RENIEC
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES"
" AÑO DE LA LUCHA CONTRA LA CORRUPCION Y LA IMPUNIDAD "

RESOLUCIÓN JEFATURAL N° 28 -2019/JNAC/RENIEC

Lima, 22 FEB. 2019

VISTOS:

La Hoja de Elevación N°000151-2018/GRCD/RENIEC (16NOV2018), emitida por la Gerencia de Registros de Certificación Digital; el Informe N°000033-2018/GRCD/SGREGD/RENIEC (16NOV2018), emitido por la Sub Gerencia de Regulación Digital de la Gerencia de Registros de Certificación Digital; los Informes N°000023-2018/RDM/GAJ/RENIEC (27DIC2018) y N° 000005-2019/RDM/GAJ/RENIEC (06FEB2019) y la Hoja de Elevación N° 000102-2018/GAJ/RENIEC (12FEB2019) emitidos por la Gerencia de Asesoría Jurídica;

CONSIDERANDO:

Que mediante Ley N° 26497, se creó el Registro Nacional de Identificación y Estado Civil (RENIEC), con arreglo a los artículos 177° y 183° de la Constitución Política del Perú, como organismo constitucionalmente autónomo, con personería jurídica de derecho público interno, que goza de atribuciones en materia registral, técnica, administrativa, económica y financiera; encargado, entre otros, de manera exclusiva y excluyente de organizar y actualizar el Registro Único de Identificación de las Personas Naturales, así como de inscribir los hechos y actos relativos a su capacidad y estado civil;

Que conforme al artículo 47° del Decreto Supremo N°052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales, se designa al Registro Nacional de Identificación y Estado Civil - RENIEC como Entidad de Certificación Nacional para el Estado Peruano, (ECERNEP), Entidad de Certificación para el Estado Peruano (ECEP), y Entidad de Registro o Verificación para el Estado Peruano (EREP); precisándose que los servicios a ser prestados en cumplimiento de los roles señalados estarán a disposición de todas las Entidades Públicas del Estado Peruano y de todas las personas naturales y jurídicas que mantengan vínculos con él, no excluyendo ninguna representación del Estado Peruano en el territorio nacional o en el extranjero;

Que en dicho contexto, el RENIEC mediante Resolución N°144-2017/CFE-INDECOPI (28DIC2017), emitida por el Presidente de la Comisión para la Gestión de la Infraestructura Oficial de la Firma Electrónica, obtiene la renovación de su acreditación como Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), al haber cumplido con los requisitos de la Guía de Acreditación de Entidades de Certificación para el Nivel de Seguridad Medio, en lo referido a los procedimientos y políticas seguidos por su personal, la interoperabilidad y la usabilidad de su infraestructura de clave pública y los demás requisitos de la Guía, conforme se señala en la Resolución acotada;

Que asimismo, a través de los documentos del visto la Gerencia de Registros de Certificación Digital, en virtud de las funciones establecidas en el Reglamento de Organización de Funciones, solicita que se gestione la aprobación del texto de Convenio de Colaboración Interinstitucional para otorgar el servicio de certificación digital para las Entidades de Certificación para el Estado Peruano (ECEP) debidamente acreditadas ante la Autoridad Administrativa Competente - AAC

en el marco de las funciones del RENIEC como Entidad de Certificación Nacional para el Estado Peruano (ECERNEP);

Que al respecto, en la Ley N°26497 – Ley Orgánica del Registro Nacional de Identificación y Estado Civil, se establece que el Jefe del Registro Nacional de Identificación y Estado Civil – RENIEC, es la máxima autoridad de dicho organismo, quien ejerce su representación legal y es el encargado de dirigir y controlar la institución;

Que de igual manera, en el literal m) del artículo 15° del Reglamento de Organización de Funciones del RENIEC, aprobado mediante Resolución Jefatural N°073-2016/JNAC/RENIEC (31MAY2016); se establece que, son funciones y atribuciones del Jefe Nacional, celebrar y suscribir en representación de la Institución, todo tipo de acuerdos y convenios de cooperación con organismos públicos o privados, nacionales o internacionales;

Que en ese sentido, al existir, mandato imperativo de carácter legal y administrativo de un documento que garantice el acuerdo de las partes, resulta legalmente viable aprobar el texto del Convenio de Colaboración Interinstitucional para otorgar el servicio de certificación digital para las Entidades de Certificación para el Estado Peruano (ECEP), en el marco de las funciones del RENIEC como Entidad de Certificación Nacional para el Estado Peruano (ECERNEP);

Que mediante la Resolución Jefatural N° 000015-2019/JNAC/RENIEC (05FEB2019) se declara que el señor Bernardo Juan Pachas Serrano, en su calidad de Gerente General, asume interinamente las funciones de Jefe Nacional del Registro Nacional de Identificación y Estado Civil en tanto se designe al nuevo titular de la institución y este asuma las funciones que por ley le corresponden; y,

Estando a lo opinado por la Gerencia de Asesoría Jurídica y a las atribuciones conferidas por la Ley N° 26497, Ley Orgánica del Registro Nacional de Identificación y Estado Civil y el Reglamento de Organización y Funciones del RENIEC, aprobado mediante Resolución Jefatural N°073-2016/JNAC/RENIEC (31MAY2016) y su modificatoria;

SE RESUELVE:

Artículo Primero. - Aprobar el texto contenido en el anexo Convenio de Colaboración Interinstitucional para otorgar el servicio de certificación digital para las Entidades de Certificación para el Estado Peruano (ECEP) debidamente acreditadas ante la Autoridad Administrativa Competente - AAC en el marco de las funciones del RENIEC como Entidad de Certificación Nacional para el Estado Peruano (ECERNEP); el mismo que forma parte integrante de la presente Resolución Jefatural.

Artículo Segundo. - Disponer que la Gerencia de Registros de Certificación Digital, informe a la Jefatura Nacional, los convenios suscritos en el marco de la presente Resolución.

Regístrese, comuníquese y cúmplase.

BERNARDO JUAN PACHAS SERRANO
Jefe Nacional (i)
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

BPS/RRC/JAY/rdm

CONVENIO DE COLABORACIÓN INTERINSTITUCIONAL PARA OTORGAR EL SERVICIO DE CERTIFICACIÓN DIGITAL A LAS ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA ACREDITADAS ANTE LA AUTORIDAD ADMINISTRATIVA COMPETENTE COMO ENTIDADES DE CERTIFICACIÓN PARA EL ESTADO PERUANO EN EL MARCO DE LAS FUNCIONES ASIGNADAS AL REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL COMO ENTIDAD DE CERTIFICACIÓN NACIONAL PARA EL ESTADO PERUANO.

Conste por el presente documento, el Convenio de Colaboración Interinstitucional para otorgar el Servicio de Certificación Digital a las entidades de la Administración Pública acreditadas ante la Autoridad Administrativa Competente (AAC) como Entidades de Certificación para el Estado Peruano (ECEP), en el marco de las funciones asignadas como Entidad de Certificación Nacional para el Estado Peruano (ECERNEP) y acreditada mediante Resolución de la Comisión para la Gestión de la Infraestructura Oficial de Firma Electrónica (IOFE) N° 144-2017/CFE-INDECOPI de fecha 28 de Diciembre del 2017, que suscriben de una parte, el Registro Nacional de Identificación y Estado Civil, con RUC N° 20295613620, y domicilio en el Jr. Bolivia N° 109, Lima, a quien en adelante se le denominará EL **RENIEC**, representado por el señor Ricardo Javier Enrique Saavedra Mavila, identificado con DNI N° 06667808, en virtud a la facultad contenida en la Resolución Jefatural N°04-2019/JNAC/RENIEC (09/01/2019); y de la otra parte, xxxxxxxxxxxxxxxxxxxxxx, con RUC N° xxxxxxxxxxxxx, con domicilio en xxxxxxxxxxxxxxxx, distrito de xxxxxxxxxxxxx, provincia de xxxxxxxxxx, departamento de xxxxxxxxx, en su calidad de Entidad de Certificación para el Estado Peruano (ECEP-....), acreditada por la AAC mediante Resolución de la Comisión para la Gestión de la Infraestructura Oficial de Firma Electrónica N°----/CFE-INDECOPI de fecha....., en adelante LA **ENTIDAD**, representada por xxxxxxxxxxxxxxxx, identificado con DNI N° xxxxxxxxxxxx, con el cargo de xxxxxxxxxxxxx, designado mediante Resolución xxxxxxxxxxxx N° .....de fecha ..... y facultado mediante Resolución xxxxxxxxxxxxxxxx N° xxx-xxx-xxxxx de fecha xx de xxxx del xxxxx, en los términos y condiciones establecidos en las siguientes cláusulas:

CLÁUSULA PRIMERA: DE LAS PARTES

El Registro Nacional de Identificación y Estado Civil – RENIEC, creado mediante Ley 26497, es un organismo constitucionalmente autónomo, con personería jurídica de derecho público interno, que goza de atribuciones en materia registral, técnica, administrativa, económica y financiera. Está encargado de organizar y mantener el Registro Único de Identificación de las Personas Naturales e inscribir los hechos y actos relativos a su capacidad y estado civil.

En el marco de los dispuesto por la Ley N° 27269 – Ley de Firmas y Certificados Digitales (En adelante La Ley) y por disposición expresa del Reglamento de la Ley de Firmas y Certificados Digitales aprobado por D.S. 052-2008-PCM (en adelante El Reglamento de la Ley), El RENIEC ha sido designado como la única Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), acreditada mediante Resolución de la Comisión para la Gestión de la Infraestructura Oficial de Firma Electrónica N° 144-2017/CFE-INDECOPI de fecha 28 de diciembre del 2017, en su rol de Autoridad Administrativa Competente (AAC).

Mediante el Art. 46° del Reglamento de la Ley, se establece la Estructura Jerárquica de Certificación del Estado Peruano en el marco de la IOFE, siendo el primer componente la ECERNEP, encargada de emitir y cancelar los certificados raíz para las ECEP que así lo soliciten, además de proponer a la AAC, las políticas y estándares que rigen para las Entidades de Certificación Digital (ECEP) las Entidades de Registro y Verificación para el

Estado Peruano (EREP). Además, en su Art. 47° se establece que las ECEP y/o EREP deberán cumplir con las políticas y estándares que sean propuestos por la ECERNEP y aprobados por la AAC. Conforme a ello, se ha desarrollado la "Política General de Certificación" y la "Declaración de Prácticas de Certificación", alineados a la "Guía de Acreditación de Entidades de Certificación EC" y a su Anexo 1, "Marco de la Política de Emisión de Certificados Digitales" versión 3.3 publicada por la AAC.

Asimismo, ha establecido a través de su Reglamento de Organización y Funciones del 2016 aprobado por Resolución Jefatural N° 73-2016/JNAC/RENIEC de fecha 31 de mayo del 2016, que la Sub Gerencia de Regulación Digital sea la encargada de representar a la ECERNEP, siendo la responsable de la acreditación y su mantenimiento ante la AAC, así como de establecer las políticas y estándares para los Prestadores de Servicios de Certificación (PSC) que operen bajo la Estructura Jerárquica de Certificación del Estado Peruano de la IOFE; consecuentemente será la unidad orgánica encargada de emitir y cancelar el certificado digital para ECEP (de Nivel 2 en la jerarquía PKI), materia del presente convenio.

La ENTIDAD, es .....

CLÁUSULA SEGUNDA: DE LA JUSTIFICACIÓN

EL RENIEC en su rol de ECERNEP, ha emitido un certificado digital raíz que da origen a la jerarquía PKI "ECERNEP PERU CA Root 3", la cual se encuentra estructurada en tres niveles de Autoridades de Certificación, correspondiendo el NIVEL 1 al certificado raíz gestionado por la ECERNEP y el NIVEL 2 a los certificados digitales para las ECEP que cuenten con la correspondiente acreditación para ello y que operen subordinadas en dicha jerarquía PKI a la ECERNEP.

En el literal e) de la Política 35 del Acuerdo Nacional sobre Sociedad de la Información y Sociedad del Conocimiento, se señala que el Estado fomentará su modernización, mediante el uso de las Tecnologías de la Información y la Comunicación (TIC), con un enfoque descentralista, planificador e integral.

A través del Decreto Supremo Nº 04-2013-PCM se aprueba la Política Nacional de Modernización de la Gestión Pública al 2021, cuyo anexo contiene el literal e) del numeral 2.4 "Principios Orientadores de la Política de Modernización", donde se establece que para alcanzar los resultados que la ciudadanía espera, se requiere que las entidades públicas avancen en un proceso constante de revisión y renovación de los procesos y procedimientos mediante los cuales implementan sus acciones, lo cual llevará a implementar nuevas propuestas de servicios o procedimientos que innoven su gestión para responder mejor a las expectativas de los ciudadanos y empresas, debiéndose incorporar el aprovechamiento intensivo de tecnologías apropiadas no solo a nivel de dependencias prestadoras de servicios, sino también de aquellas responsables de sistemas administrativos, de manera que dichas tecnologías contribuyan al cambio y mejora de la gestión pública.

Asimismo, el Decreto Supremo N° 033-2018-PCM, que crea "La Plataforma Digital Única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital", define el Servicio Público Digital como *"Aquel servicio público ofrecido de forma total o parcial a través de internet u otra red equivalente, que se caracteriza por ser automático, no presencial y utilizar de manera intensiva las tecnologías digitales, para la producción y acceso a datos, servicios y contenidos que generen valor público para los ciudadanos y personas en general"*, concepto igualmente recogido por el Decreto Legislativo N° 1412 que aprueba la Ley de Gobierno Digital, y que establece, entre otros conceptos, que el gobierno

digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público, y tiene como finalidad promover la colaboración entre las entidades de la Administración Pública, así como la participación de ciudadanos y otros interesados para el desarrollo del gobierno digital y la sociedad del conocimiento.

Al amparo de las normas legales acotadas y en aras de promover y desplegar la prestación de servicios públicos digitales seguros, EL RENIEC y LA ENTIDAD celebran el presente Convenio a fin de que esta última pueda hacer uso del servicio de Certificación Digital para las ECEP, gozando de las presunciones legales y efectos jurídicos conforme a lo dispuesto por el Reglamento de la Ley.

CLÁUSULA TERCERA: DEL OBJETO DEL CONVENIO

Por el presente Convenio EL RENIEC en su rol de ECERNEP, tramita la solicitud que LA ENTIDAD haya formulado generando la emisión de un (01) certificado digital de Nivel 2 de la jerarquía PKI "ECERNEP PERU CA ROOT3", siendo para uso exclusivo conforme a lo detallado en el numeral 1.4.1 de la Política General de Certificación, cuyo Anexo 02 define todos los posibles tipos de certificados que comprenden este nivel con sus correspondientes perfiles, y de igual manera aquellos que LA ENTIDAD, en su rol de ECEP, puede emitir a entidades de Nivel 3 que corresponden a las clases de certificados, y a partir de éstas a las entidades finales; sin embargo, es potestad de LA ENTIDAD determinar, debiendo luego declarar, cuáles de estos tipos de certificado digital de clase o de entidad final emitirán.

Cabe resaltar que la Clase 2 de los certificados digitales emitidos para entidades finales de Nivel 3, está reservada únicamente para EL RENIEC.

Asimismo, de conformidad con el numeral 4.9 de la Declaración de Prácticas de Certificación, la ECERNEP tramita la solicitud de cancelación del certificado digital de Nivel 2 para las ECEP ante la proximidad a su vencimiento, lo que supone la emisión de un nuevo certificado digital, para lo cual deberá suscribirse y celebrarse nuevo convenio de colaboración interinstitucional u otro aplicable de ser el caso.

EL RENIEC en su rol de ECERNEP:

- No brinda el servicio de renovación del certificado digital.
- No brinda el servicio de reemisión de certificado digital con renovación de llaves.
- No brinda el servicio de modificación del certificado.
- No brinda el servicio de consulta del estado de certificado digital en línea (Online Certificate Status Protocol - OCSP).

CLÁUSULA CUARTA: DEL COMPROMISO DE LAS PARTES

Por el presente Convenio, EL RENIEC en su rol de ECERNEP se compromete a prestar a LA ENTIDAD el servicio de certificación digital, el cual comprende la emisión y/o cancelación del certificado digital materia del presente convenio, conforme a lo declarado en el numeral 1.3.1 de la Política General de Certificación.

Del mismo modo, el RENIEC en su rol de ECERNEP se compromete a lo siguiente:

- Gestionar sus repositorios de acuerdo a lo indicado en el numeral 2.1 de la Declaración de Prácticas de Certificación.
- Mantener actualizada la información de sus repositorios en función a la frecuencia de publicación detallada en el numeral 2.3 de la Declaración de Prácticas de Certificación.

- Mantener disponible la información de forma pública en la Web en la dirección: https://pki.reniec.gob.pe/repositorio, las veinticuatro (24) horas del día y los siete (07) días de la semana.
- No limitar el acceso de lectura a la información de su repositorio.
- Garantizar la existencia de controles físicos y lógicos a su repositorio para impedir que de forma no autorizada se puedan añadir, modificar o borrar registros, bajo las medidas descritas en los puntos correspondientes al numeral 2.4 de la Declaración de Prácticas de Certificación.
- Que todos los certificados digitales de la jerarquía PKI ECERNEP PERU CA ROOT3, contengan información distintiva que permita identificar al emisor y al titular y/o suscriptor, conforme se describe en el numeral 3.1 tanto de la Política General de Certificación, como en la Declaración de Prácticas de Certificación.
- Garantiza que el *SubjectDN* de los certificados digitales que emite es único no sólo durante el periodo de vigencia del certificado, sino durante la entera existencia de la jerarquía de certificación digital.

Por su parte, LA ENTIDAD se compromete a:

- Desarrollar su Declaración de Prácticas de Certificación en conformidad con lo dispuesto en la Política General de Certificación, y efectuar sus operaciones alienado a ello.
- Observar y respetar los procedimientos y controles establecidos por la ECERNEP en su Declaración de Prácticas de Certificación.
- Tener como función principal gestionar el ciclo de vida de los certificados digitales de Entidades Finales, el cual comprenderá los servicios de emisión y cancelación de certificados digitales y optativamente su suspensión.
- No brindar estos servicios directamente a las Entidades Finales, sino que deben hacerlo únicamente a través de entidades acreditadas ante la AAC como EREP.
- Usar exclusivamente el certificado digital de Nivel 2, que se le otorgó mediante el presente, para la emisión de sus correspondientes certificados digitales de Nivel 3 de clases y estos a su vez para la emisión de certificados digitales de entidad final solicitados a través de una EREP conforme se establece en la Política General de Certificación.
- Gestionar sus repositorios en la Web, conteniendo como mínimo la siguiente información:
  - ✓ Directorio de certificados digitales emitidos
  - ✓ Listas de certificados cancelados.
  - ✓ Declaraciones de Prácticas de Certificación.
  - ✓ Políticas de Privacidad.
  - ✓ Políticas de Seguridad.
  - ✓ Otros instrumentos legales vinculantes con suscriptores, titulares y terceros que confían.

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

  El directorio de certificados digitales emitidos y la Lista de certificados cancelados deben estar disponible las 24 horas de cada día, durante los siete días de cada semana. En caso de indisponibilidad no imputable a LA ENTIDAD, el mismo debe aplicar la máxima diligencia en recuperar la disponibilidad en el periodo mínimo de 99% anual, con un tiempo programado de inactividad máximo de 0.5%.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL

CLÁUSULA QUINTA: DE LAS OBLIGACIONES DE LAS PARTES

El RENIEC en su rol de ECERNEP se obliga con LA ENTIDAD a:

a. Validar el derecho que posee LA ENTIDAD solicitante de un certificado digital subordinado verificando y registrando la identidad y los poderes de representación correspondiente, así como los requisitos señalados en el numeral 4.1.2 de la Declaración de Prácticas de Certificación.
b. Verificar y procesar la solicitud de emisión de certificado digital presentada por LA ENTIDAD, conforme al numeral 4.2 de la Declaración de Prácticas de Certificación.
c. Verificar y procesar la solicitud de cancelación de los certificados digitales presentados por LA ENTIDAD por cualquiera de los motivos expuestos en el numeral 4.9.1 de la Declaración de Prácticas de Certificación.
d. Validar y procesar el derecho de petición de cancelación de las personas indicadas en el numeral 4.9.2 de la Declaración de Prácticas de Certificación.
e. Emitir y cancelar el certificado digital previa evaluación y aprobación de la solicitud correspondiente.
f. Incluir el certificado digital cancelado en la Lista de Certificados Digitales Cancelados (CRL), así como mantener dicha lista actualizada.
g. Brindar de forma irrestricta, el servicio de verificación del estado de los certificados mediante la publicación de la CRL, la cual es firmada digitalmente y cuenta con registro de hora y fecha, siendo la disponibilidad del servicio conforme a lo detallado en el numeral 4.10.2 de la Declaración de Prácticas de Certificación.
h. Mantener la confidencialidad de la información relativa al titular y/o suscriptor, observando lo dispuesto en el numeral 9.3 de la Declaración de Prácticas de Certificación, limitando su empleo a las necesidades propias del servicio de certificación, salvo por orden judicial o mandato de autoridad competente amparados por la Ley, o a pedido del titular y/o suscriptor.
i. Entregar el certificado digital al titular y/o suscriptor conforme a las condiciones definidas en los numerales 4.3 y 4.4 de la Declaración de Prácticas de Certificación referidos a la entrega y aceptación del certificado, en lo que sean aplicables.
j. Publicar este documento y los relacionados al servicio, garantizando el acceso a la versión actual y las anteriores.
k. Garantizar que los procedimientos de la ECERNEP, en particular los referidos a la emisión y cancelación de certificados digitales, cumplen con lo descrito en sus documentos operacionales y técnicos correspondientes a la jerarquía PKI "ECERNEP PERU CA ROOT3".

La ENTIDAD se obliga a:

a. Entregar información veraz y actualizarla cuando corresponda, bajo su responsabilidad.
b. Proporcionar evidencia de haber realizado una ceremonia de llaves para generar su par de llaves según lo indicado en el numeral 6.1.1 de la Política general de Certificación.
c. Demostrar la posesión de su llave privada mediante el envío de la solicitud de firma de certificado (Certificate Signing Request o CSR) en formato PKCS#10.
d. Emplear su certificado digital de Nivel 2 (ECEP offline) únicamente para emitir certificados de Nivel 3 (ECEP online) y emplear estos últimos para emitir únicamente certificados digitales de Entidad Final.

e. Ser diligente en la custodia de sus llaves privadas, con el fin de evitar pérdida, revelación, modificación o usos no autorizados.
f. Observar las condiciones establecidas por la ECERNEP para la debida utilización del certificado digital y la generación de las firmas digitales, descritas tanto en la Política General de Certificación como en la Declaración de Prácticas de Certificación.
g. Notificar, sin retrasos injustificados, al Sub Gerente de Regulación Digital del RENIEC, persona de contacto de la ECERNEP o del presente convenio, para que proceda a la cancelación del certificado digital indicado, en los siguientes casos:
    - Pérdida, robo o extravío del dispositivo Hardware Security Module (HSM) que almacena su llave privada.
    - Compromiso potencial de su llave privada, por deterioro, alteración, exposición, puesta en peligro o uso indebido.
    - Pérdida de control sobre su llave privada, debido al compromiso de los datos de activación o por cualquier otra causa.
    - Ante inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor y/o titular, o que la información contenida en el certificado ya no resulte correcta
    - Cuando el titular y suscriptor deja de ser miembro de la comunidad de interés, por pérdida de su acreditación ante la IOFE, o se sustrae de aquellos intereses relativos a la ECERNEP.
h. Dejar de utilizar la llave privada, transcurrido el plazo de vigencia del certificado
i. No monitorear, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de la IOFE, sin permiso previo por escrito de la AAC.
j. No comprometer intencionalmente la seguridad de la IOFE.
k. Establecer con su(s) EREP(s) asociada(s), el contenido del contrato del suscriptor, reflejando las responsabilidades de la propia ECEP, de la EREP y la de los suscriptores y titulares, alineado a lo indicado en la Política General de Certificación, e incorporar la siguiente información para los suscriptores y titulares:
    - Política de aplicación del certificado digital, limitaciones y prohibiciones de uso.
    - Las responsabilidades del suscriptor y del titular frente a: la actualización de sus datos, la solicitud de cancelación del certificado en caso de que la llave privada se vea comprometida antes de la expiración del certificado.
    - Información sobre cómo validar el certificado, incluyendo el requisito de comprobar el estado del mismo y las condiciones en las cuales se puede confiar razonablemente en el certificado, lo cual resulta también aplicable cuando el suscriptor actúa como tercero que confía.
    - Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la ECEP acepta o excluye su responsabilidad.
    - Ley aplicable y jurisdicción competente.
    - Declaración de Prácticas de Certificación de la ECEP y Declaración de Prácticas de Registro de EREP aprobadas por la AAC.
    - Información acerca de los módulos criptográficos de usuario final.
l. Establecer en su Declaración de Prácticas de Certificación u otra documentación relevante el plazo necesario para el procesamiento de solicitudes de emisión de certificados, el cual no debe ser mayor a 5 días hábiles a partir de la entrevista presencial del solicitante en la EREP, considerando el tiempo requerido para el intercambio de información entre la ECEP y la EREP, y 24 horas siguientes a la realización de la solicitud de cancelación de certificados en la EREP asociada.

m. Brindar de forma obligatoria e irrestricta, el servicio de verificación de estado del certificado mediante la Lista de Certificados Cancelados (CRL) y el servicio de Verificación en Línea (OCSP).
n. En caso de finalizar sus actividades, debe informar a la ECERNEP y a la AAC, así como a los titulares, suscriptores y terceros que confían sobre el cese de sus operaciones con un mínimo de treinta (30) días calendario de anticipación.
o. Requerir al tercero que confía, como mínimo lo siguiente:

- No monitorear, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de la Jerarquía ECERNEP PERU CA Root3 de la IOFE, sin autorización por escrito.
- No comprometer intencionalmente la seguridad de la Jerarquía ECERNEP PERU CA Root 3 de la IOFE.
- Aplicar los criterios de verificación adecuados para la validación de un certificado durante su uso en las transacciones electrónicas.
- Denunciar cualquier situación en la que la ECEP deba revocar el certificado de un titular, siempre y cuando se tenga pruebas fehacientes del compromiso de la llave privada o de su uso ilegal. Por ejemplo debe denunciar la pérdida, robo o extravío del dispositivo criptográfico que almacena una llave privada que no le pertenece (Computador, token criptográfico o tarjeta inteligente).
- Remitir anualmente al Sub Gerente de la SGREGD, la resolución de aprobación de la auditoria de seguimiento anual a ser realizada por la AAC.

En caso LA ENTIDAD incumpla estas obligaciones parcial o totalmente, es potestad unilateral de EL RENIEC evaluar y decidir si continúa con la atención del servicio de certificación digital o si cancela el servicio.

CLÁUSULA SEXTA: RESPONSABILIDADES DE LA ENTIDAD

LA ENTIDAD se constituirá en el titular y suscriptor del certificado digital, siendo su representante legal o apoderado (persona natural) debidamente acreditado quien suscribirá la solicitud correspondiente. LA ENTIDAD asumirá las responsabilidades a que hubiere lugar por los daños y perjuicios que pudiese causarse por aportar datos falsos, incompletos o inexactos, así como es de su exclusiva responsabilidad el uso indebido, incorrecto o no acorde al fin para el que fue extendido el certificado.

De igual modo, la ENTIDAD es responsable de cualquier daño indirecto que pueda resultar o derivarse del incumplimiento de sus obligaciones o de la utilización incorrecta del servicio.

CLÁUSULA SÉPTIMA: LIMITACIÓN DE RESPONSABILIDADES DEL RENIEC

El RENIEC en su rol de ECERNEP, opera en concordancia con la Política General de Certificación y su Declaración de Prácticas de Certificación y todos los documentos normativos correspondientes, y asumirá responsabilidad por la emisión, cancelación y consulta del estado del certificado digital.

El RENIEC no será responsable por:

- Los daños derivados o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del titular y/o suscriptor.
-

- Cualquier violación a la confidencialidad en la que en uso de datos personales pudiera incurrir el propio titular y/o suscriptor.
- La utilización incorrecta del certificado digital y de las claves, así como de cualquier daño indirecto que pueda resultar de la utilización del certificado digital o de la información almacenada en el procesador del dispositivo criptográfico.
- Los daños que puedan derivarse de aquellas operaciones en que se hayan incumplido las limitaciones de uso del certificado digital.
- Del contenido de los certificados digitales emitidos por LA ENTIDAD.
- La falta de diligencia o cuidado del titular y/o suscriptor en la protección del dispositivo Hardware Security Module (HSM) y los datos de activación de la llave privada de la ECEP.
- De los errores en la verificación de la validez de los certificados digitales emitidos por las ECEP a sus usuarios o de las conclusiones erróneas condicionadas por omisiones o por las consecuencias de tales conclusiones erróneas.

LA ECERNEP, en ningún caso será responsable por daños o perjuicios causados por el incumplimiento de LA ENTIDAD de las obligaciones que le tocan conforme a la Política General de Certificación, o aquellos originados por catástrofes naturales, casos de guerra, actos de terrorismo y/o sabotaje u otros actos de fuerza mayor.

CLÁUSULA OCTAVA: DE LIBRE ADHESIÓN Y SEPARACIÓN

En cumplimiento de lo establecido por el numera del artículo 88.3 del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, EL RENIEC y LA ENTIDAD declaran expresamente que el presente convenio es de libre adhesión y separación para ambas partes.

CLÁUSULA NOVENA: DE LA VIGENCIA DEL CONVENIO

El presente Convenio tiene una vigencia de un año (01) año contado a partir de su suscripción. Durante esta vigencia, se podrá recibir la solicitud por parte de LA ENTIDAD para la emisión del correspondiente certificado digital, siempre y cuando se mantenga vigente los poderes del representante legal y/o máxima autoridad que suscribió el presente convenio así como la vigencia de los requisitos exigibles, siendo uno de ellos el mantenimiento de su acreditación correspondiente.

Asimismo, EL RENIEC, en cumplimiento de su rol como ECERNEP, continuará brindando de forma irrestricta el servicio de verificación del estado del certificado mediante la publicación de la Lista de Certificados Cancelados (CRL), en aplicación del numeral 4.10 de la Declaración de Prácticas de Certificación.

Sobre el particular, el RENIEC en su rol de ECERNEP establece que el servicio de certificación digital objeto del presente convenio, finaliza por lo siguiente:

- Al cancelarse el certificado digital emitido en el marco del presente convenio, antes de la fecha de expiración del certificado.
- Al expirar el certificado digital emitido en el marco del presente convenio.
- En caso se aplique la Cláusula Décimo Segunda "De la resolución" del presente convenio.

No operará renovación del presente convenio.

CLÁUSULA DÉCIMO: DE LAS COMUNICACIONES Y DOMICILIO DE LAS PARTES

Todas las comunicaciones que las partes se deban cursar en la ejecución de este Convenio se entenderán realizadas en los domicilios indicados en la parte introductoria del presente documento. Toda variación del domicilio sólo tendrá efecto después de ser comunicada por escrito a la otra parte.

CLÁUSULA DÉCIMO PRIMERA: DE LA COORDINACIÓN

Con la finalidad de mantener una adecuada coordinación, cada una de las instituciones acuerda designar a un coordinador con capacidad para tomar decisiones operativas que resulten necesarias a fin de asegurar la ejecución del presente Convenio. Los representantes designados pueden ser reemplazados, conforme lo señale la parte correspondiente para lo cual bastará la remisión de una comunicación por escrito a la otra parte. Asimismo, sin perjuicio de cumplir lo antes expuesto, se podrá cursar notificaciones y comunicaciones individuales entre los participantes conforme a lo descrito en el numeral 9.11 de la "Declaración de Prácticas de Certificación"

Para efectos de la coordinación del presente Convenio, las partes designan como coordinadores:

Por el RENIEC:

Cargo	:	Sub-Gerente de Regulación Digital
Teléfono	:	3152700 Anexo xxxx-... RPM: #xxxx
Correo	:	.....

Por la ENTIDAD:

Cargo	:
Teléfono	:
Correo	:

CLÁUSULA DÉCIMO SEGUNDA: DE LA RESOLUCIÓN

En caso LA ENTIDAD incumpla con las obligaciones citadas en la Cláusula Quinta del presente convenio de forma parcial o totalmente, es potestad unilateral de EL RENIEC evaluar y decidir si continúa con la atención del servicio de certificación digital de Nivel 2 o procede a la cancelación del certificado, lo cual será una causal de resolución del convenio.

Asimismo, el presente convenio podrá ser resuelto por cualquiera de las partes, bastando para ello una comunicación escrita con un plazo de anticipación de treinta (30) días calendario anterior a la fecha en que se desea dejar sin efecto el convenio. La solicitud de resolución del Convenio no liberará a las partes de las obligaciones previamente asumidas, ni impedirá la continuación de las actividades que se estuvieran desarrollando.

CLÁUSULA DÉCIMO TERCERA: DE LA SOLUCIÓN DE CONTROVERSIAS

El presente Convenio se suscribe sobre la base del principio de la buena fe, razón por la cual las partes convienen que, en caso de producirse alguna controversia, reclamo o disputa, previamente deberán proceder conforme a lo descrito en el "Procedimiento sobre resolución de disputas" de la Declaración de Prácticas de Certificación

En caso no se solucionen dichas controversias y/o discrepancias por el trato directo, se podrán resolver a través de un Arbitraje de Derecho. Para tales efectos las partes designarán un árbitro cada uno y ambos árbitros designarán al tercero quien presidirá el Tribunal Arbitral.

En señal de conformidad y aceptación, las partes suscriben el presente Convenio en dos (02) ejemplares, en la ciudad de Lima a los días del mes de del

Sr. Ricardo Javier Enrique Saavedra Mavila	**Sr. xxxxxxxxxxxxxxxxxxxx**
Registro Nacional de Identificación y Estado Civil	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx