



## **DIRECTIVA DE GERENCIA GENERAL**

### **NORMAS Y PROCEDIMIENTOS PARA EL USO DE FIRMAS DIGITALES EN LA CPMP**

**DGG N° 01-GI-2023**

**San Isidro, 16/11/2023  
Pág. N° 1 de 14**

#### **1. FINALIDAD**

Establecer las disposiciones, actividades y responsabilidades para garantizar el correcto uso de las firmas digitales e impulsar el proceso de simplificación administrativa a través de la utilización de las firmas digitales, en las diversas actividades que se rigen en la Caja de Pensiones Militar Policial (CPMP).

#### **2. REFERENCIA LEGAL Y NORMATIVA**

- Constitución Política del Perú de 1993
- Decreto Ley N° 21021 – Ley de Creación de la Caja de Pensiones Militar Policial y sus modificatorias
- Decreto Supremo N°005-75-CCFA – Reglamento del Decreto Ley N° 21021 y sus modificatorias
- Decreto Ley N° 19846 – Ley de Pensiones Militar Policial y sus modificatorias
- Decreto Supremo N° 009-DE-CCFA – Reglamento de la Ley de Pensiones Militar Policial
- Decreto Legislativo N° 1133 – Decreto Legislativo para el Ordenamiento Definitivo del Régimen de Pensiones del Personal Militar y Policial y sus modificatorias
- Decreto Supremo N° 101-2021-EF – Normas Reglamentarias y Complementarias del Decreto Legislativo N° 1133, Decreto Legislativo para el Ordenamiento Definitivo del Régimen de Pensiones del Personal Militar y Policial
- Ley N° 27444 – Ley del Procedimiento Administrativo General y sus modificatorias
- Ley N° 27269 – Ley de Firmas y Certificados Digitales y sus modificatorias
- Ley N° 27658 – Ley Marco de modernización de la Gestión del Estado y sus modificatorias
- Decreto Legislativo N° 1310 – Decreto Legislativo que aprueba medidas adicionales de Simplificación Administrativa y su modificatoria

- Decreto Legislativo N° 1412 – Decreto Legislativo que aprueba la Ley de Gobierno Digital y sus modificatorias
- Decreto Supremo N° 004-2019-JUS – Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General y sus modificatorias
- Decreto Supremo N° 029-2021-PCM – 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
- Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2021-PCM/SGTD – Aprueban la Directiva N° 002-2021 – PCM/SGTD, Directiva que regula la generación y el uso del Código de Verificación Digital en las entidades de la Administración Pública
- 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 las entidades de la Administración Pública
- Ley N° 28403 – Ley que dispone la recaudación de un aporte por supervisión y control anual por parte de INDECOPI de las entidades de certificación y de verificación/registros de firmas digitales acreditadas bajo su ámbito
- Decreto Supremo N° 030-2002-PCM – Aprueban Reglamento de la Ley Marco de Modernización de la Gestión del Estado
- Decreto Supremo N° 004-2013-PCM – Aprueba la Política Nacional de Modernización de la Gestión Pública
- Decreto Supremo N° 026-2016-PCM – Aprueban 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
- Decreto Supremo N° 052-2008-PCM – Reglamento de la Ley de Firmas y Certificados Digitales y sus modificatorias
- Resolución Ministerial N° 186-2015-PCM – Aprueba el Manual para Mejorar la Atención a la Ciudadanía en las Entidades de la Administración Pública
- Reglamento Interno de Trabajo de la Caja de Pensiones Militar Policial
- Manual de Organización y Funciones de la Caja de Pensiones Militar Policial
- Manual de Descripción de Cargos de la Caja de Pensiones Militar Policial

### **3. ALCANCE**

Las disposiciones contenidas en la presente directiva comprenden a la Gerencia de Informática, a la Gerencia de Administración y Finanzas, al Departamento de Recursos Humanos, a la Gerencia de Riesgos y Desarrollo y a las demás unidades orgánicas de la CPMP.

## **4. GLOSARIO**

- 4.1 Certificado digital:** Es el documento electrónico generado y firmado digitalmente por una entidad de certificación, que vincula un par de claves con una persona determinada, confirmando su identidad. Este debe contener, al menos, los datos que identifiquen indubitablemente al suscriptor y la entidad de certificación, la clave pública, metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos, número de serie del certificado y su vigencia; así como la firma digital de la entidad de certificación. Este certificado se cancela a pedido del titular de la firma digital, por revocatoria de la entidad de certificación, por expiración del plazo de vigencia o por cese de operaciones de la entidad de certificación.
- 4.2 Código de Verificación Digital - CVD:** Es una secuencia de dieciséis (16) dígitos que permite verificar la autenticidad de una reproducción impresa mediante el cotejo con una representación imprimible localizada en la sede digital de la CPMP.
- 4.3 Código QR:** 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.
- 4.4 Documento electrónico:** Es la unidad básica estructurada de información registrada, pública o no, susceptible de ser generada, clasificada, gestionada, transmitida, procesada o conservada por una persona o una entidad de acuerdo a sus requisitos funcionales, utilizando sistemas informáticos; constituida por un conjunto de datos basados en bits o impulsos electromagnéticos, elaborados, generados, transmitidos, comunicados y archivados a través de medios electrónicos, ópticos o cualquier otro análogo.
- 4.5 Entidad certificadora:** Es la persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital, por revocatoria de la entidad de certificación o por expiración del plazo de vigencia.
- 4.6 Firma digital:** Es aquella firma electrónica que utiliza una técnica de criptografía asimétrica; permite la identificación del signatario y ha sido creada por medios que este mantiene bajo su control, con la finalidad de asegurar la integridad del mensaje de datos a través de un código de verificación, así como para vincular al titular de la firma digital y el mensaje de datos remitido.
- 4.7 Firma electrónica:** Es cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse, autenticar y

garantizar la integridad de un documento electrónico o un mensaje de datos, cumpliendo todas o algunas de las funciones características de una firma ológrafa, con la misma validez y eficacia jurídica que esta última.

- 4.8 Firma ológrafa:** Es un trazo gráfico o grafo manuscrito que representa el nombre y el apellido o el título que escribe una persona de su propia mano y tiene fines identificatorios, jurídicos, bancarios, representativos y diplomáticos.
- 4.9 Glosa:** Es aquella información incorporada, dentro de un cuadro de texto, en la parte inferior de cada página de una reproducción imprimible, y comprende: (i) leyenda informativa, (ii) URL de verificación, (iii) código QR y (iv) CDV.
- 4.10 Representante de la entidad:** Es el Gerente de Administración y Finanzas, que cuenta con facultades para representar a la CPMP en los trámites de certificado digital ante el RENIEC.
- 4.11 Suscriptor:** Es el colaborador de la CPMP, responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente.
- 4.12 Titular de la firma digital:** Es la persona natural a quien se le vincula de manera exclusiva con un mensaje de datos firmado digitalmente, utilizando su clave privada.
- 4.13 Token:** Es un *token* de seguridad, denominado también *token* de autenticación o *token* criptográfico, es un dispositivo electrónico que se le entrega al usuario utilizado de un servicio computarizado para facilitar el proceso de autenticación.

## **5. DISPOSICIONES GENERALES**

- 5.1** Los tipos de documentos electrónicos enunciativos, para la aplicación de la firma digital, son:
- Carta externa
  - Contrato
  - Constancia
  - Informe
  - Memorando o memorándum
  - Oficio
  - Actas
  - Certificados
  - Boletas de Pago

- Documentos automáticos generados por un sistema de información; y, otros que se vayan agregando al Sistema Integrado de Trámite Documentario (SITD)
- 5.2** Solo los documentos internos y/o externos descritos en el numeral 5.1 son firmados con firma digital; excepto aquellos, que por su propia naturaleza o porque así lo requiera norma alguna, se usa firma ológrafa y medio físico para su entrega.
- 5.3** El dispositivo que almacena el certificado digital, por defecto es el computador del usuario.
- 5.4** El certificado digital tiene una vigencia de un (1) año.
- 5.5** La Gerencia de Informática capacita sobre el uso adecuado de la firma digital a implementar en todo documento que emitan las unidades orgánicas, además debe instruir al personal operativo en el uso adecuado del *software* que producen documentos electrónicos.
- 5.6** La Gerencia de Informática provee de herramientas de *software*, necesarias, para tener la opción de firmar documentos digitalmente.
- 5.7** Todos los documentos internos y/o externos que emita la entidad son ingresados al SITD.
- 5.8** Solo pueden ser firmados los documentos que estén ingresados en el SITD de la entidad.
- 5.9** El personal autorizado en el uso de las firmas electrónicas se constituye en las personas naturales obligadas, por tener la responsabilidad de firmar electrónicamente los documentos de su competencia.
- 5.10** De preferencia, los documentos con firma digital no se imprimen y son enviados por un medio electrónico (SITD, correo electrónico, intranet, publicaciones, etcétera) y por los canales autorizados por la CPMP. En caso sea necesaria la copia de un documento electrónico firmado digitalmente, se debe usar un código de verificación para acreditar su autenticidad, de acuerdo a lo dispuesto en la Directiva N° 002-2021-PCM/SGTD “Directiva que regula la generación y el uso del Código de Verificación Digital en las entidades de la Administración Pública”, el procedimiento se menciona en el numeral 6.4.
- 5.11** El documento electrónico firmado digitalmente, debe ser presentado en un archivo PDF y almacenado en el sistema de trámite documentario o en el directorio de red

asignado. Los documentos considerados para la aplicación de la firma digital son los mencionados en el numeral 5.1.

- 5.12** Cuando no se pueda generar la firma digital, por razones técnicas y exista alguna urgencia, las unidades orgánicas pueden emitir su documento solo con firma ológrafa, de manera excepcional.
- 5.13** La Gerencia de Informática, comunica a las unidades orgánicas, sobre el procedimiento de la implementación de la firma digital en la CPMP.
- 5.14** Para todo lo no previsto en la presente directiva, es la aplicación de las normas legales vigentes que regulan el uso de las firmas digitales; en las cuales debe prevalecer estas últimas en caso de discrepancia o conflicto con la primera.
- 5.15** La Gerencia de Informática debe brindar soporte a la Gerencia de Administración y Finanzas en la gestión y obtención de los certificados digitales de persona jurídica para funcionarios o colaboradores de la CPMP, en adelante el suscriptor.
- 5.16** Cada unidad orgánica es responsable de solicitar la obtención del certificado digital de sus colaboradores que, debido a la naturaleza de sus funciones, requieran hacer uso de su firma digital.
- 5.17 Requisitos que se deben cumplir para la implementación de la firma digital**
  - 5.17.1** La obtención de un certificado digital de persona jurídica (en adelante certificado digital).
  - 5.17.2** El *software* que realiza la firma; debe estar acreditado por el Instituto Nacional de Defensa de la Competencia de la Protección de la Propiedad Intelectual (INDECOP), en su condición de entidad certificadora.
  - 5.17.3** Para la obtención del dispositivo que almacena el certificado digital (puede ser un *smart card*, un *token*, o un computador designado) es necesario que el solicitante cumpla con los requisitos indicados por la empresa prestadora de servicio o entidad pública. Asimismo, la clave asignada a cada poseedor del dispositivo es única e intransferible.
  - 5.17.4** El suscriptor debe completar el formato word de la “Declaración jurada de identificación no presencial para solicitar certificado digital - Persona jurídica en el marco del Decreto Supremo N° 008-2020-SA y Decreto Supremo 044-2020-PCM y modificatorias, que declara el Estado de Emergencia Nacional “y/o cualquier otro documento que le sea solicitado

por la entidad certificadora para la implementación de la firma digital solicitada.

- 5.18** El suscriptor debe estar atento a la recepción del correo electrónico emitido por el RENIEC con la aprobación del certificado digital o las observaciones del trámite del certificado digital.

**5.19 Disposiciones necesarias para verificar documentos con firma digital**

- 5.19.1** Los documentos digitales en formato PDF, deben ser validados mediante la plataforma FIRMAPERU utilizando el siguiente enlace:  
<https://apps.firmaperu.gob.pe/web/validador.xhtm>.

- 5.19.2** La plataforma designada es la encargada de verificar la integridad del documento, así como las firmas digitales incrustadas. Los pasos para seguir se encuentran en el numeral 6.2.

- 5.19.3** La Gerencia de Informática difunde el uso de las plataformas para la validación de la firma digital en los documentos emitidos.

**5.20 Requisito necesario para la reproducción de documentos con firma digital**

- 5.20.1** Para expedir una reproducción impresa de un documento firmado digitalmente, primero se debe validar que el documento cumpla con los requisitos mínimos, los cuales son la glosa y el código QR, descritos en el numeral 6.4.

- 5.20.2** Teniendo las glosas y textos incrustados en el documento, el solicitante puede validar tanto el contenido como las firmas digitales.

- La glosa en el documento permite validar el contenido del documento, mediante el código CVD y la plataforma proporcionada por la CPMP:  
<https://www.gob.pe/CPMP/verifica-cvd>.
- Mientras que el texto incrustado en el lateral izquierdo permite validar las firmas digitales mediante la plataforma de FIRMAPERU:  
<https://apps.firmaperu.gob.pe/web/validador.xhtm>.

**5.21 Motivos para solicitar la cancelación de la firma digital**

- 5.21.1** Cuando es solicitado por el titular de la firma digital, previa coordinación y aprobación de la gerencia o jefatura de la unidad orgánica.

**5.21.2** Cuando termina el plazo de vigencia de la firma digital, previa coordinación y aprobación de la gerencia o jefatura de la unidad orgánica.

**5.21.3** Cuando el colaborador cesa en la institución.

**5.22 Motivos para solicitar la revocación del certificado digital**

**5.22.1** Se determine que la información contenida en el certificado digital es inexacta o ha sido modificada.

**5.22.2** A solicitud del Departamento de Recursos Humanos, por desvinculación laboral o fallecimiento.

**5.22.3** Para la cancelación o revocación del certificado digital, es necesario que el Departamento de Recursos Humanos informe oportunamente a la Gerencia informática para su ejecución.

**5.23 Otras recomendaciones para no invalidar documentos con firma digital**

**5.23.1** No unir varios documentos firmados digitalmente de forma independiente en un solo archivo.

**5.23.2** No editar el documento una vez firmado digitalmente.

**5.23.3** No combinar firmas digitales y firmas ológrafas que estén insertadas digitalmente en un mismo documento.

**5.23.4** No colocar sellos, marca de agua, cintillos o similares, en un documento firmado digitalmente.

**5.24 Responsabilidades del suscriptor**

**5.24.1** El suscriptor es responsable del uso y aplicación de la firma digital en los documentos suscritos.

**5.24.2** El suscriptor es responsable del contenido de los documentos electrónicos firmados digitalmente.

**5.24.3** Comunicar a su jefe inmediato superior sobre los cambios en su certificado digital, así como la fecha próxima del término del plazo de vigencia de la firma digital, para su trámite respectivo con la Gerencia de Administración y Finanzas.

**5.24.4** Comunicar a la Gerencia de Informática cualquier incidencia con el equipo o dispositivo asignado para su firma digital.

**5.24.5** Proteger el acceso y uso del equipo o dispositivo en el cual se almacene el certificado digital.

**5.24.6** Dejar de utilizar la clave privada, transcurrido el plazo de vigencia del certificado digital.

**5.25 Responsabilidades de la Gerencia de Administración y Finanzas**

**5.25.1** Solicitar la emisión, renovación o cancelación de los certificados digitales ante la EREP – RENIEC.

**5.25.2** Entregar información veraz en los trámites ante RENIEC, y cumplir las condiciones establecidas por la Entidad de Certificación para el uso del certificado.

**5.26 Responsabilidades de la Gerencia de Informática**

**5.26.1** Instalar y configurar el aplicativo ReFirma propiedad del RENIEC en el equipo asignado del suscriptor para el uso de la firma digital.

**5.26.2** Brindar capacitación y asistencia técnica en el uso del equipo y software asignados para el uso de la firma digital.

**5.26.3** Atender cualquier incidencia técnica de los suscriptores con respecto a la instalación y uso de las firmas digitales.

**5.26.4** Difundir comunicados sobre el uso de la Firma Digital.

**5.26.5** Informar a la Gerencia General sobre la implementación de proyectos de tecnologías, relacionados a la firma digital en la CPMP, como parte de los informes de gestión trimestrales.

**6. DESCRIPCIÓN DE LOS PROCEDIMIENTOS**

**6.1 Atención de requerimiento de firma digital**

**6.1.1** Cada unidad orgánica solicita, mediante memorando, el inicio del trámite para la obtención de la firma digital, a la Gerencia de Administración y Finanzas con copia a la Gerencia de Informática.

- 6.1.2** La Gerencia de Informática y/o la Gerencia de Administración y Finanzas remite a las unidades orgánicas, a través de las asistentes de gerencia, vía correo electrónico y otro medio disponible o de existir alguna actualización, el formato word “declaración jurada de identificación no presencial para solicitar certificado digital - persona jurídica en el marco del Decreto Supremo N° 008-2020-SA y Decreto Supremo 044-2020 y modificatorias, que declara el Estado de Emergencia Nacional” y el formato excel “estructura carga masiva” (datos de los suscriptores) e infografía/instructivo (pasos para rellenar correctamente la DJ), proporcionados por el RENIEC.
- 6.1.3** El suscriptor, completa la citada declaración jurada del RENIEC con sus datos personales, firma y fotografía actual, el formato excel “estructura carga masiva” (datos de los suscriptores) y las declaraciones juradas del correcto uso de firma digital (Anexo 1) y la autorización de descuento del colaborador (Anexo 2), y lo remite mediante memorando, a través de su gerencia, a la Gerencia de Administración y Finanzas con copia a la Gerencia de Informática. La declaración jurada del RENIEC debe ser remitida en archivo PDF y no mayor a 5MB.
- 6.1.4** La Gerencia de Administración y Finanzas registra los datos en la Plataforma Integrada de la entidad de Registro (Plataforma PIER) del RENIEC, con el usuario y contraseña del representante de la entidad ante el RENIEC, en este caso, el Gerente de Administración y Finanzas.
- 6.1.5** La Gerencia de Administración y Finanzas gestiona, el pago del certificado digital de persona jurídica, según establecido en el Texto Único de Procedimientos Administrativos (TUPA) del RENIEC vigente, e ingresa el voucher de pago a la Plataforma PIER del RENIEC.
- 6.1.6** El Gerente de Administración y Finanzas firma digitalmente la autorización para el trámite del certificado digital de persona jurídica, en la Plataforma PIER del RENIEC, que debe emitir respuesta al suscriptor, mediante correo electrónico.
- 6.1.7** Identidad Digital del RENIEC, remite automáticamente, el primer correo electrónico con el siguiente probable título "Aspirante a suscriptor habilitado para la atención de su solicitud de certificado digital", el cual es recepcionado en la bandeja del suscriptor.
- 6.1.8** Posteriormente, el suscriptor recibe el segundo correo electrónico de

Identidad Digital del RENIEC, con el siguiente probable título: “Contrato y solicitud de emisión del certificado digital de persona jurídica”. Asimismo, el primer y el segundo correo electrónico que son emitidos por el RENIEC son de carácter informativo.

- 6.1.9** Finalmente, el suscriptor recibe el tercer y último correo electrónico de Identidad Digital del RENIEC, con el siguiente probable título: “Aprobación de solicitud del certificado digital de persona jurídica” o “Denegación”.
- 6.1.10** En caso el trámite ha tenido como resultado una “Denegación”, y de ser las observaciones subsanables, entonces la Gerencia de Informática, brinda el soporte para subsanar las observaciones, caso contrario se da por finalizado el trámite y se informa el resultado a la unidad orgánica solicitante mediante un memorando u otro medio que se estime conveniente.
- 6.1.11** En caso el trámite haya resultado exitoso, el suscriptor debe comunicar a la Gerencia de Informática, mediante la generación de una Solicitud de Trabajo (SDT), o mediante correo electrónico, estableciendo un plazo no mayor de cinco (5) días hábiles para su atención. La Gerencia de Informática debe brindar el soporte correspondiente en la descarga del certificado digital al medio de descarga del suscriptor.
- 6.1.12** La Gerencia de Informática procede a configurar el certificado digital, en el medio de descarga asignado (*token* o computador personal). El suscriptor toma posesión de su certificado digital asignándole una clave única e intransferible, convirtiéndose desde ese momento en el titular de su firma digital, asumiendo la responsabilidad total de su uso.
- 6.1.13** La Gerencia de Informática procede a instalar el *software* de firma digital, debidamente acreditado por la Autoridad Administrativa Competente (AAC) de la Infraestructura Oficial de Firma Electrónica (IOFE), ReFirma propiedad del RENIEC, en el computador personal del suscriptor.
- 6.1.14** La Gerencia de Informática realiza la capacitación a los titulares de firma digital, en el uso de la firma digital.
- 6.1.15** La Gerencia de Informática comunica a la unidad orgánica la implementación de la firma digital solicitada.

## **6.2 Verificación de documentos con firma digital**

- 6.2.1** Obtener el documento digital en formato PDF, a verificar.

**6.2.2** El suscriptor accede a la plataforma “FIRMA PERÚ”: <https://apps.firmaperu.gob.pe/web/validador.xhtml>, y selecciona el archivo que contiene el documento firmado digitalmente.

**6.2.3** La plataforma verifica el documento y emite un mensaje final, el cual puede ser conforme u observado, este último ocurre cuando la integridad del documento y/o de alguna(s) de la(s) firma(s) ha sido comprometida indicando las posibles causas.

### **6.3 Cancelación o Revocación de certificado digital**

**6.3.1** La cancelación de un certificado digital puede solicitarse de acuerdo con los motivos descritos en el numeral 5.21.

**6.3.2** La revocación de un certificado digital puede efectuarse por los motivos descritos en el numeral 5.22.

**6.3.3** Para iniciar la cancelación o revocación de un certificado digital, el departamento de Recursos Humanos coordina con la Gerencia de Informática, mediante un Memorándum o Solicitud de Trabajo, en el cual indica el tipo de operación y el motivo.

**6.3.4** La Gerencia de Informática procede a realizar las coordinaciones con la Gerencia de Riesgos y Desarrollo y se procede a ejecutar el pedido de cancelación o revocación.

### **6.4 Reproducciones impresas de documentos con firma digital**

**6.4.1** El suscriptor utiliza la plantilla distribuida por la Gerencia Informática, para generar el documento PDF, el cual considera los textos predefinidos y glosas según los lineamientos dispuestos en la Directiva N° 002-2021-PCM/SGTD.

**6.4.2** Dicho documento cuenta con los siguientes elementos para su verificación:

- a) **Glosa de representación imprimible:** De acuerdo al artículo 8 “Glosa de una representación imprimible” de la Directiva N°002-2021-PCM/SGTD, la glosa de representación imprimible está compuesta por una nota informativa que es colocada en la parte inferior de cada página del documento, la cual contiene como mínimo la siguiente información:

- Leyenda informativa
- URL de verificación
- Código QR
- CVD

Como se evidencia a continuación, se utiliza el tipo de letra “Courier New” en número 8 y la sección de URL y CVD en número 10.

Esta es una representación impresa cuya autenticidad puede ser contrastada con la representación imprimible localizada en la sede digital de la Caja de Pensiones Militar Policial. La representación imprimible ha sido generada atendiendo a lo dispuesto en la directiva N°002-2021-PCM/SGTD. La verificación puede ser efectuada a partir de la fecha de emisión del documento. Base Legal: Decreto Legislativo N°1412, Decreto Supremo N°029-2021-PCM y la Directiva N°002-2021-PCM/SGTD.



URL: <https://validador.lacaja.com.pe/>  
CVD: 0000 0000 0000 0000

- b) Texto Vertical:** Se puede incluir, según el artículo 10° “Firma digital de la representación imprimible” de la Directiva N°002-2021-PCM/SGTD, un texto en la parte lateral izquierda, donde se indica el mecanismo para validar la autenticidad de la firma digital.

Documento electrónico firmado digitalmente en el marco de la Ley N°27269, su Reglamento y modificatorias. Su autenticidad e integridad pueden ser verificadas en <https://apps.firmaperu.gob.pe/web/validador.xhtml>.

- 6.1.1** El suscriptor debe verificar los datos importantes en el documento como la fecha de emisión y colocar el CVD generado en el sistema de trámite documentario; los otros elementos mencionados no deben ser alterados o retirados del documento.
- 6.1.2** Luego, debe convertir el documento a formato PDF, el cual debe ser firmado de forma digital.
- 6.1.3** Posterior a la firma digital del documento, este no debe ser alterado o editado.

## **6.5 Servicio de verificación de representaciones impresas**

- 6.5.1** La CPMP ha implementado un servicio de verificación de las representaciones impresas a fin de comprobar su autenticidad; mediante la URL indicada en la glosa de representación imprimible, indicada en el numeral 6.4.2.

- 6.5.2** A fin de verificar la autenticidad de las representaciones impresas, se debe ingresar a la URL indicada en el numeral anterior y se debe completar el formulario ingresando el CVD del documento y la fecha de emisión, en caso se requiera. Luego se presiona el botón de búsqueda y el sistema busca el documento.
- 6.5.3** Al encontrarse el documento, este es visualizado en la pantalla, caso contrario se recibe un mensaje indicando que el documento no fue encontrado.
- 6.5.4** En caso de que se desee verificar las firmas digitales del documento, se debe realizar los pasos establecidos en el numeral 6.2.

## **7 ANEXOS**

- Anexo 1: Declaración jurada de correcto uso de firma digital.
- Anexo 2: Declaración jurada de autorización de descuento del colaborador.

**CAJA DE PENSIONES MILITAR POLICIAL**

**DECLARACIÓN JURADA DE CORRECTO USO DE FIRMA DIGITAL**

Yo, \_\_\_\_\_, identificado(a) con DNI N° \_\_\_\_\_,  
con domicilio en \_\_\_\_\_, distrito de \_\_\_\_\_,  
colaborador de la CAJA DE PENSIONES MILITAR POLICIAL.

**DECLARO BAJO JURAMENTO**

Que, me comprometo a hacer un buen uso de la firma digital que se ha tramitado para mi desempeño personal en las labores del trabajo, conforme a lo señalado en el artículo 5 de la Ley N° 27269 – Ley de Firmas y Certificados Digitales; artículo 10 del Decreto Supremo N°052-2008-PCM – Reglamento de la Ley de Firmas y Certificados Digitales; y al numeral 5.2.6 del Código de Ética y Conducta Profesional de la CPMP.

En caso no cumpla con lo anteriormente señalado, quedo sujeto a las sanciones correspondientes ocasionados por falta de diligencia al compromiso asumido; en caso de ocasionar un perjuicio a la CPMP, que conlleve a la aplicación de lo estipulado en el artículo 15-A sobre infracciones y sanciones de la Ley N° 27269.

Firma en Lima, a los \_\_\_\_ días del mes de \_\_\_\_\_ del año 202\_\_

\_\_\_\_\_

DNI N° \_\_\_\_\_

**DECLARACIÓN JURADA DE AUTORIZACIÓN DE DESCUENTO DEL  
COLABORADOR**

Yo, \_\_\_\_\_, identificado(a) con DNI N° \_\_\_\_\_, con domicilio en \_\_\_\_\_, distrito de \_\_\_\_\_, colaborador de la CAJA DE PENSIONES MILITAR POLICIAL.

**DECLARO BAJO JURAMENTO**

Que, me comprometo a comunicar a la Gerencia de Informática, la aprobación de la solicitud del certificado digital dentro del plazo de cinco (5) días hábiles, contados desde la recepción del correo electrónico emitido por el RENIEC con la aprobación del certificado digital o las observaciones del trámite del certificado digital.

Así mismo, en caso no brinde aviso oportuno a la Gerencia de Informática para la descarga del certificado digital o para la subsanación de las observaciones, autorizo el descuento correspondiente por los gastos derivados de la caducidad del certificado digital que origine un nuevo trámite y costo adicional, como consecuencia del incumplimiento de lo indicado en el plazo establecido.

Firma en Lima, a los \_\_\_\_ días del mes de \_\_\_\_\_ del año 202\_\_

\_\_\_\_\_

Firma y huella