GOBIERNO REGIONAL DE ANCASH

"Año de la Recuperación y Consolidación de la Economía Peruana"

RESOLUCION GERENCIAL GENERAL REGIONAL N° 399-2025-GRA/GGR

Huaraz, 02 de julio de 2025

VISTO:

La Resolución Gerencial General Regional N° 411-2021-GRA/GGR que aprueba la Directiva N° 010-2021-GRA-GRPPAT/SGDITI-UTI denominada: "Directiva para el uso de Firma y Certificado Digital en el Gobierno Regional de Ancash", el Informe N° 201-2025-GRA/GRAD/SGTII de fecha 25 de junio de 2025, el Informe N° 039-2025-GRA/GRPPAT/SGMDI-09 de fecha 26 de junio de 2025, el Informe Legal N° 595-2025-GRA/GRAJ de fecha 01 de julio de 2025, y;

CONSIDERANDO:

Que, el artículo 191° de la Constitución Política del Perú, modificada por Ley N° 30305, concordante con el artículo 2° de la Ley N° 27867, Ley Orgánica de Gobiernos Regionales, establece que los Gobiernos Regionales son personas jurídicas de derecho público, con autonomía política, económica y administrativa en los asuntos de su competencia;

Que, la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, tiene por finalidad la mejora de la gestión pública, de manera que se logre mayores niveles de eficiencia y una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos del Estado;

Que, el numeral 1.2) del artículo 1º del Texto Único Ordenado de la Ley Nº 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 004-2019-JUS, señala que no son actos administrativos los actos de administración interna de las entidades destinadas a organizar o hacer funcionar sus propias actividades o servicios. Estos actos son regulados por cada entidad, con sujeción a las disposiciones del Título Preliminar de ésta Ley y de aquellas normas que expresamente así lo establezcan;

Que, mediante Resolución Gerencial General Regional N° 411-2021-GRA/GGR se aprueba la Directiva N° 010-2021-GRA-GRPPAT/SGDITI-UTI denominada: "Directiva para el uso de Firma y Certificado Digital en el Gobierno Regional de Ancash" con el fin de que las diferentes unidades de organización puedan hacer uso de la herramienta tecnológica aplicada a las comunicaciones escritas;

Que, mediante Informe N° 201-2025-GRA/GRAD/SGTII de fecha 25 de junio de 2025, la Sub Gerencia de Tecnología de la Información e Innovación remite el Informe Técnico sobre el Proyecto de Directiva Regional que regula el uso de la Firma Digital en el Gobierno Regional de Ancash, Versión 02 que amplía y actualiza las definiciones, procedimientos y responsabilidades para la emisión de certificados digitales, el uso de la firma digital y la validación de documentos electrónicos, asegurando su congruencia con los estándares nacionales y la plataforma nacional

de firma digital, cuyos beneficios son la simplificación administrativa, reducción del uso de papel, fortalecimiento de la seguridad jurídica y garantía del principio de no repudio;

Que, la Sub Gerencia de Modernización y Desarrollo Institucional de la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial, luego de la revisión sustentatoria de la propuesta de Directiva Regional que regula el uso de la Firma Digital en el Gobierno Regional de Ancash, Versión 02, emite el Informe N° 039-2025-GRA/GRPPAT/SGMDI-09 de fecha 26 de junio de 2025 concluyendo que el procedimiento descrito en Directiva, garantiza el principio de seguridad jurídica, al establecer procedimientos y responsabilidades claramente definidos desde la emisión del Certificado Digital, Uso de la firma y Certificado Digital de los suscriptores, procedimiento de cancelación y anulación de la solicitud de los certificados digitales, administración del token criptográfico y la operación de validación de la firma digital, así como establece mecanismos de responsabilidad respecto al Administrador del Certificado Digital, Sub Gerencia de Tecnologías de la Información e Innovación y al Suscriptor, resultando viable, necesaria y pertinente para garantizar la validez jurídica, trazabilidad y autenticidad de los actos administrativos y documentos digitales emitidos en la Entidad

Que, la Gerencia Regional de Asesoría Jurídica, en razón de la información recopilada y del análisis de la propuesta de Directiva Regional que regula el uso de la Firma Digital en el Gobierno Regional de Ancash, Versión 02, determina que es una propuesta positiva y necesaria para modernizar la administración pública, dependiendo su éxito en gran medida, de su adecuada implementación, la capacitación del personal y la voluntad de adaptarse a los cambios y mejoras continuas, emitiendo así el Informe Legal N° 595-2025-GRA/GRAJ de fecha 01 de julio de 2025 concluyendo que la citada Directiva Regional se encuentra elaborada de una manera sólida y necesaria para la gestión administrativa de la Entidad, encuadrando dentro de las facultades de auto organización de un Gobierno Regional y busca asegurar la legalidad, eficiencia y transparencia en sus comunicaciones, resultando viable su aprobación mediante el acto resolutivo correspondiente;

Que, en consecuencia, resulta necesaria la aprobación de la Directiva Regional que regula el uso de la Firma Digital en el Gobierno Regional de Ancash, Versión 02 a fin de uniformizar criterios y estableciendo disposiciones para su formulación, actualización, revisión y aprobación, así como las responsabilidades de aquellos que intervienen en el proceso, correspondiendo su aprobación conforme a lo precisado en el Informe N° 039-2025-GRA/GRPPAT/SGMDI-09 de fecha 26 de junio de 2025 y en el Informe Legal N° 595-2025-GRA/GRAJ de fecha 01 de julio de 2025;

Que, finalmente, en el ejercicio de la función pública, debe procurarse la implementación de buenas prácticas de gestión que permitan asegurar la calidad y eficiencia en el cumplimiento de las funciones asignadas, así como la adecuada y oportuna toma de decisiones, por lo que, resulta conveniente establecer la Norma que regula el uso de la Firma Digital en el Gobierno Regional de Ancash, Versión 02;

Que, estando a las consideraciones expuestas y a las facultades conferidas mediante Resolución Ejecutiva Regional Nº 080 - 2024-GRA/GR de fecha 31 de diciembre de 2024, en uso de las atribuciones establecidas en la Ley N°27867 - Ley Orgánica de Gobiernos Regionales y sus modificatorias; y demás antecedentes;

SE RESUELVE:

ARTÍCULO PRIMERO. – DEJAR SIN EFECTO la Directiva N° 010-2021-GRA-GRPPAT/SGDITI-UTI denominada: "Directiva para el uso de Firma y Certificado Digital en el Gobierno Regional de Ancash"" Versión 01 aprobada mediante Resolución Gerencial General Regional N° 411-2021-GRA/GGR, por las consideraciones expuestas en la presente Resolución.

ARTÍCULO SEGUNDO. - APROBAR la Directiva Regional N° 04-2025-GRA/GRAD/SGTII que regula el uso de la Firma Digital en el Gobierno Regional de Ancash, Versión 02, la misma que como anexo forma parte integrante de la presente Resolución, por los argumentos expuestos en la misma.

ARTÍCULO TERCERO. - ENCARGAR a los Órganos y Unidades Orgánicas del Gobiernos Regional de Ancash, el cumplimiento de lo dispuesto en la presente Resolución.

ARTICULO CUARTO. - ENCARGAR a la Secretaria General del Gobierno Regional de Ancash la publicación de la presente Resolución Gerencial General con la Directiva que forma parte de la presente Resolución en el Portal Web Institucional, la misma que entra en vigencia a partir del día siguiente de su publicación.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE

GOBIERNO REGIONAL DE ANCASH

ABG. MARCO ANTONIO LA ROSA SÁNCHEZ PAREDES
GERENTE GENERAL REGIONAL

DIRECTIVA REGIONAL QUE REGULA EL USO DE FIRMA DIGITAL EN EL GOBIERNO REGIONAL DE ANCASH

CUADRO DE INFORMACIÓN DE APROBACIÓN			
RESOLUCIÓN DE APROBACIÓN:			
CÓDIGO:	**VERSIÓN:**	**PÁGINAS:**	**FECHA DE APROBACIÓN:**
DIRECTIVA REGIONAL N° 4 -2025-GRA/GRAD/SGTII	02	24	02 JUL. 2025

CUADRO DE VALIDACIONES				
ELABORADO POR:	REVISADO POR:			APROBADO POR:
ING. JOSEPH DARWIN ALVARADO TOLENTINO Subgerente de Tecnologías de la Información e Innovación	**CPC. RUDI ANTONIO ABANTO GIL** Gerente Regional de Administración	**ING. GILMER ROLIN MENDOZA CAUSHI** Subgerente de Modernización y Desarrollo Institucional	**ABOG. DANIEL ÁLVARO DIESTRA VIVAR** Gerente Regional de Asesoría Jurídica	**ABOG. MARCO ANTONIO LA ROSA SÁNCHEZ PAREDES** Gerente General Regional
FECHA: 02 JUL 2025	FECHA: 02 JUL 2025	FECHA: 02 JUL 2025	FECHA: 02 JUL 2025	FECHA: 02 JUL 2025

CUADRO DE CONTROL DE CAMBIOS		
VERSIÓN:	**FECHA:**	**MODIFICACIÓN:**
02	19/06/2025	Se actualizo la directiva en base a la actualización de la Directiva Nº 001-2025-GRA/GRPPAT/SGMDI "Directiva Regional que regula las Normas y Procedimientos para la Formulación, Actualización, Revisión y Aprobación de Documentos Técnico Normativos y Orientadores en el Gobierno Regional de Ancash". Se actualizo la directiva por la implementación del Sistema de Trámite Documental (STD). Se incorporó los flujogramas de los procesos y procedimientos relacionados a la directiva. Se incorporó consideraciones relacionados a la emisión del certificado digital.

Tabla de Contenido

DIRECTIVA REGIONAL QUE REGULA EL USO DE FIRMA DIGITAL EN EL GOBIERNO REGIONAL DE ANCASH

DIRECTIVA REGIONAL N° 4 -2025-GRA/GRAD/SGTII

1. FINALIDAD:

Contribuir en la prestación de servicios digitales de manera segura e interoperable, mediante la implementación de la firma digital en los documentos producidos por los servidores civiles del GRA, y que en el ejercicio de sus funciones deban firmar digitalmente documentos electrónicos en el marco de los procesos de las unidades de organización a las que pertenecen.

2. OBJETIVO:

Establecer procedimientos y responsabilidades para la implementación y uso adecuado de firmas digitales en el Gobierno Regional de Ancash.

3. ALCANCE:

Son de aplicación y cumplimiento obligatorio por todos los servidores civiles que pertenecen a las unidades de organización que conforman el Pliego 441 del Gobierno Regional de Ancash, para hacer uso de la firma digital en el marco de sus funciones y procesos de sus respectivas dependencias.

4. BASE LEGAL:

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley Nº 27269, Ley de Firmas y Certificados Digitales y modificatorias.
- Ley N° 31965, Ley que autoriza a la SUNAT facilitar la obtención del Certificado Digital Tributario (CDT) para la emisión de comprobantes electrónicos.
- Decreto Legislativo N° 1246, Decreto Legislativo que aprueba diversas medidas de simplificación administrativa.
- Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Legislativo N° 1310 – Decreto Legislativo que aprueba medidas adicionales de simplificación administrativa.
- Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Decreto Supremo Nº 052-2008-PCM y modificatorias, Decreto Supremo que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales.

- Decreto Supremo Nº 026-2016-PCM, Decreto Supremo que aprueba las medidas para el fortalecimiento de la infraestructura oficial de firma electrónica y la implementación de la firma digital en el Sector Público y Privado.
- Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- Ordenanza Regional Nº 003-2023-GRA/CR que aprueba el Reglamento de Organización y Funciones del Gobierno Regional de Ancash.
- Resolución de Secretaría de Gobierno Digital N° 001-2017-PCM/SEGDI, que aprueba el Modelo de Gestión Documental en el marco del Decreto Legislativo N° 1310.
- Resolución N°002-2022- PCM/SGTD, que aprueba la Guía para el uso e integración de la Plataforma Nacional de Firma Digital en las entidades de la Administración Pública.
- Resolución de Secretaría de Gobierno y Transformación Digital N.° 007-2024-PCM/SGTD, que aprueba la Directiva N° 002-2024-PCM/SGTD que regula el uso de la firma digital en las entidades públicas.
- Resolución Ejecutiva Regional Nº 212-2020-GRA/GR, que designa al Jefe de la Unidad de Tecnología de la Información, la representación ante el Registro Nacional de Identificación y Estado Civil (RENIEC) Entidad de registro o verificación para el Estado Peruano (EREP) para la gestión de emisión y cancelación de los Certificados Digitales de suscriptores a nombre del Gobierno Regional de Ancash.
- Resolución Gerencial General Regional Nº 380-2025-GRA/GGR, que aprueba la Directiva Regional Nº 001-2025-GRA/GRPPAT/SGMDI "Directiva Regional que regula las Normas y Procedimientos para la Formulación, Actualización, Revisión y Aprobación de Documentos Técnico Normativos y Orientadores en el Gobierno Regional de Ancash".
- Contrato de Prestación de Servicios de Certificación Digital Certificado Clase III – Persona jurídica en el marco del Decreto Supremo Nº 070-2011-PCM y Decreto Supremo Nº 105-2012-PCM, suscrito entre el RENIEC y el Gobierno Regional de Ancash.

5. DEFINICIONES

5.1. Siglas o acrónimos

En la presente Directiva se utilizan los siguientes acrónimos:

- GRA : Gobierno Regional de Ancash.
- SGTII : Sub Gerencia de Tecnologías de la Información e Innovación
- SGMDI : Subgerencia de Modernización y Desarrollo Institucional
- ACD : Administrador del Certificado Digital
- RENIEC : Registro Nacional de Identificación y Estado Civil
- EREP : Entidad de Registro o Verificación
- PIER : Plataforma Integrada de la Entidad de Registro

- DNIe : Documento Nacional de Identidad electrónico
- PDF : Portable Document Format (ISO 32000)
- IOFE : Infraestructura Oficial de la Firma Electrónica.
- AAC : Autoridad Administrativa Competente.

5.2. Glosario de términos

Para efectos de la presente Directiva se entiende como:

- **Administrador del Certificado Digital:** Es el servidor designado por el Gobierno Regional de Ancash, responsable en coordinar las gestiones de Certificados Digitales ante RENIEC.
- **Área usuaria:** Es la unidad de organización del Gobierno Regional de Ancash.
- **Autoría:** Proceso que permite determinar la identidad del firmante, en función del documento electrónico firmado digitalmente por éste, garantizando su vinculación e integridad.
- **Autoridad Administrativa Competente:** Es el organismo público responsable de acreditar las Entidades de Certificación, a las Entidades de Registro o Verificación y a los Prestadores de Servicios de Valor Añadido, públicos y privados, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura y 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.
- **Clave Pin:** es una secuencia de números o letras para la identificación, autenticación de algún usuario usada para desencriptar los mensajes entrantes y firmar los salientes verificando que alguien está autorizado para acceder a un servicio o un sistema.
- **Clave Privada:** Es una de las claves de un sistema de criptografía asimétrica que es usada para generar una firma digital en un documento electrónico. La clave privada sólo debe permanecer en propiedad del 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.
- **Certificado Digital:** Es el documento credencial electrónico generado y firmado digitalmente por una Entidad de Certificación que vincula un par de claves con una persona natural o jurídica confirmando su identidad. El ciclo de vida de un certificado digital podría comprender:
    - La suspensión consiste en inhabilitar la validez de un certificado digital por un período de tiempo establecido en el momento de la solicitud de suspensión, dicho período no puede superar la fecha de expiración del certificado digital.

- La modificación de la información contenida en un certificado sin la re-emisión de sus claves.
- La re-emisión consiste en generar un nuevo par de claves y un nuevo certificado, correspondiente a una nueva clave pública, pero manteniendo la mayor parte de la información del suscriptor contenida en el certificado a expirar.

- **Código QR** (o "*Quick Response Code*" por su denominación en inglés)**:** Es un tipo de código de barras bidimensional que contiene datos codificados en la forma de cuadrados negros organizados en una grilla cuadrada de fondo blanco, que pueden ser decodificados por dispositivos electrónicos tales como un teléfono inteligente. El uso de códigos QR es libre de licencias y su especificación se encuentra estandarizada en el ISO/IEC 18004:2006.
- **Dispositivo Criptográfico:** Elemento de hardware, tal como un token criptográfico o tarjeta inteligente que permite almacenar de manera segura el certificado digital y la clave privada de los usuarios o suscriptores que cuentan con un certificado digital. Deben cumplir con certificaciones y estándares de seguridad.
- **Documento electrónico:** Es la unidad básica estructurada de información, es susceptible de ser clasificada, transmitida, procesada o conservada utilizando medios electrónicos, sistemas de información o similares. Contiene información de cualquier naturaleza, es registrado en un soporte electrónico o digital, en formato abierto y de aceptación general, a fin de facilitar su recuperación y conservación en el largo plazo. Asimismo, tiene asociado datos que permiten su individualización, identificación, gestión y puesta al servicio del ciudadano. El documento electrónico tiene el mismo valor legal que aquellos documentos en soporte papel, de conformidad con lo establecido en el numeral 30.3 del artículo 30 del TUO de la Ley Nº 27444.
- **Documento Nacional de Identificación Electrónico (DNIe):** Es una credencial de identidad emitida por el RENIEC, que acredita presencial y no presencialmente la identidad de las personas.
- **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.
- **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 aceptación y autorización de las solicitudes de cancelación de certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.
- **Expediente electrónico:** es el conjunto organizado de documentos electrónicos que respetando su integridad documental están vinculados lógicamente y

forman parte de un procedimiento administrativo o servicio prestado en exclusividad en una determinada entidad de la Administración Pública.

- **Firma Digital:** Es aquella firma electrónica que utilizando una técnica de criptografía asimétrica, permite la identificación del signatario y ha sido creada por medios, incluso a distancia, que garantizan que éste mantiene bajo su control con un elevado grado de confianza, de manera que está vinculada únicamente al signatario y a los datos a los que refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior, tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita, siempre y cuando haya sido generada por un Prestador de Servicios de Certificación Digital debidamente acreditado que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica, y que no medie ninguno de los vicios de la voluntad previstos en el Título VIII del Libro IV del Código Civil.
- **Firma Electrónica:** Es cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita.
- **Firma Manuscrita:** La firma manuscrita es aquella imagen que significa nuestro nombre, apellido o título realizada por nuestra propia mano y plasmada en un documento para darle autenticidad o para manifestar la aprobación de su contenido.
- **No Repudio:** Es la imposibilidad para una persona de desdecirse de sus actos cuando ha plasmado su voluntad en un documento y lo ha firmado en forma manuscrita o digitalmente con un certificado emitido por una Entidad de Certificación acreditada en cooperación de una Entidad de Registro o Verificación acreditada, salvo que la misma entidad tenga ambas calidades, empleando un software de firmas digitales acreditado, y siempre que cumpla con lo previsto en la legislación civil'. El no repudio hace referencia a la vinculación de un individuo (o institución) con el documento electrónico, de tal manera que no puede negar su vinculación con él ni reclamar supuestas modificaciones de tal documento (falsificación).
- **Suscriptor:** Son aquellos Servidores que cuentan con autorización para firmar digitalmente documentos electrónicos, mediante la utilización de certificados digitales emitidos por una Entidad de certificación debidamente acreditada.
- **Infraestructura Oficial de Firma Electrónica (OIFE):** Es el sistema confiable, acreditado, regulado y supervisado por la AAC que cuenta con los instrumentos legales y técnicos para garantizar los procesos de certificación digital. Es decir, es la infraestructura dentro de la cual se generan las firmas y certificados digitales seguros y confiables, siempre y cuando se respeten sus disposiciones y normatividad.
- **Tarjeta Inteligente (SMART CARD):** En el contexto de firmas y certificados digitales, es un dispositivo de almacenamiento, del tamaño y forma de una tarjeta de crédito convencional, que cuenta con un chip criptográfico para almacenar de

manera segura y confiable las claves privada y pública, los certificados digitales y otros datos.

- **Token Criptográfico:** Es un dispositivo físico del tamaño y forma de una memoria USB convencional. Este pequeño dispositivo contiene un chip criptográfico donde se almacena la clave privada de manera segura.

6. DISPOSICIONES GENERALES:

6.1. La suscripción de un documento electrónico con firma digital, otorga validez y eficacia jurídica.

6.2. La implementación de la firma digital tendrá los siguientes beneficios:

- Simplificación administrativa, considerando que no necesitará desplazamiento de los documentos en físico para hacer trámites o recibir respuestas.
- Reducir impactos ambientales con la utilización de papel, lo cual busca una gestión Ecoeficiente.
- Aportar el aumento de la confianza electrónica.
- Otorgar mayor seguridad e integridad a los documentos.

6.3. Los servidores civiles deben utilizar la firma digital:

a. Aplicando las disposiciones establecidas en la presente Directiva.
b. Para la emisión, publicación o intercambio de datos, información o documentos electrónicos con otras entidades públicas, ciudadanos o personas en general.
c. En escenarios con alto riesgo de que su autoría pueda ser cuestionada o desconocida.

6.4. Para los efectos de la presente Directiva toda vez que se haga mención a la firma digital debe entenderse que se refiere a la firma electrónica cualificada establecida en el artículo 1A del Decreto Supremo N.º 052-2008-PCM Reglamento de la Ley N° 27269.

6.5. Validez legal de la firma digital:

6.5.1. La firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica (IOFE), tiene la misma validez y eficacia jurídica que una firma manuscrita, siempre y cuando haya sido generada por un prestador de servicios de certificación debidamente acreditado. En este caso el GRA usa un software de firma digital acreditado por la IOFE: Firma Perú.

6.5.2. Para la presente directiva, un documento electrónico puede contar con una o varias firmas digitales o vistos de diferentes servidores civiles de la entidad u otras entidades.

6.5.3. Por excepción, las entidades de la administración pública, a pedido expreso del solicitante, pueden expedir reproducciones impresas de los documentos electrónicos firmados digitalmente en el marco de la IOFE, siempre que incluyan en la impresión la dirección web necesaria que permita contrastar su autenticidad mediante el acceso a los archivos electrónicos de la

administración. El cumplimiento de dicha formalidad otorga la condición de copias auténticas a las reproducciones impresas conforme a los dispuesto en la tercera disposición complementaria final del Decreto Supremo N° 026-2016-PCM.

6.6. Los administrados, pueden usar DNIe o Certificado Digital de persona natural, los cuales son adquiridos ante el RENIEC (para el DNIe) o en cualquier entidad de certificación acreditada por la AAC. Cabe mencionar que, si el trámite de Certificado Digital de persona natural se realiza ante el RENIEC, este corresponde al trámite de adquisición del DNIe, ya que RENIEC solamente emite el Certificado Digital de persona jurídica a entidades públicas.

7. DISPOSICIONES ESPECÍFICAS:

7.1. Emisión del Certificado Digital

7.1.1. Los administrados, deben realizar la gestión de su DNIe en el RENIEC, según corresponda la naturaleza de su trámite a realizar ante el Gobierno Regional de Ancash.

7.1.2. La responsabilidad sobre los efectos jurídicos generados por la utilización de una firma digital corresponde al titular del certificado digital.

7.1.3. Certificado Digital de Persona Jurídica para uso institucional

El trámite de certificado digital se inicia con la manifestación de necesidad del servidor civil de firmar digitalmente los documentos, el cual se realiza mediante la Solicitud del Certificado Digital, dirigida al Subgerente de Tecnologías de la Información e Innovación, para su trámite correspondiente con el Administrador del Certificado Digital.

El Administrador del Certificado Digital es la autoridad máxima de la unidad ejecutora, quién es el responsable de coordinar las gestiones de Certificados Digitales ante RENIEC para el personal de la entidad.

Para dicho efecto, el Administrador del Certificado Digital debe seguir los pasos establecidos en la GUÍA TEMPORAL PARA EL REPRESENTANTE DE ENTIDAD: GENERACIÓN DE LISTA DE ASPIRANTES A SUSCRIPTOR, colgado dentro de la web del EREP-RENIEC en Manuales de la Plataforma Integrada de Entidad de Registro. https://pki.reniec.gob.pe/pier/

El Administrador del Certificado Digital debe:

a. Registrar los datos de los suscriptores a través de la Plataforma Integrada de la Entidad de Registro – PIER del EREP-RENIEC.

b. Crear la "Lista de Aspirantes a Suscriptor", registra el DNI del suscriptor y completa los datos laborales, selecciona el tipo de verificación de identidad, procede a generar el listado de aspirantes y a firmarlo digitalmente. Una vez firmado la lista de aspirantes se notifica mediante correo electrónico a los suscriptores.
c. Si se seleccionó la opción de Declaración Jurada como verificación de identidad, se debe rellenar y firmar por los aspirantes a suscriptor, el formato de DECLARACIÓN JURADA DE IDENTIFICACIÓN NO PRESENCIAL PARA SOLICITAR CERTIFICADO DIGITAL - PERSONA JURÍDICA EN EL MARCO DE LOS D.S N°008-2020-SA Y D.S 044-2020-PCM QUE DECLARA EL ESTADO DE EMERGENCIA NACIONAL, según (Anexo N° 1), el Administrador del Certificado Digital con el rol de representante de entidad deberá firmar digitalmente (en formato .pdf) por cada registro del listado de aspirantes a suscriptor que desea generar.
d. Si se seleccionó la opción Facial como verificación de identidad, se debe ingresar al correo electrónico, buscar la notificación y seleccionar la opción de verificar identidad, esto le lleva a la página web de la PIER, para la verificación de su identidad, en donde ingresa su DNI, acepta los términos y condiciones y marca el check relacionado al Captcha y le da clic a Validar. El sistema genera un código QR en pantalla, el cual debe ser escaneado por el smartphone del suscriptor mediante el aplicativo ID Perú, sigue las instrucciones y verifica en la validación exitosa en la página web de la PIER, al correo electrónico le llega el link de descarga del certificado Digital.
e. Luego de recibir el suscriptor por correo electrónico una clave y la ruta para descargar el Certificado Digital emitido por la EREP-RENIEC en un plazo máximo de cinco (05) días hábiles en su correo electrónico institucional. El suscriptor será responsable de revisar su correo tanto en la bandeja de entrada como en la bandeja de correo no deseado, la emisión de dicho certificado y sus instrucciones correspondiente por la EREP-RENIEC.
f. Recibido el correo electrónico del EREP-RENIEC, el suscriptor deberá comunicarse con la Subgerencia de Tecnologías de la Información e Innovación, para que procedan a la instalación del certificado digital en su equipo de cómputo. En el proceso de instalación del Certificado Digital se solicitará que el suscriptor ingrese una contraseña, la cual servirá, para que pueda firmar a partir de ese momento los documentos electrónicos.
g. En caso que el área usuaria considere conveniente, determinará quién o quiénes podrán hacer uso de la instalación del certificado digital mediante un token u otro dispositivo de almacenamiento del certificado digital. Se solicitará que el suscriptor ingrese un Pin, el cual servirá, para que pueda firmar a partir de ese momento los documentos electrónicos.

7.1.4. Certificado Digital de Persona natural

Los funcionarios y/o servidores civiles del GRA, deben realizar la gestión de su DNIe en el RENIEC, en caso de requerir mayor detalle sobre el trámite, deberán acercarse a la SGTII, para el asesoramiento respectivo.

7.2. Uso de la firma

7.2.1. Los suscriptores de las áreas usuarias del Gobierno Regional del Ancash deben hacer uso progresivo de la firma digital en todos los documentos electrónicos que emitan en el marco de su competencia funcional.

7.2.2. Los certificados digitales de persona natural contenidos en el DNIe pueden ser utilizados por los servidores civiles para firmas digitales que requieran generar en el ejercicio de sus funciones en una entidad pública, en los actos de administración interna, actos administrativos, durante la tramitación de procedimientos administrativos, procedimientos de gestión interna y prestación de servicios digitales; de conformidad con lo establecido en el artículo 17 la Ley de Gobierno Digital.

7.2.3. Los certificados digitales de persona jurídica entregados a servidores civiles como parte de sus herramientas de trabajo en el GRA, deben ser utilizados por éste únicamente para la creación de firmas digitales que requieran generar en el ejercicio de sus funciones en la referida entidad, en los actos de administración interna, actos administrativos, durante la tramitación de procedimientos administrativos, procedimientos de gestión interna y/o prestación de servicios digitales autorizados.

7.2.4. Para que un suscriptor pueda utilizar la firma digital en los documentos electrónicos, debe contar con el Certificado Digital, un dispositivo electrónico de seguridad que almacena su clave privada (token criptográfico y/o computador) y el Software de Firma Digital.

7.2.5. Para que un suscriptor pueda utilizar la firma digital mediante el uso del DNIe, deberá contar con un lector de DNIe y el software de firma digital correspondiente.

7.2.6. Los suscriptores de las áreas usuarias del Gobierno Regional del Ancash son responsables del contenido del documento electrónico en el que firmen digitalmente a través de los sistemas de información del Gobierno Regional del Ancash.

7.2.7. Los suscriptores harán uso de los certificados digitales de persona jurídica o DNIe, para firmar digitalmente documentos electrónicos de acuerdo a las funciones y procedimientos de su competencia. El uso de la contraseña de su certificado digital es personal e intransferible, siendo responsabilidad del

suscriptor el uso de la firma digital en cualquier documento electrónico, lo que generará el no repudio de esta.

7.2.8. Con relación al uso de la clave privada y del certificado digital por parte del suscriptor, este deberá cumplir con lo siguiente:

a. Emplear adecuadamente su certificado digital conforme a lo dispuesto en la Ley N° 27269 – Ley de Firmas y Certificados Digitales y su Reglamento y sus modificatorias.
b. En caso de extravío o pérdida de la tarjeta inteligente o token criptográfico se estaría garantizando que nadie que no conozca dicha contraseña o PIN de acceso podrá hacer uso de su firma digital.
c. Custodiar su contraseña o PIN de acceso de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado.
d. En caso de que el PIN quede comprometida en su seguridad, el suscriptor debe notificarlo de inmediato al Administrador del Certificado Digital del GRA; para que proceda a la cancelación del certificado digital.
e. En caso de que el PIN del DNIe quede comprometida en su seguridad, el suscriptor debe acercarse ante el RENIEC, para su actualización.

7.2.9. El suscriptor debe elaborar el documento y convertirlo a formato PDF para firmarlo digitalmente. En caso no se haya efectuado la firma digital, podrá modificar el documento las veces que sea necesario para su posterior firma.

7.2.10. Para firmar digitalmente un documento electrónico, se deberá seleccionar y cargar el documento electrónico a firmar mediante el Software de Firma digital.

7.2.11. En caso se requiere firmar documentos de forma masiva se deberá realizar la firma en bloque, es decir agrupados en un solo archivo.

Según lo establecido en la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2022-PCM/SGTD - Guía para el uso e integración de la Plataforma Nacional de Firma Digital en la Administración Pública, la Firma digital en lote es:

a. La firma digital en lote es aquella operación de creación de firma digital en la cual múltiples documentos son firmados por un único firmante.
b. Dependiendo del módulo criptográfico utilizado, el firmante debe ingresar su PIN o contraseña una única vez por todo el lote o una vez por cada documento del lote. Es potestad del firmante contar con un módulo criptográfico de creación de firma digital que satisfaga el caso de uso exigido por su sistema de información y la IOFE.

7.2.12. Tener en cuenta que el software de firma digital que usa el GRA, utiliza el formato de firma siguiente:

c. PAdES (PDF Advanced Electronic Signatures), según la especificación técnica ETSI TS 102 778-3, es el formato más adecuado cuando el documento original se encuentra en formato PDF. Opcionalmente, con este formato de firma se puede tener asociado una representación gráfica de la firma digital en la página del documento que el suscriptor defina.

Según lo establecido en la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2022-PCM/SGTD - Guía para el uso e integración de la Plataforma Nacional de Firma Digital en la Administración Pública.

7.3. Procedimiento de Cancelación y Anulación de la solicitud de los Certificados Digitales

7.3.1. Procede en los siguientes casos:

d. Cuando por error de la unidad de organización, del solicitante y/o del Administrador del Certificado Digital se haya consignado información inexacta en la solicitud.
e. Por deterioro, alteración o cualquier otro hecho que afecte la clave privada o la contraseña de acceso a su clave privada.
f. Por la pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada (computador o token criptográfico).
g. Cada vez que haya desvinculación o rotación de personal el Gerente / Sub Gerente / Jefe inmediato de la unidad funcional al que se encuentre asignado el personal, remitirá al Administrador del Certificado Digital la relación de personal con su DNI.
h. Cuando el suscriptor del certificado digital solicite inmediatamente al Administrador del Certificado Digital la cancelación de su certificado, cuando sospeche el compromiso potencial de su clave privada, debido a la pérdida de su contraseña o sospecha que un tercero conozca o pueda deducir dicha contraseña.

7.3.2. El Administrador del Certificado Digital deberá seguir los pasos establecidos en la GUÍA DE USUARIO: OPERADOR DE REGISTRO DIGITAL, colgado dentro de la web del EREP-RENIEC en Manuales de la Plataforma Integrada de Entidad de Registro, sección del Manual: Cancelación de Certificados Digitales. https://pki.reniec.gob.pe/pier/

7.4. La administración del Token Criptográfico

7.4.1. La SGTII administra el token criptográfico de la entidad y asigna un token a solicitud del servidor civil del GRA, en caso no cuente con DNIe ni certificado digital.

7.4.2. La asignación del token la realiza la SGTII, se efectúa mediante el formato de Asignación de Dispositivo Criptográfico, según Anexo N° 2.

7.4.3. La SGTII, instruye a los suscriptores, respecto al almacenamiento del certificado en el token.

7.4.4. En caso de bloqueo de password o PIN del token, el suscriptor está en la obligación de comunicar a la SGTII, quién verifica si se trata de un bloqueo momentáneo o permanente.

7.4.5. Si fuera un bloqueo permanente, el Administrador del Certificado Digital, se comunica con la EREP-RENIEC para la revocación del certificado digital y generación de uno nuevo.

7.4.6. El suscriptor es responsable del token criptográfico asignado. En caso este haya sido perdido, sustraído, deteriorado, averiado o robado, éste deberá ser sustituido con otro token con características iguales o mejores, el cual debe ser aprobado por la SGTII, según Anexo N° 3.

7.4.7. En el caso de cese de labores, el suscriptor deberá devolver el Dispositivo Electrónico como parte de la entrega de cargo a la SGTII.

7.5. Operación de validación de la firma digital

7.5.1. La validación de la firma digital es la operación mediante la cual un verificador comprueba su validez utilizando un software de validación de firmas digitales, de acuerdo con lo establecido en el artículo 4 del Reglamento de la Ley N° 27269. Para la validación de una firma digital se debe utilizar el servicio de validación de firmas digitales de la Plataforma Nacional de Firma Digital, aplicando lo establecido en la Guía para el uso e integración de la Plataforma Nacional de Firma Digital en las entidades de la Administración Pública, aprobada mediante Resolución N°002-2022- PCM/SGTD o norma vigente.

7.5.2. Para la validación de una firma digital, un verificador utiliza los siguientes elementos de forma obligatoria:

a. El archivo firmado digitalmente.
b. El software de validación de firmas digitales.

7.5.3. La verificación de la validez de una firma digital se desarrolla en dos escenarios:

a. Con intervención humana: Este escenario se da cuando el verificador es una persona natural, pudiendo ser el firmante o un tercero.
b. Sin intervención humana: Este escenario se da cuando el verificador es un sistema de información que invoca de manera automatizada a un software de validación de firmas digitales.

7.5.4. Un verificador puede validar firmas digitales de dos maneras:

a. Interactivamente. Se caracteriza porque se efectúa la operación de validación de un único dato firmado.
b. En lote. Se caracteriza porque se efectúa la operación de validación de múltiples datos firmados, de manera continua.

7.5.5. Para la validación de una firma digital, con software de validación adicional al considerado en el numeral 7.5.1. de la presente directiva tenemos:
- https://apps.pide.gob.pe/validadorfirma
- Sunat: Validador de Documentos Electrónicos
- Software lector de PDF con reconocimiento de firmas digital.

7.5.6. La validación de una firma digital, acorde a lo estipulado en la Resolución de Secretaría de Gobierno y Transformación Digital N°007-2024-PCM/SGTD, que Aprueba la Directiva N° 002-2024-PCM/SGTD que regula el uso de la firma digital en las entidades públicas, puede generar como resultado una de las siguientes respuestas:
a. VÁLIDA. Significa que, en el momento de la validación, la firma digital ha superado satisfactoriamente todos los criterios de validez establecidos en el estándar ETSI EN 319 102-1 y en la Guía de Acreditación de Aplicaciones de Software, en su versión vigente, aprobada por la AAC de la IOFE.
b. NO VÁLIDA. Significa que, en el momento de la validación, la firma digital no cumple con alguno o algunos de los criterios de validez establecidos en el estándar ETSI EN 319 102-1 y en la Guía de Acreditación de Aplicaciones de Software, en su versión vigente, aprobada por la AAC de la IOFE. Algunos de estos criterios de validez pueden ser, por ejemplo: conformidad de la firma digital (formato, hash, cifrado) y/o conformidad del certificado digital (cancelado, expirado, aún no válido).
c. INDETERMINADA. Significa que, en el momento de la validación, no es posible afirmar si una firma digital es VÁLIDA o es NO VÁLIDA.

8. RESPONSABILIDAD:

8.1. Administrador del Certificado Digital
a. Entregar información veraz durante la solicitud de emisión de certificados y demás procesos: suspensión, anulación, cancelación ante RENIEC.
b. Cumplir permanentemente las condiciones establecidas por la Entidad de Certificación para la utilización del Certificado.
c. El Administrador del Certificado Digital solicita a la EREP-RENIEC la emisión y cancelación de los certificados digitales del/ la suscriptor/a, asumiendo las obligaciones del Titular, estipuladas en el artículo 15 del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado con Decreto Supremo N° 052-2008-PCM.

8.2. Subgerencia de Tecnologías de la Información e Innovación.

a. La SGTII, es la responsable de difundir la presente directiva en coordinación con la Gerencia Regional de Administración.
b. La SGTII es el responsable operativo de la implementación de la firma digital, así como de los procesos asociados que consideren la firma digital de los funcionarios y servidores públicos del Gobierno Regional del Ancash en los sistemas de información.
c. La SGTII, gestiona las condiciones para la firma digital como equipamiento de recursos humanos, normas de regulación para la implementación de las firmas y certificados digitales en el Gobierno Regional de Ancash.
d. El área usuaria efectuará las coordinaciones necesarias con la SGTII en caso de presentarse situaciones como: olvido o pérdida de la contraseña o renovación del certificado digital, entre otros, a fin de poder solucionar la incidencia.
e. La SGTII, realizará la capacitación sobre el uso de la firma digital con el certificado digital a los funcionarios y servidores públicos del Gobierno Regional de Ancash, así como la explicación del proceso en que se utilizará dicha firma.

8.3. Suscriptor.

a. Todo/a suscriptor/a que tiene asignado un token u otro dispositivo de almacenamiento de certificado digital es responsable de cambiar el PIN para su uso. Puede realizar los cambios de PIN que considere convenientes a través de la opción de gestión de dispositivo, pudiendo solicitar el apoyo de la SGTII, siendo responsable de mantener la confidencialidad de la misma.
b. Emplear adecuadamente su certificado digital, conforme a la normativa vigente.
c. Dejar de utilizar el PIN, transcurrido el plazo de vigencia del certificado digital.
d. Notificará a la EREP- RENIEC, a través del Administrador de los Certificados Digitales sin retrasos las inexactitudes o cambios en el contenido del certificado digital.
e. Proteger el acceso al repositorio del certificado digital (computador, tarjeta inteligente, token criptográfico).
f. En caso de la pérdida del token criptográfico, laptop o Pc, el suscriptor debe comunicar inmediatamente a la SGTII, para la gestión de la cancelación y baja correspondiente ante el RENIEC.
g. El PIN es personal e intransferible. En tal sentido, el suscriptor es responsable de la misma, por lo que deberá mantener su control y la reserva bajo responsabilidad.
h. Al ser responsables de los trámites y actuaciones que se realicen utilizando su firma digital, deberán evitar que terceras personas utilicen los certificados digitales.
i. A partir de la recepción del certificado digital de persona jurídica, los servidores civiles del Gobierno Regional de Ancash reconocen como propio y auténtico los documentos que por su medio se generen y acepten las consecuencias derivadas del uso de la firma digital, siendo responsables de la veracidad del contenido de la información registrada en todos los documentos autorizados.

9. DISPOSICIONES COMPLEMENTARIAS

9.1. Por la naturaleza de la utilización de las firmas y certificados digitales, lo dispuesto en la presente directiva será ejecutado progresivamente de acuerdo a las necesidades de cada unidad orgánica, con la finalidad de que no dificulte su labor administrativa o procedimiento en un inicio.

10. ANEXOS

10.1. Anexo N° 1 - Declaración Jurada de Identificación No Presencial para Solicitar Certificado Digital - Persona Jurídica en el Marco de los D.S N°008-2020-SA y D.S 044-2020-PCM que declara el Estado de Emergencia Nacional.
10.2. Anexo N° 2 - Asignación de token.
10.3. Anexo N° 3 - Reposición de token.
10.4. Anexo N° 4 – Flujo de emisión de certificado Digital de Persona Jurídica para uso institucional.
10.5. Anexo N° 5 – Flujo de Proceso del uso de la firma y certificado digital de los suscriptores.
10.6. Anexo N° 6 – Flujo de Proceso de la Administración del Token Criptográfico.

ANEXO N° 1 - DECLARACIÓN JURADA DE IDENTIFICACIÓN NO PRESENCIAL PARA SOLICITAR CERTIFICADO DIGITAL - PERSONA JURÍDICA EN EL MARCO DE LOS D.S N°008-2020-SA Y D.S 044-2020-PCM QUE DECLARA EL ESTADO DE EMERGENCIA NACIONAL

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Identidad digital @

DECLARACIÓN JURADA DE IDENTIFICACIÓN NO PRESENCIAL PARA SOLICITAR CERTIFICADO DIGITAL - PERSONA JURÍDICA EN EL MARCO DE LOS D.S N°008-2020-SA Y D.S 044-2020-PCM Y MODIFICATORIAS, QUE DECLARA EL ESTADO DE EMERGENCIA NACIONAL

El Suscrito,

_____

Identificado (a) con DNI N° _____, con fecha de emisión ___/___/_____ (verificar fecha de emisión en su DNI físico).

Nombre de la Entidad: _____

Información del trabajador (En departamento, provincia y distrito consignar de acuerdo a su sede laboral)

Sede Laboral: _____

Departamento: _____ Provincia: _____

Distrito: _____

DECLARO ante RENIEC, que la información consignada es veraz, y se remite a fin de iniciar el trámite de mi Certificado Digital de Persona Jurídica para uso institucional.

Para dar conformidad, adjunto como evidencia mi fotografía y firma, a fin de que sea evaluada como sustento en la aprobación de mi trámite para la obtención de mi certificado digital.

FOTOGRAFIA RECIENTE	FIRMA DEL SUSCRIPTOR Y FECHA
IMPORTANTE: La fotografía debe ser reciente tomada en la fecha de la solicitud, de manera frontal mirando hacia la cámara y sin accesorios en el rostro. No debe ser la misma del DNI, ni de declaraciones juradas presentadas anteriormente.	**IMPORTANTE:** En caso de firma manuscrita debe ser la más parecida a la suscrita en su DNI (sin sellos), luego debe colocarse la fecha, igualmente de manera manuscrita en la parte inferior de la firma, sin superponerla y con el mismo lapicero, para evidenciar que se realiza en el mismo momento en que se firma.

IMPORTANTE: La firma debe ser la más parecida a la suscrita en su DNI, caso contrario el trámite será denegado. No se deben colocar sellos.

Lugar y fecha: _____

*.En caso de falsa declaración en procedimiento administrativo se aplicará el Artículo 411 del Cód. Penal: "El que, en un procedimiento administrativo, hace una falsa declaración en relación a hechos o circunstancias que le corresponde probar, violando la presunción de veracidad establecida por ley, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años".

(*) Esta declaración jurada no debe tener una antigüedad mayor a 30 días calendarios.

ANEXO N° 2 - ASIGNACIÓN DE TOKEN.

DECLARACIÓN JURADA N° -2025-GRA/SGTII

DE : Nombres y Apellidos
Cargo

ASUNTO : Entrega y asignación de token físico para firma digital

FECHA : día de mes del año.

Yo, _____, identificado con DNI N° _____, con cargo de _____, en la unidad orgánica de _____ del Gobierno Regional de Áncash, en pleno uso de mis facultades y bajo juramento, declaro lo siguiente:

1. Información del token asignado:

- Token asignado : _____
- ID del dispositivo : _____
- Fecha de asignación : _____
- Propósito del token : _____

2. Conformación de recepción y uso del token:

- Declaro haber recibido el token asignado y el dispositivo correspondiente en perfectas condiciones.
- Me comprometo a utilizar el token y dispositivo exclusivamente para los fines establecidos en el ámbito de mis funciones dentro de la unidad orgánica del Gobierno Regional de Áncash.
- Me hago responsable del uso adecuado del dispositivo y del token, así como su devolución en perfectas condiciones al cese de mis funciones.

3. Compromiso ante pérdida o daño del token:

En caso de pérdida, robo o daño del token o del dispositivo asignado, me comprometo a informar de manera inmediata a la entidad correspondiente, de acuerdo con los procedimientos establecidos, y a asumir las consecuencias legales y administrativas que puedan derivarse.

4. Autorización para el tratamiento de datos personales:

Autorizo al Gobierno Regional de Áncash el tratamiento de mis datos personales conforme a la Ley de Protección de Datos Personales N° 29733 y la política de privacidad vigente para fines relacionados con la asignación y seguimiento del uso del token y dispositivo.

NOMBRES Y APELLIDOS CARGO	NOMBRES Y APELLIDOS SUBGERENTE DE TECNOLOGÍAS DE LA INFORMACIÓN E INNOVACIÓN

ANEXO N° 3 - REPOSICIÓN DE TOKEN.

DECLARACIÓN JURADA N° -2025-GRA/SGTII

DE : Nombres y Apellidos
Cargo

ASUNTO : Reposición de token físico para firma digital

FECHA : día de mes del año.

Yo, _____, identificado con DNI N° _____, con cargo de

El día de mes del año, mediante la DECLARACIÓN JURADA N° ___-202_-GRA/SGTII, se me asignó el token

En consecuencia, procedí a realizar la reposición del token a través del que se detalla en el Ítem 1:

1. Información del token asignado:

- Token asignado : _____
- Token en reposición : _____
- Fecha de asignación : _____
- Propósito del token : _____

2. Conformación de recepción y uso del token:

- Declaro haber recibido el token asignado y el dispositivo correspondiente en perfectas condiciones.
- Me comprometo a utilizar el token y dispositivo exclusivamente para los fines establecidos en el
- Me hago responsable del uso adecuado del dispositivo y del token, así como su devolución en

3. Compromiso ante pérdida o daño del token:

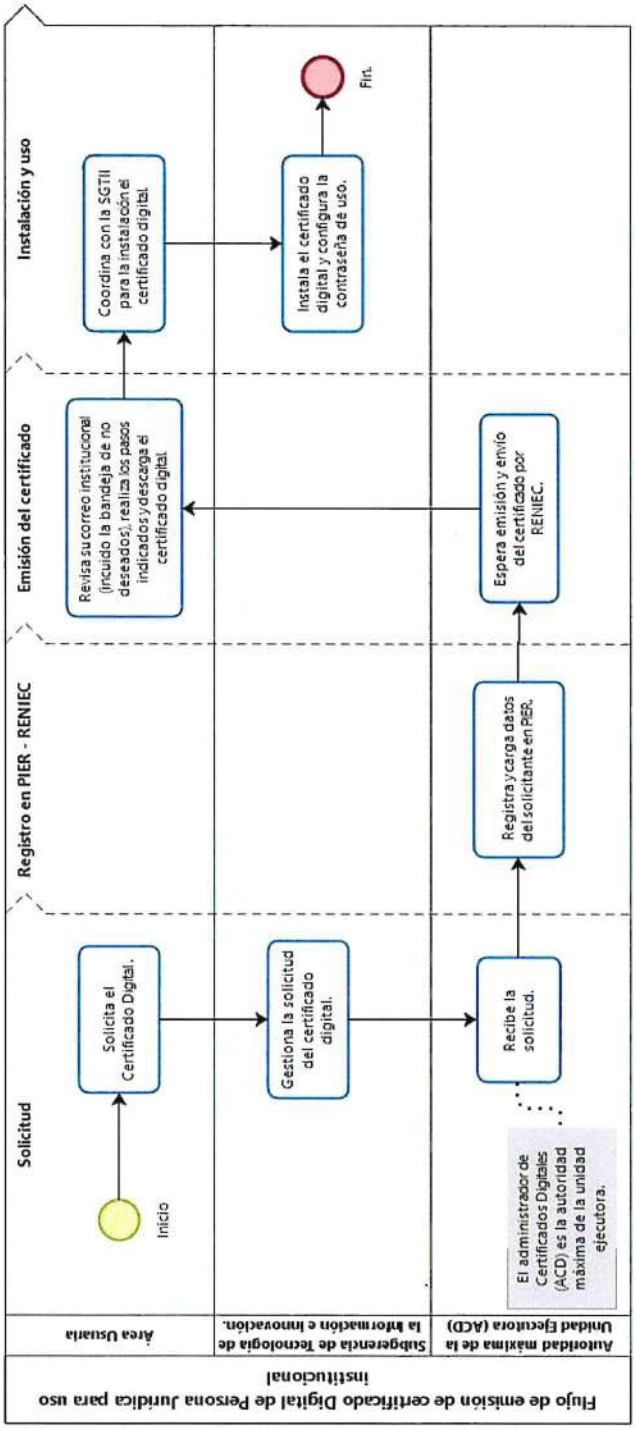
En caso de pérdida, robo o daño del token o del dispositivo asignado, me comprometo a informar y reemplazar

4. Autorización para el tratamiento de datos personales:

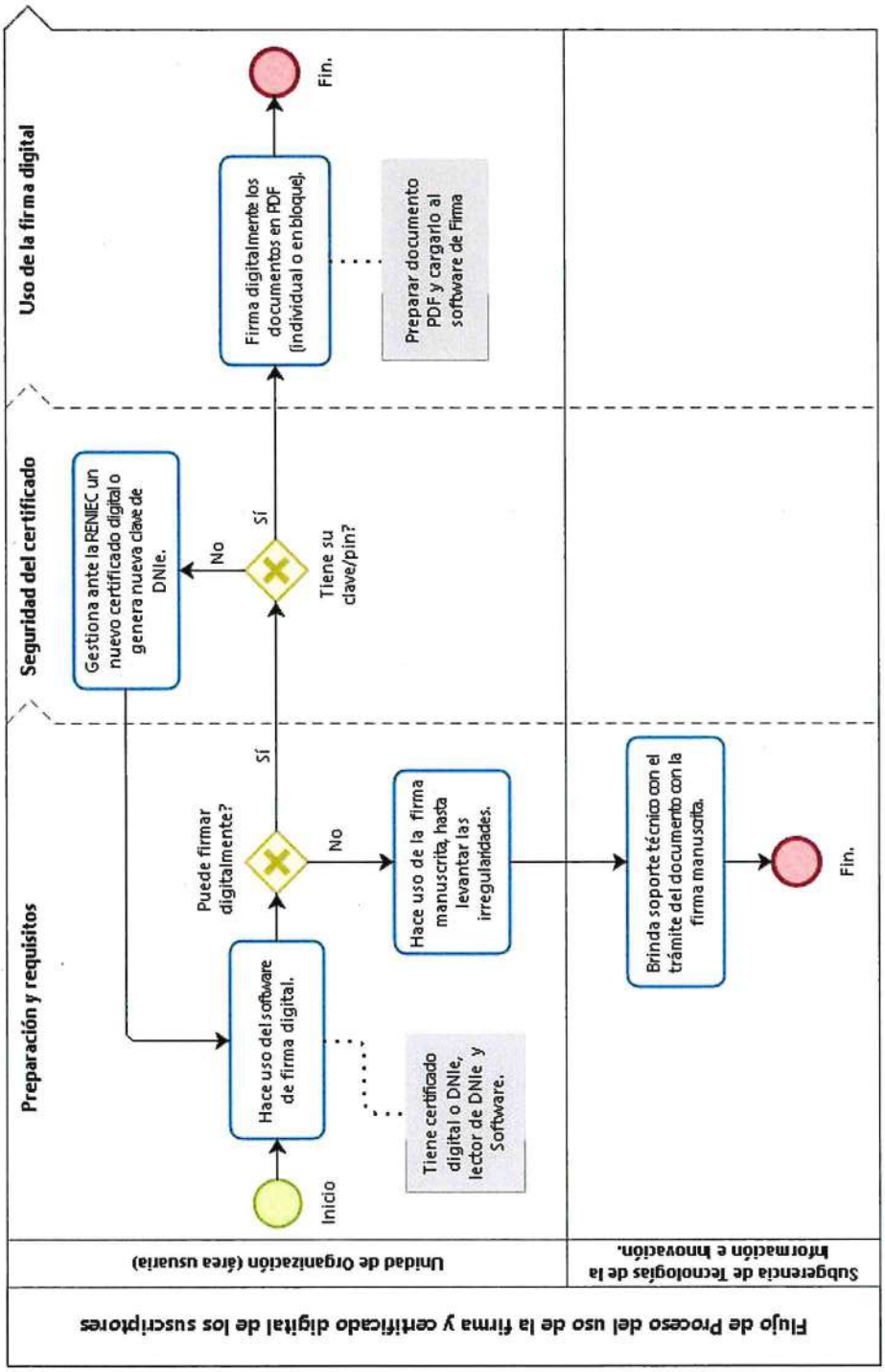
Autorizo al Gobierno Regional de Áncash el tratamiento de mis datos personales conforme a la Ley de

NOMBRES Y APELLIDOS	**NOMBRES Y APELLIDOS**
CARGO	SUBGERENTE DE TECNOLOGÍAS DE LA INFORMACIÓN E INNOVACIÓN

ANEXO N° 4 – FLUJO DE EMISIÓN DE CERTIFICADO DIGITAL DE PERSONA JURÍDICA PARA USO INSTITUCIONAL



ANEXO N° 5 – FLUJO DE PROCESO DEL USO DE LA FIRMA Y CERTIFICADO DIGITAL DE LOS SUSCRIPTORES.



ANEXO N° 6 – FLUJO DE PROCESO DE LA ADMINISTRACIÓN DEL TOKEN CRIPTOGRÁFICO