

RESOLUCIÓN GERENCIAL GENERAL REGIONAL N° 556 -2017-GRL-GGR.

Belén, 7 de abril del 2017

Visto, el Oficio N° 168-2017-GRL-GGR-OEDII, fecha 13 de marzo 2017, mediante la cual el Jefe de la Oficina Ejecutiva de Desarrollo Institucional e Informática, remite Propuesta de Directiva **"Uso de Firmas y Certificados Digitales Generados en Documentos Electrónicos Oficiales, en el Sistema de Información de Tramite Documentario - SITD"**, y;

CONSIDERANDO:

Que, a fojas 001 a 014, obra el Informe N° 003-2017-GRL-GGR-OEDII/CZS, de fecha 01 de marzo 2017, mediante el cual el Ing. Carlos Zumaeta Sánchez, remite Propuesta de Directiva **"Uso de Firmas y Certificados Digitales Generados en Documentos Electrónicos Oficiales, en el Sistema de Información de Tramite Documentario - SITD"**.

A fojas 015 a 029, obra el Informe N° 006-2017-GRL-GGR-OEDII-JHQI, de fecha 02 de marzo 2017, mediante el cual el Sr. Jesús Hugo Quezada López – Técnico Administrativo II, remite revisión de proyecto de directiva.

A fojas 031, obra el Informe N° 004-2017-GRL-GGR-OEDII-CZS, de fecha 08 de marzo 2017, mediante el cual el Ing. Carlos Zumaeta Sánchez del área de Coordinación Interna de Informática - OEDII, remite correcciones de la Propuesta de Directiva **"Uso de Firmas y Certificados Digitales Generados en Documentos Electrónicos Oficiales, en el Sistema de Información de Tramite Documentario - SITD"**.

A fojas 033 a 034, obra el Informe N° 007-2017-GRL-GGR-OEDII-JHQL, de fecha 10 de marzo 2017, mediante el cual el Sr. Jesús Hugo Quezada López – Técnico Administrativo II, remite revisión de proyecto de directiva.

A fojas 035, obra el Oficio N° 168-2017-GRL-GGR-OEDII, fecha 13 de marzo 2017, mediante la cual el Jefe de la Oficina Ejecutiva de Desarrollo Institucional e Informática, remite a la Oficina Ejecutiva de Asesoría Jurídica de fecha 14 de marzo 2017, para Opinión legal a la Propuesta de Directiva **"Uso de Firmas y Certificados Digitales Generados en Documentos Electrónicos Oficiales, en el Sistema de Información de Tramite Documentario - SITD"**.

Que, el artículo 191° de la Constitución Política del Perú en concordancia con la Ley N° 27867, Ley Orgánica de Gobiernos Regionales, en sus artículos 2° y 4° respectivamente, establecen que, los Gobiernos Regionales son personas de derecho público, con autonomía política, económica y administrativa en asuntos de su competencia, constituyendo para su administración económica y financiera, un Pliego Presupuestal. Los Gobiernos Regionales, tienen por finalidad esencial fomentar el desarrollo regional integral sostenible, promoviendo la inversión pública y privada y el empleo y garantizar el ejercicio pleno de los derechos y la igualdad de oportunidades de sus habitantes, de acuerdo con los planes y programas nacionales, regionales y locales de desarrollo.

En ese mismo orden de ideas el numeral 2) del artículo 8° de la Ley N° 27867, Ley Orgánica de Gobiernos Regionales, que señala como uno de los Principios rectores de las políticas y la gestión regional **Transparencia**.- Los planes, presupuestos, objetivos, metas y resultados del Gobierno Regional serán difundidos a la población. La implementación de portales electrónicos en internet y cualquier otro medio de acceso a la información pública se rigen por la Ley de Transparencia y Acceso a la Información Pública N° 27806.

Que, mediante Resolución Ejecutiva Regional N° 475-2012-GRL-P, de fecha 11 de junio de 2012 se aprobó la Directiva General N° 004-2012-GRL-GGR/OEDII — Normas para la Formulación, Trámite, Aprobación y Actualización de Directivas, donde se establece en el artículo V, numeral V.7), punto V.7.1: Las Directivas Generales serán aprobadas por el Presidente Regional.

RESOLUCIÓN GERENCIAL GENERAL REGIONAL N° 556 -2017-GRL-GGR.

Belén, 7 de abril del 2017

Que, mediante la **Resolución Ejecutiva Regional N° 373-2016-GRL-P**, de fecha 11 de julio de 2016; se delega las facultades conferidas por el Reglamento de Organización y Funciones del Gobierno Regional de Loreto al Gerente General del Gobierno regional de Loreto, delegación que fue aprobada por la Ordenanza Regional N° 017-2016-GRL-CR, de fecha 25 de julio de 2016.

Con **Resolución Ejecutiva Regional N° 817-2012-GRL-P**, de fecha 23 de agosto de 2012, se aprobó el Modelo o Instructivo para la Elaboración de Reglamentos Generales y/o Internos que se emitan en el Gobierno Regional de Loreto., misma que mediante **Ordenanza Regional N° 017-2016-GRL-CR**, se aprueba el Reglamento de organización y funciones del Gobierno Regional de Loreto.

La Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, Texto Único Ordenado, aprobado por Decreto Supremo N° 043-2003-PCM, así mismo el Decreto Supremo N° 072-2003-PCM, que aprueba el Reglamento de la Ley de Transparencia y Acceso a la Información Pública, que fuese modificada por el Decreto Supremo N° 070-2013-PCM.

Resulta necesario mencionar que la propuesta de **Directiva "Uso de Firmas y Certificados Digitales Generados en Documentos Electrónicos Oficiales, en el Sistema de Información de Tramite Documentario - SITD"**; tiene como objetivo la de establecer las normas y procedimientos que permitan regular el tramite documentario en el Gobierno Regional de Loreto, que comprende la recepción, registro, foliación, derivación, atención, distribución, seguimiento y control de los documentos internos y externos que se tramiten Gobierno Regional de Loreto – GOREL, a través del adecuado uso del Sistema de Tramite Documentario –SITD y otras tecnologías de información y comunicación, para el uso de token, firmas, y certificados digitales, con la finalidad de impulsar el proceso de modernización de la gestión pública en la entidad.

Así mismo, es necesario mencionar la finalidad de la mencionada Directiva, la cual es la de, simplificar la Gestión Documentaria, a través de registros, que permitan realizar el seguimiento de los documentos, para brindar un servicio de calidad al ciudadano, contribuyendo al ahorro de insumos y la conservación del medio ambiente; así como agilizar la atención de los trámites empleando las firmas digitales en el documento electrónico, a través de Certificados Digitales, emitidos por el Registro de Identificación y Estado civil – RENIEC, gozando de las presunciones legales y efectos jurídicos.

Bajo este contexto y, siendo que la directiva en cuestión, se ha elaborado en el marco de las normas legales vigentes, y adecuada a los fines y funciones del Gobierno Regional de Loreto, logrando de esta manera armonizar y estandarizar criterios técnicos y legales para la formulación, tramite, aprobación, actualización y/o modificación de directivas que se elaboren dentro de los diferentes órganos o dependencias del Gobierno Regional de Loreto, para el ejercicio eficiente de la gestión, hacia la prestación de un servicio eficaz y de calidad en servicio del ciudadano y la población en su conjunto, en concordancia con los Principios de simplicidad, celeridad y eficacia de los mismos, que se encuentran establecidos en el TUO la Ley N° 27444 - Ley del Procedimiento Administrativo General y su modificatoria Decreto Legislativo N° 1272.

En tal sentido, la presente Directiva tiene como objetivo establecer las pautas y procedimientos para la formulación, tramite, aprobación, actualización y/o modificación de Directiva, que se elaboren dentro de los diferentes órganos o dependencia del Gobierno Regional de Loreto.

Estando al **Informe Legal N° 695- 2017-GRL-ORAJ**; con las visaciones de la Oficina Regional de Asesoría Jurídica, Oficina Regional de Administración y Gerencia Regional de Planeamiento Presupuesto y Acondicionamiento Territorial del Gobierno Regional de Loreto, y;

RESOLUCIÓN GERENCIAL GENERAL REGIONAL N° 556 -2017-GRL-GGR.

Belén, 7 de abril del 2017

En uso de las facultades conferidas por el Reglamento de Organización y Funciones del Gobierno Regional de Loreto aprobada por la Ordenanza Regional N° 017-2016-GRL-CR, de fecha 25 de julio de 2016 y la Resolución Ejecutiva Regional N° 373-2016-GRL-P, de fecha 11 de julio de 2016;

SE RESUELVE:

Artículo 1°.- DECLARAR PROCEDENTE QUE SE APRUEBE MEDIANTE RESOLUCION GERENCIAL REGIONAL LA PRESENTE DIRECTIVA GENERAL N° 005-2017-GRL-GGR/OEDII "USO DE FIRMAS Y CERTIFICADOS DIGITALES GENERADOS EN DOCUMENTOS ELECTRÓNICOS OFICIALES, EN EL SISTEMA DE INFORMACION DE TRAMITE DOCUMENTARIO - SITD", el mismo que tiene por objetivo la de establecer las normas y procedimientos que permitan regular el tramite documentario en el Gobierno Regional de Loreto, que comprende la recepción, registro, foliación, derivación, atención, distribución, seguimiento y control de los documentos internos y externos que se tramiten Gobierno Regional de Loreto – GOREL, a través del adecuado uso del Sistema de Tramite Documentario –SITD y otras tecnologías de información y comunicación, para el uso de token, firmas, y certificados digitales, con la finalidad de impulsar el proceso de modernización de la gestión pública en la entidad.

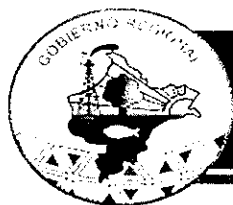
Artículo 2°.- Notifíquese la presente resolución a las instancias correspondientes del Gobierno Regional de Loreto y a los interesados conforme a Ley.

Regístrese, comuníquese y cúmplase.



GOBIERNO REGIONAL DE LORETO

Ing. Federico J. Sánchez
Gerente General Regional



**GORE
LORETO**

**GERENCIA
GENERAL
REGIONAL**

**OFICINA EJECUTIVA DE
DESARROLLO
INSTITUCIONAL E
INFORMATICA**

GERENCIA GENERAL REGIONAL

**OFICINA EJECUTIVA DE DESARROLLO INSTITUCIONAL E INFORMATICA
OEDII - GOREL**

DIRECTIVA GENERAL N° 005 - 2017-GRL-GGR-OEDII



**“USO DE FIRMAS Y CERTIFICADOS DIGITALES GENERADOS
EN DOCUMENTOS ELECTRONICOS OFICIALES, EN EL
SISTEMA DE INFORMACION DE TRAMITE DOCUMENTARIO –
SITD”**

BELEN, MARZO 2017

**DIRECTIVA USO DE FIRMAS Y CERTIFICADOS DIGITALES GENERADOS EN
DOCUMENTOS ELECTRONICOS OFICIALES, EN EL SISTEMA DE INFORMACION
DE TRÁMITE DOCUMENTARIO – SITD**

I. OBJETIVO

Establecer las normas y procedimientos que permitan regular el Trámite Documentario en el Gobierno Regional de Loreto, que comprende la recepción, registro, foliación, derivación, atención, distribución, seguimiento y control de los documentos internos y externos que se tramiten en el Gobierno Regional de Loreto – GOREL, a través del adecuado uso del Sistema de Trámite Documentario – SITD y otras tecnologías de información y comunicación, para el uso de token, firmas y certificados digitales; con la finalidad de impulsar el proceso de modernización de la gestión pública en la entidad.

II. FINALIDAD

Simplificar la Gestión Documentaria, a través de registros, que permita realizar el seguimiento de los documentos, para brindar un servicio de calidad al ciudadano, contribuyendo al ahorro de insumos y la conservación del medio ambiente.

Agilizar la atención de los trámites empleando las firmas digitales en el documento electrónico a través de Certificados Digitales emitidos por el Registro Nacional de Identificación y Estado Civil – RENIEC, gozando de las presunciones legales y efectos jurídicos.



III. BASE LEGAL

- Ley N° 27269, Ley de Firmas y Certificados Digitales
- Ley N° 27444, Ley del Procedimiento Administrativo General.
- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado
- Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de la Ley N° 27269 de Firmas y Certificados Digitales, y modificatoria/s
- Decreto Supremo N° 009-2009-MINAM, que aprueba Medidas de Ecoeficiencia para el Sector Público.
- Decreto Supremo N° 105-2012-PCM, establecen disposiciones para facilitar la puesta en marcha de la firma digital y modifican el Decreto Supremo No 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales.
- Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.
- Decreto Supremo N° 081- 2013-PCM, que aprueba la Política Nacional de Gobierno Electrónico 2013-2017.
- Decreto Supremo N° 026-2016-PCM, que aprueba medidas para el fortalecimiento de la infraestructura oficial de firma electrónica y la implementación progresiva de la firma digital en el Sector Público y Privado.
- Resolución Ministerial N° 179-2004-PCM, que aprueba uso obligatorio de la Norma Técnica Peruana " NTP- ISO/ IEC 12207:2004 Tecnología de la

Información. Procesos del Ciclo de Vida del Software, la Edición, en entidades del Sistema Nacional de Informática".

- Resolución Jefatural N° 368-2002-INEI, aprueba la Directiva, Normas Técnicas para el Almacenamiento y Respaldo de la Información procesada por las entidades de la Administración Pública.
- Resolución de Comisión de Reglamentos Técnicos y Comerciales N° 030-2008-CRT-INDECOPI, que aprueba las Guías de Acreditación de Entidades de Certificación Digital, Entidades de Registro o Verificación de Datos y Entidades de Prestación de Servicios de Valor Añadido; así como la Guía para la Acreditación del Software de Firmas Digitales.

IV. ALCANCE

Las disposiciones de la presente Directiva son de obligatorio cumplimiento de los órganos y unidades orgánicas del GOREL, en cuyos procesos se haya establecido el uso obligatorio de la firma digital, certificados digitales y token.

V. DEFINICIONES

5.1. Código Único de Trámite (CUT)

Es el código de identificación del trámite autogenerado por el SITD-GOREL, para identificar el documento y realizar el seguimiento al trámite.

5.2. Código Único de Digitalización (CUD)

Es el código de identificación que se expresa a través del código de barras, que se le da al documento digitalizado; esta codificación se genera al momento de registrar el documento en el SITD.

5.3. Digitalización de Documentos

Es la conversión de la información plasmada en papel a imágenes electrónicas o digitales sin alterar su originalidad, a través de un dispositivo de alta velocidad (scanner), generando un archivo digital o electrónico que permite almacenar, administrar y consultar documentos.

5.4. Documento Digitalizado

Es el documento físico que ha sido escaneado e indexado al SITD, que se identifica con el Código único de Digitalización (CUD) y está relacionado al Código Único de Trámite (CUT).

5.5. Autoridad Administrativa Competente

Es el organismo público responsable de acreditar a las Entidades de Certificación, a las Entidades de Registro o Verificación y a los Prestadores o de Servicios de Valor Añadido, públicos y privados, encargadas de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, y de cumplir las demás

funciones señaladas en el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales aprobado con Decreto Supremo N° 052- 2008-PCM, o aquellas que requiera en el transcurso de sus operaciones, conforme a la normativa que le resulte aplicable. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual— INDECOPI.

5.6. Entidad de Certificación

Es la persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación. Para el Estado Peruano es el Registro Nacional de Identificación Estado Civil- RENIEC.

5.7. Entidad de Registro o Verificación (EREP)

Es la persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así como de la Aje aceptación y autorización de las solicitudes de cancelación de certificados digitales. De acuerdo al Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales aprobado con Decreto Supremo N° 052-2008-PCM, el RENIEC es la única entidad de certificación, verificación y registro en nuestro país.



5.8. Certificado Digital

Es un documento electrónico usado como credencial, que ha sido generado y firmado digitalmente por una Entidad de Certificación y que permite identificar a la persona natural o jurídica que emitirá la firma digital.

5.9. Documento Electrónico

Es un documento contenido en un medio electrónico o magnético, cuya información se encuentra codificada.

5.10. Firma Electrónica

Es cualquier símbolo o proceso electrónico que permite al receptor de un documento electrónico identificar formalmente a su autor. También es conocida como firma electrónica básica.

5.11. Firma Digital

La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único, asociadas a una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no pueden derivar de ella la clave privada – PKI, de conformidad a las normas vigentes sobre firmas y certificados digitales.

5.12. Firma Principal

Es la firma digital del autor del documento o del funcionario que suscribe el documento electrónico.

5.13. Firma Visto Bueno

Es la firma Digital del asesor, especialista, asistente, o servidor o funcionario, quien elaboró el informe o reviso el documento, o el llamado por procedimiento a dar confianza administrativa a quien suscribe la firma principal del documento electrónico.

5.14. Infraestructura Oficial de Firma Electrónica

Es un sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de: 1) La integridad de los documentos electrónicos, y 2) La identidad de su autor, regulado conforme a Ley. El sistema incluye la generación de firmas digitales, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la Autoridad Administrativa Competente incluyendo a la Entidad de Certificación Nacional para el Estado Peruano, las Entidades de Registro o Verificación para el Estado Peruano y los Prestadores de Servicios de Valor Añadido para el Estado Peruano.

5.15. PDF/A

Es un formato de archivo para el guardado a largo plazo de documentos electrónicos. Está basado en la versión de Referencia 1. 4 de PDF de Adobe Systems Inc. (implementada en Adobe Acrobat 5 y versiones posteriores) y está definido por la SO 19005- 1: 2005.

5.16. PIN: (Personal Identification Number)

Es un número de identificación personal utilizado como contraseña para acceder de manera segura a ciertos sistemas informáticos.

5.17. PKI (Public Key Infrastructure)

Sistema criptográfico asimétrico en el que se basan los certificados digitales.

5.18. Representante del Titular

Persona natural que cuenta con facultades para representar a la persona jurídica en los trámites de certificado digital ante la EREP- RENIEC.

5.19. Sello de Tiempo (Time Stamping)

Es el valor de fecha y hora de firma digital de un documento, regulado de acuerdo al estándar RFC 3161 y las normas vigentes sobre firmas y certificados digitales.

5.20. Servicio de tercero neutral en intermediación electrónica

Es un servicio que proporciona el sello de tiempo externo tomado de una fuente confiable.

5.21. Suscriptor/a

Es el/ la servidor/a autorizado/a para firmar digitalmente.

5.22. Token Criptográfico

Es un dispositivo de almacenamiento criptográfico que contiene el Certificado Digital asignado al/ a la suscriptor/a que le permite firmar digitalmente. Se presenta como un dispositivo USB, que almacena de forma segura y confiable el certificado digital asignado a una persona titular que le permite firmar digitalmente, debiendo cumplir con el estándar FIPS 140.2, según Convenio suscrito con RENIEC.

5.23. SITD

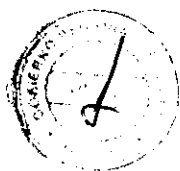
Sistema de Información de Tramite Documentario del GOREL. Es un software automatizado de gestión administrativa y de uso interno (dentro de la institución); a través de este sistema, se puede realizar un eficiente control del flujo de documentos y del envío de los mismos en formato electrónico (PDF) protegido con firma digital, lo que permite darle validez legal al documento, identificar al remitente y, gracias al proceso de almacenamiento de documentos digitales, garantizar la integridad de los mismos. El SITD será el medio electrónico que contenga los documentos digitalizados que ingresen externamente y de los documentos generados internamente que contengan el reconocimiento jurídico de los documentos emitidos, mediante la incorporación de la credencial digital (Certificado Digital) y el registro de la Firma Digital en los documentos digitales en formato PDF, emitidos por el personal de la institución a nivel de todas las dependencias funcionales. De esta manera, permite el acceso inmediato y concurrente a cualquier documento generado en el sistema, de cualquier persona involucrada en el trámite, sin importar el lugar en la que se encuentre; a la vez que contribuye a un factor importante en la preservación del medio ambiente, contribuyendo así con la ecoeficiencia.



VI. DISPOSICIONES GENERALES

- 6.1.** El uso efectivo de la firma digital en documentos electrónicos de la entidad se implementa de manera **PROGRESIVA**, siendo necesario que los órganos y las unidades orgánicas del GOREL identifiquen los procesos y actividad(es) / tarea(s) que generen documentos en los cuales resulte inexcusable y oportuna el uso de la firma digital, en concordancia con los lineamientos de simplificación administrativa que propone el Estado Peruano.

- 6.2. Los órganos que identifiquen determinados documentos que requieran el uso de la firma digital deben comunicar a la Oficina Ejecutiva de Desarrollo Institucional e Informática sobre los mismos mediante el formato: Formato A: Uso de la Firma Digital en el Gorel (DIRECTIVA GENERAL N° 002-2017-GRL-GGR-OEDII).
- 6.3. La documentación electrónica emitida bajo el alcance de la presente Directiva es aquella que cuenta con firma digital bajo la Infraestructura Oficial de Firma Electrónica – IOFE, por lo que es considerada con valor legal.
- 6.4. Los documentos electrónicos firmados digitalmente se almacenan en el repositorio de datos del Gorel, destinado además para el procesamiento, clasificación y consulta, con las medidas de seguridad correspondientes, garantizando el principio de equivalencia funcional y la integridad de su contenido.
- 6.5. El software de firma electrónica que utilice el GOREL para la emisión de documentos electrónicos seguros (garantizando la validación de su integridad y su no repudio) será el software REFIRMA de RENIEC, de acuerdo a la normativa vigente y al convenio interinstitucional entre Reniec y el Gobierno Regional de Loreto.
- 6.6. Los documentos electrónicos oficiales firmados digitalmente por los funcionarios y/o especialistas usarán el SITD del GOREL como medio de gestión y almacenamiento.
- 6.7. Los documentos firmados digitalmente deberán ser accesibles para su posterior consulta a través del SITD; ser conservados en su formato original de generación, envío, recepción u otro formato que reproduzca en forma demostrable la exactitud e integridad del contenido electrónico; y ser conservada toda la data que permita determinar el origen, destino, fecha y hora del envío y recepción.
- 6.8. Un documento electrónico podrá contar con una o varias firmas digitales de diferentes funcionarios y/o especialistas.
- 6.9. Para los efectos de la presente Directiva, las firmas digitales comprenderán tanto "firma" o "visto bueno" digitales en el documento electrónico emitido.
- 6.10. La firma digital, cuando sea el "autor del documento" o "por encargo" estará ubicada en la parte inferior derecha del documento. Para el caso de "visto bueno" (V°B°) o "en señal de conformidad" se ubicará en la franja izquierda o parte inferior de acuerdo a la naturaleza del documento a visar.
- 6.11. En caso de que un documento electrónico emitido, comprenda varias hojas, solo es necesario que contenga las firmas digitales en la 1ra. Hoja, no siendo necesario aplicarlo a las demás hojas.
- 6.12. Al personal que se le asignó tanto la firma como el certificado digital, hará uso de ellos, para todos los documentos que genere por su responsabilidad funcional.
- 6.13. En el caso que por la naturaleza del procedimiento se requiera un documento impreso en papel, generado con certificado y firma digital, tenga



validez legal, requiere ser suscrito físicamente por el autor o fedateado por fedatarios informáticos autorizados o fedatarios juramentados con especialización en informática, conforme a las normas del procedimiento administrativo general y a las especiales de la materia.

- 6.14. Los documentos generados bajo la IOFE, garantizan su disponibilidad y evitan adulteraciones, sin embargo con fines de conservación para posterior consulta serán almacenados en una base de datos en el servidor principal del GOREL y/o otros dispositivos de almacenamiento, de acuerdo a lo establecido por OEDII, garantizando cualidades de durabilidad, inalterabilidad y fijeza superiores o al menos similares a los que se emplean para los documentos impresos, los mismos que deberán estar debidamente custodiados.
- 6.15. El SITD brinda la posibilidad de que los usuarios externos puedan efectuar el seguimiento de sus trámites ante la institución a través de la página web institucional, lo cual está enmarcado en las políticas de mejora de la atención a la ciudadanía promovidas por el Estado. Esta acción será realizada por la OEDII.
- 6.16. La OEDII gestionará la generación de los certificados y firmas digitales para el personal del GOREL que esté autorizado a firmar digitalmente.



VII. MECANICA OPERATIVA

7.1. Presunciones Legales de la firma digital

Los/las suscriptores deben observar lo siguiente:

a) Principio de Autenticidad

Se presume que una firma electrónica ha sido “escrita” por la persona a quien le ha sido asignado el certificado digital emitido por la Entidad autorizada.

Esta firma electrónica, permite al tercero, presumir su certeza y a aprobación del contenido del documento sobre el cual está suscrita.

Para suscribir la firma electrónica, la persona vinculada a esta, ha hecho uso de un esquema de seguridad, bajo alguna de las modalidades “algo que yo sé”, “algo que yo tengo”, “algo que yo soy”.

b) Principio de Equivalencia Funcional

Los actos jurídicos realizados haciendo uso de medios electrónicos poseen la misma validez y eficacia jurídica que los actos jurídicos realizados por medios convencionales.

La condición es que en su realización se cumplan con las disposiciones legales vigentes.

El efecto es que los “actos jurídicos electrónicos” equivalen a los actos jurídicos materiales, para todo efecto legal.

En ese sentido, los documentos electrónicos que han sido firmados digitalmente constituyen prueba idónea en toda clase de procesos judiciales y procedimientos administrativos.

c) Principio de Inalterabilidad

Un documento electrónico firmado digitalmente, haciendo uso de un certificado digital, dentro de una infraestructura tecnológica de confianza, es posible demostrar la alteración o la no alteración de su contenido.

Si ha sido alterado, pierde valor legal. Pero si el documento permanece íntegro, su valor probatorio es pleno.

d) Principio de No Repudio

Cuando una persona firma digitalmente un documento electrónico (al igual que cuando se hace con una firma física), materializa en este acto la expresión de su voluntad, vinculando a la persona con el contenido del documento. De esta forma la persona no puede repudiar posteriormente la manifestación de su voluntad. El documento es veraz y sus efectos, plenos.



e) Presunción de veracidad

Todos los documentos generados en los sistemas con firma digital integrada en todas las formas y formalidades prescritas, responden a la verdad de los hechos que ellos firman.

7.2. Tokens

- 7.2.1. Los/las responsables de los órganos del GOREL, remiten al/la Administrador/a del Certificado Digital, la relación de servidores/as responsables de visar y/o firmar los documentos y que requieran tokens, debiendo llenar el: Formato B: Formato de Requerimiento de Dispositivo Criptográfico – Token.
- 7.2.2. La asignación del token se efectúa mediante el: Formato C: Formato de Asignación de Dispositivo Criptográfico y firma de/la suscriptor/a en señal de conformidad, previa aprobación de la relación de suscriptores.
- 7.2.3. En caso de bloqueo del password o PIN del token, el/la suscriptor/a esta en la obligación de comunicarlo al/la Administrador/a del Certificado Digital, quien verifica si se trata de un bloqueo momentáneo o permanente. Si fuera un bloqueo permanente, el/la Administrador/a del Certificado Digital se comunica con la EREP-RENIEC para la revocación del certificado digital y generación de un nuevo. En el supuesto que la revocación y generación de un nuevo certificado genere un costo, dicho costo será asumido por el GOREL.



7.3. Para la emisión del certificado digital

Una vez emitido el certificado digital a favor del GOREL, este puede iniciar el trámite para la emisión y gestión de certificados digitales para los/as suscriptores/as, a través de la administrador/a del Certificado Digital. Para dicho efecto, el/la Administrador/a del Certificado Digital debe:

- 7.3.1. Registrar los datos de los/as suscriptores/as en el formulario "Autorización de suscriptores/as" a través de su cuenta de usuario en el portal de la EREP-RENIEC.
- 7.3.2. Generar el reporte "listado de autorizaciones generadas". Este documento se firma en forma manuscrita y se envía en físico a la EREP-RENIEC.
- 7.3.3. Realizar la emisión de los certificados digitales para los/as suscriptores/as, luego de recibidas las autorizaciones de la EREP-RENIEC, bajo las siguientes dos modalidades:

7.3.3.1. No presencial, mediante la verificación con la base de datos:

- a). La EREP-RENIEC recibe la autorización y procesa los formatos respectivos que serán remitidos al correo electrónico del/la suscriptor/a o entregados al/la Administrador/a del Certificado Digital, mediante el envío a su correo electrónico o en USB a la persona que designe.
- b). Los formatos son impresos y firmados por cada suscriptor/a y son remitidos físicamente a la EREP-RENIEC.
- c). Una vez que se cuenta con esta documentación y se realice la verificación, automáticamente el sistema envía de ser procedente, un correo electrónico a la dirección electrónica registrada del/de la suscriptor/a que contiene un enlace web para realizar la descarga de su certificado digital.
- d). El/la suscriptora comunica a la OEDII, la recepción del correo para la descarga del certificado digital en el token, solicita que el/la suscriptor/a establezca el PIN o contraseña para la firma de documentos e instruye en el uso del token para firmar documentos.



7.3.3.2. Presencial.

- a). El/la suscriptor/a, previa coordinación con el/la Administrador/a del Certificado Digital, se apersona a la EREP-RENIEC portando su documentos de identidad vigente.
- b). En la EREP-RENIEC se procede a la autenticación y el registro de los formatos para su firma respectiva.
- c). Se realiza la entrega del certificado digital, instalándolo en su token.

7.3.4. Pérdida o robo de token criptográfico y certificado digital

Los funcionarios de las diferentes unidades orgánicas, están en la obligación de comunicar al titular de la Entidad, la cancelación y la emisión de un nuevo certificado digital de suscriptor a su cargo ante la Entidad de Registro o Verificación para el Estado Peruano del Registro Nacional de Identificación y Estado Civil (EREP-RENIEC), debiendo utilizar el: Formato D: "Formato de Solicitud de Emisión, autorización y cancelación de Certificado Digital para suscriptor". Para tal efecto, los Funcionarios y/o servidores de las Unidades Orgánicas del GOREL, gestionarán la adquisición del token

criptográfico para el suscriptor a su cargo y el adicional como respaldo. En caso de pérdida del Token Criptográfico, el suscriptor asumirá el costo del mismo.

7.3.5. Bloqueo del token criptográfico por superar el límite de intentos de acceso

El suscriptor del certificado digital que supere el límite de intentos de acceso al token criptográfico, generando su bloqueo, está en la obligación de comunicar el bloqueo del token criptográfico, a la OEDII o quien haga sus veces quien realizar su respectiva activación.

7.4. Procedimiento de Digitalización de documentos

7.4.1. Preparación del documento a digitalizar

El responsable de la digitalización verifica el estado físico y la cantidad de folios de los documentos o expedientes recibidos para proceder a retirar los elementos extraños (clips, grapas, residuos de goma u otros objetos).

7.4.2. Digitalización

a). Escaneo y captura del documento

- i. Los documentos se digitalizarán en formato PDF/A
- ii. Los documentos que contengan textos y/o imágenes simples, deben ser digitalizados a una resolución de 200 dpi en escala grises.
- iii. Los documentos con imágenes y/o fotos en el cual se requiera diferenciar los colores, excepcionalmente se podrán digitalizar a una resolución de 200 dpi a colores.
- iv. Las características de los documentos a escanear:
 - Textos
 - Papel de tamaño: A4, A3 y Oficio
 - Trama de papel: Bond
- v. Para la digitalización del documento se procederá a convertir el documento físico en imágenes, a través del escáner y software de captura.
- vi. Todos los documentos que ingresan por Mesa de Partes deben ser digitalizados, de acuerdo a lo establecido en los puntos i) y al v) del presente ítem a).



7.5. DE LA RECEPCIÓN EN MESA DE PARTES

- 7.5.1.** Los documentos que se ingresen o se generen en el GOREL son registrados en el SITD, según su asunto, conforme a la siguiente clasificación:
- a). Documento TUPA. Documento ingresado por la Mesa de Partes cuyo trámite se encuentra regulado en el Texto Único de Procedimientos Administrativos (TUPA) del GOREL. Forma parte de los expedientes en trámite.
 - b). Documento sin TUPA. Documento proveniente de personas naturales y jurídicas, públicas o privadas, organismos públicos y empresas del Estado, que han ingresado por la Mesa de Partes que no están relacionados con un procedimiento administrativo establecido en el TUPA del GOREL.
 - c). Documento Interno. Documento generado por un órgano del GOREL, para iniciar y/o continuar algún trámite (incluyendo los de tipo electrónico) y que pueden ser remitidos por plataformas digitales como el SITD o su equivalente.
- 7.5.2.** El SITD permite que el personal de Mesa de Partes verifique la presentación de los requisitos establecidos en el TUPA, mediante el marcado en una "lista de verificación" inserta en la Hoja de Ruta. Las listas de verificación serán actualizadas por la Oficina Ejecutiva de Desarrollo Institucional e Informática – OEDII a solicitud de los órganos del GOREL responsables de cada procedimiento administrativo.
- 7.5.3.** Al ser presentado en la Mesa de Partes un documento externo dirigido a la institución o a sus funcionarios, deberá procederse en primer lugar a verificar el destinatario y contenido, luego se registrará los datos generados de dicho documento en el SITD y el original como el cargo deben consignar datos tales como fecha, hora, folios y número de registro.
- 7.5.4.** Los documentos recibidos en la Mesa de Partes del GOREL, deberán ser escaneados, registrados y distribuidos utilizando el SITD.
- 7.5.5.** A cada documento se le asignará un número de registro que es proporcionado por el SITD, el mismo que será consignado en el documento de recepción para el seguimiento del usuario.
- 7.5.6.** Los sobres cerrados y/o correspondencia que sean de carácter personal, serán tramitados en las mismas condiciones que han sido recibidos e igualmente serán registrados en el SITD y remitidos físicamente al destinatario correspondiente.



- 7.5.7.** Los documentos originales escaneados quedarán en custodia del Archivo Central del GOREL, quien podrá proporcionar copias xerográficas (fotocopias) fedateadas de acuerdo a su procedimiento estipulado en el MAPRO. Esta acción estará supeditada a la capacidad de almacenamiento y custodia que tenga el Archivo Central, caso contrario el físico se remitirá a la Unidad Orgánica destinataria correspondiente.
- 7.5.8.** En caso de documentos originales que por su naturaleza deben formar parte de los procedimientos administrativos, como por ejemplo los recursos impugnatorios, facturas de proveedores, entre otros, serán remitidos directamente a la Unidad Orgánica correspondiente.
- 7.5.9.** El responsable de Mesa de Partes podrá realizar el seguimiento de los documentos que haya recibido, con fines de brindar información a los solicitantes, para cuyo efecto contará con el apoyo de la OEDII.

7.6. DE LA EMISIÓN DE DOCUMENTOS

7.6.1. Elaboración de documentos

El Funcionario y/o servidor público de los Órganos, Unidades Orgánicas, elaborarán el documento, debiendo convertirse en formato PDF/A.

En caso de contar con documentos adjuntos, ya sea en versión Word o Excel, deberán ser convertidos en formato PDF/A.

Los tipos de documentos que serán firmados digitalmente son:

- Oficio, Oficio Circular, Oficio Múltiple
- Memorando (M)
- Carta
- Informe
- Solicitud

7.6.2. La emisión de documentación interna en GOREL se efectuará de forma digital, empleando el certificado y firma digital, que circulará utilizando el SITD. Cuando sea necesario, será impreso en papel y seguirá el trámite convencional.

7.6.3. Un documento que, de ser conforme, se guardará en formato PDF/A, para luego ser firmado digitalmente por los funcionarios o especialistas de las diferentes Unidades Orgánicas del GOREL que tengan la firma y el certificado digital, cumpliendo con los siguientes criterios:



a). Registro de documentos y adjuntos en el SITD

El registro de documentos del GOREL debe ser mediante el uso de SITD, ingresarán al SITD para registrar el documento y cargar su respectivo archivo PDF/A, así como los documentos adjuntos, en caso de ser necesario.

Una vez registrado el documento y el adjunto en el SITD, automáticamente se enviará el archivo PDF/A, a la bandeja del Funcionario y/o servidor público de las Unidades Orgánicas, para su respectiva firma digital.

b). Firma Digital del documento y adjunto en el SITD

El funcionario y/o servidor público de la Unidad Orgánica, ingresará al SITD, donde podrá visualizar los documento en formato PDF/A.

Asimismo, seleccionará el documento para su revisión; de estar conforme, se procederá a la firma digital ingresando la contraseña o PIN de seguridad, en caso que el documento tenga adjunto, se insertará automáticamente el visto bueno digital.

Una vez firmado el documento, seleccionar la opción "Terminar" luego de lo cual concluirá el proceso de la firma.

c). Derivación del documento firmado digitalmente

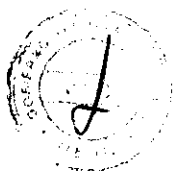
El Funcionario y/o servidor público de la Unidad Orgánica del GOREL, podrá derivar el documentos firmado directamente al destinatario a través del SITD.

d). La numeración correlativa de los documentos debe generarse haciendo uso del SITD, que será usado para los documentos con firma y certificado digital.

7.6.4. Una vez que el documento es firmado digitalmente, el especialista, personal administrativo y/o secretaria correspondiente, deberá adjuntarlo en el SITD para que prosiga con el flujo que amerite dicho trámite. Los anexos que forman parte del documento, igualmente serán almacenados en el SITD junto con el documento principal.

7.6.5. El documento electrónico con firma digital se conservará en el servidor del GOREL, bajo las normas y dispositivos vigentes de seguridad de la información y a lo señalado en las Disposiciones Generales de la presente Directiva.

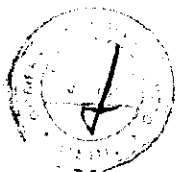
7.6.6. Cuando se trate de documentos destinados a usuarios externos, se mantendrá con la firma y certificado digital, para luego ser registrados en el SITD y remitidos en formato físico, debiendo conservarse los cargos de entrega correspondiente para su respectivo archivo.



- 7.6.7. En lo posible, se deberá evitar imprimir los documentos generados a través del SITD, como medida de ecoeficiencia y preservación de recursos naturales.

7.7. DE LA RECEPCION DE LOS DOCUMENTOS INTERNOS

- 7.7.1. Permanentemente, los gerentes, sub gerentes, jefes de oficina del GOREL, con el apoyo del personal administrativo y/o secretarias o quien haga dichas funciones, deberán ingresar al SITD del GOREL para que efectúen la recepción de los documentos derivados por las diferentes áreas, y disponer su atención.
- 7.7.2. A través del SITD se podrán enviar o recibir documentos. El régimen de horas hábiles en el horario de atención del GOREL, se rige por lo dispuesto en la legislación vigente sobre el procedimiento administrativo general. El horario de atención estará publicado en la intranet y en la página web del GOREL (www.regionloreto.gob.pe).
- 7.7.3. La validez del documento electrónico con firma digital puede verificarse haciendo uso del software autorizado por la RENIEC.



VIII. DISPOSICIONES COMPLEMENTARIAS

- 8.1. En el caso de la documentación que emita el Órgano de Control Institucional, tales como requerimiento de información, informes y otros documentos de control, estos podrán ser exonerados de los establecido en el SITD, lo cual se tramitará en forma física debiendo ser atendidas por las áreas usuarias, concordante con el inciso n) del artículo 9° de la Ley del Sistema Nacional de Control y de la Contraloría General de la Republica.
- 8.2. Los Órganos, Unidades Orgánicas del Gorel deberán gestionar la adquisición de dispositivos criptográficos – Token para el almacenamiento del certificado digital, para cumplir con el proceso de firma digital de documentos, conforme a los establecido en la presente Directiva.
- 8.3. Lo dispuesto en la presente directiva, será ejecutado progresivamente, de acuerdo a los procedimientos de cada Unidad Orgánica, con la finalidad de que no dificulten su labor administrativa o procedimental en un inicio.

IX. RESPONSABILIDADES

Los responsables del cumplimiento son:

- 9.1. Los órganos y unidades orgánicas del GOREL son responsables de velar por el cumplimiento de las disposiciones para el uso de la firma digital en documentos electrónicos de la entidad.
- 9.2. La Oficina Ejecutiva de Recursos Humanos, es responsable de informar ante la OEDII, el ingreso, rotación o cese de personal, que este autorizado a firmar digitalmente, para los respectivas eliminaciones y/o configuraciones de sus certificados digitales.
- 9.3. La Oficina Ejecutiva de Desarrollo Institucional e Informática es responsable de asegurar la disponibilidad y operatividad del Sistema de Información de Tramite Documentario, en adelante SITD, así como de brindar soporte y capacitación periódica a los usuarios de este sistema, para asegurar su adecuado uso y aplicación.
- 9.4. Es responsabilidad del personal de Mesa de Partes de la Oficina de Administración Documentaria, efectuar la recepción de los documentos externos que ingresan al GOREL, así como realizar la entrega de documentos internos generados en las Unidades orgánicas del GOREL, dirigidos a instituciones públicas o privadas y/o personas naturales, relacionadas con la gestión institucional; así mismo, orientar a los ciudadanos en la presentación de sus documentos y brindar información a los mismos respecto al estado del trámite de los documentos presentados.
- 9.5. Los usuarios del SITD, son responsables del cumplimiento de las disposiciones establecidas en la presente Directiva, así como de la tramitación oportuna de los documentos que le hayan sido derivados para su atención.



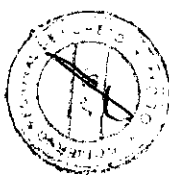
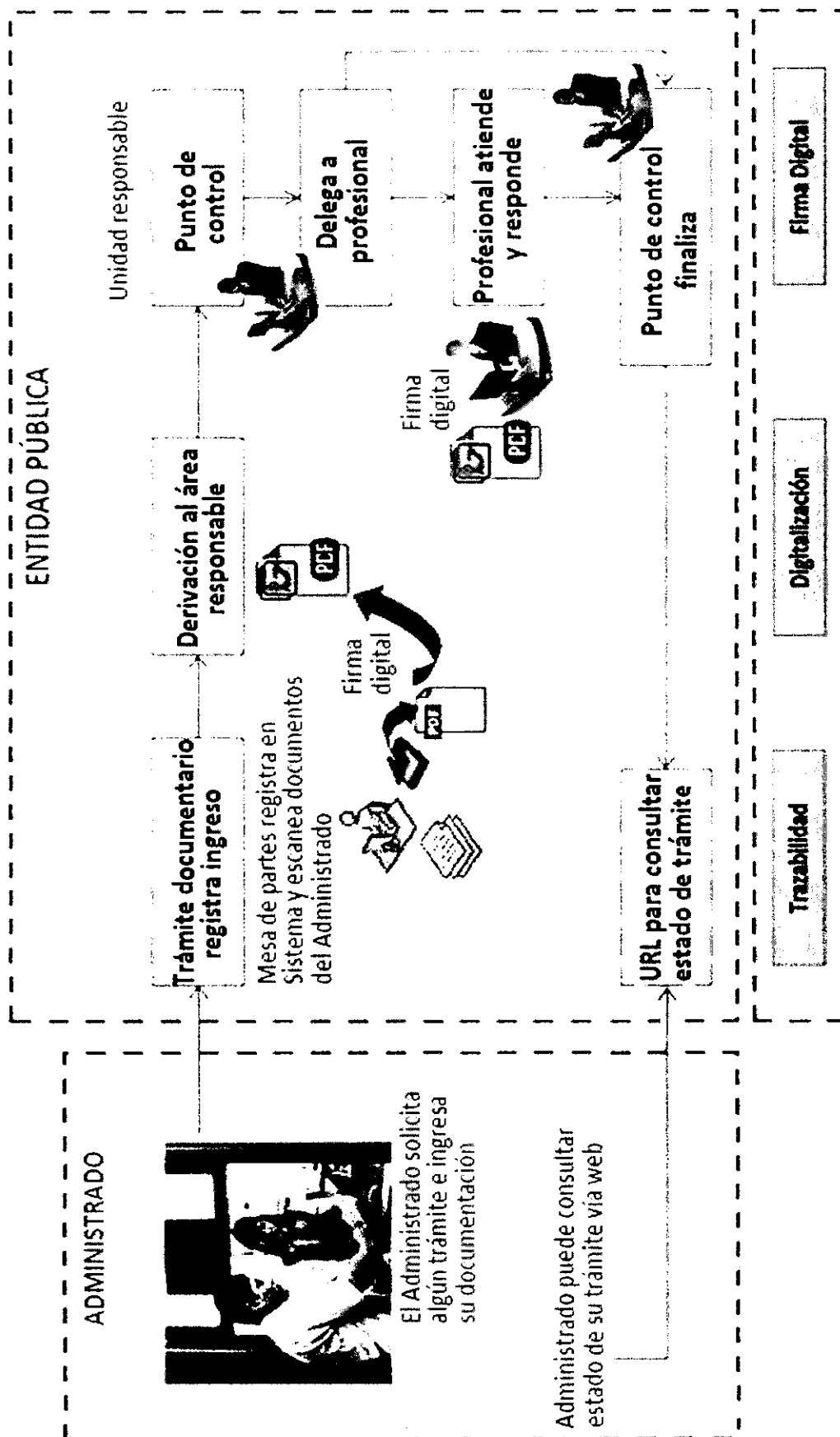
- 9.6. El funcionario encargado de cada unidad orgánica del GOREL, es responsable del trámite de los documentos registrados en el SITD, en el ámbito que le corresponda, así como de su atención oportuna.
- 9.7. La OEDII efectuará las configuraciones necesarias en los equipos de cómputo y/o en los token USB de los usuarios correspondientes, con fines de almacenar e iniciar su uso.
- 9.8. Asimismo, la OEDII instalará en los equipos de cómputo, y capacitará al personal asignado en el uso del SITD y del software de firma digital acreditado por el INDECOPI; este último sistema, se utilizará para firmar digitalmente y con valor legal los documentos en el GOREL. Se entregará el Manual de Usuario respectivo.
- 9.9. Los funcionarios y especialistas a quienes se les asigne firma y certificado digital (token USB) tienen la obligación de mantener la confidencialidad de sus claves de acceso PIN, debiendo hacer uso personalísimo de estas, al momento de generarlas en los documentos electrónicos oficiales.
- 9.10. En caso que el trabajador deje de laborar en la entidad, el Token USB, deberá formar parte de los bienes a ser devueltos al GOREL.

X. ANEXOS: FLUJOGRAMA Y FORMATOS

- **FORMATO A:** Uso de la Firma Digital en el Gorel.
- **FORMATO B:** Formato de Requerimiento de Dispositivo Criptográfico – Token
- **FORMATO C:** Formato de Asignación de Dispositivo Criptográfico y firma de/la suscriptor/a
- **FORMATO D:** Formato de Solicitud de Emisión, autorización y cancelación de Certificado Digital para suscriptor.



**FLUJO GRAMA DE PROCEDIMIENTOS DE FIRMA DIGITAL DE DOCUMENTOS EXTERNOS E INTERNOS
EN EL GOBIERNO REGIONAL DE LORETO**



 GORE LORETO GERENCIA GENERAL REGIONAL OFICINA EJECUTIVA DE DESARROLLO INSTITUCIONAL E INFORMATICA	USO DE LA FIRMA DIGITAL EN EL GOREL	FORMATO A
Nombres:	Apellidos:	Cargo:
Organo / Unidad Organica:	Correo Electronico:	Posibles documentos firmados digitalmente:
Nombre del Proceso:	Actividades o tareas <u>Orientacion:</u> Orientacion al Ciudadano ☐ ☐ Mejora de la gestion interna	



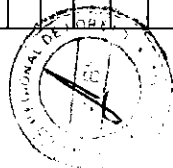
FORMATO B

[illegible]

La entrega Presencial, consiste en que el/la servidor/a se apersona físicamente al EREP-RENEC para que se le entregue el certificado digital en el dispositivo de almacenamiento (token)

La Entrega No Presencial, consiste en enviar información al EREP-RENEC, relativa a la autorización que debe tener el/la servidor/a para la habilitación de sus correspondiente certificado digital.

Luego de la validación por parte de EREP-RENEC, se recibe un enlace vía web para descargar el certificado digital e instalarlo (que lo hace la OEDII) en el token asignado al servidor.



FORMATO C: FORMATO DE ASIGNACION DE DISPOSITIVO DE ALMACENAMIENTO DE CERTIFICADO DIGITAL

 CORE LORETO GERENCIA GENERAL REGIONAL DEPARTAMENTO DE DESARROLLO INSTITUCIONAL INFORMATICA	ASIGNACION DE DISPOSITIVO DE ALMACENAMIENTO DE CERTIFICADO DIGITAL	FORMATO C
---	--	-------------------------

SUSCRIPTOR/A			
ORGANO			
UNIDAD ORGANICA			
CARGO			
SUSCRIPTOR/A			
DNI		CORREO ELECTRONICO	
TELEFONO CONTACTO		CELULAR CONTACTO	
DISPOSITIVO DE ALMACENAMIENTO DE CERTIFICADO DIGITAL			
MARCA	MODELO	N° DE SERIE	

Belen, ____ de ____ del ____



Entrega
Administrador/a del Certificado Digital

Recibi conforme
Suscriptor/a



**GORE
LORETO**

**GERENCIA
GENERAL
REGIONAL**

**OFICINA EJECUTIVA DE
DESARROLLO
INSTITUCIONAL E
INFORMÁTICA**

FORMULARIO DE SOLICITUD DE EMISIÓN, ACTUALIZACIÓN Y CANCELACIÓN DE CERTIFICADOS DIGITALES PARA SUScriptor

Ley N° 27269 - Ley de Firmas y Certificados Digitales y su Reglamento, aprobado mediante D.S N° 052-2008-PCM

N° SOLICITUD:

Oficio / Memorandum de la referencia:
(Opcional)

Fecha:

I. DATOS DEL SUScriptor:

Apellido Paterno:		Apellido Materno:	
Nombres:		N° DNI/ Carné de Extranjería N°:	
Dirección:			
Distrito:		Provincia:	
		Departamento:	
Teléfono / Celular:		Correo Electrónico:	

II. DATOS LABORAL DEL SUScriptor:

Dependencia, Org. Públicos, Prog. y Proyección (Siglas):		Dirección/Unidad Área:	
Cargo:		Código de Personal N°:	
Dirección Laboral:			
Distrito:		Provincia:	
		Departamento:	
Teléfono / Anexo:		Correo Electrónico Laboral:	

III. CERTIFICADO DIGITAL:

Requerimiento de: EMISIÓN ☐ ACTUALIZACIÓN ☐ CANCELACIÓN ☐

Importante:

Para el emisión (creación) del Certificado Digital se requerirá el documento de designación de cargo del Suscriptor.

IV. OBLIGACIONES:

Las obligaciones del Suscriptor del Certificado Digital son:

1. Entregar información veraz, bajo su responsabilidad.
2. Actualizar la información proporcionada al TITULAR de Certificado Digital del GOREL cuando estos ya no resulten exactos e son incorrectos.
3. Mantener el control y la reserva de la clave privada bajo su responsabilidad.
4. Realizar un uso debido y correcto del certificado digital.
5. Notificar de inmediato al TITULAR de Certificado Digital del GOREL en caso de que detecte que se ha incluido información incorrecta e inexacta en el certificado digital.
6. Solicitar inmediatamente al TITULAR de Certificado Digital del GOREL la cancelación de su certificado digital en caso de tener conocimiento o sospecha de la ocurrencia de alguna de las siguientes circunstancias:
 - a. Exposición, puesta en peligro o uso indebido de la clave privada o de la contraseña o PIN de acceso a su clave privada.
 - b. Deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada o la contraseña o PIN de acceso a su clave privada.

V. DECLARACIONES:

1. El Suscriptor manifiesta que previamente a la firma del presente documento no cuenta con inhabilitación declarada administrativamente, o incapacidad declarada judicialmente.
2. El Suscriptor declara que todos los datos proporcionados son verdaderos.
3. El Suscriptor declara haber leído, comprendido y aceptado el contenido del presente documento.

Firmas para autorización

V° B° Funcionario y/o Director

V° B° Suscriptor