GOBIERNO REGIONAL DEL CALLAO

C.A.F.E.D.

Directiva N° 003-2026-CAFED

"LINEAMIENTOS GENERALES PARA EL USO DE FIRMA Y CERTIFICADO DIGITAL EN EL COMITÉ DE ADMINISTRACIÓN DEL FONDO EDUCATIVO DEL CALLAO – CAFED"

Febrero
2026

"LINEAMIENTOS GENERALES PARA EL USO DE FIRMA Y CERTIFICADO DIGITAL EN EL COMITÉ DE ADMINISTRACIÓN DEL FONDO EDUCATIVO DEL CALLAO – CAFED"

DIRECTIVA GENERAL Nº 003-2025-CAFED/GPP

FORMULADA POR: GERENCIA DE PLANIFICACIÓN Y PRESUPUESTO

1. Objetivo

Establecer los lineamientos para fortalecer la seguridad de la información, la celeridad de los procesos y la transparencia en la gestión de los documentos internos y externos, se establece la presente directiva para regular el uso de la firma y certificado digital en las funciones y actuaciones de los colaboradores del CAFED y cumplir con el proceso de Implementación del Gobierno y Transformación Digital.

2. Finalidad

Implementar y optimizar la gestión de los documentos internos mediante el uso de las firmas digitales en los Sistemas de Información tales como el Sistema de Gestión de Documentos (SGD) ente otros, mejorando la eficiencia, seguridad y accesibilidad de la información, al tiempo que se garantiza la validez legal y la integridad de los documentos digitalizados.

3. Alcance

La presente Directiva es de aplicación y cumplimiento para todo el personal que use el Sistema de Gestión Documental – SGD y/o genere documentos de gestión interna en todas las áreas del CAFED, que cuenten con un certificado digital activo, y que, en ejercicio de sus funciones, firmen digitalmente documentos electrónicos en el marco de los órganos y unidades orgánicas asignadas

4. Base Legal

4.1. Constitución Política del Perú de 1993 y sus modificatorias.

4.2. Ley Nº 27867, Ley Orgánica de Gobiernos Regionales.

4.3. Ley N° 29626 - Ley de Presupuesto del Sector Publico para el Año Fiscal 2011, a través del literal m) de la Vigésima Novena Disposición Final Transitoria, crea el Comité de Administración del Fondo Educativo del Callao – CAFED, a través del literal m) de la Vigésima Novena Disposición Final Transitoria, crea el Comité de Administración del Fondo Educativo del Callao – CAFED. Ley N° 29775, Ley que precisa los programas a cargo del Fondo Educativo de la Provincia Constitucional del Callao. Ley N° 27613, Ley de Participación en Rentas de Aduanas.

4.7. Ley N° 30878, Ley que modifica la Ley N° 27613 y la Ley N° 29775.

4.8. Ordenanza Regional N° 00007 de fecha 25 de enero del 2011, modificado mediante Ordenanza Regional N° 00004 del 21 de febrero del 2012, que aprueba el Reglamento de Organización y Funciones (ROF) del Comité de Administración del Fondo Educativo del Callao – CAFED.

4.9. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.

4.10. Decreto Supremo Nº 030-2002-PCM, Decreto Supremo que aprueba el Reglamento de la ley Marco de Modernización de la Gestión del Estado.

4.11. Decreto Supremo Nº 103-2022-PCM, Decreto Supremo que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030.

4.12. Ley Nº 27444, Ley del Procedimiento Administrativo General y sus modificatorias.

4.13. Ley Nº 27867, Ley Orgánica de Gobiernos Regionales y sus modificatorias.

4.14. Ley Nº 28716, Ley del Control Interno de las entidades del Estado.

4.15. Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.

4.16. Resolución Ministerial N.º 246-2007-PCM, del 22 de agosto de 2007, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

4.17. Ley Nº 27269, Ley de Firmas y Certificados Digitales, y sus normas ampliatorias, modificatorias.

4.18. Resolución de Secretaría de Gobierno y Transformación Digital N° 007-2024-PCM/SGTD.

4.19. Ley Nº 27658, Ley Legislativo que aprueba la Ley de Gobierno Digital.

4.20. Decreto Supremo Nº 103-2022-PCM, el cual aprueba la Política Nacional de Modernización de la Gestión Pública al 2030.

4.21. Decreto Supremo Nº 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.

4.22. Decreto Supremo Nº 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo Nº 1412, Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.

4.23. Decreto Legislativo Nº 681: Regula el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la información elaborada en forma convencional y la producida por procedimientos informáticos en computadoras.

4.24. Decreto Legislativo Nº 827: Amplían los alcances del D.L. N° 681 a las entidades públicas a fin de modernizar el sistema de archivos oficiales.

4.25. Decreto Legislativo N° 1310, Aprueba medidas adicionales de simplificación administrativa.

4.26. Decreto Supremo N° 081-2013-PCM, que aprueba la Política de Gobierno Electrónico 2013-2017.

4.27. Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.

4.28. 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, Reglamento de la Ley de Firmas y Certificados Digitales.

4.29. Decreto Supremo N° 070-2011-PCM, que modifica el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados y establece normas aplicables al procedimiento registral en virtud del Decreto Legislativo N° 681 y Ampliatorias.

4.30. Decreto Supremo N° 033-2018-PCM que crea la Plataforma Digital Única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital.

5. Disposiciones Generales

5.1. Los funcionarios, deberán velar por el uso correcto de la firma digital en sus respectivas oficinas.

5.2. Es valido el uso de la firma digital en cualquier documento que generen los sistemas de información que maneja la Institución, tales como el SGD, SIGA, SIAF y otros sistemas que maneje o implemente la entidad.

5.3. El uso de la contraseña de su firma y certificado digital es intransferible, siendo responsabilidad del suscriptor el uso de la firma en cualquier documento electrónico usando su usuario y contraseña.

5.4. Emplear adecuadamente el uso del certificado digital conforme a lo establecido en la Ley N° 27269 Ley de Firmas y Certificados Digitales, su Reglamento y sus Modificatorias.

5.5. Los documentos que serán afectos a la firma digital serán de uso interno y externo, entre los cuales detallamos a continuación:

- ✓ Documentos internos, tales como: Memorando, Oficio, Informe y los demás que se generan de manera interna en la entidad.
- ✓ Documento externo, tales como: Resoluciones, Carta, Oficio, Actas de concejo y los demás que genere la Institución.

5.6. Los documentos para firmar y certificar deberán estar en formato PDF, siendo cada usuario responsable de la conversión al formato PDF con los aplicativos instalados en su equipo computacional por el personal de la oficina de OTIC.

5.7. Una vez firmado un documento ya no será posible su modificación, solo pudiendo agregar firmas digitales o vistos buenos según sea necesario.

5.8. Para la verificación del registro de la firma digital de un documento firmado en el Sistemas de Gestión Documental (SGD) o para firma digital de otros documentos, se utilizará el software de firma digital autorizados tales como (REFIRMA, FIRMA ONPE) según lo designe la oficina de OTIC.

5.9. Un documento electrónico puede contar con una o varias firmas digitales de diferentes funcionarios, especialistas y otros colaboradores de la entidad.

5.10. En el caso que se necesite imprimir un documento firmado digitalmente, se puede realizar siendo la impresión una copia simple del documento electrónico firmado digitalmente.

5.11. Los documentos deberán tener un pie de página que indique el número de páginas que contiene el documento a ser firmado digitalmente (Pág. 1 de X).

6. Disposiciones Especificas

6.1. Procedimiento de Emisión de Firma y Certificado Digital

6.1.1. El trámite de la firma y certificado digital se inicia con la solicitud que genera el área usuaria cuando tiene ingreso de un nuevo personal que a su vez tendrá que presentar documentos y ser firmados digitalmente. (Anexo N° 01: Solicitud De Emisión / Cancelación De Firma Y Certificado Digital)

6.1.2. La Gerencia General se encargará de la aprobación de la nueva firma y certificado digital en el CAFED, en coordinación con la Oficina de OTIC.

6.1.3. La Oficina de Tecnologías de la Información y Comunicaciones (OTIC) se encargará de la gestión de los certificados digitales en el CAFED. Sus responsabilidades incluyen la custodia técnica de los repositorios, la emisión, revocación de certificados digitales y el soporte técnico a los usuarios. Esto asegura la seguridad y el correcto funcionamiento de los certificados digitales, un elemento crucial para la autenticación y la seguridad de la información en el entorno del CAFED, garantizando su validez y disponibilidad.

6.1.4. El responsable de la oficina de OTIC, deberá iniciar el proceso para obtener la firma digital. Para lo cual efectuara los siguientes pasos:

- ✓ Coordinar el pago por el derecho a la firma digital con el área que maneje la caja chica o a quien corresponda de la institución, que se realice el pago. Código de concepto a pagar es el (00529 - Emisión De Certificados Digitales Para Entidades De La Administración Pública, registrar el RUC de la Institución N° 20543026574).
- ✓ Una vez realizado el pago (después de dos (02) horas en promedio para la respuesta de RENIEC para la emisión del Certificado Digital), registrar los datos del suscriptor de la nueva firma digital a través de la plataforma integrada de la entidad de registro del EREP-RENIEC (https://erep.reniec.gob.pe/pier/login.jsf).
- ✓ En el portal EREP RENIEC, se deberá aprobar el alta de la nueva firma solicitada.

6.1.5. Una vez aprobada la suscripción de la firma digital el personal técnico de la oficina de OTIC, procederá con la instalación del certificado digital en el equipo de cómputo asignado al nuevo personal.

6.1.6. En el proceso de instalación del certificado digital se solicitará que el suscriptor ingrese una contraseña que fue enviada al correo registrado en la solicitud de nueva firma digital, la cual servirá para que pueda firmar a partir de ese momento los documentos electrónicos.

6.1.7. En el caso de que la entidad considere que se use otro dispositivo para el certificado digital como un Token Criptográfico u otro dispositivo de almacenamiento del certificado digital. Se solicitará que el suscriptor de la nueva firma ingrese un PIN, el cual servirá para que pueda firmar a partir de ese momento los documentos electrónicos.

6.2. Procedimiento de Uso de la Firma y Certificado Digital de los Suscriptores

6.2.1. Para que el suscriptor pueda usar la firma digital en los documentos electrónicos, debe contar con el certificado digital, un dispositivo electrónico de seguridad que almacene su clave privada (TOKEN Criptográfico y/o computador) y el software de firma digital.

6.2.2. Los suscriptores harán uso de los certificados digitales para para firmar digitalmente los documentos electrónicos de acuerdo con las funciones y/o procedimientos de su competencia.

6.2.3. En relación con el uso de la clave privada del certificado digital por parte del suscriptor este deberá cumplir con lo siguiente:

- ✓ Mantener el control y absoluta reserva de la clave privada bajo su responsabilidad y debe ser conocida únicamente por el suscriptor.
- ✓ Salvaguardar su contraseña o PIN de acceso de forma diligente, tomando las precauciones para evitar su perdida, revelación, modificación o uso no autorizado.
- ✓ El suscriptor es responsable del correcto uso y seguridad del Certificado Digital instalado en su equipo de cómputo y de los documentos a procesar para la firma digital.

6.3. Procedimiento de Uso de la Firma Y Certificado Digital en los Documentos

6.3.1. Los suscriptores son los responsables del contenido de los documentos electrónicos firmados digitalmente.

6.3.2. Si un documento contiene más 1 de página, cuando se realice la firma y certificado digital aplica para todo el documento sin importar el número de páginas, solo la primera hoja contendrá la firma y certificado digital, pero será válido para todas las páginas que contenga el documento.

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

6.3.4. Para firmar digitalmente un documento electrónico, deberá usar el Sistema de Gestión Documental (SGD) el cual está preparado para acceder al software autenticador de Firmas Digitales.

6.3.5. Para el caso de otro documento que no se generaron por el SGD, deberán utilizar el software homologado como el REFIRMA o FIRMA ONPE entre otros. para firmar y validar el certificado digital.

6.4. Procedimiento de Cancelación y Anulación de la Firma y Certificado Digital

6.4.1. En caso de extravío o pérdida de la tarjeta inteligente o el token criptográfico, el uso de su firma digital queda protegido mediante el PIN de acceso o contraseña, impidiendo que terceros no autorizados puedan utilizarla

6.4.2. En caso de que la clave privada quede comprometida, el suscriptor deberá notificarlo de inmediato al administrador de certificados digitales, para proceder con la revocación del certificado digital

6.4.3. Cuando la oficina solicitante, haya consignado información errada.

6.4.4. Por perdida de Token USB o llave criptográfica.

6.4.5. Por rotación de funcionarios y/o colaboradores, que cuenten con certificado digital.

6.4.6. Cuando el suscriptor finalice su vínculo laboral.

6.4.7. Cuando el suscriptor del certificado digital, solicite al administrador de los certificados digitales la cancelación, cuando sospeche que su contraseña está comprometida.

6.4.8. En caso de que el suscriptor renuncie o deje de laborar, la oficina a la cual pertenece deber presentar la solicitud de cancelación del certificado digital al Administrador de los Certificados Digitales.

7. Responsabilidades

7.1. Del Administrador del Certificado Digital

7.1.1. Entregar información veraz durante la solicitud de emisión de certificados y demás procesos: suspensión, anulación, cancelación ante RENIEC.

7.1.2. Cumplir permanentemente las condiciones establecidas por la Entidad de Certificación para la utilización del Certificado.

7.1.3. Solicitar la generación, renovación, actualización, cancelación o anulación de los certificados digitales ante la EREP-RENIEC.

7.1.4. El Administrador del Certificado Digital solicita a la EREP-RENIEC la emisión y cancelación de los certificados digitales de los suscriptor/a, asumiendo las obligaciones del Titular de la entidad, estipuladas en el artículo 15 del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado con Decreto Supremo N° 052- 2008-PCM.

7.2. De la Oficina de Tecnologías de la Información y Comunicaciones OTIC

7.2.1. Brindar capacitación y asistencia técnica en el uso del dispositivo de almacenamiento de certificado digital o token criptográfico.

7.2.2. Atender las incidencias técnicas de los suscriptores con respecto a la instalación de los certificados digitales y uso de las firmas digitales bajo las plataformas de Firma Digital como el REFIRMA, FIRMA ONPE, PERUFIRMA.

7.2.3. Atender las incidencias técnicas de los usuarios respecto a las fallas e instalación del software de los certificados y firmas digitales bajo las plataformas autorizadas y reconocidas como el REFIRMA y FIRMA ONPE.

7.2.4. La Oficina de OTIC, será la única encargada de instalar y configurar en los equipos de cómputo el software del certificado digital.

7.3. De los Suscriptores

7.3.1. Todo suscriptor que tiene asignado un token u otro dispositivo de almacenamiento de certificado digital es responsable de cambiar el PIN para su uso (al menos una vez al mes). Puede realizar los cambios de PIN que considere convenientes a través de la opción de gestión de dispositivo, pudiendo solicitar el

apoyo de la Oficina de OTIC, siendo responsable de mantener la confidencialidad de la misma.

7.3.2. Emplear adecuadamente su certificado digital, conforme a la normativa vigente.

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

7.3.4. Proteger el acceso al repositorio del certificado digital (computador, tarjeta inteligente, token criptográfico).

7.3.5. Las Oficinas de la institución deberán presentar una solicitud de alta/baja de firma y certificado digital a la Oficina de Gerencia General / Oficina de Tecnologías de la Información y Comunicaciones OTIC, mediante un documento con los siguientes datos que se detallan en el Anexo 01: Solicitud de Alta / Baja de Firma Y Certificado Digital

8. Disposiciones Complementarias

Primera. Vigencia. La presente Directiva entrará en vigor al día siguiente de su publicación en el Portal de Transparencia Estándar y el Portal Institucional del CAFED

Segunda. Responsabilidad. -´ La Oficina de la Gerencia General, es la responsable de la Aprobar las solicitudes de nuevas firmas y certificados digitales y el cumplimiento de la presente directiva, en coordinación de soporte con la Oficina de OTIC.

Tercera. Revisión. - Las Directivas aprobadas deben ser revisadas cada dos (2) años por los órganos proponentes, con el fin de verificar su vigencia o la pertinencia de su aplicación.

9. Anexos

9.1. Anexo 01: Glosario de Términos y Definiciones

9.1.1. Firma digital: es aquella firma electrónica que además utiliza una técnica de criptografía asimétrica, que permite la identificación del signatario y que ha sido creada por medios, incluso a distancia, que garantizan que éste mantiene bajo su control con un elevado grado de confianza, de manera que está vinculada únicamente al signatario y a los datos a los que refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior. Tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita, siempre y cuando haya sido generada por un Prestador de Servicios de Certificación Digital debidamente acreditado que su encuentre dentro de la Infraestructura Oficial de Firma Electrónica y que no medie ninguno de los vicios de la voluntad previstos en el Título VIII del Libro IV de Código Civil.

9.1.2. Autenticación digital de documentos: Acto realizado por el fedatario institucional, quien verifica, mediante cotejo entre el documento físico presentado y su versión digitalizada, la fidelidad, integridad y legibilidad de esta última. Para ello, firma electrónicamente el documento digitalizado utilizando su certificado digital. La autenticación se limita a este proceso y no implica un pronunciamiento sobre el contenido de la información del documento.

9.1.3. Copia fiel al original: Declaración del fedatario institucional que certifica que la información contenida en el documento físico presentado durante el procedimiento registral es equivalente a la de su versión digital, garantizando que ambas representaciones mantienen la misma integridad y exactitud en el contenido.

9.1.4. Digitalización: Conjunto de procesos, procedimientos y recursos informáticos que operan como una unidad de producción para convertir documentos físicos en formatos digitales. La digitalización involucra desde la preparación inicial de los documentos hasta su almacenamiento final como archivos digitales autenticados.

9.1.5. Documento electrónico: Unidad básica de información estructurada que puede ser clasificada, transmitida, procesada o conservada mediante medios

electrónicos, sistemas de información u otros similares. Tiene el mismo valor legal que los documentos en soporte papel, de conformidad con la normativa vigente.

9.1.6. Documento físico: Instrumento textual o gráfico que contiene información, hechos fijados o registrados en un material de soporte, utilizado para verificar o acreditar una situación específica.

9.1.7. Documento original: Documento físico que constituye la primera manifestación completa y fidedigna de su contenido, conservando todas las características y elementos que garantizan su autenticidad, integridad y valor probatorio como.

9.1.8. Certificado Digital: es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.

9.1.9. Firmante: Es quien crea una firma electrónica en cualquiera de sus modalidades (simple, avanzada o firma digital).

9.1.10. 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.

9.1.11. Token Criptográfico: Es un dispositivo de almacenamiento criptográfico que contiene el Certificado Digital asignado a la persona titular del mismo, que le permite firmar digitalmente. El token u otro dispositivo de almacenamiento de certificado digital cumplen con el estándar FIPS 140-2, según convenio suscrito con el RENIEC.

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

9.2. Anexo N° 02: Solicitud de Emisión / Cancelación de Certificado Digital

Solicitud de:

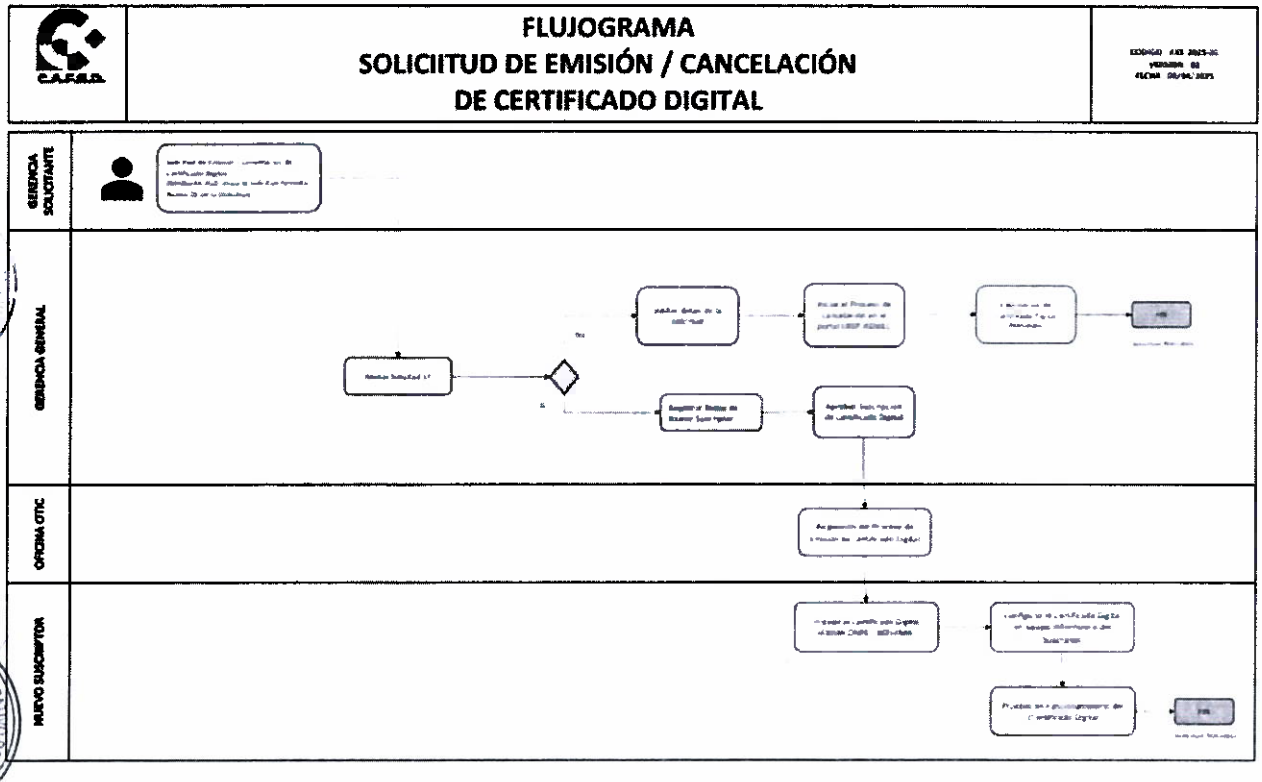
Emisión		Cancelación	

Yo,.....identificado con Documento Nacional de Identidad DNI N°.....,con el correo electrónico....., autorizo al Comité de Administración del Fondo Educativo del Callao – CAFED, en coordinación con la Oficina de Tecnologías de la Informacion OTIC la gestión del certificado digitale; en el Sistema Administrativo de Certificación Digital los datos, y su posterior envio a la EREP-RENIEC.

Atentamente,

Firma y Sello del
Gerencia Solicitante

9.3. Anexo N° 03: Diagrama de Flujo de Emisión / Cancelación de Certificado Digital



C.A.F.E.D.

Procedimiento Gestión de Firmas y Certificados Digitales

Código: PR-SGSI-21

Índice

I. Base Legal
II. Objetivo
III. Alcance
IV. Procedimiento
4.1 Autorización del Certificado Digital del Suscriptor
4.2 Cancelación del Certificado Digital Para la Firma Digital de Suscriptores
V. Responsabilidades
VI. Registro y Actualización de las Altas y Bajas de Suscriptores
VII. Aprobación y Revisión
VIII. Registros, Controles y Documentos Relacionados
IX. Control de Cambios
X. Anexos
10.1 Anexo N° 01: Solicitud de Emisión / Cancelación de Certificado Digital
10.2 Anexo N° 02: Diagrama de Flujo de Emisión / Cancelación de Firma Certificado Digital
10.3 Anexo N° 03: Glosario de Términos y Definiciones

I. Base Legal

1.1. Ley N° 27269, Ley de Firmas y Certificados Digitales.

1.2. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.

1.3. Decreto Supremo N° 052-2008-PCM, Reglamento de la Ley de Firma y Certificados Digitales.

1.4. Resolución Ministerial N° 001-2013-EF/10, de fecha 02 de enero de 2013, en donde se delegan facultades, funciones y atribuciones en diversos funcionarios del Ministerio.

1.5. Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.

1.6. Convenio de Colaboración interinstitucional de Certificación Digital en el marco del Decreto Supremo N° 070-2011-PCM y Decreto Supremo N° 105- 2012- PCM.

1.7. 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.

II. Objetivo

Establecer los lineamientos para regular la emisión y revocación de firmas y certificados digitales y el soporte a usuarios. Para asegurar la seguridad y el correcto funcionamiento de los certificados digitales, crucial para la autenticación, garantizando su validez, disponibilidad y la seguridad de la información en los Sistemas de Información del CAFED.

III. Alcance

El presente procedimiento alcanza al Titular de la entidad, así como a los funcionarios, trabajadores y colaboradores que hayan sido autorizados para el uso de Firmas o Certificados Digitales.

IV. Procedimiento

4.1 Autorización del Certificado Digital del Suscriptor

- El trámite de un nuevo certificado digital se inicia con la solicitud que genera el área usuaria y es enviada mediante el Sistema de Gestión Documental (SGD) a la Gerencia General, quien en coordinación con la Oficina de Tecnologías de la Informacion (OTIC), son los encargados de iniciar el Proceso de la Nueva Firma o Certificado Digital. Asimismo, el área usuaria, tendrá que presentar el Anexo N° 01: Solicitud De Emisión / Cancelación De Firma Y Certificado Digital.

- Para iniciar el proceso de suscripción, el nuevo suscriptor debe tener el DNI electrónico 2.0 o superior. Además, es necesario obtener la clave digital que RENIEC genera al emitir este documento.

- La oficina de OTIC, deberá iniciar el proceso para obtener la firma digital. Para lo cual efectuara los siguientes pasos:
  - ✓ Coordinar el pago por del derecho del nuevo certificado digital con el área que maneje la caja chica y/o a quien corresponda en la institución y que se realice el pago. Código de concepto a pagar es el **(00529 - Emisión De Certificados Digitales Para Entidades De La Administración Pública, con el ruc de la entidad 20543026574)**.
  - ✓ Luego de realizar el pago se registra los datos del suscriptor de la nueva firma digital a través de la plataforma integrada de la entidad de registro del EREP-RENIEC (https://erep.reniec.gob.pe/pier/login.jsf).
  - ✓ En el portal EREP RENIEC, se deberá aprobar el alta de la nueva firma solicitada.

- Una vez registrada la información en el "Sistema Administrativo de Certificado Digital", la EREP-RENIEC remite vía correo electrónico del suscriptor los Documentos de Compromiso de Uso del Certificado Digital - EREP - RENIEC de los futuros Suscriptores, para la descarga y firma de cada Suscriptor.

- Concluido el registro de Suscriptores, la oficina de OTIC informará mediante documento en el sistema SGD a la unidad orgánica solicitante del nuevo certificado digital y comenzará el proceso de instalación, configuración y capacitación de uso del certificado digital, en el equipo informático asignado del nuevo suscriptor.

- El "Suscriptor" verifica la operatividad necesaria para el uso de la "Firma Digital" y procede a la firma de la solicitud dando la conformidad con la instalación de los componentes necesarios para la operatividad de la firma digital y la capacitación correspondiente, en coordinación con el responsable de OTIC.

- Dichas solicitudes serán resguardadas por la oficina de OTIC para su registro, control y futuras referencias.

4.2 Cancelación del Certificado Digital Para la Firma Digital de Suscriptores

El trámite de cancelación del Certificado Digital efectuado por el Suscriptor, debe cumplir con lo siguiente:

- La Gerencia del Área solicitante, en el cual presta servicios el "Suscriptor" deberá solicitará a la oficina de OTIC, a través de memorando, la cancelación del "Certificado Digital de Suscriptor". Dicho requerimiento deberá ser acompañado por el formato descrito en el Anexo N° 01: Solicitud de Emisión / Cancelación de Certificado Digital.

- La cancelación del "Certificado Digital de Suscriptor' 'puede proceder por los siguientes motivos:
  - ✓ La reserva sobre la clave privada se haya visto comprometida.
  - ✓ La culminación de labores dentro de la institución.
  - ✓ Se revoque las facultades para el uso de la firma o certificado digital.
  - ✓ La información contenida en el Certificado Digital ya no resulte correcta.

- De corresponder la cancelación de la "Firma Digital de Suscriptor", la oficina de OTIC debe registrar la baja en el "Sistema Administrativo de Certificado Digital – EREP-RENIEC ". Posteriormente, confirmará dicha cancelación, para que proceda a retirar los recursos y servicios relacionados para el funcionamiento del Certificado Digital.

V. Responsabilidades

- La información proporcionada indica que los funcionarios, trabajadores y colaboradores que posean una firma o certificado digital deben utilizarla personalmente para firmar documentos. Se enfatiza la responsabilidad de evitar que terceros utilicen las claves asignadas. Esto sugiere la importancia por la seguridad y la integridad de los documentos electrónicos, y destaca la importancia de la autenticación personal en el proceso de firma digital.

- Tras recibir el "Certificado Digital de Suscriptor" para la "Firma Digital", los funcionarios y servidores autorizados asumen la autenticidad de los documentos generados con la firma digital. Esto implica la aceptación de las consecuencias legales y la responsabilidad sobre la veracidad de la información contenida en los documentos firmados. Se comprometen a que la firma digital representa su voluntad, con validez legal. Este proceso es fundamental para la seguridad y validez de los documentos electrónicos, estableciendo la responsabilidad clara de los firmantes.

- La Oficina de Tecnologías de la Información y Comunicaciones (OTIC) asume un rol fundamental en la gestión de certificados digitales dentro del CAFED. Sus responsabilidades abarcan la custodia técnica de repositorios, la emisión y revocación de certificados, y el soporte a usuarios. Estas tareas son cruciales para garantizar la seguridad, autenticación y correcta operación de los certificados digitales, asegurando su validez y disponibilidad dentro del entorno del CAFED. Esto implica la protección de la información y la confianza en las transacciones digitale.

VI. Registro y Actualización de las Altas y Bajas de Suscriptores

- La oficina de OTIC deberá llevar un registro actualizado de las autorizaciones y cancelaciones de los "Certificados Digitales de Suscriptor".

- Asimismo, la oficina de OTIC, debe llevar un registro actualizado de los usuarios, equipos y detalles respecto de la instalación y habilitación de los medios que otorguen la operatividad de la firma digital en el Ministerio.

VII. Aprobación y Revisión

Este documento será revisado anualmente y aprobado por el Comité de Gobierno y Transformación Digital.

VIII. Registros, Controles y Documentos Relacionados

Código	Tipo	Descripción	Responsable
FR-SGSI-29	Formato	Solicitud de Emisión-Cancelación de Certificado Digital	Oficina de OTIC / Oficial de Seguridad de la Información

IX. Control de Cambios

Versión	Fecha	Ítem	Persona que Solicito el Cambio	Descripción del Cambio
1	10/11/2025	N/A	N/A	Versión Inicial

V. Anexos

10.1 Anexo N° 01: Solicitud de Emisión / Cancelación de Certificado Digital

Solicitud de:

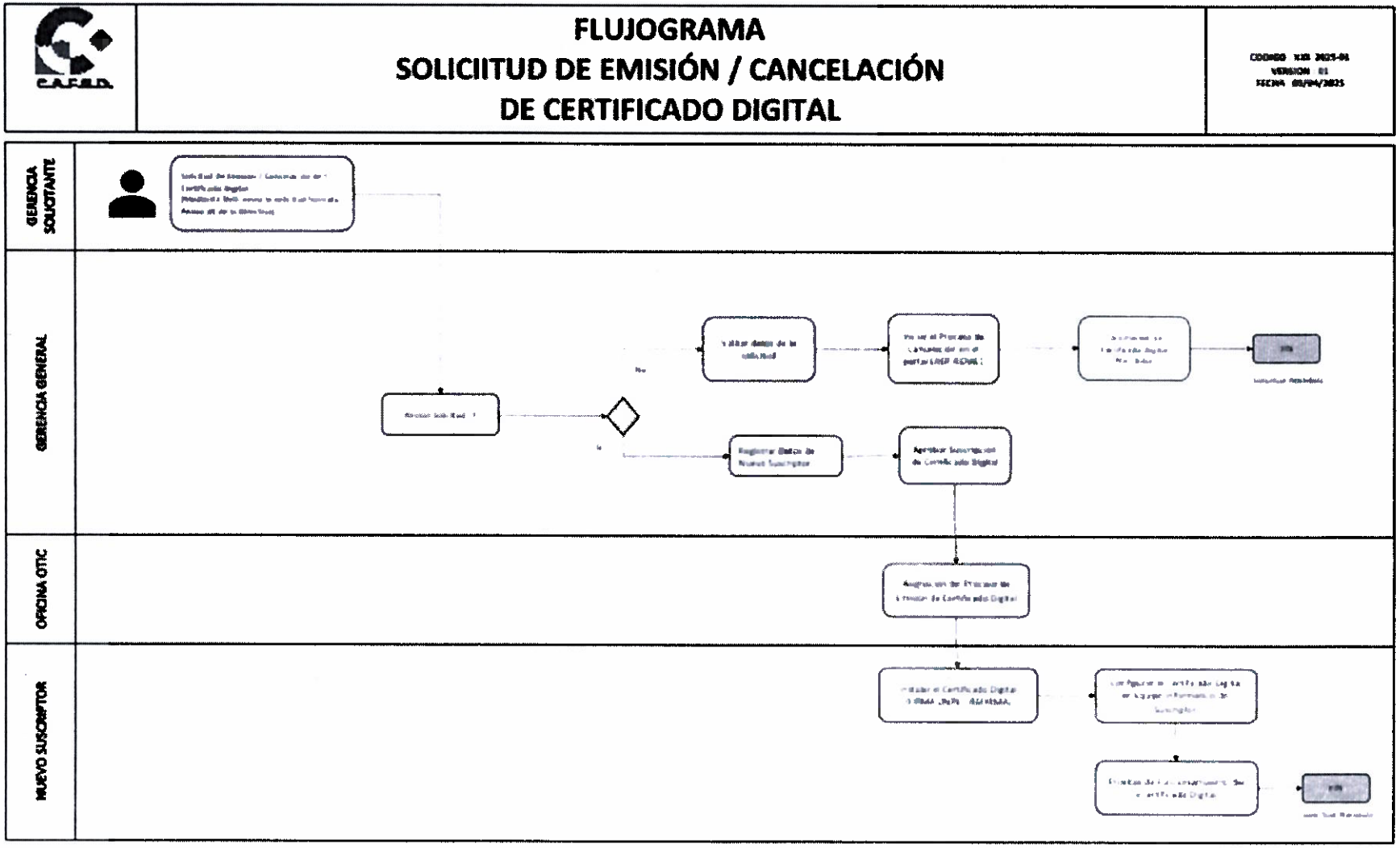
Emisión		Cancelación	

Yo,.....identificado con Documento Nacional de Identidad DNI N°.....,con el correo electrónico....., autorizo la ..... de los certificados digitales asignados, utilizados en los documentos que genere en cumplimiento de mis funciones asignadas en el Comité de Administración de los Fondos Educativos de la Región Callao, proceso que se genera mediante la plataforma integrada de la entidad de registro del EREP-RENIEC.

Atentamente,

Firma y Sello de la
Gerencia Solicitante

10.2 Anexo N° 02: Diagrama de Flujo de Emisión / Cancelación de Firma Certificado Digital



10.3 Anexo 03: Glosario de Términos y Definiciones

- **Firma digital:** es aquella firma electrónica que además utiliza una técnica de criptografía asimétrica, que permite la identificación del signatario y que ha sido creada por medios, incluso a distancia, que garantizan que éste mantiene bajo su control con un elevado grado de confianza, de manera que está vinculada únicamente al signatario y a los datos a los que refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior. Tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita, siempre y cuando haya sido generada por un Prestador de Servicios de Certificación Digital debidamente acreditado que su encuentre dentro de la Infraestructura Oficial de Firma Electrónica y que no medie ninguno de los vicios de la voluntad previstos en el Título VIII del Libro IV de Código Civil.

- **Autenticación digital de documentos:** Acto realizado por el fedatario institucional, quien verifica, mediante cotejo entre el documento físico presentado y su versión digitalizada, la fidelidad, integridad y legibilidad de esta última. Para ello, firma electrónicamente el documento digitalizado utilizando su certificado digital. La autenticación se limita a este proceso y no implica un pronunciamiento sobre el contenido de la información del documento.

- **Copia fiel al original:** Declaración del fedatario institucional que certifica que la información contenida en el documento físico presentado durante el procedimiento registral es equivalente a la de su versión digital, garantizando que ambas representaciones mantienen la misma integridad y exactitud en el contenido.

- **Digitalización:** Conjunto de procesos, procedimientos y recursos informáticos que operan como una unidad de producción para convertir documentos físicos en formatos digitales. La digitalización involucra desde la preparación inicial de los documentos hasta su almacenamiento final como archivos digitales autenticados.

- **Documento electrónico:** Unidad básica de información estructurada que puede ser clasificada, transmitida, procesada o conservada mediante medios electrónicos, sistemas de información u otros similares. Tiene el mismo valor legal que los documentos en soporte papel, de conformidad con la normativa vigente.

- **Documento físico:** Instrumento textual o gráfico que contiene información, hechos fijados o registrados en un material de soporte, utilizado para verificar o acreditar una situación específica.

- **Documento original:** Documento físico que constituye la primera manifestación completa y fidedigna de su contenido, conservando todas las características y elementos que garantizan su autenticidad, integridad y valor probatorio como.

- **Certificado Digital:** es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.

- **Firmante:** Es quien crea una firma electrónica en cualquiera de sus modalidades (simple, avanzada o firma digital).

- **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.

- **Token Criptográfico:** Es un dispositivo de almacenamiento criptográfico que contiene el Certificado Digital asignado a la persona titular del mismo, que le permite firmar digitalmente. El token u otro dispositivo de almacenamiento de certificado digital cumplen con el estándar FIPS 140-2, según convenio suscrito con el RENIEC.

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