RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Plan de Privacidad

ECERNEP

ECEP-RENIEC

EREP-RENIEC

Versión: 5.0	**Año:** 2018	
Elaborado por: Oficial de Privacidad de Datos.	**Revisado por:** Sub Gerencia de Regulación Digital de la GRCD	**Aprobado por:** Gerente de Registros de Certificación Digital

Historial de Cambios				
Ver.	**Fecha**	**Descripción**	**Responsable**	**Estado**
1.0	13/07/2012	Elaboración y Aprobación	GCRD	Aprobado
2.0	20/11/2012	Se recoge observaciones del evaluador de INDECOPI.	GCRD	Aprobado
3.0	05/07/2013	Actualización	GCRD	Aprobado
4.0	20/06/2017	Inclusión de Disposiciones aplicables a la ECERNEP y Actualización.	GRCD	Aprobado
5.0	17/10/2018	Cambio de dirección de repositorio	GRCD	Aprobado

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

INDICE

1. INTRODUCCIÓN

1.1 PREÁMBULO

Dado el incesante desarrollo y avance de las tecnologías de la información, a través del cual la información como principal activo viaja a un ritmo vertiginoso y constante por medio del Internet y, consciente de la importancia de los datos personales y del peligro que puede generar su tratamiento de modo indiscriminado, es necesario asegurar la protección de los datos personales sin crear barreras innecesarias que limiten los flujos de información, asimismo, es necesario asegurar la confidencialidad de los datos personales no públicos e información clasificada como confidencial o reservada, creada por la Gerencia de Registros de Certificación Digital o por terceros y utilizada por la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), por la Entidad de Certificación para el Estado Peruano (ECEP) y por la Entidad de Registro o Verificación para el Estado Peruano (EREP).

En ese sentido, el Registro Nacional de Identificación y Estado Civil (en adelante el RENIEC) en su rol de ECERNEP, ECEP-RENIEC y EREP-RENIEC[1], reconoce la importancia de implementar medidas de seguridad orientadas a asegurar el adecuado tratamiento de los datos personales recolectados como parte del ejercicio de sus funciones, así como también asegurar la confidencialidad de la información y la protección de los datos personales de sus Usuarios[2].

A tal fin, la Gerencia de Registros de Certificación Digital (en adelante la GRCD) ha tenido a bien elaborar el presente Plan de Privacidad, el mismo que recoge los principios establecidos en la Ley N° 29733 – Ley de Protección de Datos Personales modificada por Decreto Legislativo N° 1353, y Su Reglamento aprobado por el Decreto Supremo N° 003-2013-JUS, así como en la Norma Marco sobre Privacidad de APEC, aprobada en la 16º Reunión Ministerial de APEC[3]_ norma que forma parte integrante de los documentos que rigen a la Infraestructura Oficial de Firma Electrónica (en adelante IOFE)[4].

El presente Plan abarca la manera en que los datos personales son recolectados, utilizados, tratados, almacenados y transferidos por la ECERNEP, la ECEP-RENIEC y las EREP-RENIEC. Asimismo, es objeto del presente Plan establecer las directrices que todo el personal señalado en el numeral 1.2 del presente documento deberá de cumplir, a fin de asegurar el adecuado tratamiento de los datos personales y la confidencialidad de la información que el RENIEC administra para el ejercicio de sus funciones como ECERNEP, ECEP-RENIEC y EREP-RENIEC, evitando así posibles incidencias de seguridad como: pérdida, tratamiento o acceso no autorizado, fuga o robo de información, entre otros.

1 Mediante el Artículo 47° del D.S N° 052-2008-PCM, que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales se designa al RENIEC como ECERNEP, ECEP y EREP.

2 Para efecto del presente documento entiéndase como Usuario a los Titulares y/o Suscriptores de Certificados Digitales, en concordancia con lo dispuesto por el Artículo 9º del Reglamento de la Ley de Firmas y Certificados Digitales.

3 Llevada a cabo en Santiago de Chile el 17 y 18 de noviembre de 2004.

4 Incorporada por el INDECOPI en la normativa específica aplicable a los prestadores de servicios de certificación digital contenido en las respectivas Guías de Acreditación para Entidades de Certificación y entidades conexas aprobadas mediante la Resolución No. 030-2008/CRT, publicada el 19MAR2008

1.2 PÚBLICO AL QUE VA DIRIGIDO

El presente Plan de Privacidad es publicado a través de la página WEB http://www.reniec.gob.pe/repository/ y de obligatorio cumplimiento para todo el personal de la GRCD y terceros (personal de otras unidades orgánicas del RENIEC y contratistas) que participan o intervienen, de algún modo, en la prestación del Servicio de Certificación Digital brindado por el RENIEC en su rol de ECERNEP, ECEP-RENIEC y EREP-RENIEC.

1.3 DERECHOS DE USO

El presente Plan de Privacidad es de propiedad exclusiva del RENIEC y no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquier otro, sin autorización explícita del RENIEC.

El presente documento se encuentra amparado por los derechos de autor a que se refiere el Decreto Legislativo N° 822 y sus modificatorias, las Leyes N° 28751, 29316 y 30276 y los Decretos Legislativos N° 1076 y N° 1309; y con lo establecido por la Decisión N° 351 de la Comisión del Acuerdo de Cartagena que aprueba el Régimen Común sobre derechos de autor y derechos conexos.

2. DEFINICIONES / TERMINOLOGÍA

BANCO DE DATOS PERSONALES
Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuera la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

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

CERTIFICADO DIGITAL
Documento credencial electrónico generado y firmado digitalmente por una Entidad de Certificación que vincula un par de claves con una persona natural o jurídica confirmando su identidad.

CLAVE PRIVADA
Es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un documento electrónico y es mantenida en reserva por el titular de la firma digital.

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

DATOS PERSONALES
Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.

DATOS SENSIBLES
Es aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad.

DOCUMENTO
Cualquier escrito público o privado, impresos, fotocopias, facsímil o fax, planos, cuadros, dibujos, fotografías, radiografías, cintas cinematográficas, microformas tanto en la modalidad de microfilm como en la modalidad de soportes informáticos y otras reproducciones de audio o video, la telemática en general y demás objetos que recojan, contengan o representen algún hecho o una actividad humana o su resultado. Los documentos pueden ser archivados a través de medios físicos, electrónicos, ópticos o cualquier otro medio similar.

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

ENCARGADO DEL BANCO DE DATOS PERSONALES
Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de datos personales por encargo del titular del banco de datos personales.

ENCARGO DE TRATAMIENTO
Entrega por parte del titular del banco de datos personales a un encargado de tratamiento de datos personales en virtud de una relación jurídica que los vincula. Dicha relación jurídica delimita el ámbito de actuación del encargado de tratamiento de los datos personales.

ENTIDAD DE CERTIFICACIÓN NACIONAL PARA EL ESTADO PERUANO (ECERNEP)
La ECERNEP es la encargada de emitir los certificados raíz para las Entidades de Certificación para Estado Peruano que lo soliciten, así como proponer las políticas y estándares para aquellos y para las Entidades de Registro o Verificación para el Estado Peruano según los requerimientos de la Autoridad Administrativa Competente.

ENTIDAD DE CERTIFICACIÓN PARA EL ESTADO PERUANO (ECEP-RENIEC)
Es la encargada de proporcionar, emitir o cancelar los certificados digitales a:

a. Los administrados, personas naturales jurídicas, que serán utilizados prioritariamente en trámites, procedimientos administrativos y similares;
b. Los funcionarios, empleados y servidores públicos para el ejercicio de sus funciones y la realización de actos de administración interna e interinstitucional, y a las personas expresamente autorizadas por la entidad pública correspondiente.

ENTIDAD DE REGISTRO O VERIFICACIÓN PARA EL ESTADO PERUANO (EREP-RENIEC)
Es la encargada del levantamiento de datos, comprobación de la información del solicitante, identificación y autenticación de los titulares y suscriptores, aceptación y autorización de solicitudes de emisión, cancelación, modificación, re-emisión y suspensión de certificados digitales, así como de gestión ante la Entidad de Certificación para el Estado Peruano.

FLUJO TRANSFRONTERIZO DE DATOS PERSONALES
Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentran, los medios por los cuales se efectúo la transferencia ni el tratamiento que reciban.

FUENTES ACCESIBLES AL PÚBLICO
Bancos de datos personales de administración pública o privada, que pueden ser consultadas por cualquier persona, previo abono de la contraprestación correspondiente, de ser el caso.

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

INFORMACIÓN PERSONAL
Información relativa a una persona natural identificada o identificable.

INFORMACIÓN PÚBLICAMENTE DISPONIBLE
Información acerca de un individuo, que éste hace o permite que se haga pública o que haya sido obtenida o conseguida de manera legal de:
a) registros gubernamentales que se encuentran disponibles al público;
b) reportes periodísticos; o
c) información requerida por ley para hacerse disponible al público.

LISTA DE CERTIFICADOS CANCELADOS (CRL)
Es aquella en la que se deberá incorporar todos los certificados cancelados por la Entidad de Certificación de acuerdo con lo establecido en el Reglamento de la Ley de Firmas y Certificados Digitales.

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

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

MEDIOS TELEMÁTICOS
Conjunto de bienes y elementos técnicos informáticos que en unión con las telecomunicaciones permiten la generación, procesamiento, transmisión, comunicación y archivo de datos e información.

NIVEL SUFICIENTE DE PROTECCIÓN PARA LOS DATOS PERSONALES
Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de la Ley N°29733 - Ley de Protección de Datos Personales, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos que se trate.

PERSONAL DEL RENIEC
Se refiere en términos generales a los funcionarios y servidores del RENIEC no importando el régimen laboral al cual se encuentren sometidos en su relación con la correspondiente institución.

PERSONA JURÍDICA
También denominadas personas morales o colectivas, son entidades, asociaciones, o empresas a las cuales el Derecho atribuye y reconoce una personalidad jurídica propia y, en consecuencia, capacidad suficiente para contraer obligaciones y realizar actividades que generan plena responsabilidad jurídica, frente a sí mismos y frente a terceros.

Dentro del concepto de persona jurídica se encuentra tanto las entidades de Derecho Público como Privado con y sin fines de lucro.

PERSONA NATURAL
Toda persona física, individuo o miembro de la especie humana susceptible de adquirir derechos y contraer obligaciones conforme a lo establecido por el ordenamiento jurídico nacional y, para los efectos del presente documento, se trate de una persona que pueda ser identificada o identificable a través de su información personal.

PROCEDIMIENTO DE ANONIMIZACIÓN
Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.

PROCEDIMIENTO DE DISOCIACIÓN
Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es reversible.

REGISTRO
En términos informáticos es un conjunto de datos relacionados entre sí, que constituyen una unidad de información en una base de datos.

REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL - RENIEC
Es un organismo constitucional, público y autónomo que cuenta con personería jurídica de derecho público interno y goza de atribuciones exclusivas y excluyentes en materia registral, técnica, administrativa, económica y financiera. Fue creada por Ley No. 26497 de fecha 12 de julio de 1995, en concordancia con los artículos 177° y 183° de la Constitución Política del Perú de 1993.

Por disposición expresa del Artículo 47 del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo N° 052-2008-PCM, el RENIEC ha asumido los roles de ECERNEP, ECEP y EREP.

SUSCRIPTOR DE CERTIFICADO DIGITAL
Persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un mensaje de datos firmado digitalmente utilizando

su clave privada. En el caso que el titular del certificado sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

TERCERO QUE CONFÍA O TERCER USUARIO
Se refiere a las personas físicas, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado emitido por un certificado específico y/o verifica alguna firma digital en la que se utilizó dicho certificado.

TITULAR DE BANCO DE DATOS PERSONALES
Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.

TITULAR DE CERTIFICADO DIGITAL
Persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

TITULAR DE DATOS PERSONALES
Persona natural a quien corresponde los datos personales.

TRANSFERENCIA DE DATOS PERSONALES
Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.

TRATAMIENTO DE DATOS PERSONALES
Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación, o interconexión de los datos personales.

USUARIO
Para todos los efectos del presente documento se entenderá por Usuario al Suscriptor y/o Titular de un Certificado Digital.

3. ACRÓNIMOS

VOCABLO	SIGNIFICADO
AAC	AUTORIDAD ADMINISTRATIVA COMPETENTE (EN CONCRETO LA COMISIÓN TRANSITORIA PARA LA GESTIÓN DE LA INFRAESTRUCTURA OFICIAL DE FIRMA ELECTRÓNICA – CFE, DEL INDECOPI)
APEC	FORO DE COOPERACIÓN ECONÓMICA ASIA PACIFICO
CRL	LISTA DE CERTIFICADOS DIGITALES CANCELADOS
ECERNEP	ENTIDAD DE CERTIFICACIÓN NACIONAL PARA EL ESTADO PERUANO.
ECEP	ENTIDAD DE CERTIFICACIÓN PARA EL ESTADO PERUANO
EREP	ENTIDAD DE REGISTRO O VERIFICACIÓN PARA EL ESTADO PERUANO
GRCD	GERENCIA DE REGISTROS DE CERTIFICACION DIGITAL
INDECOPI	INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
IOFE	INFRAESTRUCTURA OFICIAL DE FIRMA ELECTRÓNICA
PSC	PRESTADOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL
RENIEC	REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

4. DECLARACIÓN DE PRIVACIDAD DE LA INFORMACIÓN

El RENIEC en su rol de ECERNEP, ECEP-RENIEC y EREP-RENIEC presta sus servicios de certificación digital a personas naturales y Personas Jurídicas, en especial, entidades de la Administración Pública en forma óptima, responsable y segura, asegurando, además, la protección de los datos personales proporcionada por aquellos de manera voluntaria en los trámites de emisión o cancelación de Certificados Digitales.

Este Plan de Privacidad se aplica a las actividades que realiza el RENIEC en su rol de ECERNEP, ECEP-RENIEC y EREP-RENIEC.

4.1 RESPONSABLE DEL PLAN DE PRIVACIDAD

De conformidad con lo señalado en las Guías de Acreditación de Entidades de Registro y Certificación, la GRCD ha designado un Oficial de Privacidad de Datos,

quien será la persona de contacto de la ECERNEP, ECEP-RENIEC y EREP-RENIEC, en todos los asuntos relativos a la protección de los datos personales.

Cualquier consulta, sugerencia o comentario con relación al mismo, deberá ser dirigido al Oficial de Privacidad de Datos a la dirección de correo electrónico: identidaddigital@reniec.gob.pe.

4.2 MEDIOS DE PUBLICACIÓN

La Política de Privacidad estará a disposición del público usuario de los servicios de certificación digital, el presente Plan se publicará en la página WEB http://www.reniec.gob.pe/repository/ y estará a disposición del personal del RENIEC que participa o interviene en el proceso de certificación digital y, de ser el caso, estará a disposición de los administrados y terceros (contratistas) que intervengan en la operación del Servicio de Certificación Digital prestado por el RENIEC.

4.3 RESPONSABLE DEL TRATAMIENTO DE LOS DATOS PERSONALES

Para todos los efectos de la prestación del Servicio de Certificación Digital a cargo de la ECERNEP, ECEP-RENIEC, y EREP-RENIEC, el RENIEC es el titular del banco de datos personales de dicho servicio.

La ECERNEP, ECEP-RENIEC, y EREP-RENIEC, y cuando corresponda la Gerencia de Tecnología de la Información (quien brinda el soporte técnico), son responsables del tratamiento de los datos personales, es decir, de la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación, o interconexión de los datos personales.

4.4 OFICIAL DE PRIVACIDAD DE DATOS

El Oficial de Privacidad de Datos es la persona de contacto de la ECERNEP, ECEP-RENIEC y EREP-RENIEC en todos los asuntos relativos a la protección de los datos personales, siendo sus funciones:

(i) Velar por el cumplimiento de la Política y el Plan de Privacidad, así como lo señalado por la Ley de Protección de Datos Personales y la Norma Marco sobre Privacidad del APEC, en lo que corresponda.

(ii) Brindar a los Usuarios[5] la información necesaria sobre el ejercicio de sus derechos, la corrección de sus datos personales, organizaciones a las que su información personal podría ser transferida, entre otros.

(iii) Actualizar la Política y el presente Plan de Privacidad, proponer los lineamientos y mecanismos orientados a asegurar la adecuada protección de los datos personales.

[5] Para efecto del presente documento entiéndase como Usuario a los titulares y/o suscriptores de certificados digitales.

(iv) Emitir opinión, cuando corresponda, sobre la transferencia de datos personales que pudiese efectuarse dentro del marco de la Infraestructura Oficial de Firma Electrónica o dentro del marco de colaboración entre entidades de la Administración Pública, llevando un registro del mismo.

(v) Coordinar los planes de auditoría en materia de protección de datos personales, sea de carácter interno o externo.

(vi) Evaluar el impacto sobre el marco de privacidad y la protección de los datos personales de nuevos proyectos o de normas que afecten a la organización.

(vii) Gestionar las reclamaciones formuladas por los titulares de los datos personales.

(viii) Impulsar la adopción de medidas correctoras y de mejora para asegurar el cumplimiento de la normativa de protección de datos.

(ix) Impulsar y promover buenas prácticas en protección de datos.

(x) Promover e impulsar la formación, educación y concientización en materia de protección de datos.

(xi) Otros que sean encomendados por el Gerente de Registros de Certificación Digital.

5. DATOS PERSONALES GESTIONADOS POR LA ECEP-RENIEC Y EREP-RENIEC

5.1 CONCEPTO DE DATO O INFORMACIÓN PERSONAL

De conformidad con lo establecido por el Reglamento de la Ley de Protección de Datos Personales - Ley N° 29733, se entiende por “datos personales” a aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.

5.2 TIPO DE DATOS PERSONALES RECOLECTADOS

Las EREP-RENIEC recogerán únicamente datos personales de las personas naturales o información de relevancia de las personas jurídicas para la emisión o cancelación de los Certificados Digitales respectivos. Estos datos o información serán proporcionados por los solicitantes o por el Usuario a través de los respectivos Formatos. Lo expuesto aplicará para los casos en que la ECERNEP en mérito a sus labores, otorgue el servicio a otras ECEP.

En ningún caso se recopilarán datos personales que revelen el origen étnico o racial, opiniones o convicciones políticas, creencias filosóficas o religiosas o morales, ingresos económicos, afiliación a algún sindicato, e información relacionada a la salud o vida sexual.

Mediante el Contrato de Prestación del Servicio de Certificación Digital (en adelante el Contrato) se recogerá únicamente datos de identificación de la persona natural y persona jurídica solicitante del Servicio de Certificación Digital.

Los datos o información personal recogida tienen como finalidad verificar y autenticar la identidad del Usuario y comprobar la información presentada por aquel a efecto de emitir su Certificado Digital (identidad digital para medios no presenciales), así como para brindar de manera oportuna y eficiente Servicio de Certificación Digital.

En ese sentido, es función de las EREP-RENIEC hacer el levantamiento de los datos personales e información de las personas jurídicas, identificar y autenticar la identidad del titular o suscriptor de un Certificado Digital, comprobar la información proporcionada por aquel, aprobar o denegar las solicitudes respectivas y gestionar ante la ECEP-RENIEC la emisión o cancelación de los Certificados Digitales.

Adicionalmente, es función de la ECERNEP y la ECEP-RENIEC observar los lineamientos establecidos por la Autoridad Administrativa Competente en relación al grado de seguridad adecuado en la selección del algoritmo, en la longitud de la clave, en el medio de almacenamiento de la clave privada y en la implementación de los algoritmos empleados, así como el contenido de los certificados digitales que permitan la interoperabilidad entre los distintos componentes tecnológicos, aplicaciones informáticas e infraestructura de firmas digitales.

Asimismo, es función de la ECEP-RENIEC emitir o cancelar los Certificados Digitales previa autorización de las EREP-RENIEC, publicar en el Repositorio los certificados emitidos y mantener actualizada la Lista de Certificados Digitales Cancelados (conocida en inglés como Certificate Revocation List, en adelante CRL), a fin de que el Tercero de Confianza[6] pueda tener acceso a la misma para verificar el estado del Certificado Digital.

El nivel de identificación es diferente para las distintas clases de Certificados Digitales; si es para persona natural se verifica y comprueba la identidad y la capacidad de ejercicio de los derechos civiles del solicitante mediante la consulta al Registro Único de Identificación de Personas Naturales (en adelante RUIPN), y cuando corresponda en el Registro Personal de la Superintendencia Nacional de Registros Públicos (en adelante SUNARP).

En caso de personas jurídicas, la existencia de la entidad será comprobada a través de su ley de creación, o inscripción en la SUNARP; el representante legal de la misma deberá acreditar sus facultades de representación mediante el documento correspondiente.

Una vez verificada la existencia de la personas jurídica, se verificará y comprobará la identidad del representante legal o apoderado, y de aquellas personas naturales que se constituirán en Suscriptores, a quienes el representante legal hubiese autorizado la emisión de un Certificado Digital a nombre del Titular (la entidad).

[6] La Décimo Cuarta Disposición Complementaria Final del Reglamento de la Ley de Firmas y Certificados Digitales define como “Tercero que confía o tercer usuario” 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.

La identificación y comprobación de ciudadanos extranjeros se realiza mediante su carné de extranjería y la consulta a la base de datos de la Superintendencia Nacional de Migraciones.

El Certificado Digital contendrá los datos de identificación de la persona natural o de la persona jurídica; en caso de la persona jurídica se incorpora los datos del Titular y Suscriptor del Certificado Digital. Estos datos serán avalados por el RENIEC en su rol de ECEP-RENIEC y EREP-RENIEC a efecto del otorgamiento de su Identidad Digital, la cual le permitirá al Usuario identificarse digitalmente en un medio no presencial.

En caso de la emisión de un Certificado Digital para uso de firma digital, éste contendrá el correo electrónico oficial del Titular y/o Suscriptor.

Las direcciones de correo electrónico para fines de contacto, así como la información que ha sido proporcionada por el Usuario no deben ser compartidas con terceras personas, salvo expresa autorización de aquel.

Toda la información proporcionada por el Usuario estará incluida en la base de datos que será administrada por la EREP-RENIEC y ECEP-RENIEC, así como por la Gerencia de Tecnología de la Información, cuando corresponda, para los fines de la prestación del Servicio de Certificación Digital.

5.3 DATOS PERSONALES GESTIONADOS

La ECERNEP, la ECEP-RENIEC y las EREP-RENIEC para el ejercicio de sus funciones mantiene la siguiente información de los Usuarios:

a. Datos de identificación personal (de ser el caso se puede incluir la fotografía que aparece en el documento de identidad oficial).

b. Información relevante de las personas jurídicas para la emisión o cancelación de su certificado digital.

c. Datos del domicilio del Usuario.

d. Correos electrónicos personales y/o números telefónicos (fijo o celular), en caso de ser proporcionados por los Usuarios.

e. Expediente, el cual contiene la solicitud de emisión o cancelación de un Certificado Digital, y todos los documentos anexos a la solicitud.

f. De ser el caso, información personal provista por los Usuarios que no sea la autorizada para estar contenida en los Certificados Digitales, en el repositorio y en la CRL.

5.4 INFORMACIÓN CONFIDENCIAL

Conforme a lo establecido en las Guías de Acreditación de Entidades de Registro y Entidades de Certificación, versión 3.3[7] y el Reglamento de Firmas y Certificados Digitales[8], el personal que colabora en la prestación del Servicio de Certificación Digital debe mantener la confidencialidad de la siguiente información:

a. Material o información reservada de la ECERNEP, ECEP-RENIEC y EREP-RENIEC, incluyendo términos contractuales, planes de negocio e información que verse sobre derechos de propiedad intelectual.

b. La información del negocio suministrada por la ECERNEP, ECEP-RENIEC o por sus proveedores y otras personas con las que la EREP-RENIEC tiene el deber de guardar secreto establecido de modo convencional.

c. Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los Usuarios.

d. Información que pueda permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los Usuarios o Terceros que Confían.

e. La causal que motivó la cancelación o revocación de oficio del Certificado Digital.

f. Información personal provista por los Usuarios que no sea la autorizada para estar contenida en los Certificados Digitales ni en la CRL.

g. Toda la documentación contenida en el expediente que custodia la EREP-RENIEC y que no forma parte de la información contenida en el Certificado Digital.

h. El código de activación del certificado digital (código PUK)

i. Toda la información clasificada como “confidencial”, por la ECERNEP, ECEP-RENIEC y la EREP-RENIEC.

De otro lado, se considera información confidencial y de uso exclusivo de la GRCD y de los colaboradores del RENIEC, en función a los roles que desempeñen, el presente documento, la Política de Seguridad y los documentos que la conforman.

5.5 INFORMACIÓN PÚBLICA - NO CONFIDENCIAL

Los datos personales que serán públicos son aquellos que se incluye en los Certificados Digitales y en la CRL.

Asimismo, se considera no confidencial y por lo tanto accesible por terceros a la siguiente información que se detalla, pero no se limita, a:

- Los Certificados Digitales emitidos por la ECERNEP y ECEP-RENIEC, así como las informaciones contenidas en éstos y el estado de los mismos.

[7] Numeral 9.3 sobre confidencialidad de la información del negocio y numeral 9.4.2 sobre información tratada como privada.
[8] Aprobado por el Decreto Supremo N° 052-2008-PCM

- Certificados Digitales cancelados o revocados de oficio.
- Datos de identidad del Titular y/o Suscriptor que figuran en el Certificado Digital.
- Usos y límites de uso de los Certificados Digitales.
- Las fechas de emisión y de caducidad del Certificado Digital.
- El número de serie del Certificado Digital.
- Aquella información personal que los Usuarios soliciten o autoricen que se publique.
- La contenida en la Declaración de Prácticas de Registro.
- La contenida en la Declaración de Prácticas de Certificación.
- La contenida en la Política de Privacidad.
- La Lista de Certificados Digitales Cancelados.
- Toda otra información clasificada como "pública" por la ECERNEP, la ECEP-RENIEC y las EREP-RENIEC.

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

5.6 EXCEPCIONES A LA RESERVA DE LA INFORMACIÓN CONFIDENCIAL

La información confidencial del Usuario será únicamente revelada o comunicada al Poder Judicial cuando una orden judicial así lo exija o, cuando ésta sea solicitada, de manera expresa, por el titular de los datos personales.

5.7 PERIODO DE CONSERVACIÓN DE LA INFORMACIÓN

La ECERNEP, la ECEP-RENIEC y las EREP-RENIEC mantendrán la información personal de los solicitantes de los certificados digitales por un periodo de diez (10) años computados a partir de la fecha de cancelación o revocación del referido certificado[9].

6. ACCESO Y CORRECCIÓN DE LA INFORMACIÓN PERSONAL

[9] Artículo 26, numeral g) del Reglamento de la Ley de Firmas y Certificados Digitales.

6.1 ACCESO A LA INFORMACIÓN PERSONAL

6.1.1 Usuarios:

Los Usuarios pueden ejercer los siguientes derechos:

- Acceder a su información personal y solicitar se modifiquen sus datos personales cuando no sean correctos o no estén actualizados. El acceso gratuito es limitado a una vez durante un año.
- Solicitar todo tipo de información referente a: ciclo de vida del Certificado Digital, usos del Certificado y procedimientos de acceso y corrección de los datos contenidos en el Certificado Digital, la finalidad del tratamiento de sus datos, a quiénes se puede o se ha transmitido sus datos. El sitio web del RENIEC deberá contener la mayor información posible sobre el uso de firmas y Certificados Digitales y sobre el Servicios de Certificación Digital.
- Solicitar información respecto de las entidades de la Administración Pública u organismos a quienes sus datos han sido transmitidos.

El Usuario podrá ejercer sus derechos dirigiéndose a cualquier Agencia EREP-RENIEC y deberá identificarse mediante su documento de identidad, el cual debe encontrarse vigente**.**

6.1.2 Tercero que Confía:

El Tercero que Confía únicamente tendrá acceso a la información personal de los Titulares o Suscriptores de Certificados Digitales que sea necesaria para verificar el estado del mismo.

6.1.3 Entidades de la Administración Pública:

Las entidades de la Administración Pública podrán acceder a la información personal que obra en poder de la ECERNEP, la ECEP-RENIEC y las EREP-RENIEC, y que se encuentra en archivos electrónicos, previo la suscripción con el RENIEC del respectivo Convenio. El Convenio deberá especificar las condiciones y los criterios para el acceso a dicha información conforme lo establecido en el Artículo 55° del Reglamento de la Ley de Firmas y Certificados Digitales y lo señalado en el Decreto Legislativo N° 1246 (10NOV2016) sobre Interoperabilidad entre entidades de la Administración Pública y en el documento “Estándares y Especificaciones de Interoperabilidad del Estado Peruano”, aprobado mediante Resolución Ministerial N° 381-2008-PCM (19NOV2008).

Las entidades de la Administración Pública, a través de la interoperabilidad, interconectan, ponen a disposición, permiten el acceso o suministran la información o base de datos actualizadas, que administran, recaben, sistematicen, crean o posean respecto de los usuarios o administrados, que las demás entidades requieran necesariamente y de acuerdo a ley, para la tramitación de sus procedimientos administrativos y para sus actos de administración interna.

6.1.4 Personal que desarrolla funciones y/o labores en la prestación del Servicio de Certificación Digital:

El personal de la ECERNEP, la ECEP-RENIEC y las EREP-RENIEC, y de los órganos que intervienen en el proceso para la prestación del Servicio de Certificación Digital sólo tendrá acceso a los datos o información personal de los Usuarios o información confidencial de acuerdo al perfil asignado, y siempre que dicho acceso sea necesario para el desempeño de sus funciones.

Se deberá llevar el control respectivo del personal que tiene acceso a dicha información.

6.2 MECANISMOS DE ACCESO A LA INFORMACIÓN PERSONAL

De manera presencial en las Agencias EREP autorizadas por el RENIEC.

Para el ejercicio de los derechos señalados en el numeral 6.1.1, previamente la EREP-RENIEC deberá verificar la identidad del Usuario mediante su documento de identidad vigente.

La información solicitada deberá ser provista al día siguiente de presentada la solicitud, o más tardar dentro de los tres (3) días siguientes de presentada la solicitud, según sea el caso de complejidad. A solicitud del Usuario se podrá enviar dicha información a su correo electrónico.

6.3 CORRECCIÓN DE LA INFORMACIÓN PERSONAL

6.3.1 Origen de la información personal incluida en el Certificado Digital del Usuario

Los Certificados Digitales serán emitidos sobre la base de la información provista para tales efectos por los Usuarios en el respectivo Formulario. No obstante, es obligación del Operador de Registro de la EREP-RENIEC verificar que la información consignada por el solicitante en el Formulario coincide con su documento de identificación oficial (DNI) o carné de extranjería.

Durante el trámite de la solicitud del Certificado Digital, el Operador de Registro de la EREP-RENIEC debe recordar al Usuario sobre su obligación de mantener permanentemente actualizada su información personal que obra en su Certificado Digital, debiendo poner en conocimiento, de manera inmediata, a la EREP-RENIEC cualquier cambio o variación en la misma.

La EREP-RENIEC no asumirá responsabilidad alguna cuando el error u omisión obedece a información que ha sido indebida, inadecuada o erróneamente consignada por el Usuario en la respectiva solicitud. Sin embargo, ello no exime al Operador de Registro de su obligación de verificar correctamente la información proporcionada por el Usuario.

6.3.2 Procedimiento de corrección y/o modificación de los datos

La EREP-RENIEC podrá corregir y/o modificar los datos personales incorporados en el Certificado Digital, previa solicitud expresa del Usuario, en caso hubiese algún error en los datos personales.

En este caso, la EREP-RENIEC debe actualizar los datos personales en su sistema, y deberá revocar el Certificado Digital y emitir un nuevo Certificado Digital.

7. MEDIDAS DE SEGURIDAD

El personal de la GRCD y de los órganos que intervienen en el proceso para la prestación del Servicio de Certificación Digital, sólo accederán a aquellos datos y recursos que precise para el desarrollo de sus funciones y deberá cumplir con las medidas de seguridad estipuladas por el RENIEC y con la Política de Seguridad.

Los documentos que contengan datos personales no públicos e información confidencial deberán estar archivados o almacenados en soportes que permitan identificar el tipo de información que contienen y serán inventariados. Estos soportes deberán encontrarse en un lugar que cuente con seguridad. El acceso a dichos soportes será restringido, y sólo tendrán acceso las personas previamente autorizadas por el Oficial de Seguridad de la Información, o de ser el caso, por el Gerente de la Unidad Orgánica que interviene en el proceso para la prestación del Servicio de Certificación Digital.

Los responsables de la administración de la ECERNEP, la ECEP-RENIEC y las EREP-RENIEC deberán prever el establecimiento de mecanismos que eviten que uno de los colaboradores (personal) acceda a la información o recursos no autorizados. Asimismo, serán responsables de velar por la disponibilidad, la integridad, autenticidad, confidencialidad y la conservación de los datos personales que posee el RENIEC en sus roles de ECEP-RENIEC y EREP-RENIEC.

Las medidas de seguridad estarán orientadas a proteger en todo momento la información frente a riesgos como:

- Pérdida de información.
- Acceso no autorizado.
- Modificación de la información.
- Mal uso de la información.
- Revelación de información no autorizada.
- Almacenamiento no autorizado de información.
- Transferencia no autorizada de información.

Todo el personal de la GRCD y de los órganos que intervienen en el proceso para la prestación del Servicio de Certificación Digital tienen la obligación de cumplir con todas las prescripciones y medidas señalas en el documento “Política de Seguridad”, por tanto, están obligados a conocer y observar las medidas, normas, procedimientos,

reglas y estándares que afecten las funciones que desarrollan; su incumplimiento dará origen a la aplicación de la sanción administrativa respectiva, y en el caso del contratista, a la aplicación de la penalidad que corresponda.

Asimismo, dicho personal deberá guardar el debido secreto y confidencialidad sobre los datos personales e información confidencial que conozca en el desarrollo de su trabajo.

En caso de existir personal ajeno a la GRCD y los órganos antes referidos, que traten los datos personales para desarrollar sus actividades y necesitan acceso a los mismos, serán debidamente informados y formados acerca de todas las obligaciones en materia de protección de datos personales establecidas en el presente Plan y en la Política de Seguridad.

Es obligación del referido personal y de los terceros (contratistas) notificar al Oficial de Seguridad de Información las incidencias de seguridad[10] de las que tengan conocimiento respecto a la información y los recursos protegidos, de acuerdo a los procedimientos establecidos para tales fines.

La GRCD y los órganos que intervienen en el proceso para la prestación del Servicio de Certificación Digital solicitarán a su personal y terceros (contratistas) que tengan acceso a la información confidencial o a los datos personales no públicos, la suscripción del acuerdo de confidencialidad. En dicho acuerdo se debe prever: (i) la obligación de no divulgar cualquier información que pudiera facilitar o coadyuvar a la vulneración de la privacidad de los datos personales y confidencialidad de la información, aún después de extinguido el vínculo laboral o contractual y, (ii) las consecuencias civiles o penales derivadas de su incumplimiento.

En el supuesto que se vulnere la confidencialidad de los datos personales no públicos o la información confidencial, por parte de algún colaborador del RENIEC (funcionario o servidores), se deberá notificar a la Gerencia de Talento Humano para que inicie el procedimiento sancionador contra aquél. Si se tratase del personal del contratista se deberá notificar al órgano correspondiente para que realice las acciones del caso.

7.1 NIVELES DE SEGURIDAD Y PERFILES DE ACCESO

La GRCD y los órganos que intervienen en el proceso para la prestación del Servicio de Certificación Digital implementarán las medidas de seguridad adecuadas para proteger los datos personales no públicos y la información confidencial que tratan como resultado de sus actividades de certificación digital.

Los niveles de seguridad estarán en función del tipo de dato personal o información confidencial, y comprenderá medidas técnicas y organizativas necesarias para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos recolectados.

Asimismo, la ECERNEP, ECEP-RENIEC y las EREP-RENIEC deben establecer perfiles para cada tipo y nivel de acceso y/o consulta a este tipo de información.

8. USO DE LOS DATOS PERSONALES

[10] Entiéndase como incidencia cualquier anomalía que afecte o pudiera afectar a la seguridad, a la integridad, confidencialidad o disponibilidad de los datos.

La ECERNEP, la ECEP-RENIEC y las EREP-RENIEC usarán los datos personales proporcionados por los Usuarios o por un tercero que solicita la cancelación del Certificado Digital, únicamente para el ejercicio de sus funciones.

Es obligación del personal de la GRCD y de los órganos que intervienen en el proceso para la prestación del Servicio de Certificación Digital realizar sus funciones con la debida diligencia, resguardando en todo momento la confidencialidad de la información, así como velar por la integridad y seguridad de la misma.

La ECEP-RENIEC y las EREP-RENIEC, en caso precise utilizar los datos personales no públicos para fines distintos a la prestación del Servicio de Certificación Digital, deberán previamente solicitar al Usuario su consentimiento.

8.1 INFORMACIÓN AL USUARIO

Los formatos de solicitud de emisión y cancelación de Certificados Digitales especifican los datos personales del Usuario que son recolectados por las EREP-RENIEC. El Contrato de prestación del Servicio de Certificación Digital únicamente recoge datos de identificación de la persona natural persona jurídica.

La ECERNEP, ECEP-RENIEC y las EREP-RENIEC brindarán información al Usuario mediante la publicación de su Política de Privacidad que estará disponible en el sitio web del RENIEC, la cual informará sobre:

- Datos personales que se recolecta;
- Titular del banco de datos y responsable del tratamiento de los datos personales.
- Finalidad del tratamiento de los datos personales;
- Información pública y confidencial;
- Sobre las medidas de seguridad;
- Las circunstancias bajo las cuales será divulgada, cedida o transferida la información personal;
- Los derechos de los usuarios,
- Responsabilidad de los Usuarios,
- Corrección de la información personal,
- El tiempo del almacenamiento de los datos personales, entre otros.

Asimismo, a través del sitio web se mantendrá permanentemente informado al Usuario sobre el Servicio de Certificación Digital, las distintas clases de Certificados Digitales, los requisitos para obtener un Certificado Digital, como usar adecuadamente su Certificado Digital, entre otros temas de interés que la ECERNEP, ECEP-RENIEC y EREP-RENIEC así lo consideren.

8.2 CONSENTIMIENTO

Para el ejercicio de las funciones del RENIEC en sus roles de ECERNEP, ECEP-RENIEC y EREP-RENIEC, de conformidad con lo dispuesto en el literal 1) del Artículo 14° de la Ley N° 29733 - Ley de Protección de Datos Personales, no se requiere solicitar el consentimiento del titular de los datos para el tratamiento y transferencia de los mismos.

No obstante, en caso se precise usar los datos para fines distintos a la prestación del servicio de certificación digital, se deberá solicitar al Usuario su consentimiento previo.

El personal de la GRCD y de los órganos que intervienen en el proceso para la prestación del Servicio de Certificación Digital siendo responsables de cualquier perjuicio que pudiese producirse como consecuencia del incumplimiento de esta obligación.

9. TRANSFERENCIA DE DATOS PERSONALES

La ECERNEP, la ECEP-RENIEC y las EREP-RENIEC, dentro del marco de la IOFE, así como, dentro del marco de colaboración entre entidades del sector público, podrán transferir a organismos del Estado, u otras Entidades Prestadores de Servicios de Certificación Digital, así como a los Terceros que Confían, los datos personales de los Usuarios.

Dentro del marco de colaboración entre Entidades de la Administración Pública, la transferencia se realizará de acuerdo a lo señalado en el Convenio respectivo que suscriba el RENIEC y la entidad pública solicitante. Conforme a lo establecido en el Artículo 55° del Reglamento de la Ley de Firmas y Certificados Digitales, la disponibilidad de la información personal requerida por la Entidad de la Administración Pública solicitante está limitada a que ésta use la información únicamente para la tramitación y resolución de los procedimientos de su competencia.

La entidad receptora deberá garantizar la protección de los datos personales transferidos, bajo su exclusiva responsabilidad.

El Oficial de Privacidad de Datos, cuando corresponda, emitirá opinión sobre la aprobación de la transferencia de los datos personales que pudiese efectuarse dentro del marco de la IOFE o dentro del marco de colaboración entre Entidades de la Administración Pública, asimismo, deberá llevar un registro de las transferencias que se hubiesen realizado.

10 TRATAMIENTO DE LOS DATOS PERSONALES

La ECERNEP, la ECEP-RENIEC y las EREP-RENIEC efectuarán el tratamiento de aquellos datos personales o información que han sido recolectados en los trámites referidos al ciclo de vida del certificado digital (emisión o cancelación del Certificado Digital) o como motivo de la prestación del Servicio de Certificación Digital.

Los procesos de tratamiento de información tendrán como propósito la adecuada gestión y control de los servicios contratados por el Usuario, así como también las acciones orientadas a impulsar el uso de la firma digital, la visualización o envío por medios impresos y/o telemáticos de información acerca de los servicios ofrecidos por la ECERNEP, la ECEP-RENIEC y las EREP-RENIEC. Estos procesos de tratamiento incluye, pero no se encuentra limitado a:

- Emisión, cancelación o revocación de oficio de Certificados Digitales.
- Actualización de la información personal del Usuario.
- Verificación del estado de cancelación o revocación de los Certificados Digitales en la CRL.
- Publicación de los Certificados Digitales emitidos en el Repositorio.
- Creación de un banco de datos de administración pública para gestionar los datos personales de manera efectiva y eficiente.
- Sistema de gestión de las EREP-RENIEC y ECEP-RENIEC.

En ese sentido, los datos personales de los Usuarios podrán ser objeto de los siguientes tratamientos: recolección, registro, organización, visualización, almacenamiento, procesamiento, conservación, elaboración, modificación, extracción, consulta, bloqueo, supresión, comunicación, transferencia y uso.

La ECERNEP, la ECEP-RENIEC y las EREP-RENIEC llevarán un registro electrónico de todos los accesos que se hubiesen realizado al banco de datos, conforme a lo señalado en la Política de Seguridad.

11 PROCEDIMIENTO DE REVISION

Para fines de salvaguardar y comprobar la correcta aplicación del presente Plan de Privacidad se implementa los siguientes procedimientos:

11.1 REVISIÓN RUTINARIA

El Oficial de Privacidad de Datos realizará, cada año, una auditoría de la adecuada protección de los datos personales y cumplimiento de lo señalado en el Plan y la Política de Privacidad por parte de todo el personal de la GRCD y de los órganos que intervienen en el proceso para la prestación del Servicio de Certificación Digital, debiendo revisar el Plan y la Política de Privacidad y proponer los cambios que sean necesarios, acorde con la normativa vigente sobre protección de datos personales. Para tal fin, emitirá el informe respectivo con las recomendaciones a que hubiera lugar.

11.2 REVISIÓN EXTRAORDINARIA

El Oficial de Privacidad de Datos, de creerlo necesario, llevará a cabo en cualquier momento una auditoría extraordinaria, para verificar el cumplimiento de las medidas de seguridad orientadas a proteger los datos personales y la información confidencial.

12 CUMPLIMIENTO DE LOS PRINCIPIOS DE PRIVACIDAD DE LA INFORMACIÓN

De conformidad con lo establecido por el APEC a través de la Norma Marco sobre Privacidad, existen nueve principios que deben ser observados siempre que se realice algún tipo de labor o función que involucre la recolección, procesamiento, uso, transferencia de la información personal.

En ese sentido, se establecen los siguientes lineamientos y medidas que el personal de la GRCD y de los órganos que intervienen en el proceso para la prestación del Servicio de Certificación Digital, observará en todo momento respecto de los procedimientos que se desarrollen como parte de sus funciones y en aras de asegurar la protección de los datos personales, así como, la confidencialidad de la información de la ECERNEP, la ECEP-RENIEC y las EREP-RENIEC:

1. Con relación al principio de Prevención del Daño:	• Se recogerá únicamente información que resulte indispensable para la prestación del Servicio de Certificación Digital. • El personal de la GRCD, de los órganos que intervienen en el proceso para la prestación del

	Servicio de Certificación Digital y terceros (contratistas), deben cumplir estrictamente con lo establecido en la Política de Seguridad, a fin de prevenir y evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos los datos personales o información que mantiene la ECERNEP, la ECEP-RENIEC, y las EREP-RENIEC. • De ser el caso, se establecerá un procedimiento para la transferencia de la información. • Se capacitará al personal en temas específicos sobre protección de datos personales y se pondrá en conocimiento sus obligaciones y funciones respecto al resguardo de la privacidad de la información.
2. Con relación al principio de Información:	A través de la Política de Privacidad, se informará al Usuario sobre: • Datos personales que se recolecta; • Titular del banco de datos y responsable del tratamiento de los datos personales. • Finalidad del tratamiento de los datos personales; • información pública y confidencial; • Sobre las medidas de seguridad; • Las circunstancias bajo las cuales será divulgada, o transferida la información personal; • Los derechos de los Usuarios, • Responsabilidad de los Usuarios, • Corrección de la información personal, • El tiempo del almacenamiento de los datos personales, entre otros. Asimismo, en el sitio web se pondrá a disposición del público en general y en particular de los Usuarios información relativa a firmas y Certificados Digitales y su uso adecuado.
3. Con relación al principio de Limitaciones a la Recolección:	La recolección y el tratamiento de los datos personales y de la información provista por las personas jurídicas tienen como propósito la adecuada gestión, administración y control del Servicio de Certificación Digital contratado por el Usuario, así como también la visualización o envío por medios impresos y/o telemáticos de información acerca de los servicios ofrecidos por el RENIEC en sus roles de ECERNEP, ECEP-RENIEC y EREP-RENIEC.
4. Con relación al principio de Uso de la Información Personal:	El uso de los datos personales o la información provista por el Usuario, está estrictamente limitada a la prestación del Servicio de Certificación Digital que es provisto por el RENIEC en sus roles de ECERNEP, ECEP-RENIEC y EREP-RENIEC. Estos servicios comprenden, pero no se encuentran limitados a:

	• Emisión, cancelación o revocación de oficio de Certificados Digitales. • Verificación del estado de cancelación o revocación de los Certificados Digitales en la CRL. • Creación de un banco de datos para gestionar los datos personales de manera efectiva y eficiente. • Sistema de gestión de la ECERNEP, ECEP-RENIEC y EREP-RENIEC Como excepción, la información personal podrá ser usada para fines distintos a los señalados líneas arriba cuando: a. Exista consentimiento del Usuario. b. Fuese necesaria para la provisión de un servicio solicitado por el Usuario. c. Por disposición legal que así lo señale.
5. Con relación al principio de Elección:	El Usuario estará debidamente informado mediante la Política de Privacidad sobre los datos personales que la EREP-RENIEC recolecta así como del uso de los mismos y de los derechos inherentes a él. Los formatos de solicitud de emisión y cancelación especificarán claramente los datos o información personal que la EREP-RENIEC recolecta. De conformidad con lo dispuesto en el literal 1) del Artículo 14° de la Ley N° 29733 - Ley de Protección de Datos Personales, la EREP-RENIEC no requiere solicitar el consentimiento del titular de los datos para el tratamiento y transferencia de los mismos.
6. Con relación al principio de Integridad de la Información personal:	La información personal que es recolectada por la EREP-RENIEC será almacenada en el banco de datos, manteniendo su integridad, es decir, se asegurará que la información no sea alterada desde la transmisión hasta su registro. La información será actualizada a solicitud del Usuario.
7. Con relación al principio de Medidas de Seguridad:	La ECERNEP, la ECEP-RENIEC y las EREP-RENIEC establecerán sus medidas de seguridad acorde con las normativas tanto nacionales como internacionales en materia de infraestructura, comunicaciones, recursos humanos así como también en seguridad de la información. Las medidas de seguridad estarán orientadas a proteger en todo momento la información frente a riesgos como: • Pérdida de información. • Acceso no autorizado.

	• Modificación de la información. • Mal uso de la información. • Publicación de información no autorizada. • Almacenamiento no autorizado de información. • Transferencia no autorizada de información. Asimismo, estas medidas de seguridad estarán sometidas a evaluaciones y reevaluaciones periódicas para asegurar el cabal cumplimiento de este principio. Las medidas de seguridad serán implementadas de acuerdo a la Política de Seguridad.
8. Con relación al principio de Acceso y Corrección:	La ECERNEP, la ECEP-RENIEC y las EREP-RENIEC tendrán procedimientos claros orientados a asegurar que los Usuarios puedan: 1. Tener acceso a su información. 2. Obtener información sobre las condiciones de emisión, motivos de cancelación o revocación de oficio y uso de sus Certificados Digitales. 3. Obtener información respecto de las entidades de la Administración Pública u otras entidades a quienes sus datos han sido transmitidos. 4. Actualizar o corregir sus datos personales consignados en su Certificado Digital.
9. Con relación al principio de Responsabilidades:	La EREP-RENIEC debe informar al Usuario sobre sus obligaciones, específicamente que debe: • Mantener actualizada su información. • Asegurar que el software y hardware cumplen con las especificaciones técnicas mínimas requeridas. La ECERNEP, la ECEP-RENIEC y las EREP-RENIEC deben cumplir con el presente Plan de Privacidad y la Política de Seguridad, debiendo asegurar la protección de los datos personales en el proceso de certificación digital.