IVAN PEREYRA VILLANUEVA
Sub Director de Servicios de Certificación Digital
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: PEREYRA VILLANUEVA Ivan FAU 20295613620 soft
Motivo: En señal de conformidad
Fecha: 06/06/2022 11:18:29-0500

ERNESTO ANTONIO ARANDA VERGARA
Director de Certificación y Servicios Digitales
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

Firmado digitalmente por: ARANDA VERGARA Ernesto Antonio FAU 20295613620 hard
Motivo: En señal de conformidad
Fecha: 06/06/2022 11:25:37-0500

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Declaración de Prácticas de Registro

Entidad de Registro o Verificación para el Estado Peruano

Personal Natural

EREP – RENIEC – PN

(Certificados Digitales en el DNIe)

Código: DA-DCSD/SDSCD-002		
OID: 1.3.6.4.1.35300.1.2.1.2		
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

FIRMA DIGITAL

Firmado digitalmente por: RAMIREZ SALAZAR Alejandro Javier FIR 43520433 hard
Motivo: Soy el autor del documento
Fecha: 06/06/2022 10:00:20-0500

FIRMA DIGITAL

Firmado digitalmente por: GALLO MONTANI Alfredo Rafael FAU 20295613620 soft
Motivo: En señal de conformidad
Fecha: 06/06/2022 10:28:50-0500

Historial de Cambios				
Ver.	**Fecha**	**Descripción**	**Responsable**	**Estado**
1.0	22/07/2012	Elaboración	Sub Gerencia de Apoyo Administrativo Sub Gerencia de Procesamiento de Identificación Sub Gerencia de Archivo Registral Físico	Elaborado
1.0	30/07/2012	Aprobación	Sub Jefatura Nacional	Aprobado
2.0	24/09/2012	Actualización del proceso	Sub Gerencia de Apoyo Administrativo Sub Gerencia de Archivo Registral Físico	Actualizado
2.0	12/11/2012	Aprobación	Sub Jefatura Nacional	Aprobado
3.0	02/01/2013	Se recogen observaciones realizadas por el evaluador de INDECOPI	Sub Gerencia de Apoyo Administrativo Sub Gerencia de Archivo Registral Físico	Actualizado
3.0	29/01/2013	Aprobación	Gerencia General	Aprobado
4.0	31/07/2017	Actualización	Sub Gerencia de Registro Digital	Actualizado
4.0	25/08/2017	Aprobación	Gerencia de Registros de Certificación Digital	Aprobado
5.0	24/01/2022	Actualización	Sub Dirección de Servicios de Certificación Digital	Actualizado
5.0	06/06/2022	Aprobación	Dirección de Servicios de Certificación Digital	Aprobado

INDICE

1. INTRODUCCIÓN.

El Reglamento de la Ley de Firmas y Certificados Digitales, en su artículo 47º, 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 Autoridad Administrativa Competente (en adelante 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.

El RENIEC, en su calidad de Entidad de Registro, 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, 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*".

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

En el Artículo 45° del referido Reglamento se indica que un Documento Nacional de Identidad electrónico (DNIe) es un documento que acredita presencial y electrónicamente la identidad de una persona, permite la firma digital de documentos electrónicos y el ejercicio del voto electrónico no presencial.

Con la finalidad de dar cumplimiento a lo dispuesto por el Reglamento de la Ley de Firmas y Certificados Digitales, la presente Declaración de Prácticas y Políticas de Registro (DPR) describe las prácticas y funciones del RENIEC, en su calidad de Entidad de Registro o Verificación para el Estado Peruano para Personas Naturales (EREP–RENIEC–PN), cada vez que a un ciudadano se le emitan certificados digitales en el DNIe.

La presente Declaración de Prácticas y Políticas de Registro (conocida también por su acrónimo en Inglés como RPS[1]) 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–PN".

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

Finalmente, con relación a la prestación de servicios de certificación digital la EREP–RENIEC–PN se encuentra vinculada con la ECEP-RENIEC. A tal efecto, los certificados digitales gestionados por la EREP–RENIEC–PN y emitidos por la ECEP–RENIEC gozan de las presunciones legales establecidas en el Reglamento de la Ley de Firmas y Certificados Digitales[2].
El presente documento es aplicable y de obligado cumplimiento a toda la comunidad de usuarios a la que se alude en la Sub-Sección 1.3.

1.1. Visión General.

El RENIEC a través de procedimientos de identificación[3] comprueba la identidad de los ciudadanos que requieren la emisión de un DNIe. Si se verifica la pertinencia de la solicitud del trámite y la documentación de sustento presentada por aquellos con dicho fin, entonces se procede con el registro o actualización de los datos del ciudadano en el Registro Único de Identificación de Personas Naturales (RUIPN), en adelante *"Base de Datos del RENIEC"*.

Finalizada la identificación y el registro, se personaliza una tarjeta criptográfica con los datos e imágenes (foto, huella dactilar y firma manuscrita) del solicitante, quedando lista para serle entregada. En ese momento, la tarjeta personalizada no contiene certificados digitales, pero se encuentra lista para la inyección de los mismos, lo cual ocurrirá una vez que el titular se apersone a recogerla.

De acuerdo al Artículo 45 del Decreto Supremo 052-2008-PCM, un DNIe es un documento que acredita presencial y/o electrónicamente la identidad personal de su titular, además de permitirle firmar digitalmente documentos electrónicos y el ejercicio del voto electrónico. Para tal efecto, todo DNIe emitido contendrá, como mínimo, los siguientes certificados digitales:

- 01 certificado digital de tipo autenticación.
- 01 certificado digital de tipo firma digital.

El DNIe podrá a su vez contener un certificado digital para fines de cifrado de documentos electrónicos.

---

[2] 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.

[3] GP-380-GOR/016 Recepción y entrega del documento nacional de identidad electrónico (DNIe) Emisión de certificados digitales de persona natural

De esta forma, la EREP-RENIEC-PN gestionará los certificados digitales para el DNIe ante la ECEP-RENIEC y solo podrán ser inyectados en él para el caso de aquellos ciudadanos a los que se les ha personalizado una tarjeta criptográfica producto del trámite para la obtención de un DNIe. Por lo tanto, los certificados digitales para personas naturales gestionados por la EREP-RENIEC-PN serán emitidos únicamente a los ciudadanos peruanos registrados en la "*Base de Datos del RENIEC"*.

Conforme a los niveles de seguridad PKI establecidos en la Guía de Acreditación de Entidades de Registro, para la verificación de la identidad de los ciudadanos la EREP-RENIEC-PN empleará la *"Base de Datos del RENIEC"* y su sistema biométrico AFIS.

Para hacer uso de los certificados digitales de firma y autenticación del DNIe, el usuario final debe hacer uso de software que implemente el estándar PKCS#11, el cual define una interfaz para dispositivos criptográficos independiente del sistema operativo en uso. Además, los usuarios de Windows pueden hacer uso de la interfaz MS-CAPI (Microsoft Cryptography API) para las operaciones de firma digital y autenticación.

1.2. Nombre e identificación del documento.

El presente documento: Declaración de Prácticas de Registro de la Entidad de Registro o Verificación para el Estado Peruano - Persona Natural (EREP-RENIEC-PN), en adelante DPR, es identificado de la siguiente forma:

Nombre del documento	Declaración de Prácticas de Registro Entidad de Registro o Verificación para el Estado Peruano - Persona Natural (EREP-RENIEC-PN)
OID	1.3.6.4.1.35300.1.2.1.2
Versión del documento	5.0
Estado del documento	Aprobado
Fecha de emisión	06/06/2022
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-PN. Los servicios ofrecidos por la ECEP-RENIEC comprenden aquellos orientados a la gestión del ciclo de vida de los certificados, entre los cuales tenemos: emisión, cancelación, verificación de estado y directorio de certificados, el cual se encuentra implementado por la ECEP-RENIEC. La vinculación de la EREP-RENIEC-PN 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 para el Estado Peruano – Persona Natural (EREP-RENIEC-PN).

La EREP–RENIEC-PN es la entidad encargada de verificar la identidad del ciudadano, de la comprobación de la correspondencia entre la tarjeta criptográfica y el solicitante, de la autorización de solicitudes de emisión de certificados digitales, y su respectiva gestión ante la ECEP–RENIEC a fin de que aquella genere los certificados digitales emitidos a nombre del ciudadano.

Al momento de la entrega del DNIe, la EREP-RENIEC-PN:

- Verifica la identidad del titular usando la "*Base de Datos del RENIEC"*.
- Verifica si la tarjeta personalizada le corresponde al ciudadano (si ha sido personalizada con sus datos); para lo cual se verifican los datos impresos en la tarjeta y se hace uso del aplicativo MatchOnCard de la tarjeta. En el caso que el ciudadano no cuente con huellas dactilares en la tarjeta personalizada se utiliza un código de desbloqueo (PUK).
- A través de un medio seguro (SSL) comunica a la ECEP-RENIEC las respectivas autorizaciones para que ésta emita y/o cancele los certificados digitales.
- Inyecta los certificados en el DNIe y permite al ciudadano definir sus PINes de acceso a los mismos.

Toda la documentación de los procedimientos a cargo de la EREP-RENIEC-PN es registrada, archivada y preservada el tiempo definido por la legislación vigente. A los datos personales de los ciudadanos les son aplicables, en lo que corresponda, lo establecido en las sub secciones 9.3 y 9.4 del presente documento, referidas a la confidencialidad y protección de los datos personales.

1.3.3 Titulares de Certificados.

La EREP-RENIEC-PN declara que la comunidad de usuarios definidos como titulares de certificados son los ciudadanos peruanos

que se encuentren registrados en la "*Base de Datos del RENIEC"* y que tengan plena capacidad de ejercer sus derechos civiles. Los ciudadanos peruanos son personas naturales a quienes se les atribuye de manera exclusiva un DNIe. El ciudadano se constituirá en titular y suscriptor de los certificados digitales contenidos en el DNIe.

1.3.4 Terceros que Confían.

Los Terceros que Confían son las personas naturales o jurídicas (diferentes al titular de los certificados digitales contenidos en el DNIe), 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.

La EREP-RENIEC-PN declara que la comunidad de usuarios definidos como Terceros que Confían se encuentra de acuerdo a 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-PN 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-PN, 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-PN.

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-PN.

1.4.2. Uso prohibido del certificado.

No aplica a la EREP–RENIEC-PN.

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 – Centro Cívico, 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 el 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 – Centro Cívico, 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–PN 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-PN.

2.2. Publicación de la información sobre certificación.

La presente DPR es un documento de conocimiento público y de acceso libre, en tal sentido se encuentra disponible en la página web: https://pki.reniec.gob.pe/repositorio/

La EREP–RENIEC-PN 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 estará disponible en la página web: https://pki.reniec.gob.pe/repositorio/. En caso de cambios mayores, es decir, aquellos que afectan a los procesos de registro o verificación de identidad se requerirá previamente la aprobación del INDECOPI.

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"*, *"Guías de procedimientos"*) a la EREP–RENIEC–PN 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-PN 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-PN, realiza la comprobación de la identidad del solicitante.

3.1. Nombre.

No aplica a la EREP–RENIEC-PN.

3.1.1 Tipos de nombres.

No aplica a la EREP–RENIEC-PN.

3.1.2 Necesidad que los nombres tengan un significado.

No aplica a la EREP–RENIEC-PN.

3.1.3 Anonimato o seudónimo de los suscriptores.

No aplica a la EREP–RENIEC-PN.

3.1.4 Reglas para interpretar las diferentes modalidades de nombres.

No aplica a la EREP–RENIEC-PN.

3.1.5 Singularidad de los nombres.

No aplica a la EREP–RENIEC-PN.

3.1.6 Reconocimiento, autenticación y rol de las marcas registradas.

No aplica a la EREP–RENIEC-PN.

3.2. Validación inicial de la identidad.

La validación de la identidad del ciudadano consiste en verificar la correspondencia entre la "*Base de Datos del RENIEC"*, la tarjeta personalizada y las huellas dactilares del ciudadano.[4]

3.2.1. Método para probar la posesión de la llave privada.

Un DNIe es personalizado con los datos de un ciudadano. La comprobación de la correspondencia del DNIe al ciudadano es efectuada mediante la verificación de la huella dactilar almacenada en el chip usando el aplicativo MatchOnCard del DNIe. Adicionalmente, se efectúa una verificación visual de los datos e imágenes impresos en la tarjeta. Si la autenticación es exitosa, y en concordancia con lo señalado en la DPC de la ECEP-RENIEC, se procede a la generación de las llaves pública y privada dentro del chip de la tarjeta personalizada**.**

[4] GP-380-GOR/016 Recepción y entrega del documento nacional de identidad electrónico (DNIe) Emisión de certificados digitales de persona natural

Para cada certificado, sea este de autenticación, de firma o de cifrado, se genera la petición de certificado Certificate Signing Request (CSR) en formato PKCS#10, la cual es firmada con la llave privada correspondiente. Luego, las peticiones son enviadas a la ECEP-RENIEC, y ésta devuelve los certificados que finalmente son inyectados en el DNIe, los mismos que podrán ser usados mediante la contraseña o pines de acceso (PIN) establecidos previamente por el ciudadano.

En el caso que el ciudadano no pueda hacer uso de sus huellas dactilares para autenticar su identidad utilizará un código de desbloqueo (PUK) proporcionado por la EREP-RENIEC-PN.[5]

3.2.2. Autenticación de la Identidad de una persona jurídica.

No aplica a la EREP–RENIEC-PN.

3.2.3. Autenticación de Identidad individual (persona natural).

La validación de la identidad del ciudadano consiste en verificar la correspondencia entre la "*Base de Datos del RENIEC"*, la tarjeta personalizada y las huellas dactilares del ciudadano.

Primero se verifica la correspondencia entre el número de serie de la tarjeta con el registrado en la *"Base de Datos del RENIEC"* para dicho ciudadano.

Luego se realiza la comparación de la huella dactilar del ciudadano con la huella almacenada en el chip de la tarjeta personalizada, utilizando la funcionalidad MatchOnCard de la tarjeta criptográfica.

Excepcionalmente se comprobará la identidad en la base de datos del Registro Único de Identificación de Personas Naturales (RUIPN), en el supuesto que el solicitante tuviese alguno de sus dedos amputados, anquilosados o sin crestas, o no haya sido posible verificar la identidad del solicitante a través del Servicio de Verificación Biométrica del RENIEC, por alguna razón fundamentada.[6]

3.2.4. Información no verificada del suscriptor.

La EREP-RENIEC-PN no aceptará cambios ni información adicional del ciudadano al momento de la emisión de sus certificados digitales. En este sentido, se utilizarán los datos ya registrados en la *"Base de Datos del RENIEC"* para las solicitudes de los certificados digitales del ciudadano previo a la entrega de su DNIe.

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

[5] GP-380-GOR/016 Recepción y entrega del documento nacional de identidad electrónico (DNIe) Emisión de certificados digitales de persona natural
[6] GP-380-GOR/016 Recepción y entrega del documento nacional de identidad electrónico (DNIe) Emisión de certificados digitales de persona natural

3.2.5. Validación de la autoridad.

No aplica a la EREP–RENIEC–PN.

3.2.6. Criterios para la interoperabilidad.

La EREP–RENIEC–PN 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, y contenidos en el DNIe, tienen la misma validez y eficacia jurídica que el uso de una firma manuscrita (principio de equivalencia funcional). La EREP–RENIEC-PN no contempla el establecimiento de relaciones de confianza con otra Entidad de Certificación.

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

La ECEP-RENIEC no brinda este servicio; por lo tanto, la EREP-RENIEC-PN tampoco brindará dicho servicio.

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

No aplica a la EREP–RENIEC-PN.

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

No aplica a la EREP–RENIEC-PN.

3.4. Identificación y autenticación de la solicitud de cancelación.

La solicitud para la cancelación de un certificado digital puede ser presentada por el titular de manera presencial. La verificación y autenticación de su identidad se realizará consultando la "*Base de Datos del RENIEC*". Adicionalmente, la EREP-RENIEC-PN ha puesto a disposición en su portal web (https://erep.reniec.gob.pe/pier/login.jsf) un servicio con el que de manera remota se podrá solicitar la cancelación de sus certificados digitales.

La cancelación de un certificado digital puede ser solicitada por un tercero, quien deberá apersonarse a una oficina de la EREP–RENIEC-PN presentando su documento identidad vigente y los documentos respectivos, y deberá probar de manera fehaciente alguna de las circunstancias señaladas en la sub sección 4.9.1 del presente documento. El levantamiento de sus datos, su validación, y verificación de su identidad, se realizará de acuerdo al procedimiento descrito en el numeral 3.2.3 del presente documento.

La EREP–RENIEC–PN, realizará las validaciones correspondientes consultando a través del Registro Único de Identificación de Personas Naturales (RUIPN), antes de proceder con la cancelación de un certificado digital.

Para mayor información sobre el procedimiento[7] y personas habilitadas para solicitar la cancelación del certificado digital remitirse al numeral 4.9.2 del presente documento.

Todo suscriptor dispone 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. El acceso a la plataforma y a los instructivos y manuales correspondientes está 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.

De acuerdo al Decreto Supremo 052-2008-PCM, un DNIe es un documento que acredita presencial y/o electrónicamente la identidad personal de su titular, además de permitirle firmar digitalmente documentos electrónicos y el ejercicio del voto electrónico. Para tal efecto, todo DNIe emitido contendrá, como mínimo, los siguientes certificados digitales:

- 01 certificado digital de tipo autenticación.
- 01 certificado digital de tipo firma digital.

pudiendo contener también un certificado digital de tipo cifrado.

Conforme a lo establecido, respecto a los niveles de seguridad en las Guías de Acreditación de la Entidad de Registro, los certificados digitales emitidos tendrán una vigencia de acuerdo a lo que se indique en la respectiva DPC de la ECEP-RENIEC (contados a partir de la fecha de generación).

El ciclo de vida de los certificados digitales se encuentra determinado por el periodo de vigencia de los mismos, el cual inicia y finaliza en las fechas indicadas en ellos, salvo en los supuestos de cancelación conforme a lo señalado en el respectivo contrato o que la tarjeta expire primero.

Conforme a lo establecido en la Ley 26497, ley que aprueba la "Ley Orgánica del Registro Nacional de Identificación y Estado Civil", en su artículo 37, el DNI tendrá una validez de ocho (08) años.

En el caso que se hayan emitido certificados digitales cuyo periodo de vigencia sea mayor al periodo de vigencia de la tarjeta, se procederá a la cancelación por oficio de los certificados digitales en la fecha de caducidad de la tarjeta.

4.1. Solicitud del certificado.

4.1.1. Habilitados para presentar la solicitud de un certificado.

En virtud del Artículo 45 del Reglamento de la Ley de Firmas y Certificados Digitales, la EREP-RENIEC-PN solicita a la ECEP-RENIEC la emisión, como mínimo, de 02 certificados digitales (de autenticación y firma) cada vez que se entrega un DNIe. La EREP-RENIEC-PN podrá solicitar a su vez un certificado digital adicional para fines de cifrado. En tal sentido, se encuentran habilitados para obtener los certificados digitales los ciudadanos peruanos habilitados para obtener un Documento Nacional de Identidad, que se encuentren en plena capacidad de ejercicio de sus derechos civiles y que se encuentren registrados en la *"Base de Datos del RENIEC"*; y para los cuales se les ha personalizado una tarjeta criptográfica.

En el caso que el solicitante tenga certificados válidos en su DNIe al momento de la entrega de un nuevo DNIe, la EREP-RENIEC-PN solicitará la cancelación de los mismos previo a la generación de los nuevos certificados.

La EREP-RENIEC-PN establece que la emisión de los certificados digitales a inyectarse en el DNIe es una actividad que requiere la

presencia física del ciudadano, por lo tanto, es personal e indelegable.

4.1.2. Proceso de solicitud y responsabilidades.

El pedido de un certificado digital se inicia con la generación del par de llaves (privada y pública) dentro del chip de la tarjeta criptográfica personalizada. En seguida, se genera la solicitud de firma de certificado (CSR[8]) en formato PKCS#10 conteniendo la llave pública y los datos de la persona a quien se emitirá el certificado digital, siendo tal solicitud firmada con la llave privada generada. Luego, la CSR es enviada a la ECEP-RENIEC la cual procede a emitir el certificado digital que incluye dicha llave pública y datos de la persona solicitante firmándolo digitalmente, lo reconoce dentro de la ruta de certificación correspondiente y lo remite a la EREP-RENIEC-PN.

La EREP-RENIEC-PN recibe el certificado y lo inyecta en el DNIe.[9]

Los datos de la persona son obtenidos de la *"Base de Datos del RENIEC"*. La EREP-RENIEC-PN no incluye datos adicionales ni modifica los obtenidos.

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-PN.

4.2. Procesamiento de la solicitud de un certificado.

La solicitud de emisión de certificados digitales es una actividad que se realiza al momento de la entrega del DNIe. Dado que para ese instante el titular ha sido identificado y sus datos se encuentran registrados en la Base de Datos del RENIEC, la solicitud de emisión es generada, aprobada y procesada inmediatamente, previa verificación de la correspondencia entre la tarjeta personalizada y los datos del ciudadano.[10]

4.2.1. Realización de las funciones de identificación y autenticación.

Durante la entrega de certificados digitales en el DNIe, la autenticación de la identidad del titular es realizada mediante la consulta a la Base de Datos del RENIEC.

El personal responsable de la EREP-RENIEC-PN, realiza la validación de la identidad del ciudadano, la cual consiste en verificar la correspondencia entre la Base de Datos del RENIEC, la tarjeta personalizada y las huellas dactilares del ciudadano.

---

[8] Del inglés *Certificate Signing Request.*

[9] GP-380-GOR/016 Recepción y entrega del documento nacional de identidad electrónico (DNIe) Emisión de certificados digitales de persona natural

[10] GP-380-GOR/016 Recepción y entrega del documento nacional de identidad electrónico (DNIe) Emisión de certificados digitales de persona natural

Primero se verifica la correspondencia entre el número de serie de la tarjeta con el registrado en la Base de Datos del RENIEC para dicho ciudadano.

Luego se realiza la comparación de las huellas dactilares del ciudadano con las huellas almacenadas en el chip de la tarjeta personalizada, utilizando la funcionalidad MatchOnCard de la tarjeta criptográfica.

Excepcionalmente se comprobará la identidad en la base de datos del Registro Único de Identificación de Personas Naturales (RUIPN), en el supuesto que el solicitante tuviese alguno de sus dedos amputados, anquilosados o sin crestas, o no haya sido posible verificar la identidad del solicitante a través del Servicio de Verificación Biométrica AFIS, por alguna razón fundamentada.

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

De conformidad con la legislación vigente[11], una Entidad de Registro tiene como función aprobar o denegar una solicitud relacionada con el ciclo de vida del certificado digital.

En el caso de las personas naturales, la solicitud de los certificados digitales está supeditada a la aprobación del trámite para la obtención del DNIe. La EREP-RENIEC-PN solicitará la emisión de los certificados digitales de autenticación y firma digital solo para aquellos ciudadanos que se encuentran en la Base de Datos del RENIEC y para los cuales se ha personalizado una tarjeta criptográfica.

La EREP-RENIEC-PN no generará una solicitud en los siguientes supuestos:

- Suplantación de identidad.
- En caso no se hubiese podido confirmar y acreditar 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 denegación o la no aceptación; si el motivo fuese por un caso de suplantación de identidad, el RENIEC se reserva su derecho para iniciar las acciones judiciales respectivas. En este caso el Administrador de la Oficina dispondrá el archivo del expediente.

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

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

Verificada la identidad del titular y una vez aprobada su solicitud, la EREP-RENIEC-PN comunicará a la ECEP-RENIEC, a fin de que se realicé la emisión de los certificados digitales, la ECEP-RENIEC procederá a generarlos en forma inmediata. La EREP-RENIEC-PN a través del sistema inyectará los certificados digitales en el DNIe en forma inmediata. En conformidad con lo requerido en las Guías de Acreditación de ER y EC, el procesamiento de la solicitud de un certificado digital y la generación del mismo tendrá una duración de algunos minutos, por lo que no será mayor a cinco (05) días útiles.

4.3. Generación de llaves y emisión del certificado.

No aplica a la EREP–RENIEC-PN.

4.3.1. Acciones de la EC durante la emisión del certificado.

No aplica a la EREP–RENIEC-PN.

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

No aplica a la EREP–RENIEC-PN.

4.4. Aceptación del certificado.

4.4.1. Conducta constitutiva de la aceptación de un certificado.

No aplica a la EREP–RENIEC-PN.

4.4.2. Publicación del certificado por parte de la EC.

No aplica a la EREP–RENIEC-PN.

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

No aplica a la EREP–RENIEC-PN.

4.5. Par de llaves y uso del certificado.

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

No aplica a la EREP–RENIEC-PN.

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

No aplica a la EREP–RENIEC-PN.

4.6. Renovación del certificado.

No aplica a la EREP-RENIEC-PN.

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

No aplica a la EREP-RENIEC-PN.

4.6.2. Personas habilitadas para solicitar la renovación.

No aplica a la EREP-RENIEC-PN.

4.6.3. Procesamiento de la solicitud de renovación de certificado.

No aplica a la EREP-RENIEC-PN.

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

No aplica a la EREP-RENIEC-PN.

4.6.5. Conducta constitutiva de aceptación de renovación de certificado.

No aplica a la EREP-RENIEC-PN.

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

No aplica a la EREP-RENIEC-PN.

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

No aplica a la EREP-RENIEC-PN.

4.7. Re-emisión de certificado.

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

4.8. Modificación del certificado.

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

4.9. Cancelación y suspensión del certificado.

La cancelación de un 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 mismo por parte del titular.[12]

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

La cancelación de los certificados digitales contenidos en el DNIe es un mecanismo a usar 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[13], 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 un certificado digital, cuando tenga conocimiento de alguna de las causales indicadas en el numeral 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.

4.9.1. Circunstancias para la cancelación.

Los certificados digitales pueden ser cancelados por las causas siguientes:

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

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.
   - 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.

d. Por circunstancias que afectan al DNIe:
   - Por defecto físico del DNIe.
   - Por datos erróneos en el DNIe.

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

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).

f. Por cambio de tarjeta criptográfica.

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 sub sección 4.9.1 del presente documento, las siguientes personas:

- El titular y/o suscriptor.

- La ECEP–RENIEC, a través de la EREP–RENIEC–PN, podrá hacerlo de oficio, cuando tenga conocimiento de alguna de las circunstancias señaladas en la sub sección 4.9.1 del presente documento.

- Un juez que de acuerdo a la Ley decida cancelar el certificado digital.

- Un tercero, en caso tenga pruebas fehacientes 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) Inhabilitación o incapacidad declarada judicialmente.
  d) Cuando la información contenida en el certificado digital es inexacta o ha sido modificada.

4.9.3. Procedimiento para la solicitud de cancelación.

La solicitud de cancelación de un certificado digital contenido en el DNIe puede ser presentada a la EREP-RENIEC-PN por el titular y suscriptor, de manera presencial o vía internet mediante el portal web de la EREP-RENIEC-PN. En caso de un tercero, el trámite se realiza necesariamente de manera presencial, de acuerdo al procedimiento de cancelación del Certificado Digital.[14]

La EREP-RENIEC-PN verificará la identidad del solicitante (titular o tercero) según el procedimiento señalado en la sub sección 3.4 del presente documento, y tratándose de alguna de las circunstancias señaladas en la sub sección 4.9.1 del presente documento, comprobará la información presentada por el tercero a través de la

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

consulta en el Registro Único de Identificación de Personas Naturales (RUIPN) en la Base de Datos del RENIEC.

Las resoluciones judiciales o administrativas que ordenen la cancelación del certificado digital deben ser presentadas a la EREP-RENIEC-PN.

La EREP–RENIEC-PN archivará toda la información respecto a la aprobación o denegación de la solicitud, así como registrará toda la información relacionada con la persona que efectúa el requerimiento, la relación que ésta tiene con el titular y suscriptor, las circunstancias de la cancelación, fecha y hora de la notificación a la ECEP-RENIEC e incorporará toda la información en el archivo respectivo.

La denegación de la solicitud se determinará cuando el pedido no se ajuste a las circunstancias para la cancelación de un certificado digital indicadas en la sub sección 4.9.1 del presente documento.

Los solicitantes (titular o tercero) pueden acceder al formato respectivo de cancelación en el portal web de la EREP-RENIEC-PN.

4.9.4. Periodo de gracia de la solicitud de cancelación.

Según lo señalado por la ECEP-RENIEC en su DPC, la cancelación del certificado digital se llevará a cabo de forma inmediata a la recepción de la comunicación de la EREP-RENIEC-PN. Por lo tanto, no existe ningún periodo de gracia asociado a este proceso en el que se pueda anular la solicitud de cancelación.

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

No aplica a la EREP-RENIEC-PN.

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

No aplica a la EREP–RENIEC-PN.

4.9.7. Frecuencia de emisión de CRL.

No aplica a la EREP–RENIEC-PN.

4.9.8. Máxima latencia para CRLs.

No aplica a la EREP–RENIEC-PN.

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

No aplica a la EREP–RENIEC-PN.

4.9.10. Requisitos para la verificación en línea de la cancelación.

No aplica a la EREP–RENIEC-PN.

4.9.11. Otras formas disponibles de publicar la cancelación.

No aplica a la EREP–RENIEC-PN.

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

No aplica a la EREP–RENIEC-PN.

4.9.13. Circunstancias para la suspensión.

No aplica a la EREP–RENIEC-PN.

4.9.14. Personas habilitadas para solicitar la suspensión.

No aplica a la EREP–RENIEC-PN.

4.9.15. Procedimiento para solicitar la suspensión

No aplica a la EREP–RENIEC-PN.

4.9.16. Límite del periodo de suspensión

No aplica a la EREP–RENIEC-PN.

4.10. Servicios de estado de certificado.

No aplica a la EREP–RENIEC-PN.

4.10.1. Características operacionales.

No aplica a la EREP–RENIEC-PN.

4.10.2. Disponibilidad del servicio.

No aplica a la EREP–RENIEC-PN.

4.10.3. Rasgos operacionales.

No aplica a la EREP–RENIEC-PN.

4.11. Finalización de la suscripción.

No aplica a la EREP–RENIEC-PN.

4.12. Depósito y recuperación de llaves.

No aplica a la EREP–RENIEC-PN.

4.12.1. Políticas y prácticas de recuperación de Depósito de llaves.

No aplica a la EREP–RENIEC-PN.

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

No aplica a la EREP–RENIEC-PN.

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

De acuerdo con los lineamientos establecidos por la AAC–INDECOPI, la presente sección describe las medidas que ha implementado el RENIEC, en su calidad de EREP–RENIEC–PN, con la finalidad de garantizar los requerimientos que en materia de seguridad se encuentran asociados a los procesos de identificación y registro, y entrega de certificados digitales. En las sub secciones siguientes se señalan las medidas adoptadas más relevantes.

5.1. Controles físicos.

En ésta sub sección se describen los controles que se aplicarán a los recursos físicos que comprenden las instalaciones de la EREP- RENIEC-PN, la 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-PN 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.[15]

5.1.2. Acceso físico.

En las áreas donde se desarrollan las actividades y operaciones de la EREP-RENIEC-PN se han establecido perímetros de seguridad, implementando 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-PN, visitantes o proveedores.[16]

5.1.3. Energía y aire acondicionado.

Las instalaciones de las agencias sucursales de la EREP-RENIEC-PN, 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 protección de los equipos y un óptimo funcionamiento de los mismos, logrando un entorno de operaciones fiable.

[15] DI-206-OSDN/001 "Seguridad de las Instalaciones en Sedes, Oficinas Registrales, Agencias, Locales y/o Puntos de Atención", Séptima Versión.

[16] 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.

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.[17]

5.1.4. Exposición al agua.

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

5.1.5. Prevención y protección contra fuego.

En las instalaciones donde se desarrollan las actividades y operaciones de la EREP-RENIEC-PN, 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-PN se cuentan con equipos adecuados como extintores que permiten detectar y sofocar un eventual siniestro, según las recomendaciones del órgano competente del RENIEC.[18]

5.1.6. Archivo de material.

La EREP-RENIEC-PN ha establecido lineamientos[19] para la clasificación de la información, 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, los 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 como proteger dicha información de algún daño o destrucción deliberada o accidental (ej. robo, alteración no autorizada, agua, incendio y electromagnetismo).

---

[17] Unidad de Servicios Generales y Control Patrimonial del RENIEC.

[18] DI-206-OSDN/001 "Seguridad de las Instalaciones en Sedes, Oficinas Registrales, Agencias, Locales y/o Puntos de Atención", Séptima Versión
NAI-368-OSDN/003 "Indicaciones a Seguir Ante Señales de Alerta del Sistema de Alarma de Incendio y Aniego", Tercera Versión.

[19] 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.

Adicionalmente las copias de seguridad se encuentran en ambientes diferentes, que cuentan con controles de protección contra fuego, humedad 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 a la legislación vigente y los procedimientos establecidos por la EREP-RENIEC-PN.[20]

5.1.8. Copia de seguridad externa.

En general para las copias de seguridad de la información correspondiente a la EREP-RENIEC-PN es efectuado de acuerdo a las funciones del órgano competente y sus procedimientos internos establecidos en RENIEC.

5.2. Controles procesales.

5.2.1. Roles de confianza.

La EREP-RENIEC-PN 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 supervisar a los operadores a su cargo, así como el cumplimiento de la calidad del servicio de la oficina, organizar la atención del público en la oficina a su cargo y dentro de su zona de influencia, cautelar el cumplimiento del TUPA, controlar el cumplimiento de las disposiciones legales, Normas Internas, Declaración de Prácticas y Políticas de Registro y otras que correspondan a las actividades dentro de la Infraestructura Oficial de Firma Electrónica, controlar y asegurar el correcto envío de los documentos que acreditan los trámites realizados, administrar los recursos y bienes que le han sido asignados, cumplir y hacer cumplir los plazos de los trámites establecidos para los trámites realizados, impresión y entrega de la llave PUK a su titular.

- **Supervisor de Registro Digital EREP:** Almacenar y custodiar en el día los formatos relacionados al certificado digital y DNIe, preparar y registrar el despacho de documentación de los trámites realizados, recepcionar y controlar los DNIe, impresión y entrega de la llave PUK a su titular, brindar orientación al público en general y cumplir con las disposiciones legales, Normas Internas, Declaración de Prácticas y Políticas de Registro y otras que

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

correspondan a las actividades dentro de la Infraestructura Oficial de Firmas Electrónica.

5.2.2. Número de personas requeridas por labor.

Para la entrega de certificados en el DNIe, la EREP-RENIEC-PN ha definido el rol de Operador de Registro Digital quien opera el sistema de manera independiente, para lo cual ha sido autorizado en el sistema según los perfiles de usuario establecidos.

5.2.3. Identificación y autenticación para cada rol.

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

El personal de la EREP-RENIEC-PN que opera el sistema, solo tendrá permisos de acuerdo a su rol designado, autenticándose con su usuario y contraseña y/o con biometría a través de su huella dactilar, a fin de verificar su identidad y autenticar el permiso de acceso al aplicativo respectivo.

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-PN se desempeñarán diferentes responsables.

5.3. Controles de personal.

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

En ambos casos, el personal que ejerza labores en la EREP-RENIEC-PN y tenga acceso a la información clasificada como “confidencial” o “reservada” debe suscribir el respectivo acuerdo de confidencialidad de no divulgación de la información y/o documentos.

5.3.1. Cualidades y requisitos, experiencia y certificados.

Los procedimientos[21] y requisitos dispuestos por el RENIEC para la gestión del personal que desarrolla funciones en la EREP- RENIEC,

[21] 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.

buscan asegurar que se acredite de manera suficiente y fehaciente las cualificaciones y experiencia profesional.

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

La definición de los puestos de trabajo y sus funciones se encuentran delineadas en la Memoria Descriptiva y Organigrama Estructural y Funcional de la EREP-RENIEC-PN; el contrato de trabajo respectivo regulará las relaciones de trabajo entre el RENIEC y su personal.

En caso de personal a cargo de terceros, será responsabilidad del contratista acreditar la formación y experiencia de aquellos, de acuerdo con los requerimientos de la EREP-RENIEC-PN, 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:

- 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-PN reciba desde su ingreso una instrucción – inducción – acorde con la función a desempeñar. Dicho personal se encontrará sujeto a un plan de capacitación continúo con el fin 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 sub sección 5.3.4 del presente documento.

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

- Aspectos relevantes de la Declaración de Prácticas de Registro, Política de Seguridad, Plan y Política 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 y administración para cada rol específico.
- Procedimientos de 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 del personal.

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

5.3.4. Frecuencia y requisitos de las re-capacitaciones.

La capacitación se efectuará necesariamente cuando el personal sea sustituido o rotado, así como cuando se realicen cambios en los procedimientos de operaciones o en la Declaración de Prácticas y Políticas de Registro, Política de Seguridad, Plan y Política de Privacidad o en cualquier otro documento que resulte relevante para la EREP– RENIEC-PN 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 sub sección 5.3.3 del presente documento.

5.3.5. Frecuencia y secuencia de la rotación en el trabajo.

La EREP-RENIEC-PN, 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-PN, se considerarán acciones no autorizadas las que contravengan el presente documento, la Política de Seguridad, la Política y Plan de Privacidad, así como, las Directivas, Guías de Procedimiento, Normas Administrativas Internas y otras normas de alcance a su personal, que emita el RENIEC, de manera negligente o malintencionada.

La EREP-RENIEC-PN inmediatamente 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-PN informará al área de Talento Humano a fin que por su intermedio se inicie el procedimiento sancionador correspondiente, y de ser el caso, se inicie 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 que el RENIEC, en su calidad de EREP-RENIEC-PN, 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 sub sección 5.3 en lo que resulte aplicable, en los mismos criterios de funciones y seguridad aplicados a empleados de la EREP-RENIEC-PN en posición similar.[22]

5.3.8. Documentación suministrada al personal.

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

- Reglamento de Organizaciones y Funciones (ROF) y Manual de Organizaciones y Funciones (MOF).
- Manual de funcionamiento de equipos y software que debe operar en la EREP–RENIEC–PN.

[22] GP-344-OSDN-004 Ingreso Contratistas y Visitantes del RENIEC en días y horarios No Laborables a las instalaciones del RENIEC.

- La presente "Declaración de Prácticas de Registro, "Política de Seguridad", "Política y Plan de Privacidad".
- Normas Legales y marco regulatorio aplicables a sus funciones en la EREP–RENIEC–PN.
- Guías de procedimientos y demás documentos normativos.
- Documentación aplicable en caso de contingencias.
- Otra documentación relevante en relación a sus funciones en la EREP – RENIEC–PN.

5.4. Procedimiento de registro de auditorías.

En esta sub sección se establecen y describen los controles implementados por la EREP-RENIEC-PN, respecto de 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-PN 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[23], 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.
- Encendido y apagado de los sistemas que procesan información sensible.

Adicionalmente, la EREP–RENIEC 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-PN o faltas a la seguridad de la información.

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

[23] DT-GRCD/SGCID-008 "Gestión de Registros de Auditoría", Quinta Versión.

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 la revisión 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-PN conservará todos los registros de auditoría y su correspondiente documentación por un periodo mínimo de diez (10) años, conforme lo dispone la AAC – INDECOPI.

5.4.4. Protección del registro de auditoría.

La EREP-RENIEC-PN 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 – INDECOPI, 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.[24]

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 al procedimiento[25] establecido por la EREP-RENIEC-PN 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-PN, conforme a lo dispuesto en la sub sección 5.5.6 del presente documento.

[24] Legislación archivística publicada por el Archivo General de la Nación como ente rector para las entidades de la administración pública: http://repositorio.agn.gob.pe/xmlui/handle/123456789/51.
[25] DT-GRCD/SGCID-008 “Gestión de Registros de Auditoría”, Quinta Versión.

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

La EREP–RENIEC-PN realiza, como mínimo una vez al año, una auditoría interna a los archivos que contienen los registros de auditoría. Las auditorías externas corresponden al 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-PN, bajo cualquier modalidad, conoce algún evento que pudiera comprometer la seguridad de la información, debe informar inmediatamente al Supervisor de Seguridad de Información y 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-PN dispone en la Política de Seguridad[26] la evaluación periódica de los riesgos y vulnerabilidades detectadas.

5.5. Archivo de registros.

En esta sub-sección se establece 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-PN.

5.5.1. Tipos de eventos registrados.

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

a. Respecto de los solicitantes
   - Formulario de solicitud (emisión o cancelación), con los datos requeridos (soporte papel o electrónico).
   - Documentación aportada por el solicitante.
   - Datos personales de los titulares y/o suscriptores.
   - Contrato para la prestación del servicio de certificación digital firmado por el solicitante (soporte papel o electrónico).
   - Fecha de la última identificación presencial del solicitante.

b. Respecto del proceso de identificación a cargo de la EREP-RENIEC-PN
   - Agencia sucursal EREP–RENIEC-PN donde se tramitó la solicitud.

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

- Autorizaciones de acceso del Operador de Registro Digital a los sistemas de información de la EREP–RENIEC.
- Identidad del Operador de Registro Digital que realiza el proceso de identificación y autenticación del solicitante.
- Datos del responsable de la EREP-RENIEC-PN que efectúa la comunicación a la ECEP-RENIEC de la autorización de las solicitudes relativas al ciclo de vida de los certificados digitales.
- Fecha y hora de la comunicación enviada a la ECEP-RENIEC.

c. Respecto de la EREP-RENIEC-PN
- Los registros de auditoría especificados en la sub sección 5.4 del presente documento.
- Convenio o acuerdo de colaboración suscrito con las entidades encargadas de administrar la base de datos a las que se requiera acceder para validar la información.
- Nombramientos o designaciones de las personas encargadas de las operaciones y administración de la EREP-RENIEC-PN.
- Los registros de las auditorías internas y externas, así como de las visitas comprobatorias de la AAC – INDECOPI, 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-PN 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.[27]

5.5.3. Protección del archivo.

La EREP-RENIEC-PN dispone de medidas de seguridad destinadas a proteger la información que se encuentre archivada de accesos no autorizados, sean internos o externos, así como asegurar la confidencialidad de la información, de modo que sólo personas autorizadas puedan acceder a ella. Estas medidas de seguridad se hallan desarrolladas en la Política de Seguridad.[28]

5.5.4. Procedimientos para copia de seguridad del archivo.

Los archivos a los que se aluden en la sub sección 5.5.1 del presente documento, así como el software esencial de uso exclusivo de la EREP-RENIEC-PN, serán realizados de acuerdo al procedimiento de

[27] Guía de Acreditación de Entidad de Registro, Versión 4.0, Anexo 1, requerimiento 101.
Legislación archivística publicada por el Archivo General de la Nación como ente rector para las entidades de la administración pública: http://repositorio.agn.gob.pe/xmlui/handle/123456789/51.
[28] https://pki.reniec.gob.pe/repositorio/

respaldo o copia de seguridad[29] 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-PN, conforme a lo dispuesto en la sub sección 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-PN consignan la fecha y hora en la que fueron generados.

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 cualificado autorizado por la EREP-RENIEC-PN.[30]

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

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 llave.

No aplica a la EREP–RENIEC–PN.

5.7. Recuperación frente al compromiso y desastre.

En esta sub sección se describe la política de la EREP-RENIEC-PN, 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-PN ha implementado controles físicos, de procedimientos y lógicos con la finalidad de minimizar el riesgo y potencial impacto en las operaciones de los procesos de

[29] DT-GRCD/SGCID-005 Respaldo de Información de la Planta de Certificación Digital.

[30] 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.

identificación y registro, y entrega de certificados digitales frente a la posibilidad de desastre, sean éstos producidos en forma intencional o accidental.

En cualquier caso, los procedimientos ante desastres[31] han sido desarrollados para minimizar el potencial impacto de tal ocurrencia y restablecer los servicios básicos a cargo de la EREP-RENIEC-PN en un plazo razonable.

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

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

La EREP–RENIEC-PN ha implementado los procedimientos[32] 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 llave privada de la entidad.

Tratándose del compromiso de la llave privada del ciudadano, se procederá inmediatamente a cancelar el certificado digital correspondiente, de acuerdo al procedimiento de cancelación establecido.[33]

5.7.4. Capacidad de continuidad de negocio luego de un desastre.

La ECEP–RENIEC cuenta con un Centro de Datos de contingencia y un Plan de Contingencia Informático[34], permitiéndole garantizar la continuidad de los servicios.

5.8. Finalización de la EC o ER.

En caso que el RENIEC comunique a la EREP-RENIEC-PN la finalización de sus actividades, ésta 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 sub sección 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.

[31] Plan de Continuidad Operativa del RENIEC 2022-2024
[32] DT-GRCD/SGCID-006 Gestión del Software.
[33] GP-413-GRCD/SGRD/001 Cancelación del certificado digital
[34] DT-GRCD/SGCID-001 Plan de Contingencia.

6. CONTROLES DE SEGURIDAD TÉCNICA

De conformidad con los lineamientos establecidos por la AAC–INDECOPI en la Guía de Acreditación de Entidades de Registro, la EREP-RENIEC-PN 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 llaves.

6.1.1. Generación del par de llaves.

En concordancia con lo señalado en la DPC de la ECEP-RENIEC, la generación del par de llaves de entidades finales (titulares y/o suscriptores) se realiza utilizando un dispositivo criptográfico (DNIe) que cumple con la certificación FIPS 140-2, nivel de seguridad 3 o Common Criteria EAL6+, que impide que las llaves privadas puedan ser extraídas del mismo. La generación de llaves es precedida de un procedimiento de autenticación usando la funcionalidad MatchOnCard de la tarjeta para verificar que el DNIe ha sido personalizado con los datos del titular y/o suscriptor.[35]

6.1.2. Entrega al suscriptor de la llave privada.

Las llaves privadas son generadas únicamente dentro del DNIe y le son entregadas al titular al proveérsele el mismo, conforme al procedimiento correspondiente para la entrega del DNIe[36], el cual asegura su posesión y control exclusivo.

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

Una vez que una llave privada es generada en el chip del DNIe, se genera una estructura PKCS#10 con la llave pública y todos los datos de la persona asociada, la misma que es firmada digitalmente con la llave privada generada, y enviada a la ECEP-RENIEC para su procesamiento. La EREP-RENIEC-PN recibe el certificado y lo inyecta en el DNIe.

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

No aplica a la EREP–RENIEC-PN.

6.1.5. Tamaño de las llaves.

No aplica a la EREP–RENIEC-PN.

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

No aplica a la EREP–RENIEC-PN.

[35] GP-380-GOR/016 Recepción y entrega del documento nacional de identidad electrónico (DNIe) Emisión de certificados digitales de persona natural
[36] GP-380-GOR/016 Recepción y entrega del documento nacional de identidad electrónico (DNIe) Emisión de certificados digitales de persona natural

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

No aplica a la EREP–RENIEC-PN.

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

6.2.1. Estándares y controles para el módulo criptográfico.

Las tarjetas criptográficas (DNIe), usadas para la generación de las llaves del ciudadano, cumplen con la certificación FIPS 140-2, nivel de seguridad 3 o Common Criteria EAL 6+.[37]

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

No aplica a la EREP–RENIEC-PN.

6.2.3. Depósito de llave privada.

La EREP–RENIEC-PN no almacena copias de las llaves privadas de los ciudadanos, puesto que son generadas dentro del DNIe y, conforme a sus niveles de certificación de seguridad no pueden ser extraídas del mismo.

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

No aplica a la EREP–RENIEC-PN.

6.2.5. Archivo de la llave privada.

La EREP–RENIEC-PN no archiva copias de las llaves privadas de los ciudadanos, puesto que son generadas dentro del DNIe y, conforme a sus niveles de certificación de seguridad no pueden ser extraídas del mismo.

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

No aplica a la EREP–RENIEC-PN.

6.2.7. Almacenamiento de la llave privada en un módulo criptográfico.

No aplica a la EREP–RENIEC-PN.

6.2.8. Método de activación de la llave privada.

No aplica a la EREP–RENIEC-PN.

6.2.9. Método de desactivación de la llave privada.

[37] https://www.commoncriteriaportal.org/files/epfiles/1059a_pdf.pdf

No aplica a la EREP–RENIEC-PN.

6.2.10. Método de destrucción de la llave privada.

No aplica a la EREP–RENIEC-PN.

6.2.11. Clasificación del módulo criptográfico.

De acuerdo a las Guías de Acreditación para Entidades de Registro el DNIe (tarjeta criptográfica) usado como medio portador de los certificados digitales del ciudadano cumple con el estándar FIPS 140-2 nivel de seguridad 3.[38]

6.3. Otros aspectos de la gestión del par de llaves.

No aplica a la EREP–RENIEC-PN.

6.3.1. Archivo de la llave pública.

No aplica a la EREP–RENIEC-PN.

6.3.2. Períodos operacionales del certificado y periodo de uso de las llaves.

No aplica a la EREP–RENIEC-PN.

6.4. Datos de activación.

6.4.1. Generación e instalación de datos de activación.

No aplica a la EREP–RENIEC-PN.

6.4.2. Protección de los datos de activación.

El acceso a cada certificado se realiza a través del PIN elegido por el ciudadano, el cual se bloquea luego de un número determinado de intentos fallidos.

6.4.3. Otros aspectos de los datos de activación.

La EREP-RENIEC-PN recomienda a los titulares y suscriptores que en la generación de los datos de activación (PIN o contraseña) para acceder a su llave privada cumplan con lo siguiente:

- Sean generados por el titular y/o suscriptor sin la intermediación de un tercero.
- Tengan al menos entre 6 y 8 caracteres.
- No contengan demasiadas veces el mismo carácter.
- No sean igual al nombre del usuario.

[38] https://www.commoncriteriaportal.org/files/epfiles/1059a_pdf.pdf

6.5. Controles de seguridad computacional.

En esta sub sección se describen los controles y evaluaciones de seguridad computacionales que ha implementado el RENIEC, en su calidad de EREP–RENIEC-PN, a efectos de proteger la información sensible que mantiene o procesa.[39]

6.5.1. Requisitos técnicos específicos para seguridad computacional.

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

- Norma *ISO/IEC 17799 "Information technology – Code of practice for information security management"* y la norma *ISO/IEC TR13335 "Information technology - Guidelines for the management of IT Security"*.
- 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.

El cumplimiento de los controles establecidos es compatible de ser evaluado con:

- La norma ISO/IEC 15408 *"Information technology – Security techniques - Evaluation criteria for IT security"*.

6.6. Controles técnicos del ciclo de vida.

No aplica a la EREP–RENIEC-PN.

6.6.1. Controles de desarrollo del sistema.

No aplica a la EREP–RENIEC-PN.

[39] Documentos técnicos:
DT-GRCD/SGCID-001 Plan de Contingencia
DT-GRCD/SGCID-002 Gestión de Cambios en Sistemas
DT-GRCD/SGCID-004 Pase a Producción de Sistemas de Información
DT-GRCD/SGCID-005 Respaldo de Información de la Planta de Certificación Digital
DT-GRCD/SGCID-006 Gestión del Software
DT-GRCD/SGCID-007 Gestión de Acceso Lógico de Usuarios Externos
DT-GRCD/SGCID-008 Gestión de Registros de Auditoría
DT-GRCD/SGCID-011 Gestión Base de Datos
DT-GRCD/SGCID-012 Control de Acceso Físico
DT-GRCD/SGCID-013 Gestión de Red de Datos
DT-GRCD/SGCID-015 Gestión de Cuentas de Usuario
DT-GRCD/SGCID-016 Gestión de Estructura Física
DT-GRCD/SGCID-017 Gestión de la Capacidad Tecnológica
DT-GRCD/SGCID-020 Gestión de Medios Removibles y Borrado Seguro
DT-GRCD/SGCID-021 Gestión de Repositorios de Código Fuente
DT-GRCD/SGCID-023 Gestión de Contraseñas
DT-GRCD/SGCID-027 Infraestructura de Centro de Datos
DT-GRCD/SGCID-031 Gestión de la Configuración

6.6.2. Controles de gestión de seguridad.

No aplica a la EREP–RENIEC-PN.

6.6.3. Evaluación de seguridad de ciclo de vida.

No aplica a la EREP–RENIEC-PN.

6.7. Controles de seguridad de la red.

No aplica a la EREP–RENIEC-PN.

6.8. Sello de tiempo.

No aplica a la EREP–RENIEC-PN.

7. PERFILES DE CERTIFICADO.

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

7.1. Perfil de certificado.

No aplica a la EREP–RENIEC-PN.

7.2. Perfil CRL.

No aplica a la EREP–RENIEC-PN.

7.3. Perfil OCSP.

No aplica a la EREP–RENIEC-PN.

8. AUDITORIAS DE COMPATIBILIDAD Y OTRAS EVALUACIONES.

De acuerdo con los lineamientos establecidos por la AAC, la EREP–RENIEC-PN 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 sub sección 8.6, el resultado de estas auditorías serán publicadas por el INDECOPI. Sin perjuicio de las auditorías externas, se realizarán auditorías internas o evaluaciones de conformidad en la EREP–RENIEC–PN, a fin de verificar el cumplimiento de los procedimientos establecidos y velar por la seguridad de la información.

La EREP–RENIEC–PN, 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–PN 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. Ésta 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 sub sección 8.6 del presente documento.

Sin perjuicio de las auditorías externas, se realizarán auditorías internas o evaluaciones de conformidad en la EREP–RENIEC–PN 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, Políticas de Seguridad, Guías de Procedimientos y demás documentos normativos.

El resultado de las auditorías internas será informado a la Dirección de Certificación y Servicios Digitales, a la Dirección de Registros de Identificación, y a la Gerencia General del RENIEC, a la vez que al Representante de la EREP-RENIEC-PN, debiendo los órganos involucrados del RENIEC, de ser el caso, desarrollar las acciones a fin de subsanar posibles observaciones que se pudieran presentar durante el proceso de auditorías internas.

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 tecnologías de PKI y criptográficas, en seguridad, en tecnologías de la información y procesos de auditoría.

De conformidad con lo señalado por INDECOPI 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-PN.

En el caso de los auditores internos, la EREP-RENIEC-PN deberá definir los requisitos y cualificaciones del equipo auditor y 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-PN como entidad prestadora de servicio 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 a 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-PN.

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-PN que continúe sus operaciones hasta la próxima auditoría.

- Permitir a la EREP-RENIEC-PN 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-PN.

En el supuesto que la AAC tome la opción de suspender las operaciones de la EREP-RENIEC-PN, 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-INDECOPI y a la EREP-RENIEC-PN, el cual será publicado por esta última.[40]

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

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 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-PN 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 (TUPA) del RENIEC. Esta tasa es un tributo que grava la emisión del certificado digital.

9.1.2. Tarifas de acceso a certificados.

La ECEP-RENIEC no aplica ninguna tasa por el acceso a los certificados digitales, ni a sus repositorios públicos como son la CRL y certificados emitidos.

9.1.3. Tarifas para información sobre cancelación o estado.

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

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-PN y ECEP-RENIEC.

9.1.5. Políticas de reembolso.

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

9.2. Responsabilidad financiera.

9.2.1. Cobertura de seguro.

El RENIEC dispondrá de una garantía con cobertura suficiente de responsabilidad civil, a través de su seguro contratado. El referido seguro podrá cubrir 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-PN.

9.2.2. Otros activos.

La EREP-RENIEC-PN, 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 de negocio.

La EREP-RENIEC-PN 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-PN declara expresamente como información confidencial, que no podrá ser divulgada a terceros y que se mantendrá con carácter de reservado, excepto en aquellos supuestos previstos legalmente:

- Material o información reservada de la EREP-RENIEC-PN- incluyendo términos contractuales, planes de negocio e información que versa sobre derechos de propiedad intelectual.
- La información de la Entidad de Registro suministrada por la ECEP-RENIEC o, en caso corresponda, por sus proveedores y otras personas con las que la EREP-RENIEC-PN tiene el deber de guardar secreto establecida de modo convencional.
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los titulares y suscriptores.
- Información que pueda permitir a partes no autorizados establecer la existencia o naturaleza de las relaciones entre los titulares y suscriptores y el tercero que confía.
- La causal que motivó la cancelación del certificado digital.
- Información personal provista por los titulares y 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”. Y
- 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).
- Toda otra información clasificada como "pública".

En todo caso, el acceso a dicha información será permitido sin perjuicio que la EREP-RENIEC-PN 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-PN, 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-PN asegura a los titulares y 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-PN conjuntamente 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-PN, 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.

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

Las sanciones que la EREP-RENIEC-PN 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-PN 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-PN 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-PN 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 no considerada privada 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 suscriptor y que sirven para autenticar a aquel.
- Usos y límites de uso de los certificados digitales.

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

a. Certificados digitales emitidos o en trámite de emisión.

b. Certificados digitales cancelados.

c. Datos de identificación que figuran en el certificado digital del titular y suscriptor.

d. Usos y límites de uso de los certificados digitales.

e. Aquella información personal que los titulares y 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-PN 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.

En tal sentido, la EREP-RENIEC-PN 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 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 suscriptores que son recolectados por la EREP-RENIEC-PN.

De conformidad con lo dispuesto en el numeral 1 del Artículo 14[41] de la Ley N° 29733 – Ley de Protección de Datos Personales, la EREP-RENIEC-PN está exceptuado de solicitar el consentimiento al titular de los datos, para el tratamiento y transferencia de sus datos personales, no obstante, se informa al titular y/o al suscriptor sobre la publicación de su certificado digital sobre lo cual debe manifestar su conformidad.

La EREP-RENIEC-PN, mediante la Política de Privacidad informa al titular y 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;

[41] "**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…"

- Los derechos del titular y 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 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 suscriptor.

9.4.7. Otras circunstancias para divulgación de información.

La EREP-RENIEC-PN, dentro del marco de colaboración entre entidades del sector público, podrá comunicar o ceder a otras 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 a la Ley N° 29733 – Ley de Protección de Datos Personales, y en lo que fuese aplicable, en el caso de las entidades de la Administración Pública, según lo señalado en el artículo 55 del Reglamento de la Ley de Firmas y Certificados Digitales.

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

9.5. Derechos de propiedad intelectual.

Todos los derechos de propiedad intelectual incluyendo los que corresponden a las aplicaciones o software desarrollado para las actividades de la EREP-RENIEC-PN, OIDs, la presente DPR, la Política de Seguridad, la Política 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-PN 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-PN y ECEP-RENIEC, sin la autorización expresa del RENIEC.

Las llaves privadas y las llaves 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-PN.

9.6.2. Responsabilidades y garantías de la ER.

Son obligaciones de la EREP-RENIEC-PN:

- 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 certificados digitales, limitando su empleo a las necesidades propias del servicio de certificación digital, salvo orden judicial o pedido del titular y suscriptor del certificado digital.
- En general, es obligación de la EREP-RENIEC-PN cumplir con todo lo estipulado en el artículo 30º del Reglamento de la Ley de Firmas y Certificados digitales, así como las contenidas en el presente documento.

La EREP-RENIEC-PN 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-PN 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-PN 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-PN cuando estos ya no resulten exactos o son incorrectos.
- Custodiar su contraseña (PIN[42]) de acceso a su llave 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.

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

- Notificar de inmediato a la EREP-RENIEC-PN en caso de que detecte que se ha incluido información incorrecta o inexacta en el certificado digital.
- Solicitar inmediatamente a la EREP-RENIEC-PN 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 llave privada o de la contraseña o PIN de acceso a su llave privada.
  b. Deterioro, alteración o cualquier otro hecho u acto que afecte la llave privada o la contraseña o PIN de acceso a su llave privada.

  El compromiso de la llave privada del certificado digital entre otras causas puede darse por: pérdida, robo o conocimiento por terceros de la contraseña o PIN de acceso.

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

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

Asimismo, el titular y suscriptor del certificado asumirá las responsabilidades, a que hubiese lugar, por los daños y perjuicios que pudiese causar por aportar datos falsos, incompletos o inexactos, así como, es de su exclusiva responsabilidad el uso indebido, incorrecto o no acorde a los fines para el que fue extendido el certificado. A tal efecto, la EREP-RENIEC-PN 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 Política 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-PN está exenta del pago de indemnización alguna en caso que el hecho o circunstancia acaecida no sea consecuencia de lo declarado en la sección 9.9.

9.8. Limitaciones a la responsabilidad.

La EREP–RENIEC-PN 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-PN 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 suscriptor.
- Cuando el error o la omisión de algún dato contenido en el certificado digital deviene de la información consignada por el titular y suscriptor en los respectivas formatos de solicitud de emisión.
- Por cualquier violación a la confidencialidad que en el uso de datos personales pudieran incurrir el propio titular y suscriptor del certificado digital.
- Cuando el titular y suscriptor no ha tenido la debida diligencia o cuidado en la creación de su contraseña (PIN[43]) de acceso a su llave privada.

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

- La utilización incorrecta de los certificados digitales ni de las llaves, 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 suscriptor.

Finalmente, si el DNIe o los certificados digitales expiraron, la EREP-RENIEC-PN 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

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

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-PN, 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-PN.

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 que implica su ingreso a la IOFE, manteniendo su validez durante un período 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-PN o el INDECOPI siguiéndose lo establecido para dicho fin en las sub secciones 1.5.3 y 1.5.4 respectivamente.

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

9.10.2. Terminación.

En caso de cese de las actividades de la EREP–RENIEC-PN, el RENIEC informará al INDECOPI, titulares y 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, el ciudadano podrá consultar en cualquier momento el periodo de validez

de sus certificados digitales o DNIe a través del portal web de la EREP-RENIEC-PN.

9.12. Enmendaduras.

9.12.1. Procedimiento para enmendaduras.

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

9.12.2. Mecanismos y periodo de notificación

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

El mecanismo de comunicación se efectuará a través de la página web: https://pki.reniec.gob.pe/repositorio/, 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 - PN.

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-PN o la ECEP-RENIEC, se deberá acercar a una oficina EREP-RENIEC-PN para presentar su reclamo respectivo.

El reclamo será resuelto por la EREP-RENIEC-PN 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-PN, 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, versión vigente.
- Ley N° 29733 – Ley de Protección de Datos Personales y su Reglamento.

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

9.15. Conformidad con la ley aplicable.

Es responsabilidad de la EREP–RENIEC-PN, en la prestación de sus servicios velar por el cumplimiento de la legislación aplicable recogida en la sub sección 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 realice sobre el mismo, los cuales estarán disponibles en la siguiente dirección electrónica https://pki.reniec.gob.pe/repositorio/.

De otro lado, el contrato recoge el acuerdo íntegro entre la EREP-RENIEC-PN y 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-PN, no serán objeto de cesión de ningún tipo a terceros, así como ninguna tercera entidad podrá subrogarse en dicha posición jurídica, salvo por disposición legal que expresamente disponga lo contrario.

9.16.3. Divisibilidad.

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

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

No se estipula.

9.16.5. Fuerza mayor.

La EREP-RENIEC-PN, 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-PN dentro de lo posible asegurará la continuidad del negocio y recuperación ante desastres.

9.17. Otras cláusulas.

La EREP-RENIEC-PN, 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 su modificatorias, el Decreto Supremo N° 070-2011-PCM y el Decreto Supremo N° 105-2012-PCM
- Ley N° 29733, de Protección de Datos Personales.
- ANEXO 1: Marco de la Política de Registro para la Emisión de Certificados Digitales de la Guía de Acreditación de Entidades de Registro ER, versión 4.0, expedido por la AAC.
- RFC 3647 “Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framewortk” del Internet Engineering Task Force (IETF) (que sustituye a la RFC 2527).
- Norma Marco sobre Privacidad para los países integrantes del APEC, aprobada en la 16º Reunión Ministerial del APEC, Santiago de Chile, 17 y 18 de noviembre de 2004.
- Norma Técnica Peruana “NTP ISO/IEC 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.
- **CPDNIe** Centro de Personalización del DNIe.
- **CP** Certificate Policy (Política de Certificación).
- **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)
- **DPR o RPS** Declaración de Prácticas y Políticas de Registro (Registration Authority Practice Statement).
- **DPC o CPS** Declaración de Prácticas de Certificación (Certificate Practice Statement).
- **DNI** Documento Nacional de Identidad.
- **DNIe** Documento Nacional de Identidad electrónico.
- **EC** Entidad de Certificación.
- **ECEP–RENIEC** Entidad de Certificación para el Estado Peruano.
- **EREP–RENIEC-PN** Entidad de Registro o Verificación para el Estado Peruano para Persona Natural.
- **GRCD** Gerencia de Registros de Certificación Digital
- **HSM** Hardware de seguridad criptográfica (Hardware Security Module, por sus siglas en inglés)
- **INDECOPI** Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.
- **IOFE** Infraestructura Oficial de Firma Electrónica.
- **LCR o CRL** Lista de Certificados Digitales Cancelados (Certificate Revocation List).
- **OCSP** Online Certificate Status Protocol (Protocolo del estado en línea del certificado).
- **PIN** Personal Identification Number (Número de identificación personal).
- **PKCS#10** Estándar criptográfico de llave pública que define la sintaxis de una petición de certificado (Certification Request Syntax Standard).
- **PSC** Prestador de Servicios de Certificación Digital.
- **PUK** Personal Unlock Key (Llave de desbloqueo personal).
- **RENIEC** Registro Nacional de Identificación y Estado Civil.
- **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)
- **TNP** Tarjeta No Personalizada.
- **TUPA** Texto Único de Procedimiento Administrativo.

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:** 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 del certificado digital:** referido al registro del número de serie del certificado en la lista de certificados cancelados CRL.

- **Centro de Personalización:** Ambiente físico especialmente diseñado para la personalización del DNIe.

- **Certificado Digital**: es el documento credencial electrónico generado y firmado digitalmente por una Entidad de Certificación que vincula un par de llaves 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.

- **Llave Privada**: es una de la llaves 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.

- **Llave Pública**: es la otra llave 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 llave pública puede ser conocida por cualquiera persona.

- **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.

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

- **Documento Nacional de Identidad Electrónico (DNIe):** según el Artículo N° 45 del Reglamento de la Ley de Firmas y Certificados Digitales: "es un Documento de Identidad emitido por el Registro Nacional de Identificación y Estado Civil - RENIEC, que acredita presencial y electrónicamente la identidad personal de su titular, permitiendo la firma digital de documentos electrónicos y el ejercicio del voto electrónico presencial. A diferencia de los certificados digitales que pudiesen ser provistos por otras Entidades de Certificación públicas o privadas, el certificado que se incorpora al Documento Nacional de Identidad electrónico (DNIe) cuenta con la facultad adicional de poder ser utilizado para el ejercicio del voto electrónico primordialmente no presencial en los procesos electorales".
  El DNIe es provisto de un certificado de autenticación y otro de firma 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.

- **Inyectar:** Insertar los certificados digitales en el chip del DNIe.

- **Lista de Certificados Digitales Cancelados**: 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.

- **Personalización:** Proceso por el cual las imágenes (el retrato, la firma, la plantilla de las impresiones dactilares) y los datos biográficos asociados al titular del DNIe son incorporados a la Tarjeta No Personalizada (TNP), tanto de manera física como en formato electrónico o lógico. En esta etapa también se generan las llaves privadas y públicas correspondientes a los certificados digitales. Las llaves públicas son enviadas a la ECEP – RENIEC la cual devuelve los certificados a ser inyectados en el DNIe.

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

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

- **Re-certificación:** Renovación de certificados usando el mismo para de llaves.

- **Re-emisión:** es una nueva emisión de certificados digitales haciendo uso de un nuevo par de llaves, los cuales se inyectan en el chip de la misma tarjeta del DNIe.

- **Suscriptor**: es la persona natural responsable del uso de la llave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su llave privada.

- **Tarjeta No Personalizada:** tarjeta de policarbonato, con elementos de seguridad, con un chip de contacto con sistema operativo Javacard, la seguridad lógica y las aplicaciones necesarias para su funcionalidad.

- **Tarjeta Personalizada:** es la tarjeta personalizada, que contiene la data variable.

- **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 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.