

DIRECTIVA ADMINISTRATIVA N° 002-HR "MAMLL" A/2022/UEI.

**"DIRECTIVA QUE ESTABLECE EL USO DE CERTIFICADOS DIGITALES EN EL HOSPITAL REGIONAL
"MIGUEL ÁNGEL MARISCAL LLERENA DE AYACUCHO".**

I. FINALIDAD

Establecer el procedimiento para la emisión, reemisión, instalación, cancelación y uso de los certificados digitales en los diferentes niveles de puestos de los servidores del Hospital Regional "Miguel A. Mariscal Llerena" de Ayacucho.

II. OBJETIVO

Gestionar eficiente y sistemáticamente la emisión, reemisión, instalación, cancelación y uso adecuado de los certificados digitales en el Hospital Regional "Miguel A. Mariscal Llerena" de Ayacucho.

III. ALCANCE

Esta directiva es de cumplimiento obligatorio para funcionarios y servidores públicos del Hospital Regional de Ayacucho "Miguel A. Mariscal Llerena"

IV. BASE LEGAL

- a. Constitución Política del Estado Peruano.
- b. Ley N° 29158, Ley Orgánica del Poder Ejecutivo, concordante con el Decreto Supremo N° 022-2017-PCM, establece que la Secretaría de Gobierno Digital es el órgano de línea, con autoridad técnico normativa a nivel nacional, responsable de formular y proponer políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de Informática y de Gobierno Electrónico.
- c. 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.
- d. 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.
- e. 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.º 052-2008-PCM.
- f. Decreto Supremo N.º 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N.º 27444, Ley del Procedimiento Administrativo General.
- g. Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública al 2021. La cual se ha estimado una temporalidad hasta el año 2030, aprobándose la Política Nacional de Modernización de la Gestión Pública al 2030, mediante Decreto Supremo N° 103-2022-PCM



- h. Decreto Supremo N° 081-2013-PCM, que aprueba la Política Nacional de Gobierno Electrónico.
- i. 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.
- j. Decreto Legislativo N° 1310, que aprueba medidas adicionales de Simplificación Administrativa.
- k. Contrato de Prestación de Servicios de Certificación Digital - Certificado Clase III - Persona Jurídica, celebrado entre Hospital Regional de Ayacucho y RENIEC, cuyos efectos inician el 15 de junio de 2022.
- l. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
- m. Decreto Supremo N° 123-2018-PCM, que aprueba el Reglamento del Sistema Administrativo de Modernización de la Gestión Pública.
- n. Decreto de Urgencia N° 06-2020, se crea el Sistema Nacional de Transformación Digital.
- o. Decreto de Urgencia N° 07-2020, se aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- p. 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
- q. 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. Modificado por el Decreto de Urgencia N° 115-2021.
- r. Decreto Supremo N° 008-2020-SA, que declara la emergencia sanitaria nacional y dicta medidas de prevención y control del COVID-19. Modificado por Decreto Supremo N°015-2022-SA que prorroga a partir del 29 de agosto del 2022, por un plazo de 180 días calendarios.



V. RESPONSABILIDADES

- a. **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 Hospital Regional de Ayacucho o Unidades Ejecutoras.
- b. **Entidad Titular.** Es la persona jurídica, Hospital Regional "Miguel Ángel Mariscal Llerena" de Ayacucho – Unidad Ejecutora 401, titular de los certificados digitales solicitados ante EREP – RENIEC por el representante de la entidad.

- c. **El Representante de la entidad.** Es la persona natural, que ostenta la condición de funcionario del Hospital Regional de Ayacucho, que cuenta con facultades legales de representación del Hospital Regional "Miguel Ángel Mariscal Llerena de Ayacucho" en los trámites de certificado digital ante la EREP – RENIEC.
- d. **Área de Informática.** Es el área del Hospital Regional de Ayacucho, adscrita a la Unidad de Estadística e Informática, responsable de la gestión de los certificados digitales de persona jurídica emitidos por RENIEC a nombre del Hospital Regional de Ayacucho; 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 Hospital Regional de Ayacucho. El Área de Informática es responsable del presupuesto de certificados digitales en el Hospital Regional de Ayacucho. Así mismo es responsable de la aplicación, supervisión y cumplimiento adecuado de las disposiciones establecidas en la presente directiva.
- e. **Unidad de Personal.** Es la unidad que forma parte de los Órganos de Apoyo del Hospital Regional de Ayacucho, adscrita a la Dirección de Administración, responsable de reportar adecuadamente conforme a vinculación contractual y aplicativos INFORHUS/ AIRSHP las bajas del personal del Hospital Regional de Ayacucho para motivos de cancelación de certificados digitales.
- f. **Funcionarios y servidores públicos.** Son todas aquellas personas naturales, que tienen vínculo laboral con el Hospital Regional de Ayacucho, responsables del cumplimiento correcto de las disposiciones de la presente directiva. Asimismo, una vez adquiere calidad de suscriptor utilizando su clave privada, se convierte en el único responsable del manejo adecuado y custodia de dicha clave; con la consecuente responsabilidad administrativa, civil y/o penal que deriven del uso inadecuado y/o ilegal del mismo.



VI. DISPOSICIONES GENERALES

- a. La documentación electrónica oficial emitida en el Hospital Regional de Ayacucho 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.
- b. El Representante de la entidad gestionará los certificados digitales en la Plataforma Integrada de la Entidad de Registro – PIER, a nombre del Hospital Regional "Miguel Ángel Mariscal Llerena" de Ayacucho – Unidad Ejecutora N° 401.
- c. Los funcionarios y servidores públicos del Hospital Regional de Ayacucho son responsables de la generación, uso y manejo adecuado 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.

- d. 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, bajo responsabilidad.
- e. Los procesos de certificación digital son: **A)** Solicitud de emisión de certificado digital, **B)** Solicitud de reemisión de certificado digital, **C)** Solicitud de instalación de certificado digital y **D)** Solicitud de cancelación de certificado digital.

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 Hospital Regional de Ayacucho, Unidad Ejecutora correspondiente o funcionario o servidor público responsable, 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 Hospital Regional de Ayacucho 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 Hospital Regional de Ayacucho 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 Hospital Regional de Ayacucho 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 usuario responsable 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 Hospital Regional de Ayacucho.
 - 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 Hospital Regional de Ayacucho.
 - 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 Hospital Regional de Ayacucho.
- d. El Hospital Regional "Miguel Ángel Mariscal Llerena" de Ayacucho asumirán el costo de los certificados digitales para: trabajo remoto (un certificado), trabajo presencial (un certificado) y trabajo mixto (dos certificados).
- e. El Área de Informática 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 el Área de Informática 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 al correo certificadodigital@hrayacucho.gob.pe, habilitado para el Hospital Regional de Ayacucho.
- h. El área de informática se encargará de consolidar las solicitudes de emisión o reemisión de certificados digitales y enviarlas a la plataforma de la PIER. Las solicitudes se recibirán hasta el día viernes laborable de cada semana hasta las 11:00 a.m. en orden de llegada e independientemente de la urgencia. En caso el viernes sea un día no laborable, la recepción se realizará el día laborable siguiente. Todas las solicitudes enviadas después del día y la hora establecida anteriormente serán procesadas la semana siguiente.
- 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. El Área de Informática 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 medio del correo electrónico certificadodigital@hrayacucho.gob.pe y por EREP – RENIEC al correo electrónico institucional del funcionario solicitante
- k. Se podrán recibir las solicitudes de emisión y reemisión de certificado digital conforme al literal h) Numeral VII. Disposiciones Específicas, de la presente Directiva.

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 el usuario y contraseña juntamente con un link del aplicativo DCDelivery, que permitirá generar el certificado digital, el cual deberá ser instalado únicamente por personal del área de informática, 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 el Área de Informática a través del correo institucional certificadodigital@hrayacucho.gob.pe, 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 usuario. El Área de Informática 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 la desvinculación laboral, sanción disciplinaria vigente del funcionario o servidor del Hospital Regional de Ayacucho remitido bajo responsabilidad por la Unidad de personal, 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 funcionario o servidor del Hospital Regional de Ayacucho, con motivo de término de vínculo contractual, cambio de designación de Funcionario, u otro.
 - 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 de parte, debidamente motivada;
- 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.
 - f. El funcionario o servidor público que desee realizar la cancelación de su certificado digital, deberá solicitarlo al correo certificadodigital@hrayacucho.gob.pe facilitando los datos que se le requiera.



7.4. Del uso del certificado digital

- a. El funcionario o servidor público debe ser razonablemente diligente y cauteloso en la custodia de su clave privada, con el fin de evitar usos no autorizados bajo estricta responsabilidad.
- b. El funcionario o servidor para proteger diligentemente 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 inmediatamente al área de informática mediante el correo certificadodigital@hrayacucho.gob.pe, los acontecimientos indicados a continuación:
 - La pérdida, robo, extravío o daño severo del dispositivo electrónico de seguridad que almacena su clave privada (computadora de escritorio, computadora portátil, token criptográfico o tarjeta inteligente).
 - El hecho de que la seguridad de su clave privada se encuentre potencialmente comprometida.
 - La pérdida de control sobre su clave privada.
 - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

La comunicación de los acontecimientos señalados supra, son de forma inmediata, salvo motivos de fuerza mayor debidamente justificados

VIII. DISPOSICIONES COMPLEMENTARIAS

Primero. - 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, adulteración, etc.)

Segundo. - El área de informática, propondrá lineamientos de forma periódica, para la mejora continua de la gestión de certificados digitales en el Hospital Regional de Ayacucho.

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,

X. GLOSARIO DE TÉRMINOS

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 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:
 - ✓ Datos que identifiquen indubitablemente al suscriptor.
 - ✓ Datos que identifiquen a la Entidad de Certificación.
 - ✓ La clave pública.
 - ✓ La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos.
 - ✓ Número de serie del certificado.
 - ✓ Vigencia del certificado.
 - ✓ 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:
 - Emisión:** cuando se solicita por primera vez, el anterior expiró o fue cancelado.
 - 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.
 - 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.
- **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, letras y/o números 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 con 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 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 (ERP), 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 ERP, asimismo los Lineamientos de Seguridad de la Información del RENIEC; respetando las normas de privacidad para el manejo de toda la información.
- **Confidencialidad de la información.** - La entidad de registro recabará los datos personales del solicitante de la firma digital directamente de éste y para los fines señalados en la presente directiva. Asimismo, la información relativa a las claves privadas y datos que no sean materia de certificación se mantiene bajo la reserva correspondiente. Sólo puede ser levantada por orden judicial o pedido expreso del suscriptor de la firma digital
- **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 – ERP 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.
- **ERP:**
Entidad acreditada por la Autoridad Administrativa Competente (INDECOPI), encargada del levantamiento de datos, comprobación de la información del solicitante, identificación y autenticación de los titulares y suscriptores, aceptación y autorización de solicitudes de emisión y cancelación de certificados digitales además



de su gestión ante las Entidades de Certificación; para proporcionar, emitir o cancelar los certificados digitales.

- **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 natural o jurídica 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.
- **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. ANEXOS

- Formato de Declaración Jurada de Identificación no presencial para solicitar Certificado Digital. (01 folio)
- Esquema del Flujoograma de Emisión, Reemisión y Cancelación de Certificados Digitales en el Hospital Regional de Ayacucho. (01 Folio)

DIRECTIVA ADMINISTRATIVA N° 002-HR "MAMLL" A/2022/UEI.
DIRECTIVA ADMINISTRATIVA QUE ESTABLECE EL USO DE CERTIFICADOS DIGITALES EN EL HOSPITAL REGIONAL "MIGUEL ÁNGEL MARISCAL LLERENA" DE
AYACUCHO.



ANEXOS

**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: **HOSPITAL REGIONAL DE AYACUCHO**

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

Sede Laboral: HOSPITAL REGIONAL DE AYACUCHO

Departamento: AYACUCHO

Provincia: HUAMANGA

Distrito: ANDRÉS AVELINO CÁCERES DORREGARAY

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
SOSTENIENDO HOJA
CON FECHA**

NOTA: Fotografía debe ser
un "selfie" sin filtros,
sosteniendo un papel con
la fecha en la que se está
rellenando la Declaración
Jurada.

FIRMA DEL SUSCRIPTOR Y FECHA

NOTA: En caso de firma manuscrita debe
ser la más parecida a la suscrita en su
DNI (Sin sellos). La fecha debe colocarse
en la parte inferior de la firma, sin
superponerla.

Lugar y fecha: _____, ____/____/____. * (Todas las fechas deben coincidir)

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

FLUJOGRAMA: PROCESO DE EMISIÓN, REEMISIÓN Y CANCELACIÓN DE CERTIFICADOS DIGITAL EN EL HOSPITAL REGIONAL DE AYACUCHO

PROCESO DE EMISIÓN, REEMISIÓN Y CANCELACIÓN DE CERTIFICADO DIGITAL

