 GOBIERNO REGIONAL CAJAMARCA <small>A tu servicio con transparencia</small>	DIRECTIVA N° 7-2021-GR.CAJ/DRTD	Código: DRTD-D001
	CERTIFICACIÓN DIGITAL	Versión: 1.0

DIRECTIVA N° 7 -2021-GR.CAJ/DRTD

DIRECTIVA QUE ESTABLECE EL USO DE CERTIFICADOS DIGITALES EN EL GOBIERNO REGIONAL CAJAMARCA

I. FINALIDAD

Establecer el procedimiento para la emisión, reemisión, instalación, cancelación y uso de los certificados digitales en el Gobierno Regional Cajamarca.

II. OBJETIVO


Gestionar eficiente y sistemáticamente la emisión, reemisión, instalación, cancelación y uso de los certificados digitales en el Gobierno Regional Cajamarca.

III. ALCANCE

Esta directiva es de cumplimiento obligatorio para funcionarios y servidores públicos de la sede central del Gobierno Regional Cajamarca y de las Unidades Ejecutoras que requieran hacer uso de certificados digitales.

IV. BASE LEGAL


- 4.1. Ley N° 27269, Ley de Firmas y Certificados Digitales, modificada por la Ley N° 27310, y su Reglamento aprobado con Decreto Supremo N° 052-2008-PCM y su modificatoria aprobada con Decreto Supremo N° 070-2011-PCM.
- 4.2. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, sus modificatorias, y su Reglamento aprobado con Decreto Supremo N° 030-2002-PCM.
- 4.3. Decreto Supremo N° 105-2012-PCM, que establece disposiciones para facilitar la puesta en marcha de la firma digital y modifica el Decreto Supremo N° 052-2008-PCM.
- 4.4. Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley de Procedimiento Administrativo General.
- 4.5. Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública al 2021.
- 4.6. Decreto Supremo N° 081-2013-PCM, que aprueba la Política Nacional de Gobierno Electrónico.
- 4.7. 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.
- 4.8. Decreto Legislativo N° 1310, que aprueba medidas adicionales de Simplificación Administrativa.

 GOBIERNO REGIONAL CAJAMARCA <small>A tu servicio con transparencia</small>	DIRECTIVA N° 7-2021-GR.CAJ/DRTD	Código: DRTD-D001
	CERTIFICACIÓN DIGITAL	Versión: 1.0

- 4.9. Resolución Gerencia General Regional N° 024-2017-GR.CAJ.GGR, que aprueba la Directiva N° 001-2017-GR.CAJ-GRPPAT/SGDI, “Normas para la Formulación, Actualización y Aprobación de Directivas en el Gobierno Regional Cajamarca”.
- 4.10. Ordenanza Regional N° 005-2017-GR.CAJ-CR, que aprueba el Reglamento de Organización y Funciones del Gobierno Regional Cajamarca, modificado por Ordenanza Regional N° 010-2017-GR.CAJ-CR y Ordenanza Regional N° D000001-2021-GRC-CR.
- 4.11. Contrato de Prestación de Servicios de Certificación Digital - Certificado Clase III - Persona Jurídica, celebrado entre GORECAJ y RENIEC, cuyos efectos inician el 09 de mayo de 2018.
- 4.12. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
- 4.13. Decreto Supremo N° 123-2018-PCM, que aprueba el Reglamento del Sistema Administrativo de Modernización de la Gestión Pública.
- 4.14. Decreto de Urgencia N° 06-2020, se crea el Sistema Nacional de Transformación Digital.
- 4.15. Decreto de Urgencia N° 07-2020, se aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- 4.16. Resolución Jefatural N° 000011-2020/JNAC/RENIEC, que aprueba la ampliación de la vigencia de la gratuidad de la emisión de Certificados Digitales a favor de las entidades del Sector Público en su calidad de titular y a todos los suscriptores que estas soliciten hasta el 30 de junio de 2020.
- 4.17. Decreto de Urgencia N° 026-2020, que establece diversas medidas excepcionales y temporales para prevenir la propagación del coronavirus (COVID-19) en el territorio nacional.
- 4.18. Resolución Jefatural N° 000078-2020/JNAC/RENIEC, que aprueba la ampliación de la vigencia de la gratuidad de la emisión de Certificados Digitales a favor de las entidades del Sector Público en su calidad de titular y a todos los suscriptores que estas soliciten hasta el 30 de setiembre de 2020.

V. RESPONSABILIDADES


- 5.1. **Registro Nacional de Identificación y Estado Civil – RENIEC.** Tiene la facultad de emitir certificados digitales para personas naturales y jurídicas que lo soliciten como Entidad de Registro o Verificación para el Estado Peruano – EREP, prestando los servicios de Certificación Digital, los cuales serán emitidos al personal autorizado y designado por el Gobierno Regional Cajamarca o Unidades Ejecutoras.
- 5.2. **Entidad Titular.** Es la persona jurídica, Gobierno Regional Cajamarca o Unidades Ejecutoras, titular de los certificados digitales solicitados ante EREP – RENIEC por el representante de la entidad.
- 5.3. **El Representante de la entidad.** Es la persona natural, integrante del Gobierno Regional Cajamarca o Unidades Ejecutoras, que cuenta con facultades para representar a la persona jurídica en los trámites de certificado digital ante la EREP – RENIEC.

 GOBIERNO REGIONAL CAJAMARCA <small>A tu servicio con transparencia</small>	DIRECTIVA N° 7-2021-GR.CAJ/DRTD	Código: DRTD-D001
	CERTIFICACIÓN DIGITAL	Versión: 1.0

- 5.4. Dirección Regional de Transformación Digital – DRTD.** Es la unidad de organización del Gobierno Regional Cajamarca, responsable de la gestión de los certificados digitales de persona jurídica emitidos por RENIEC a nombre del Gobierno Regional Cajamarca; brinda soporte a los funcionarios o servidores públicos en la solicitud de emisión, reemisión, instalación, cancelación y en el uso de los certificados digitales en el Gobierno Regional Cajamarca. La DRTD es responsable del presupuesto de certificados digitales en el Gobierno Regional Cajamarca. Así mismo es responsable de la aplicación, supervisión y cumplimiento de las disposiciones establecidas en la presente directiva. En las Unidades Ejecutoras corresponde esta responsabilidad a quien haga sus veces.
- 5.5. Dirección de Personal.** Es la unidad de organización del Gobierno Regional Cajamarca, responsable de reportar las bajas del personal del Gobierno Regional Cajamarca para motivos de cancelación de certificados digitales. En las Unidades Ejecutoras corresponde esta responsabilidad a quien haga sus veces.
- 5.6. Funcionarios y servidores públicos.** Son responsables del cumplimiento de las disposiciones de la presente directiva.

VI. DISPOSICIONES GENERALES


- 6.1.** La documentación electrónica oficial emitida en el Gobierno Regional Cajamarca o Unidades Ejecutoras es aquella que cuenta con firma digital, para lo cual corresponde gestionar los certificados digitales de persona jurídica (clase III – suscriptor) de los funcionarios y servidores públicos ante RENIEC - EREP.
- 6.2.** El Representante de la entidad gestionará los certificados digitales en la Plataforma Integrada de la Entidad de Registro – PIER, a nombre del Gobierno Regional Cajamarca o Unidades Ejecutoras.
- 6.3.** Los funcionarios y servidores públicos deberán activar su cuenta en el Módulo - Mesa de Servicios del Sistema de Aplicaciones Regional v 2.1, para realizar la solicitud de emisión, reemisión, instalación y cancelación de certificado digital.
- 6.4.** Los funcionarios y servidores públicos son responsables de la generación y uso de la clave privada del certificado digital, son los suscriptores a quienes se les vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.
- 6.5.** Los certificados digitales pueden ser instalados en computadora de escritorio, computadora portátil, token criptográfico o tarjeta inteligente, y al momento de la instalación el funcionario o servidor público creará una contraseña o PIN de protección de la clave privada, la cual deberá ser confidencial, debiendo hacerse uso personalísimo de ésta al momento de generar los documentos electrónicos oficiales.
- 6.6.** Los procesos de certificación digital son: solicitud de emisión de certificado digital, solicitud de reemisión de certificado digital, solicitud de instalación de certificado digital y solicitud de cancelación de certificado digital.

 GOBIERNO REGIONAL CAJAMARCA A tu servicio con transparencia	DIRECTIVA N° 7-2021-GR.CAJ/DRTD	Código: DRTD-D001
	CERTIFICACIÓN DIGITAL	Versión: 1.0

VII. DISPOSICIONES ESPECÍFICAS

7.1. De la solicitud de emisión o reemisión de certificado digital:


- a) La solicitud de emisión o reemisión de certificado digital se inicia con el pago de trámite por Certificado Clase III - Persona Jurídica, el cual se efectuará por el Gobierno Regional Cajamarca, Unidad Ejecutora correspondiente o funcionario o servidor público, a través de los canales de recaudación del Banco de la Nación (presenciales o virtuales), consignando el RUC de la entidad titular y el código de tributo correspondiente.
- b) El Gobierno Regional Cajamarca o las Unidades Ejecutoras asumirán el costo por Certificado Clase III – Persona Jurídica en las solicitudes de:
 - Emisión de certificado digital por primera vez para personal nuevo o personal activo;
 - Emisión de certificado digital por expiración del certificado digital;
 - Reemisión de certificado digital por formateo de lugar de almacenamiento (computadora de escritorio, computadora portátil, token criptográfico o tarjeta inteligente), siempre y cuando sea propiedad del Gobierno Regional Cajamarca o Unidad Ejecutora.
 - Reemisión de certificado digital por problemas técnicos de lugar de almacenamiento (computadora de escritorio, computadora portátil, token criptográfico o tarjeta inteligente), siempre y cuando sea propiedad del Gobierno Regional Cajamarca o Unidad Ejecutora y su desperfecto no haya sido ocasionado por el funcionario o servidor público a quién se le asignó bien.
- c) El funcionario o servidor público asumirá el costo por Certificado Clase III – Persona Jurídica en las solicitudes de:
 - Reemisión de certificado digital por olvido de contraseña de acceso a la clave privada;
 - Reemisión de certificado digital por instalación errónea del certificado por el funcionario o servidor público.
 - Reemisión de certificado digital por vencimiento del plazo de descarga del certificado digital;
 - Reemisión de certificado digital por formateo de lugar de almacenamiento (computadora de escritorio, computadora portátil, token criptográfico o tarjeta inteligente), siempre y cuando NO sea propiedad del Gobierno Regional Cajamarca o Unidad Ejecutora.
 - Reemisión de certificado digital por problemas técnicos de lugar de almacenamiento (computadora de escritorio, computadora portátil, token criptográfico o tarjeta inteligente), siempre y cuando NO sea de propiedad del Gobierno Regional Cajamarca.
 - Emisión de certificado digital por necesidad de contar con él en computadora de escritorio, computadora portátil, token criptográfico o tarjeta inteligente que NO sea propiedad del Gobierno Regional Cajamarca o Unidad Ejecutora.
- d) El Gobierno Regional Cajamarca o las Unidades Ejecutoras asumirán el costo de los certificados digitales para: trabajo remoto (un certificado), trabajo presencial (un certificado) y trabajo mixto (dos certificados).

 GOBIERNO REGIONAL CAJAMARCA <small>A tu servicio con transparencia</small>	DIRECTIVA N° 7-2021-GR.CAJ/DRTD	Código: DRTD-D001
	CERTIFICACIÓN DIGITAL	Versión: 1.0

- e) La Dirección Regional de Transformación Digital o quien haga sus veces en las Unidades Ejecutoras verificará la casuística y determinará a quién le corresponde asumir el costo de un nuevo trámite por Certificado Clase III - Persona Jurídica.
- f) El funcionario o servidor público que solicite la emisión o reemisión de certificado digital, deberá cumplir con entregar la información que la Dirección Regional de Transformación Digital solicite, asumiendo el funcionario o servidor público la responsabilidad de la veracidad y exactitud de la información proporcionada.
- g) El funcionario o servidor público (SOLICITANTE) deberá solicitar la emisión o reemisión de certificado digital enviando la información requerida a través del Módulo - Mesa de Servicios del Sistema de Aplicaciones Regional v 2.1, habilitado tanto para el Gobierno Regional Cajamarca como para las Unidades Ejecutoras.
- h) La Dirección Regional de Transformación Digital o la que haga sus veces en las Unidades Ejecutoras, se encargará de consolidar las solicitudes de emisión o reemisión de certificado digital y enviarlas a través de la PIER. El envío se realizará cada viernes laborable a las 4:30 p.m. en orden de llegada e independientemente de la urgencia. En caso el día viernes sea día no laborable, el envío se realizará el día laborable siguiente a primera hora. Todas las solicitudes enviadas después de la hora establecida anteriormente, serán procesadas el día viernes de la siguiente semana.
- i) El funcionario o servidor público que solicite la emisión de certificado digital por expiración del certificado digital, deberá hacerlo con una anticipación máxima de 10 días calendarios a la expiración del certificado digital. La Dirección Regional de Transformación Digital o la que haga sus veces en las Unidades Ejecutoras no se responsabiliza de la expiración de los certificados digitales.
- j) El funcionario o servidor público que solicite la emisión o reemisión de certificado digital, será notificado sobre su trámite por la DRTD a la bandeja correspondiente del Módulo – Mesa de Servicios del Sistema de Aplicaciones Regional v 2.1 y por EREP – RENIEC al correo electrónico oficial.
- k) Se podrán recibir las solicitudes de emisión y reemisión de certificado digital las 24 horas del día, durante los 365 días del año.

7.2. De la instalación de certificado digital:

- a) De ser aprobada la solicitud de emisión o reemisión de certificado digital por EREP - RENIEC, el funcionario o servidor público (SUSCRIPTOR) recibirá un email conteniendo: link del DCDelivery, usuario y contraseña que permitirán generar el certificado digital, el cual deberá ser instalado únicamente por personal de la Dirección Regional de Transformación Digital o la que haga sus veces en las Unidades Ejecutoras, de no ser así, el funcionario o servidor público será responsable de cualquier desperfecto.
- b) El funcionario o servidor público aprobado por EREP - RENIEC como suscriptor, será responsable de contactarse con la Dirección Regional de Transformación Digital o con la que haga sus veces en las Unidades


 GOBIERNO REGIONAL CAJAMARCA <small>A tu servicio con transparencia</small>	DIRECTIVA N° 7-2021-GR.CAJ/DRTD	Código: DRTD-D001
	CERTIFICACIÓN DIGITAL	Versión: 1.0

Ejecutoras a través del Módulo - Mesa de Servicios del Sistema de Aplicaciones Regional v 2.1, para solicitar la instalación del certificado digital y brindar la información solicitada.

- c) En caso venciera el plazo de descarga del certificado digital (30 días calendario), el costo de un nuevo trámite será asumido por el funcionario o servidor público. La Dirección Regional de Transformación Digital o la que haga sus veces en las Unidades Ejecutoras no se responsabiliza del vencimiento de dicho plazo.
- d) El funcionario o servidor público deberá crear una contraseña o PIN de acceso a clave privada al momento de la instalación del certificado digital en computadora de escritorio, computadora portátil, token criptográfico o tarjeta inteligente, que deberá ser confidencial, debiendo hacerse uso personalísimo de esta al momento de firmar los documentos electrónicos oficiales.
- e) El funcionario o servidor público puede formatear el token, pero ello implica perder el certificado digital almacenado. En este caso el costo de un nuevo trámite será asumido por el funcionario o servidor público.
- f) En caso el funcionario o servidor público olvide la contraseña de acceso a la clave privada, el costo de un nuevo trámite será asumido por este.

7.3. De la solicitud de cancelación de certificado digital

- a) La solicitud de cancelación de certificado digital se inicia con el reporte de bajas del personal del Gobierno Regional Cajamarca o Unidades Ejecutoras, remitido por la Dirección de Personal o la que haga sus veces en las unidades ejecutoras a la Dirección Regional de Transformación Digital o la que haga sus veces en las unidades ejecutoras, o por solicitud del funcionario o servidor público indicando el motivo.
- b) Los motivos por los que se realiza la cancelación de certificados digitales son:
 - cuando el suscriptor deja de ser miembro de la entidad;
 - cuando la información contenida en el certificado ya no resulte correcta;
 - deterioro o alteración o pérdida que afecte la contraseña o PIN de acceso a la clave privada;
 - exposición o uso indebido de la contraseña o PIN de acceso a la clave privada;
 - autoridad de certificación comprometida;
 - por extinción de la personería jurídica de la entidad;
 - solicitud expresa;
- c) Pueden solicitar la cancelación de un certificado digital el suscriptor del certificado y el representante de la entidad.
- d) Al cancelarse el certificado digital, la suscripción al servicio de certificación con EREP - RENIEC finaliza.
- e) El representante de la entidad realizará la cancelación de los certificados digitales ante EREP - RENIEC a través de la PIER.

 GOBIERNO REGIONAL CAJAMARCA <small>A tu servicio con transparencia</small>	DIRECTIVA N° 7-2021-GR.CAJ/DRTD	Código: DRTD-D001
	CERTIFICACIÓN DIGITAL	Versión: 1.0

- f) El funcionario o servidor público que desee realizar la cancelación de su certificado digital, deberá hacerlo a través del Módulo - Mesa de Servicios del Sistema de Aplicaciones Regional v 2.1, facilitando los datos que se le requiera.

7.4. Del uso del certificado digital


- a) El funcionario o servidor público debe ser razonablemente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados.
- b) El funcionario o servidor para proteger su certificado digital, deberá proteger el lugar donde está almacenado (computadora de escritorio, computadora portátil, token criptográfico o tarjeta inteligente) y la contraseña o PIN de acceso a éste.
- c) El funcionario o servidor público deberá notificar a la Dirección Regional de Transformación Digital o la que haga sus veces en las Unidades Ejecutoras a través del Módulo - Mesa de Servicios del Sistema de Aplicaciones Regional v 2.1, sin retrasos injustificables los motivos indicados a continuación:
- La pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada (computadora de escritorio, computadora portátil, token criptográfico o tarjeta inteligente).
 - El compromiso potencial de su clave privada.
 - La pérdida de control sobre su clave privada.
 - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

VIII. DISPOSICIONES COMPLEMENTARIAS

- Primero.- El funcionario o servidor público podrá solicitar la instalación de su certificado digital en token criptográfico o tarjeta inteligente, siempre y cuando le sean entregados por la alta dirección del Gobierno Regional Cajamarca o Unidades Ejecutoras o el mismo funcionario o servidor público haya adquirido uno previamente.
- Segundo.- El funcionario o servidor público será vinculado con el documento electrónico firmado digitalmente, por lo que no podrá negar su vinculación con él ni reclamar supuestas modificaciones de tal documento (falsificación).
- Tercero.- La Dirección Regional de Transformación Digital, propondrán lineamientos para la mejora continua de la gestión de certificados digitales en el Gobierno Regional Cajamarca y Unidades Ejecutoras.

IX. DISPOSICIONES TRANSITORIAS

- Primero.- El funcionario o servidor público podrá usar cualquier software acreditado ante INDECOPI para firmar digitalmente un documento con su certificado digital.
- Segundo.- Las Unidades Ejecutoras deberán celebrar Contrato de Prestación de Servicios de Certificación Digital - Certificado Clase III - Persona Jurídica con RENIEC para la emisión de sus propios certificados

 GOBIERNO REGIONAL CAJAMARCA <small>A tu servicio con transparencia</small>	DIRECTIVA N° 7-2021-GR.CAJ/DRTD	Código: DRTD-D001
	CERTIFICACIÓN DIGITAL	Versión: 1.0


digitales, en cuanto el Módulo de Administración Documentaria - MAD v. 3.0 sea implementado a nivel regional.

Tercero.- Las Unidades Ejecutoras podrán solicitar a la Dirección Regional de Transformación Digital la gestión ante EREP - RENIEC de los certificados digitales a nombre del Gobierno Regional Cajamarca siempre y cuando hayan realizado el pago correspondiente y no cuenten con contrato con RENIEC.


X. GLOSARIO DE TERMINOS

Para la presente directiva se considerará estos términos y definiciones:

- **Autenticación:** Es el proceso técnico que permite determinar la identidad de la persona que firma digitalmente, en función del documento electrónico firmado por éste y al cual se le vincula; este proceso no otorga certificación notarial ni fe pública.
- **Certificado digital:** Es un documento digital emitido por una entidad autorizada o Entidad de Certificación (EC). El certificado digital vincula un par de claves (una pública y otra privada) con una persona y asegura su identidad digital. Con esta identidad digital la persona podrá ejecutar acciones de comercio y gobierno electrónico con seguridad, confianza y pleno valor legal. Los certificados digitales emitidos por las entidades de certificación deben contener al menos:
 - o Datos que identifiquen indubitablemente al suscriptor.
 - o Datos que identifiquen a la Entidad de Certificación.
 - o La clave pública.
 - o La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos.
 - o Número de serie del certificado.
 - o Vigencia del certificado.
 - o Firma digital de la Entidad de Certificación.
- **El ciclo de vida del certificado digital:** son los estados por el que puede pasar un certificado digital. Los estados son:
 - o Emisión: cuando se solicita por primera vez, el anterior expiró o fue cancelado.
 - o Reemisión: cuando se solicita una renovación antes de que el certificado digital cumpla su periodo de vigencia. Este procedimiento es válido por única vez para certificados de periodo de vigencia de un año.
 - o Cancelación: cuando ya no desea que su certificado digital siga vigente o cuando vence el periodo de vigencia.
- **Clase de certificado Clase III - Persona Jurídica:** son los certificados digitales para trabajadores de la administración pública como entidad final emitidos para Persona Jurídica con periodo de validez de 1 y 2 años.
- **Clave privada:** Es una cadena de caracteres (números y letras) que, en un sistema de criptografía asimétrica, se mantiene en reserva por parte del titular de la firma digital.


 GOBIERNO REGIONAL CAJAMARCA <small>A tu servicio con transparencia</small>	DIRECTIVA N° 7-2021-GR.CAJ/DRTD	Código: DRTD-D001
	CERTIFICACIÓN DIGITAL	Versión: 1.0

- **Clave pública:** Es una cadena de caracteres (números y letras) que, en un sistema de criptografía asimétrica, puede y debe ser difundida abiertamente para facilitar y promover la comunicación.
- **Contraseña de acceso a la clave privada:** es una secuencia corta de caracteres alfanuméricos y es de conocimiento únicamente del firmante.
- **Correo electrónico:** Es el conjunto de palabras que identifican a una persona que puede enviar y recibir correo. Cada dirección es única y pertenece siempre a la misma persona.
- **Documento electrónico:** Es la unidad básica estructurada de información registrada, publicada o no, susceptible de ser generada, clasificada, gestionada, transmitida, procesada o conservada por una persona o una organización de acuerdo a sus requisitos funcionales, utilizando sistemas informáticos.
- **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.
- **Entidades de la administración pública:** Es el organismo público que ha recibido del poder político la competencia y los medios necesarios para la satisfacción de los intereses generales de los ciudadanos y la industria.
- **Entidad de Registro o Verificación para el Estado Peruano (EREP).** Cumple con las funciones y obligaciones de una Entidad de Registro o Verificación (ER) según lo indicado en el Reglamento de Firmas y Certificados Digitales.
- **Entidad final:** Es el suscriptor de un certificado digital.
- **Firma digital:** Es aquella firma electrónica que cumple con todas las funciones de la firma manuscrita, en particular se trata de aquella firma electrónica basada en criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada. Permite la identificación del signatario, la integridad del contenido y tiene la misma validez que el uso de una firma manuscrita, siempre y cuando haya sido generada dentro de la IOFE.
- **Firma electrónica:** se trata de cualquier símbolo o carácter o conjunto de símbolos o caracteres basados en medios electrónicos que cumple con alguna de las funciones de la 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.
- **Identidad digital:** Es el reconocimiento de la identidad de una persona en un medio digital (como por ejemplo Internet) a través de mecanismos tecnológicos seguros y confiables, sin necesidad de que la persona esté presente físicamente.
- **Infraestructura Oficial de Firma Electrónica (IOFE):** es el sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente (AAC) que cuenta con los instrumentos legales y técnicos para garantizar los

 GOBIERNO REGIONAL CAJAMARCA <small>A tu servicio con transparencia</small>	DIRECTIVA N° 7-2021-GR.CAJ/DRTD	Código: DRTD-D001
	CERTIFICACIÓN DIGITAL	Versión: 1.0

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.

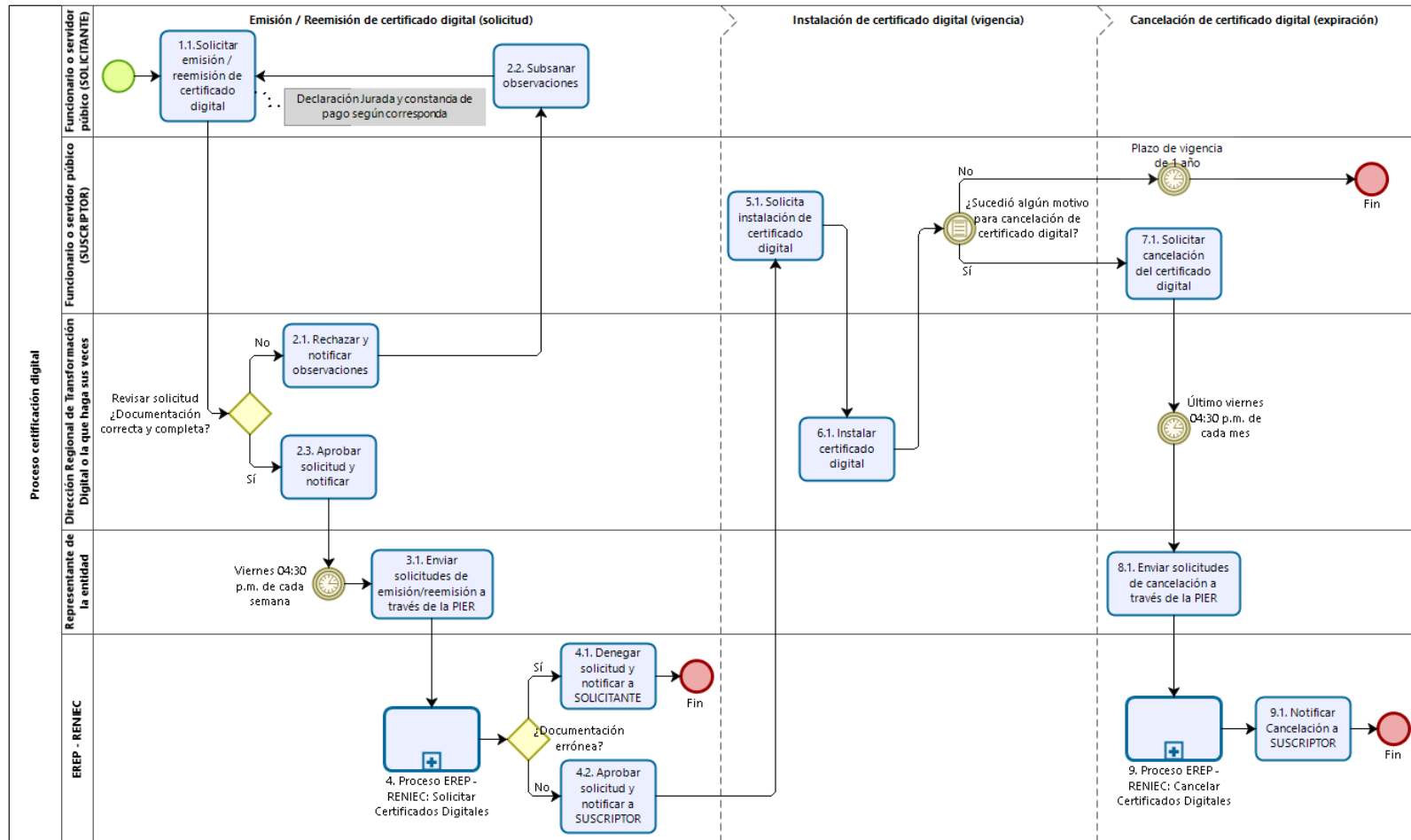
- **PIN:** El número de identificación personal, pin o PIN (de las siglas en inglés, Personal Identification Number) es un tipo de contraseña utilizado en ciertos sistemas, como la tarjeta SIM, el teléfono móvil o el cajero automático, para identificarse y obtener acceso al sistema.
- **Plataforma Integrada de la Entidad de Registro (PIER):** Es una herramienta que permitirá una gestión eficiente y eficaz gestión de los Certificados Digitales de las Entidades de la administración pública los cuales son solicitados a la Entidad de Registro y Verificación para el Estado Peruano (EREP), permitiendo brindar un servicio de calidad y seguridad. Además, permite garantizar la integridad, autenticidad y confidencialidad de la información, siguiendo para ello los lineamientos de la Política de Seguridad y Plan de Seguridad de la EREP, asimismo los Lineamientos de Seguridad de la Información del RENIEC; respetando las normas de privacidad para el manejo de toda la información.
- **Registro Nacional de Identificación y Estado Civil – RENIEC:** Es la Entidad de Certificación Nacional para el Estado Peruano - ECERNEP, Entidad de Certificación para el Estado Peruano - ECEP y Entidad de Registro o Verificación para el Estado Peruano – EREP de la Infraestructura Oficial de Firma Electrónica – IOFE. Tiene la facultad de emitir certificados digitales para personas naturales y jurídicas que lo soliciten, prestando los servicios de Certificación Digital, para el uso de autenticación y firma digital, los cuales serán emitidos al personal autorizado y designado por cada entidad del sector público, quienes se constituirán en Suscriptores.
- **Suscriptor:** Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.
- **Tarjeta inteligente (smartcard):** Es un dispositivo físico, muy similar a una tarjeta de crédito convencional. Sin embargo, este pequeño dispositivo contiene un chip criptográfico donde se almacena la clave privada del certificado digital de manera segura.
- **Titular de la firma digital:** es la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos.
- **Titular:** Es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.


 GOBIERNO REGIONAL CAJAMARCA A tu servicio con transparencia	DIRECTIVA N° 7-2021-GR.CAJ/DRTD	Código: DRTD-D001
	CERTIFICACIÓN DIGITAL	Versión: 1.0

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

XI. FLUJOGRAMAS

Proceso de certificación digital



 GOBIERNO REGIONAL CAJAMARCA A tu servicio con transparencia	DIRECTIVA N° 7-2021-GR.CAJ/DRTD	Código: DRTD-D001
	CERTIFICACIÓN DIGITAL	Versión: 1.0

XII. ANEXOS

ANEXO N° 01 Procedimiento del proceso certificación digital

NRO. ACT.	PROVEEDOR	ENTRADA	DESCRIPCIÓN DE ACTIVIDADES		SALIDA	CLIENTE
			ACTIVIDAD	RESPONSABLE		
El proceso inicia con la necesidad de contar con un certificado digital por parte del funcionario o servidor público de la sede central del Gobierno Regional Cajamarca o Unidades Ejecutoras para el cumplimiento de sus funciones.						
1	Funcionario o servidor público (SOLICITANTE)	Necesidad de contar con un certificado digital	1.1. Solicitar emisión / reemisión de certificado digital	Funcionario o servidor público (SOLICITANTE)	Solicitud de emisión/reemisión de certificado digital registrada y enviada a través del Módulo - Mesa de Servicios del Sistema de Aplicaciones Regional v 2.1 (SAR), conteniendo Declaración Jurada y constancia de pago según corresponda.	Dirección Regional de Transformación Digital o la que haga sus veces.
La Dirección Regional de Transformación Digital o la que haga sus veces en las Unidades Ejecutoras revisará la documentación presentada, en algunos casos la documentación es incorrecta o incompleta.						
2	Funcionario o servidor público (SOLICITANTE)	Solicitud de emisión/reemisión de certificado digital registrada y enviada a través del Módulo - Mesa de SAR, conteniendo Declaración Jurada y constancia de pago según corresponda.	¿Correcto / Completo?	Actividad		
			No	2.1. Rechazar y notificar observaciones	Dirección Regional de Transformación Digital o la que haga sus veces.	Observación registrada a través del Módulo - Mesa de Servicios del SAR.
			Sí	2.2. Subsanar observaciones Luego aplicar Actividad 1.1.	Funcionario o servidor público (SOLICITANTE)	Solicitud reenviada a través del Módulo - Mesa de Servicios del SAR, conteniendo Declaración Jurada y constancia de pago según corresponda subsanando observaciones.
			2.3. Aprobar solicitud y notificar	Dirección Regional de	Solicitud aprobada a través del Módulo - Mesa de Servicios del	Funcionario o servidor público

					Transformación Digital o la que haga sus veces.	SAR.	(SOLICITANTE) Representante de la entidad
3	Cada viernes laborable a las 04:30 p.m. se enviará la documentación a EREP - RENIEC. En caso el día viernes sea día no laborable, el envío se realizará el día laborable siguiente a primera hora. Todas aquellas solicitudes enviadas después de las 04:30 p.m. del día viernes serán enviadas el siguiente viernes.						
	Dirección Regional de Transformación Digital o la que haga sus veces.	<p>Solitudes aprobadas a través del Módulo - Mesa de Servicios del SAR.</p> <p>Consolidado de declaraciones juradas y constancias de pago según corresponda.</p> <p>Listado de solicitantes de certificado digital y listado de constancias de pago.</p>	3.1. Enviar solicitudes a través de la PIER		Representante de la entidad	Solicitud de emisión de certificados digitales solicitados en la PIER	EREP - RENIEC
4	Se ejecuta el Proceso EREP - RENIEC: Solicitar Certificados Digitales , en el cual se revisa la documentación presentada. En algunos casos la documentación es errónea.						
			¿Documentación errónea?	Actividad			
	Representante de la entidad	Solicitud de emisión de certificados digitales solicitados en la PIER	Sí	4.1. Denegar solicitud y notificar a SOLICITANTE Fin del procedimiento.	EREP – RENIEC	Correo denegando la solicitud de emisión del certificado digital de persona jurídica.	Funcionario o servidor público (SOLICITANTE) Representante de la entidad
		No	4.2. Aprobar solicitud y notificar a SUScriptor	EREP - RENIEC	Correo de aprobación de solicitud del certificado digital de persona	Funcionario o servidor público	

						jurídica.	(SUSCRIPTOR)
5	EREP - RENIEC	Correo de aprobación de solicitud del certificado digital de persona jurídica.	5.1. Solicita instalación de certificado digital		Funcionario o servidor público (SUSCRIPTOR)	Solicitud de instalación de certificado digital registrada a través del Módulo - Mesa de SAR.	Dirección Regional de Transformación Digital o la que haga sus veces.
6	Funcionario o servidor público (SUSCRIPTOR)	Solicitud de instalación de certificado digital registrada a través del Módulo - Mesa de SAR.	6.1. Instalar certificado digital		Dirección Regional de Transformación Digital o la que haga sus veces.	Certificado digital instalado.	Funcionario o servidor público (SUSCRIPTOR)
7	Antes de que el certificado digital expire (1 año), es posible solicitar la cancelación del certificado digital por diversos motivos.						
			¿Sucedió algún motivo para cancelación de certificado digital?	Actividad			
	Dirección Regional de Transformación Digital o la que haga sus veces.	Certificado digital instalado.	No	Se cumple el plazo de vigencia de 1 año. Fin del procedimiento	Funcionario o servidor público (SUSCRIPTOR)	Certificado digital vigente.	Funcionario o servidor público (SUSCRIPTOR)
			Sí	7.1. Solicitar cancelación del certificado digital	Funcionario o servidor público (SUSCRIPTOR)	Solicitud de cancelación de certificado digital registrada a través del Módulo - Mesa de SAR.	Representante de la entidad
8	Funcionario o servidor público (SUSCRIPTOR)	Solicitud de cancelación de certificado digital registrada a través del Módulo - Mesa de SAR.	8.1. Enviar solicitudes de cancelación a través de la PIER		Representante de la entidad	Solicitud de cancelación de certificados digitales solicitados en la PIER	EREP – RENIEC
9	Se ejecuta el Proceso EREP - RENIEC: Cancelar Certificados Digitales.						
	Representante de	Solicitud de	9.1. Notificar Cancelación	a	EREP – RENIEC	Correo de cancelación de	Funcionario o

	la entidad	cancelación de certificados digitales solicitados en la PIER	SUSCRIPTOR		certificado digital	servidor público (SUSCRIPTOR) Representante de la entidad
Fin del procedimiento.						