

La EREP-RENIEC-PJ ha implementado controles físicos, procedimentales y lógicos con la finalidad de minimizar el riesgo y potencial impacto en las operaciones del proceso: “Registros de Certificación Digital” correspondientes a la EREP-RENIEC-PJ frente a la posibilidad de desastre, sean éstos producidos en forma intencional o accidental.

En cualquier caso, los procedimientos ante desastres han sido desarrollados para minimizar el potencial impacto de tal ocurrencia y restablecer los servicios básicos a cargo de la EREP-RENIEC en un plazo razonable.

En caso de producirse un incidente en la seguridad de la información, la EREP-RENIEC-PJ recolecta y mantiene la documentación sustentatoria respectiva a fin de que el RENIEC evalúe el inicio de las acciones judiciales a que hubiere lugar.

[21] Se sigue procedimientos aplicables a la Planta de Certificación Digital del RENIEC:
DT-GRCD/SGCID-011 Gestión Base de Datos
DT-GRCD/SGCID-013 Gestión de Red de Datos
DT-GRCD/SGCID-029 Gestión de Archivos
y la directiva de la Oficina de Gestión Documental del RENIEC:
DI-434-SGEN/OAA/009 Sistema de Archivo Institucional del RENIEC.

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

La EREP-RENIEC-PJ ha implementado los procedimientos necesarios y la identificación de las fuentes alternativas de recursos computacionales, software y datos que deberán ser utilizados en caso se presente alguna falla o alteración de los mismos.

5.7.3. Procedimiento en caso de compromiso de la clave privada de la entidad

Tratándose del compromiso de la clave privada del ciudadano, se procederá inmediatamente a cancelar el certificado digital correspondiente, de acuerdo con el procedimiento de cancelación establecido.

5.7.4. Capacidad de continuidad de negocio luego de un desastre

No aplica a la EREP–RENIEC-PJ.

Sin embargo, la ECEP-RENIEC cuenta con un Centro de Datos de contingencia y un Plan de Contingencia de la SDSCD, permitiéndole garantizar la continuidad de los servicios.

5.8. Finalización de la EC o ER

En caso de que la EREP-RENIEC-PJ finalice sus actividades adoptará todas 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 la subsección 1.3 del presente documento.

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

6. CONTROLES DE SEGURIDAD TÉCNICA

De conformidad con los lineamientos establecidos por la AAC en la Guía de Acreditación de Entidades de Registro, la EREP-RENIEC-PJ utiliza sistemas y productos fiables, que están protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica del proceso que tiene a su cargo.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

En concordancia con lo señalado en la DPC de la ECEP-RENIEC, la generación del par de claves de entidades finales (titulares y/o suscriptores) se efectúa en módulos criptográficos que deben cumplir con los requisitos de seguridad FIPS 140-2 nivel de seguridad 1 como mínimo, o Common Criteria EAL4, o aquel exigido de acuerdo al nivel de acreditación de la ECEP-RENIEC.

6.1.2. Entrega al suscriptor de la clave privada

En caso de que las claves se entreguen al suscriptor en las instalaciones de la EREP-RENIEC-PJ, dicho procedimiento se lleva a cabo en un ambiente que garantice la confidencialidad en la generación de la clave privada y es totalmente controlado por el suscriptor, garantizando así su posesión y control exclusivo.

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

Una vez que una clave privada es generada en un módulo criptográfico con nivel de seguridad FIPS 140-2, nivel 1 o Common Criteria EAL4 como mínimo, se generan las estructuras PKCS#10 con las claves públicas y los datos de la persona/entidad asociada, las mismas que son firmadas digitalmente con las claves privadas generadas, y enviadas a la ECEP-RENIEC para su procesamiento. La ECEP-RENIEC verifica la integridad de la petición y de ser correcta genera el certificado digital correspondiente.

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

No aplica a la EREP-RENIEC-PJ.

6.1.5. Tamaño de las claves

No aplica a la EREP-RENIEC-PJ.

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

No aplica a la EREP-RENIEC-PJ.

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

No aplica a la EREP-RENIEC-PJ.

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

6.2.1. Estándares y controles para el módulo criptográfico

Para el almacenamiento de las claves privadas asociadas a un certificado digital solicitado por titulares y/o suscriptores, la EREP-RENIEC-PJ requerirá que los módulos criptográficos cumplan con los requerimientos señalados por la ECEP-RENIEC en su Declaración de Prácticas de Certificación, siendo estos:

- FIPS 140-2 nivel 1.
- Common Criteria EAL4.
- O aquellos requeridos de acuerdo con el nivel de acreditación de la ECEP-RENIEC, especificados en la guía de acreditación de la AAC.

6.2.2. Clave pública (n fuera de m) Control multipersonal

No aplica a la EREP-RENIEC-PJ.

6.2.3. Depósito de clave privada

La EREP-RENIEC no almacena copias de las claves privadas de los solicitantes.

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

No aplica a la EREP-RENIEC-PJ.

6.2.5. Archivo de la clave privada

La EREP-RENIEC-PJ no archiva copias de las claves privadas de los solicitantes.

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

No aplica a la EREP-RENIEC-PJ.

6.2.7. Almacenamiento de la clave privada en un módulo criptográfico

No aplica a la EREP-RENIEC-PJ.

6.2.8. Método de activación de la clave privada

No aplica a la EREP-RENIEC-PJ.

6.2.9. Método de desactivación de la clave privada

No aplica a la EREP-RENIEC-PJ.

6.2.10. Método de destrucción de la clave privada

No aplica a la EREP-RENIEC-PJ.

6.2.11. Clasificación del módulo criptográfico

En concordancia con lo señalado en la DPC de la ECEP-RENIEC, los módulos criptográficos usados por los titulares y/o suscriptores deben cumplir con los requisitos de seguridad FIPS 140-2 nivel de seguridad 1 como mínimo, o Common Criteria EAL4, o aquel exigido de acuerdo con el nivel de acreditación de la ECEP-RENIEC. Asimismo, los módulos criptográficos usados por los operadores de la EREP-RENIEC cumplen con los requisitos de seguridad FIPS 140-2 nivel de seguridad 2.

6.3. Otros aspectos de la gestión del par de claves

No aplica a la EREP-RENIEC-PJ.

6.3.1. Archivo de la clave pública

No aplica a la EREP-RENIEC-PJ.

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

No aplica a la EREP-RENIEC-PJ.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

No aplica a la EREP-RENIEC-PJ.

6.4.2. Protección de los datos de activación

El acceso a cada certificado se realiza a través del PIN elegido por el solicitante, el cual se bloquea al tercer intento fallido.

6.4.3. Otros aspectos de los datos de activación

La EREP-RENIEC-PJ recomendará a los titulares y/o suscriptores que en la generación de los datos de activación (contraseña o PIN) para acceder a su clave privada cumplan como mínimo con las características siguientes, dependiendo estas del medio portador utilizado por el titular y/o suscriptor:

- Sean generados por el titular y/o suscriptor sin la intermediación de un tercero.
- Tengan al menos 8 caracteres.
- Tengan al menos un carácter alfabético y uno numérico.
- Tengan al menos una letra minúscula.
- No contengan demasiadas veces el mismo carácter.
- No sean igual al nombre del usuario.

- No contengan una parte larga de nombre del perfil del usuario.

6.5. Controles de seguridad computacional

En esta subsección se describen los controles y evaluaciones de seguridad computacionales que ha implementado el RENIEC, en su calidad de EREP-RENIEC-PJ, a efectos de proteger la información sensible que mantiene o procesa.

6.5.1. Requisitos técnicos específicos para seguridad computacional

La EREP-RENIEC-PJ observa el cumplimiento de los controles establecidos en:

- NTP-ISO/IEC 27002:2017 *Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información.* 1ª Edición
- Norma Técnica Peruana *"NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición"* (de uso obligatorio en todas las entidades integrantes del Sistema Nacional de Informática conforme lo dispone la Resolución Ministerial Nº 004-2016-PCM de fecha el 8 de enero de 2016).

6.5.2. Evaluación de la seguridad computacional

La EREP-RENIEC-PJ mantiene sus equipos y sistemas críticos en un área restringida. Además, mantiene los equipos necesarios para el cumplimiento de sus funciones operativas (como atención y procesamiento de solicitudes) en un área dedicada y aislada de otras actividades. Al respecto, se realizan auditorías internas al menos una vez al año, según lo indicado en el numeral 6.5.1, *Requisitos técnicos específicos de seguridad computacional*.

6.6. Controles técnicos del ciclo de vida

No aplica a la EREP-RENIEC-PJ.

6.6.1. Controles de desarrollo del sistema

No aplica a la EREP-RENIEC-PJ.

6.6.2. Controles de gestión de seguridad

No aplica a la EREP-RENIEC-PJ.

6.6.3. Evaluación de seguridad de ciclo de vida

No aplica a la EREP-RENIEC-PJ.

6.7. Controles de seguridad de la red

No aplica a la EREP-RENIEC-PJ.

6.8. Sello de tiempo

No aplica a la EREP-RENIEC-PJ.

7. PERFILES DE CERTIFICADO

Esta sección no corresponde a la EREP-RENIEC-PJ. Para obtener más información sobre este tema deberá remitirse a la DPC de la ECEP-RENIEC.

7.1. Perfil de certificado

No aplica a la EREP-RENIEC-PJ.

7.2. Perfil CRL

No aplica a la EREP-RENIEC-PJ.

7.3. Perfil OCSP

No aplica a la EREP-RENIEC-PJ.

8. AUDITORIAS DE COMPATIBILIDAD Y OTRAS EVALUACIONES

De acuerdo con los lineamientos establecidos por la AAC, la EREP-RENIEC-PJ llevará a cabo auditorías externas anuales que tendrán como objetivo evaluar la conformidad de las operaciones y que éstas se encuentren alineadas al marco de la IOFE. De conformidad a lo señalado en la subsección 8.6 del presente documento, el resultado de estas auditorías será publicado por la AAC. Sin perjuicio de las auditorías externas, se realizarán auditorías internas o evaluaciones de conformidad en la EREP-RENIEC-PJ, a fin de verificar el cumplimiento de los procedimientos establecidos y velar por la seguridad de la información.

La EREP-RENIEC-PJ mantendrá un registro con toda la documentación y acciones ejecutadas como consecuencia de los procedimientos regulados en la presente sección.

8.1. Frecuencia y circunstancias de la evaluación

La EREP-RENIEC-PJ llevará a cabo una auditoría externa de forma anual que evalúe la conformidad de las operaciones y que éstas se encuentren alineadas al marco de la IOFE. Esta auditoría también podrá comprender la evaluación del cumplimiento de lo establecido en la presente DPR.

El resultado de las auditorías externas será publicado en la forma señalada en la subsección 8.6 del presente documento.

Sin perjuicio de las auditorías externas, se realizarán auditorías internas o evaluaciones de conformidad en la EREP-RENIEC en cualquier momento, a causa de alguna sospecha de incumplimiento de alguna medida de seguridad o de los procedimientos establecidos por aquella. Esta auditoría puede comprender la evaluación del cumplimiento del Plan de Privacidad.

El resultado de las auditorías internas será informado al Director de la Dirección de Certificación y Servicios Digitales, al Sub Director de la Sub Dirección de Servicios de Certificación Digital, a la Gerencia General del RENIEC y al Representante de la EREP-RENIEC-PJ.

8.2. Identidad / Calificaciones de asesores

La ejecución de un procedimiento de auditoría externa se llevará a cabo por auditores independientes de la entidad; las personas que realicen dicha auditoría deberán tener experiencia en PKI y tecnologías criptográficas, en seguridad de tecnologías de la información y procesos de auditoría.

De conformidad con lo señalado por la AAC en la respectiva Guía de Acreditación de ER, las personas que realizarán las auditorías o evaluaciones de compatibilidad bajo el marco de la IOFE serán previamente aprobadas por la AAC.

8.3. Relación del auditor con la entidad auditada

Las auditorías externas serán realizadas por auditores o asesores que no tengan relación alguna, actual o planificada, o de cualquier otra clase con el RENIEC, de modo que pueda garantizarse la independencia de aquellos con las funciones y actividades que desarrolla la EREP-RENIEC-PJ.

En el caso de los auditores internos, estos no podrán tener relación funcional con el área objeto de la auditoría.

8.4. Elementos cubiertos por la evaluación

Los auditores o asesores evaluarán el cumplimiento de la implementación de las prácticas de personal, procedimientos y medidas técnicas desplegadas por la EREP-RENIEC-PJ como entidad prestadora de servicios de certificación digital dentro del marco de la IOFE.

En tal sentido, los principales aspectos cubiertos por la auditoría son los que se detallan a continuación:

- Identificación y autenticación.
- Servicios y/o funciones operacionales.
- Los controles de seguridad física.
- Los controles para la ejecución de los procedimientos y los controles para las personas.
- Controles de seguridad técnicos.

8.5. Acciones para ser tomadas frente a resultados deficientes

La identificación de deficiencias detectadas como resultado de la auditoría externa, dará lugar a la implementación de las medidas correctivas. De conformidad a lo señalado en la respectiva Guía de Acreditación de ER, la AAC, en atención al informe técnico del auditor, determinará la acción que deberá ser adoptada por parte de la EREP-RENIEC-PJ.

En caso de detectarse alguna deficiencia o irregularidad el INDECOPI en su calidad de AAC, podrá adoptar las siguientes acciones:

- Indicar las irregularidades, pero permitir a la EREP-RENIEC-PJ que continúe sus operaciones hasta la próxima auditoría.
- Permitir a la EREP-RENIEC-PJ que continúe sus operaciones por un máximo de treinta (30) días calendarios pendientes a la corrección de los problemas antes de suspender su operación.
- Suspender la operación de la EREP-RENIEC.

En el supuesto que la AAC tome la opción de suspender las operaciones de la EREP-RENIEC-PJ, todos los certificados comprometidos emitidos por la ECEP-RENIEC serán cancelados por revocación antes de la suspensión del servicio.

8.6. Publicación de resultados

El auditor externo comunicará el resultado de las auditorías externas a la AAC y a la EREP-RENIEC-PJ, el cual será publicado por esta última.[22]

[22] https://pki.reniec.gob.pe/acreditaciones/

9. OTRAS MATERIAS DE NEGOCIO Y LEGALES

9.1. Tarifas

Las tasas respectivas por la prestación del servicio de certificación digital se encuentran establecidas en el Texto Único de Procedimientos Administrativos (TUPA) del RENIEC. Estas tasas están orientadas a los costos asociados a la prestación del servicio, el cual comprende los procesos a cargo de la EREP-RENIEC-PJ y ECEP-RENIEC.

9.1.1. Tarifas para la emisión de certificados

La emisión de certificados digitales está supeditada al pago previo de la tasa respectiva establecida en el Texto Único de Procedimientos Administrativos del RENIEC (TUPA). Esta tasa es un tributo que grava la emisión del certificado digital.

9.1.2. Tarifas de acceso a certificados

No aplica a la EREP–RENIEC-PJ.

9.1.3. Tarifas para información sobre cancelación o estado

No aplica a la EREP–RENIEC-PJ.

9.1.4. Tarifas para otros servicios

Todas las tasas respectivas por la prestación del servicio de certificación digital se encuentran establecidas en el Texto Único de Procedimientos Administrativos del RENIEC (TUPA). Estas tasas están orientadas a los costos asociados a la prestación del servicio, el cual comprende los procesos a cargo de la EREP-RENIEC-PJ y ECEP-RENIEC-PJ.

9.1.5. Políticas de reembolso

Es política del RENIEC, en su calidad de Prestador de Servicios de Certificación Digital para el Estado Peruano, reembolsar al solicitante la tasa respectiva por la emisión del certificado digital, cuando se demuestre fehacientemente que por motivos de responsabilidad de la EREP o ECEP, no se haya cumplido con la entrega del certificado digital.

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

9.2. Responsabilidad financiera

9.2.1. Cobertura de seguro

La EREP-RENIEC-PJ dispondrá de una garantía con cobertura suficiente de responsabilidad civil, a través del seguro contratado por

el RENIEC. El referido seguro cubrirá el riesgo de la responsabilidad por los daños y perjuicios que se pudiese ocasionar a terceros como resultado de las actividades a cargo de la EREP-RENIEC-PJ, cumpliendo de este modo con la obligación señalada en el artículo 31 del Reglamento de la Ley de Firmas y Certificados Digitales

9.2.2. Otros activos

La EREP-RENIEC-PJ, para la prestación del servicio de certificación a su cargo, cuenta con el respaldo económico del RENIEC y con la infraestructura e instalaciones necesarias a nivel nacional.

9.2.3. Cobertura de seguro o garantía para entidades finales

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

9.3. Confidencialidad de la información del negocio

La EREP-RENIEC-PJ mantendrá la confidencialidad de toda aquella información que ha sido clasificada como “información confidencial”.

9.3.1. Alcances de la información confidencial

La EREP-RENIEC-PJ declara expresamente como información confidencial, la misma que no podrá ser divulgada a terceros y que se mantendrá con carácter de reservado a la siguiente:

- Material o información reservada de la EREP-RENIEC-PJ incluyendo términos contractuales, planes de negocio y propiedad intelectual.
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los titulares y/o suscriptores.
- Información que pueda permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los titulares, suscriptores y el tercero que confía.
- La causal que motivó la cancelación del certificado digital.
- Información personal provista por los titulares y/o suscriptores que no sea la autorizada para estar contenida en los certificados digitales y en la Lista de Certificados Cancelados (CRL).
- Toda la información clasificada como “confidencial”.
- Las indicadas en la “*Política de Seguridad”*.

9.3.2. Información no contenida dentro del rubro de información confidencial

Se considera información pública y por tanto accesible por terceros:

- La contenida en la presente DPR.
- La contenida en la “*Política de Privacidad”*.
- Los certificados digitales emitidos por la ECEP-RENIEC, así como las informaciones contenidas en éstos y el estado de los mismos.

- La lista de certificados digitales cancelados (CRL), sin revelar la razón de dicha cancelación e información del estado de los certificados.
- Toda otra información clasificada como “pública”.

En todo caso, el acceso a dicha información será permitido sin perjuicio que la EREP-RENIEC-PJ aplique los controles de seguridad pertinentes con el fin de proteger la autenticidad e integridad de los documentos, así como impedir que personas no autorizadas puedan añadir, modificar o suprimir contenidos.

9.3.3. Responsabilidad de protección de la información confidencial

Los colaboradores de la EREP-RENIEC-PJ, el personal contratado por el RENIEC y el personal de algún proveedor, que participen en cualquiera de las actividades del proceso a cargo de aquella, están obligados a guardar secreto sobre la información clasificada como “confidencial”, según lo señalado en el “*Plan de Privacidad”*.

9.4. Privacidad de la información personal

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

La EREP-RENIEC-PJ asegura a los titulares y/o suscriptores el adecuado tratamiento de sus datos personales, los cuales serán tratados para los fines propios de la prestación del servicio de certificación digital o para otros propósitos relacionados con dichos servicios, y que permitan otorgar confianza al tercero que confía o tercer usuario, pudiendo ellos verificar el estado del certificado digital emitido por la ECEP-RENIEC.

9.4.1. Plan de privacidad

La EREP-RENIEC-PJ juntamente con la ECEP-RENIEC, han desarrollado un “*Plan de Privacidad”*, el cual recoge los principios de la Ley antes indicada, así como de la Norma Marco de Privacidad del APEC, aprobada mediante Resolución N° 030-2008-RT-INDECOPI.

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

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

9.4.2. Información tratada como privada

La EREP-RENIEC-PJ declara expresamente como información personal de carácter privado, a toda a aquella información que no se encuentre contenida en los certificados digitales ni en la Lista de Certificados Digitales Cancelados (CRL).

En todo caso, la información siguiente es considerada como privada:

- Solicitudes de certificados digitales, aprobadas o denegadas, así como toda otra información personal que tenga carácter privado y ha sido obtenida para la expedición y mantenimiento del certificado digital.
- Toda la documentación contenida en el expediente que custodia la EREP-RENIEC-PJ y que no forme parte de la información contenida en el certificado digital.
- La causal que originó la cancelación del certificado digital.
- Toda otra información personal que tenga el carácter de "información privada".

La información personal considerada como privada de acuerdo con el Plan de Privacidad de la EREP-RENIEC-PJ es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizada.

9.4.3. Información no considerada como privada

La información personal tratada como pública es aquella que se incluye en los certificados digitales y en la Lista de Certificados Digitales Cancelados (CRL). Se detalla, pero no limita a:

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

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

a. Certificados digitales emitidos o en trámite de emisión.
b. Certificados digitales cancelados.
c. Datos de identificación que figuran en el certificado digital del titular y/o suscriptor.
d. Usos y límites de uso de los certificados digitales.
e. Aquella información personal que los titulares y/o suscriptores soliciten o autoricen que se publique.
f. El periodo de validez del certificado digital, así como la fecha de emisión y fecha de caducidad del certificado digital.
g. El número de serie del certificado digital.

9.4.4. Responsabilidad de protección de la información privada

La EREP-RENIEC-PJ consciente de la importancia de la protección de los datos personales, cumple con los principios y las disposiciones establecidas en la Ley N° 29733 - Ley de Protección de Datos Personales y su Reglamento.

En tal sentido, la EREP-RENIEC ha implementado medidas de seguridad de índoles organizativas y técnicas orientadas a mantener la más estricta confidencialidad de la información y de los datos personales de carácter privado de los titulares y/o suscriptores de los certificados digitales, recogida dentro del marco de la prestación del servicio de certificación digital.

9.4.5. Notificación y consentimiento para el uso de información

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

De conformidad con lo dispuesto en el numeral 1 del Artículo 14[23] de la Ley N° 29733 - Ley de Protección de Datos Personales y su Reglamento, la EREP-RENIEC-PJ está exceptuada de solicitar el consentimiento al titular de los datos, para el tratamiento y transferencia de sus datos personales.

No obstante, la EREP-RENIEC-PJ, mediante la *"Política de Privacidad"* informa al titular y/o suscriptor respecto de:

- Los datos personales que recolecta;
- Fines del uso y tratamiento de la información personal;
- La información personal pública y de carácter privado;
- Las medidas de seguridad para proteger la información personal de carácter privado;
- Las circunstancias bajo las cuales será divulgada, o transferida la información personal;
- Los derechos del titular y/o suscriptor, entre otros.

Asimismo, a través de la página web del RENIEC se mantiene constantemente informado al usuario sobre los servicios de certificación digital, las distintas clases de certificados digitales, los requisitos para obtener un certificado digital, entre otros temas.

9.4.6. Divulgación realizada con motivo de un proceso judicial o administrativo

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

9.4.7. Otras circunstancias para divulgación de información

La EREP-RENIEC-PJ, dentro del marco de colaboración entre entidades del sector público, podrá comunicar o ceder a otras

[23] **Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales**
No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:
1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.

Entidades de la Administración Pública los datos personales de los titulares y suscriptores.

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

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

En todos los casos, la Entidad receptora debe garantizar a la EREP-RENIEC-PJ la confidencialidad de la información transferida.

9.5. Derechos de propiedad intelectual

Todos los derechos de propiedad intelectual incluyendo los que correspondan a las aplicaciones o software desarrollado para las actividades de la EREP-RENIEC-PJ, OIDs, la presente "*Declaración de Prácticas de Registro*", "*Política de Seguridad*", *"Política de Privacidad*" y "*Plan de Privacidad"*, así como cualquier otro documento, electrónico o de cualquier otro tipo, son propiedad del RENIEC y de uso exclusivo de la EREP-RENIEC-PJ y ECEP-RENIEC. Por tanto, se prohíbe cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son de titularidad de la EREP-RENIEC-PJ y ECEP-RENIEC, sin la autorización expresa del RENIEC.

Las claves privadas y las claves públicas son propiedad del titular.

9.6. Responsabilidades y garantías

9.6.1. Responsabilidades y garantías de la EC

No aplica a la EREP-RENIEC.

9.6.2. Responsabilidades y garantías de la ER

Son obligaciones de la EREP-RENIEC-PJ:

- Realizar sus operaciones de conformidad con esta DPR.
- Comprobar exhaustivamente la identidad de los solicitantes.
- Gestionar ante la ECEP-RENIEC la generación de los certificados digitales.
- Tramitar las solicitudes de cancelación de los certificados digitales.
- Mantener la confidencialidad de la información personal que tenga carácter privado de los titulares y suscriptores de los certificados digitales, limitando su empleo a las necesidades propias del servicio de certificación digital, salvo orden judicial o pedido del titular o suscriptor del certificado digital.
- En general, es obligación de la EREP-RENIEC-PJ cumplir con todo lo estipulado en el artículo 30º del Reglamento de la Ley de Firmas y Certificados digitales, así como lo contenido en el presente documento.

- Determinar objetivamente y en forma directa la veracidad de la información proporcionada por los solicitantes.

La EREP-RENIEC-PJ asume que la información personal proporcionada por los titulares y suscriptores es verídica; éste es responsable de comunicar, de manera inmediata, a la EREP-RENIEC cualquier modificación en los mismos. Los titulares y suscriptores asumirán las responsabilidades por los daños y perjuicios que pudiera causar por aportar datos falsos, incompletos o inexactos.

En ese sentido, la EREP-RENIEC-PJ está exenta de toda responsabilidad cuando el error o la omisión de algún dato contenido en el certificado digital devienen de la información consignada por los titulares y suscriptores en las respectivas solicitudes de emisión.

Estas obligaciones se encuentran recogidas en el respectivo contrato de prestación de servicios de certificación digital a ser suscrito por los titulares y suscriptores.

9.6.3. Responsabilidades y garantías de los suscriptores

Son obligaciones de los titulares y suscriptores del certificado digital:

- Entregar información veraz bajo su responsabilidad.
- Actualizar la información proporcionada a la EREP-RENIEC-PJ cuando estos ya no resulten exactos o son incorrectos.
- Custodiar su PIN o clave de identificación personal (PIN[24]) de acceso a su clave privada de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado.
- Observar las condiciones establecidas por la ECEP-RENIEC, para la utilización del certificado digital y la generación de firmas digitales.
- Realizar un uso debido y correcto del certificado digital.
- Notificar de inmediato a la EREP-RENIEC-PJ en caso se detecte que se ha incluido información incorrecta o inexacta en el certificado digital.
- Generar la clave privada y firmar digitalmente mediante los procedimientos señalados por la EREP-RENIEC-PJ.
- Mantener el control y la reserva de la clave privada, bajo su responsabilidad.
- Solicitar inmediatamente a la EREP-RENIEC-PJ la cancelación de su certificado digital en caso de tener conocimiento o sospecha de la ocurrencia de alguna de las siguientes circunstancias:
  a. Exposición, puesta en peligro o uso indebido de la clave privada o PIN de acceso a su clave privada.
  b. Deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada o el PIN de acceso a su clave privada.

[24] Corresponde con el término en inglés *Personal Identification Number* (PIN).

El compromiso de la clave privada del certificado digital entre otras causas puede ser por: pérdida, robo, conocimiento por terceros de la clave personal de acceso.

- Solicitar de inmediato a la EREP-RENIEC-PJ la cancelación del certificado cuando:
  a) La información contenida en el certificado digital ya no resulte correcta.
  b) El suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la ECEP-RENIEC.

Estas obligaciones se encuentran recogidas en el respectivo contrato a ser suscrito por los titulares y suscriptores.

De otro lado, el titular y/o suscriptor del certificado asumirá toda la responsabilidad y riesgos derivados de la fiabilidad y seguridad de su equipo informático o medio portador o repositorio desde el cual emplee su certificado digital.

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

9.6.4. Responsabilidades y garantías de los terceros que confían

Es obligación de los Terceros que Confían en los certificados digitales emitidos por la ECEP-RENIEC:

- Verificar la validez de los certificados digitales en el momento de realizar cualquier operación basada en los mismos mediante la comprobación de que el certificado es válido y no está caducado o ha sido cancelado.
- No usar los certificados digitales fuera de los términos establecidos en el marco de la IOFE.
- Limitar la fiabilidad de los certificados digitales a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados digitales y la *"Declaración de Prácticas y Políticas de Certificación"* de la ECEP-RENIEC.
- Dar lectura a la presente DPR.
- Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados digitales en los que confía, y aceptar sujetarse a las mismas.

9.6.5. Responsabilidades y garantías de otros participantes

No intervienen otros participantes.

9.7. Exención de garantías

La EREP-RENIEC-PJ está exenta del pago de indemnización alguna en caso que el hecho o circunstancia acaecida no sea consecuencia de lo declarado en la subsección 9.9 del presente documento.

9.8. Limitaciones a la responsabilidad

La EREP-RENIEC-PJ asumirá toda la responsabilidad sobre la correcta identificación de los titulares y suscriptores de los certificados digitales y la validación de sus datos; no obstante, la EREP-RENIEC-PJ está exenta de responsabilidad alguna, en los casos que a continuación se detallan:

- Por daños derivados de o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del titular y/o suscriptor.
- Cuando el error o la omisión de algún dato contenido en el certificado digital deviene de la información consignada por el titular y/o suscriptor en los respectivos formatos de solicitud de emisión.
- Por cualquier violación a la confidencialidad que en el uso de datos personales pudieran incurrir el propio titular y/o suscriptor del certificado digital.
- Cuando el titular y/o suscriptor no ha tenido la debida diligencia o cuidado en la creación de su PIN o números de identificación personal (PIN[25]) de acceso a su clave privada.

De igual modo, la EREP-RENIEC-PJ no será responsable de:

- La utilización incorrecta de los certificados digitales ni de las claves, así como de cualquier daño indirecto que pueda resultar de la utilización del certificado o de la información almacenada en el procesador del dispositivo criptográfico.
- Los daños que puedan derivarse de aquellas operaciones en que se hayan incumplido las limitaciones de uso del certificado digital.
- El contenido de aquellos documentos firmados digitalmente por el titular y/o suscriptor.

Finalmente, si los certificados digitales expiraron, la EREP-RENIEC-PJ no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones contenidas en la presente DPR si tal falta de ejecución o retraso fuera consecuencia de un supuesto de fuerza mayor, caso fortuito, o en general, cualquier circunstancia en la que no se pueda tener un control directo.

Las limitaciones de responsabilidad antes indicadas, se encuentran recogidas en el respectivo contrato a ser suscrito por los titulares y suscriptores.

9.9. Indemnizaciones

La EREP-RENIEC-PJ dispondrá de una garantía con cobertura suficiente de responsabilidad civil, a través del seguro contratado por el RENIEC. El referido seguro cubrirá el riesgo de la responsabilidad por los daños y perjuicios que se pudiese ocasionar a terceros como resultado de las actividades a cargo de la EREP-RENIEC-PJ.

[25] Corresponde con el término en inglés *Personal Identification Number* (PIN).

9.10. Término y terminación

9.10.1. Término

La presente DPR entra en vigor desde el momento que es aprobada por la AAC, dentro del procedimiento administrativo de acreditación de la EREP-RENIEC-PJ que implica su ingreso a la IOFE, manteniendo su validez durante un periodo máximo de tres (05) años, de acuerdo a la legislación vigente. No obstante, dicho documento podrá ser modificado cada vez que lo determine la EREP-RENIEC-PJ o la AAC siguiéndose lo establecido para dicho fin en las sub secciones 1.5.3 y 1.5.4 del presente documento respectivamente.

En el supuesto que caducase la acreditación o cese las operaciones de la EREP–RENIEC–PJ, se entenderá que toda la documentación relativa queda sin vigencia, aplicándose en tal situación lo señalado en la subsección 9.10.2 del presente documento.

9.10.2. Terminación

En caso de cese de las actividades de la EREP-RENIEC-PJ, el RENIEC informará a la AAC, titulares, suscriptores y terceros que confían con treinta (30) días calendario de anticipación.

9.10.3. Efecto de terminación y supervivencia

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

9.11. Notificaciones y comunicaciones individuales con los participantes

Sin perjuicio de lo señalado en la sección cuarta de la presente DPR, sobre requisitos operacionales del ciclo de vida de los certificados, los titulares y suscriptores podrán consultar en cualquier momento el periodo de validez de sus certificados digitales a través de la página web del RENIEC.

9.12. Enmendaduras

9.12.1. Procedimiento para enmendaduras

De conformidad con la legislación vigente, la EREP-RENIEC-PJ, en caso se modifique el contenido del presente documento, presentará a la AAC la nueva versión de la DPR para su respectiva aprobación.

9.12.2. Mecanismos y periodo de notificación

La EREP-RENIEC-PJ pondrá a disposición de la comunidad de usuarios la nueva versión de la DPR, una vez que la misma haya sido aprobada por la AAC.

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

9.12.3. Circunstancias bajo las cuales debe ser cambiado el OID

No aplica a la EREP-RENIEC-PJ.

9.13. Procedimiento sobre resolución de disputas

En caso el reclamo esté directamente relacionado con el servicio de certificación digital brindado por la EREP-RENIEC-PJ o la ECEP-RENIEC, se deberá acercar a una oficina EREP-RENIEC-PJ para presentar su reclamo respectivo.

El reclamo será resuelto por la EREP-RENIEC-PJ según el procedimiento establecido en el TUPA del RENIEC y, de conformidad con la Segunda Disposición Complementaria Final del Reglamento de la Ley de Firmas y Certificados Digitales, el titular o suscriptor podrá, si lo considera pertinente, recurrir en vía administrativa ante la AAC, la que en los casos en los que proceda tal reclamación dispondrá las medidas correctivas necesarias, todo ello con sujeción a la ley N° 27444, Ley del Procedimiento Administrativo General.

9.14. Ley aplicable

El funcionamiento y operaciones de la EREP-RENIEC-PJ, así como la presente DPR estarán sujetos a la normatividad que resulte aplicable y en especial a las disposiciones siguientes:

- Ley N° 27269 - Ley de Firmas y Certificados Digitales.
- Reglamento de la Ley de Firmas y Certificados aprobado mediante el Decreto Supremo Nº 052-2008-PCM y sus modificatorias.
- Guía de Acreditación de Entidades de Registro ER.
- Ley N° 29733 - Ley de Protección de Datos Personales y su Reglamento.

Así como a las disposiciones que sobre la materia dicte la AAC en el marco de la IOFE.

9.15. Conformidad con la ley aplicable

Es responsabilidad de la EREP-RENIEC-PJ, en la prestación de sus servicios velar por el cumplimiento de la legislación aplicable recogida en la subsección 9.14 del presente documento, y que la misma haya sido recogida en los correspondientes contratos.

9.16. Cláusulas misceláneas

9.16.1. Acuerdo íntegro

Los titulares y suscriptores de certificados digitales, así como los terceros que confían deben observar en su totalidad el contenido del presente documento, así como las actualizaciones que se realicen sobre el mismo, los cuales estarán disponibles en la página web del RENIEC.

De otro lado, el contrato recoge el acuerdo íntegro entre la EREP-RENIEC y la ECEP-RENIEC para la prestación del servicio de certificación digital.

9.16.2. Subrogación

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

9.16.3. Divisibilidad

No aplica a la EREP – RENIEC - PJ.

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

No se estipula.

9.16.5. Fuerza mayor

La EREP-RENIEC-PJ, así como la ECEP-RENIEC en ningún caso serán responsables por daños o perjuicios causados por:

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

Sin perjuicio de lo expuesto, la EREP-RENIEC-PJ dentro de lo posible asegurará la continuidad del negocio y recuperación ante desastres.

9.17. Otras cláusulas

La EREP-RENIEC-PJ, adicionalmente a lo señalado en el presente documento, podrá incluir en la Declaración de Prácticas y Políticas de Registro, otras disposiciones relacionadas a las actividades y operaciones que realizará bajo la IOFE.

10. BIBLIOGRAFÍA

En la redacción de la presente DPR se utilizó:

- Ley N° 27269, de Firmas y Certificados Digitales.
- Reglamento de la Ley de Firmas y Certificados Digitales aprobado mediante el Decreto Supremo Nº 052-2008-PCM, y sus modificatorias.
- Ley N° 29733, de Protección de Datos Personales.
- Guía de Acreditación de Entidades de Registro ER expedida por la AAC.
- RFC 3647 “Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framewortk” del Internet Engineering Task Force (IETF) (que sustituye a la RFC 2527).
- Norma Marco sobre Privacidad para los países integrantes del APEC, aprobada en la 16º Reunión Ministerial del APEC, Santiago de Chile, 17 y 18 de noviembre de 2004.
- Norma Técnica Peruana “NTP-ISO/IEC 27002:2017 Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información. 1ª Edición.”
- Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición” (de uso obligatorio en todas las entidades integrantes del Sistema Nacional de Informática conforme lo dispone la Resolución Ministerial Nº 004-2016-PCM de fecha el 8 de enero de 2016).

11. ACRÓNIMOS & ABREVIATURAS

- **AAC** Autoridad Administrativa Competente.
- **AFIS** Automated Fingerprint Identification System (Sistema Automático de Identificación de Huellas Dactilares).
- **APEC** Asia Pacific Economic Group.
- **CRL o LCR** Lista de Certificados Digitales Cancelados (Certificate Revocation List).
- **DCSD** Dirección de Certificación y Servicios Digitales (ex GRCD o Gerencia de Registros de Certificación Digital)
- **DPC o CPS** Declaración de Prácticas y Políticas de Certificación (Certificate Practice Statement).
- **DPR o RPS** Declaración de Prácticas y Políticas de Registro (Registration Authority Practice Statement).
- **DNI** Documento Nacional de Identidad.
- **EC** Entidad de Certificación.
- **ECEP-RENIEC** Entidad de Certificación para el Estado Peruano.
- **ER** Entidad de Registro.
- **EREP-RENIEC-PJ** Entidad de Registro o Verificación para el Estado Peruano para Persona Jurídica.
- **IOFE** Infraestructura Oficial de Firma Electrónica.
- **OCSP** Online Certificate Status Protocol (Protocolo del estado en línea del certificado).
- **OID** Identificador de objeto.
- **PIN** Personal Identification Number (Número de identificación personal).
- **PKI** Public key infrastructure (Infraestructura de clave pública)
- **PKCS10** Estándar criptográfico de clave pública que define la sintaxis de una petición de certificado (Certification Request Syntax Standard).
  Identificación personal.
- **PSC** Prestador de Servicios de Certificación Digital.
- **PUK** Personal Unlock Key (Clave de desbloqueo personal).
- **RENIEC** Registro Nacional de Identificación y Estado Civil.
- **RUC** Registro Único de Contribuyentes.
- **SVA** Prestador de Servicios de Valor Añadido.
- **SDSCD** Sub Dirección de Servicios de Certificación Digital (ex SGCID o Sub Gerencia de Certificación e Identidad Digital y ex SGRD o Sub Gerencia de Registro Digital)
- **SUNAT** Superintendencia Nacional de Administración Tributaria.
- **TUPA** Texto Único de Procedimiento Administrativo.
- **UPS** Uninterruptible Power Supply (Sistema de alimentación ininterrumpida).

12. GLOSARIO

- **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 reguladas en el Reglamento de la Ley de Firmas y Certificados Digitales a prestar los servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica.

- **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 Reglamento de la Ley de Firmas y Certificados Digitales 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.

- **Cancelación:** 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 y Políticas de Registro (DPR).

- **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.

- **Ciclo de vida del certificado digital**: referido a la emisión, suspensión, cancelación o re-emisión de un certificado digital.

- **Clave Privada**: es una de la claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un documento electrónico y es mantenida en reserva por el titular de la firma digital.

- **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 cualquiera persona.

- **Declaración de Prácticas y Políticas de Certificación (DPC)**: documento oficialmente presentado por una Entidad de Certificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Certificación.

- **Declaración de Prácticas y Políticas de Registro (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.

- **Entidad final**: es el suscriptor de un certificado digital.

- **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.

- **Firma Digital**: es aquella firma electrónica que utilizando una técnica de criptografía asimétrica permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su control, de manera que está vinculada únicamente al signatario y a los datos a los que se refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior, tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita, siempre y cuando haya sido generada por un Prestador de Servicios de Certificación Digital debidamente acreditado que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica.

- **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, DPC, etc.).

- **Infraestructura Oficial de Firma Electrónica**: 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.

- **Lista de Certificados Digitales Cancelados (CRL o LCR)**: es aquella en la que se deberá incorporar todos los certificados cancelados por la entidad de certificación de acuerdo con lo establecido en el Reglamento de la Ley de Firmas y Certificados Digitales.

- **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 Digital (PSC)**: 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.

- **Representante del Titular:** Persona designada por la entidad de la Administración Pública o persona jurídica, cuyas facultades fueron evaluadas para representar a la entidad y realizar los trámites respectivos ante la EREP-RENIEC.

- **Revocación:** La revocación supone la cancelación de oficio de los certificados por parte de la Entidad de Certificación, quien debe contar, para tal efecto, con procedimientos detallados en su Declaración de Prácticas y Políticas de Certificación.

- **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 entidad de la Administración Pública o 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 dispositivo de servidor o un sistema de intermediación electrónica, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la entidad. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma entidad.

- **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 la entidad de la Administración Pública o Persona 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.