MANUAL DE VALIDACIÓN DE FIRMA DIGITAL

MAN-005-FONDEPES-V.01

Firmado digitalmente por
CHAFLOQUE CASTRO Rafael FAU
20137921601 soft
Motivo: Doy V° B°
Fecha: 09.05.2025 09:21:08 -05:00

Propuesto por	Unidad Funcional de Tecnología de la Información y Comunicación	Fecha de Propuesta	05/05/2025
Aprobado por	Gerencia General	Fecha de Aprobación	09/05/2025

Firmado digitalmente por
FERNANDEZ WINGES Raul FAU
20137921601 soft
Motivo: Doy V° B°
Fecha: 09.05.2025 09:35:56 -05:00

Firmado digitalmente por
SANTILLAN TORRES Benji Zaid
FAU 20137921601 soft
Motivo: Doy V° B°
Fecha: 09.05.2025 09:08:34 -05:00

Firmado digitalmente por GOMEZ
VELA Berthin Enrique FAU
20137921601 hard
Motivo: Doy V° B°
Fecha: 09.05.2025 09:43:23 -05:00

ÍNDICE

INTRODUCCIÓN 3
I. OBJETIVO 4
II. FINALIDAD 4
III. BASE LEGAL 4
IV. ALCANCE 5
V. SIGLAS Y ACRÓNIMOS 5
VI. DEFINICIONES 5
VII. ASPECTOS GENERALES 8
VIII. PROCEDIMIENTO 8
8.1. Firma ONPE 9
8.2. REFIRMA 12
8.3. FIRMA PERÚ 16
IX. RESPONSABILIDADES 18
X. CONTROL DE CAMBIOS 19

INTRODUCCIÓN

El Fondo Nacional de Desarrollo Pesquero (FONDEPES) es un organismo público ejecutor adscrito al Ministerio de la Producción, con autonomía técnica, económica y administrativa. Conforme a lo establecido en los artículos 58 y 59 de la Ley General de Pesca, aprobada mediante el Decreto Legislativo N.º 25977, FONDEPES tiene como finalidad promover, ejecutar y brindar apoyo técnico, económico y financiero al desarrollo de la pesca artesanal, tanto marítima como continental. Asimismo, impulsa las actividades pesqueras y acuícolas en general, con especial atención a la mejora de la infraestructura básica que facilite la producción y distribución de los recursos pesqueros, contribuyendo así al fortalecimiento del sector a nivel nacional.

En el marco de su estructura organizativa, la Oficina General de Administración desempeña un papel fundamental en la gestión del trámite documentario, asegurando un flujo eficiente y ordenado de la información institucional. Como parte de esta oficina, la Unidad Funcional de Tecnología de la Información y Comunicación tiene a su cargo la implementación y mejora continua de herramientas tecnológicas orientadas a optimizar los procesos administrativos, garantizando la seguridad, autenticidad y validez de la documentación digital.

En este contexto, la verificación y validación de firmas digitales adquiere especial importancia, al constituirse en un mecanismo clave para asegurar la autenticidad e integridad de los documentos emitidos electrónicamente. La correcta aplicación de estos procedimientos no solo refuerza la seguridad de la información institucional, sino que también contribuye a los esfuerzos por reducir el uso de papel, impulsando la digitalización de la documentación y alineándose con las políticas de modernización y sostenibilidad del Estado.

Este manual se enmarca dentro de la estrategia institucional orientada a la transformación digital y al cumplimiento de la iniciativa gubernamental “Cero Papel”, promovida por la Presidencia del Consejo de Ministros. Dicha iniciativa busca minimizar el uso de documentación física en las entidades públicas, fomentando una administración más ágil, transparente y eficiente mediante el uso de tecnologías digitales.

El presente manual tiene como objetivo establecer lineamientos claros y prácticos para que los profesionales de FONDEPES puedan verificar y validar correctamente las firmas digitales en los documentos oficiales, utilizando los aplicativos autorizados: Firma ONPE, ReFirma y Firma Perú. Con ello, se busca garantizar la validez legal de los documentos digitales y consolidar una cultura institucional orientada a la transformación digital y sostenibilidad administrativa.

I. OBJETIVO

Establecer los lineamientos y procedimientos para la verificación y validación de firmas digitales en los documentos electrónicos, asegurando su autenticidad, integridad y validez legal. Asimismo, busca definir el proceso de verificación, garantizando que las firmas digitales cumplan con la normativa vigente y sean reconocidas legal y técnicamente.

II. FINALIDAD

Busca garantizar la correcta verificación y validación de firmas digitales en los documentos electrónicos, asegurando su autenticidad, integridad y validez legal. Su aplicación contribuye a prevenir fraudes, alteraciones o usos indebidos de documentos firmados digitalmente, fortaleciendo la seguridad de la información institucional. Asimismo, promueve el uso de herramientas tecnológicas para la gestión documental, optimizando los procesos administrativos y fomentando la transición hacia un entorno digital seguro y confiable.

III. BASE LEGAL

- Ley N° 27658 – Ley Marco de Modernización de la Gestión Pública, que fomenta la modernización, eficiencia y transparencia en la gestión pública, promoviendo la incorporación de tecnologías digitales;
- Ley N° 27269 – Ley de Firmas y Certificados Digitales, que regula el uso de la firma electrónica, otorgándole la misma eficacia jurídica que la firma manuscrita, definiendo los conceptos y procedimientos relacionados con la emisión y validación de certificados digitales;
- Ley N° 27291, que permite el uso de medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica;
- Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de la Ley de firmas y Certificados Digitales, que establece las disposiciones técnicas y operativas para la implementación de la Ley N° 27269, orientando el uso de las firmas digitales y los mecanismos de certificación en el país;
- 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;
- Resolución de Secretaría de Gobierno Digital N° 001-2017-PCM/SEGDI, que aprueba el Modelo de Gestión Documental en el marco del Decreto Legislativo N° 1310;
- Mediante Decreto Supremo N° 092-2017-PCM, que aprueba la Política Nacional de Integridad y Lucha contra la Corrupción, con el objetivo general de contar con instituciones transparentes e íntegras que practiquen y promuevan la probidad en el ámbito público, sector empresarial y la sociedad civil; y garantizar la prevención y sanción efectiva de la corrupción a nivel nacional, regional y local, con la participación de la ciudadanía;
- Decreto de Urgencia Nº 006-2020, que crea el Sistema Nacional de Transformación Digital y deroga las disposiciones contenidas en el Decreto Legislativo 604, relativas al Sistema Nacional de Informática que se opongan al Decreto de Urgencia. Entiéndase, para todos sus efectos, que el Sistema Nacional de Transformación Digital sustituye al Sistema Nacional de Informática;
- Decreto Supremo Nº 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo Nº 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 y deroga el Decreto Supremo Nº 066-2011-PCM, que aprueba el Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0.;
- Decreto Legislativo N° 1246 – Medidas de Simplificación Administrativa Aprobó diversas medidas orientadas a la simplificación de los procesos administrativos;

- Resolución de Gerencia General N° 169-2019-GG, DIR-001-FONDEPES-V.01, Directiva para la elaboración, revisión, aprobación y modificación de documentos normativos del Fondo Nacional de Desarrollo Pesquero – FONDEPES;
- Resolución de Secretaría de Gobierno y Transformación Digital N° 007-2024-PCM/SGTD, que aprueba la Directiva N° 002-2024-PCM/SGTD, que regula el uso de la firma digital en las entidades públicas;
- Decreto Supremo N° 082-2024-PCM, que dispone medidas temporales para promover el uso de la firma digital en el sector público y modifica el Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales.

IV. ALCANCE

El presente manual es de aplicación para todos los profesionales del FONDEPES que requieran verificar y validar firmas digitales en documentos electrónicos dentro de la organización. Está dirigido a las áreas jurídicas, tecnológicas y administrativas, así como a cualquier unidad de organización que gestione documentación firmada digitalmente en el ejercicio de sus funciones.

V. SIGLAS Y ACRÓNIMOS

- AAC: Autoridad Administrativa Competente
- CA: Autoridad Certificadora.
- CRL: Lista de Revocación de Certificados (Certificate Revocation List).
- DNIe: Documento Nacional de Identidad Electrónico.
- DNId: Documento Nacional de Identidad digital
- IOFE: Infraestructura Oficial de Firma Electrónica
- INDECOPI: Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual
- OCSP: Protocolo de Estado de Certificado en Línea (Online Certificate Status Protocol).
- OGA: Oficina General de Administración
- OGAJ: Oficina de Asesoría Jurídica
- ONPE: Oficina Nacional de Procesos Electorales
- PKI: Infraestructura de Clave Pública (Public Key Infrastructure).
- RA: Autoridad de Registro (Registration Authority)
- RENIEC: Registro Nacional de Procesos Electorales
- SGD: Sistema de Gestión Documental
- TSL: Lista de Servicios de Confianza (Trust Services List)
- UFTIC: Unidad Funcional de Tecnología de la Información y Comunicación

VI. DEFINICIONES

- **Autoridad Administrativa Competente (AAC):** Es la entidad encargada de administrar y supervisar la IOFE, según lo establecido en el Reglamento de la Ley de Firmas y Certificados Digitales. En el Perú, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) ha sido designado como la AAC.

- **Autoridad de Certificación (CA - Certification Authority):** Es la entidad responsable de emitir, validar y revocar certificados digitales. Su función principal es garantizar la autenticidad y

confiabilidad de los certificados emitidos, verificando la identidad de los solicitantes y asegurando el cumplimiento de las normativas establecidas.

- **Autoridad de Registro (RA - Registration Authority):** Es la entidad encargada de verificar la identidad de los solicitantes de certificados digitales antes de que sean emitidos por la Autoridad de Certificación. Actúa como intermediaria en el proceso de certificación digital.

- **Certificado Digital:** Es un documento electrónico emitido por una Autoridad de Certificación que vincula una clave pública con la identidad de su titular. Su propósito es autenticar la identidad del firmante y permitir el uso seguro de la firma digital.

  Los certificados digitales se utilizan en transacciones electrónicas seguras, comercio electrónico y gestión documental en entornos digitales. Cumplen con el estándar internacional X.509v3, que define los campos y atributos que deben contener, tales como el número de serie, el emisor, el período de validez, la clave pública y la firma de la Autoridad de Certificación.

  Un certificado digital puede encontrarse en distintos estados a lo largo de su ciclo de vida: emitido, revocado, expirado o suspendido.

- **Documento:** Es un registro de información generado o recibido por una persona natural o jurídica, entidad pública o privada, en el ejercicio de sus funciones o actividades. Puede presentarse en cualquier formato, soporte o medio, incluyendo aquellos derivados del avance tecnológico.

- **Documento Nacional de Identidad Electrónico (DNIe):** Es la versión electrónica del Documento Nacional de Identidad, que incorpora un chip criptográfico que almacena certificados digitales para la autenticación y firma digital.

- **Documento Nacional de Identidad Digital (DNId):** Es un mecanismo de identificación electrónica que permite a los ciudadanos realizar trámites y firmar documentos de manera digital con plena validez legal.

- **Documento electrónico:** Es un documento almacenado en un medio digital, electrónico o magnético, cuya información está codificada y estructurada de manera que pueda ser procesada, transmitida y almacenada electrónicamente.

- **Firma electrónica:** Es cualquier dato en formato electrónico, adjunto o lógicamente asociado a un documento electrónico, que permite identificar al firmante y demostrar su voluntad de aprobar el contenido del documento. También es conocida como firma electrónica simple o básica.

- **Firma Digital:** Es un mecanismo criptográfico que permite garantizar la autenticidad e integridad de un documento electrónico. Consiste en un dato digital adjunto, embebido o lógicamente asociado a otro dato (documento digital). La firma digital cumple con las mismas funciones que una firma manuscrita: identificar al firmante, vincular al documento con la persona que lo suscribe y garantizar la inalterabilidad del contenido firmado.
  En el Perú, cuando una firma digital es generada dentro de la IOFE, tiene la misma validez y eficacia jurídica que una firma manuscrita, según la normativa vigente.

- **Firma ONPE:** Es un aplicativo desarrollado por la Oficina Nacional de Procesos Electorales (ONPE) que permite la firma digital de documentos electrónicos cumpliendo con los estándares de la Infraestructura Oficial de Firma Electrónica (IOFE) del Perú. Este aplicativo permite a los usuarios firmar documentos con certificados digitales almacenados en dispositivos criptográficos, como el DNIe, y verificar la validez de firmas digitales en archivos electrónicos, garantizando la

autenticidad e integridad de los documentos firmados digitalmente en el ámbito electoral y administrativo.

- **Firma Perú:** Es una plataforma de firma digital proporcionada por el Estado Peruano para facilitar la firma y validación de documentos electrónicos con certificados digitales. Este aplicativo permite la firma de documentos en línea, asegurando su validez legal y cumpliendo con los estándares de la IOFE.
  Firma Perú está diseñado para ser utilizado por ciudadanos, entidades públicas y empresas privadas que requieran firmar documentos electrónicos de manera segura y con pleno respaldo normativo. Además, ofrece funciones de validación para verificar la autenticidad e integridad de documentos firmados digitalmente.

- **Infraestructura Oficial de Firma Electrónica (IOFE):** Es el sistema regulado y supervisado por la AAC, que proporciona los mecanismos técnicos y legales para la emisión, verificación y gestión de certificados digitales. Asegura que las firmas digitales generadas dentro de su marco sean seguras, confiables y con pleno valor legal.

- **Inalterabilidad:** Propiedad de un documento electrónico firmado digitalmente mediante un certificado digital dentro de una infraestructura tecnológica de confianza, que garantiza que su contenido no ha sido modificado o alterado tras su firma

- **Integridad:** Principio que asegura que un documento electrónico no ha sido alterado desde su emisión hasta su recepción. Se presume que la información contenida en el mensaje de datos es exacta y corresponde fielmente a la versión original enviada. Un documento firmado digitalmente bajo normativas vigentes mantiene esta integridad sin importar el medio en el que se almacene.

- **Interoperabilidad:** Capacidad de los sistemas y procesos de diferentes entidades para intercambiar información, datos y conocimientos de manera eficiente y segura, con el fin de optimizar la gestión pública y contribuir al desarrollo sostenible del país. La interoperabilidad es dirigida, supervisada y evaluada por la Presidencia del Consejo de Ministros.

- **Lista de Revocación de Certificados (CRL - Certificate Revocation List):** Es un registro administrado por una Autoridad de Certificación que contiene los certificados digitales que han sido revocados antes de su fecha de expiración, impidiendo su uso posterior.

- **Protocolo de Estado de Certificado en Línea (OCSP - Online Certificate Status Protocol):** Es un protocolo que permite verificar en tiempo real el estado de un certificado digital, brindando una respuesta rápida sobre su validez sin necesidad de descargar una lista de revocación completa.

- **ReFirma:** Es un aplicativo desarrollado por el Registro Nacional de Identificación y Estado Civil (RENIEC) que permite la firma digital de múltiples documentos electrónicos utilizando certificados digitales emitidos por la Autoridad de Certificación del Estado Peruano (RENIEC-ACE), en cumplimiento con la IOFE. Permitiendo verificar la validez de los documentos firmados digitalmente.

- **TSL: Lista de Servicios de Confianza (Trust Services List):** Es un registro oficial publicado y mantenido por la entidad acreditadora de cada país (en el Perú, Indecopi), que contiene información actualizada sobre los proveedores de servicios de confianza acreditados, como las Entidades de Certificación Digital. La TSL garantiza que los certificados digitales emitidos por estas entidades sean reconocidos como válidos, seguros y conformes con la normativa vigente. Su consulta permite verificar la autenticidad y vigencia de los certificados utilizados en procesos de firma digital.

- **Usuario:** Persona natural o representante de una entidad autorizado para generar documentos o realizar trámites a través del Sistema de Gestión Documental (SGD), ya sea de manera presencial o virtual.

VII. ASPECTOS GENERALES

Para garantizar la autenticidad, integridad y validez legal de los documentos firmados digitalmente en FONDEPES, se deben considerar los siguientes aspectos:

- **Uso de herramientas certificadas:** La verificación y validación de firmas digitales debe realizarse utilizando aplicativos certificados por la IOFE, tales como Firma ONPE, ReFirma y Firma Perú.
- **Comprobación de vigencia del certificado digital:** Antes de aceptar un documento firmado digitalmente, es imprescindible verificar que el certificado digital del firmante esté vigente y no haya expirado.
- **Integridad de la firma digital:** La firma digital no debe presentar alteraciones, modificaciones o signos de manipulación en su estructura.
- **Verificación del estado del certificado:** Se debe revisar que el certificado digital no haya sido revocado, suspendido o invalidado por la Autoridad de Certificación correspondiente.
- **Registro de verificaciones:** Para fines de auditoría y trazabilidad, se debe documentar las verificaciones realizadas, especialmente en procesos críticos dentro de FONDEPES.

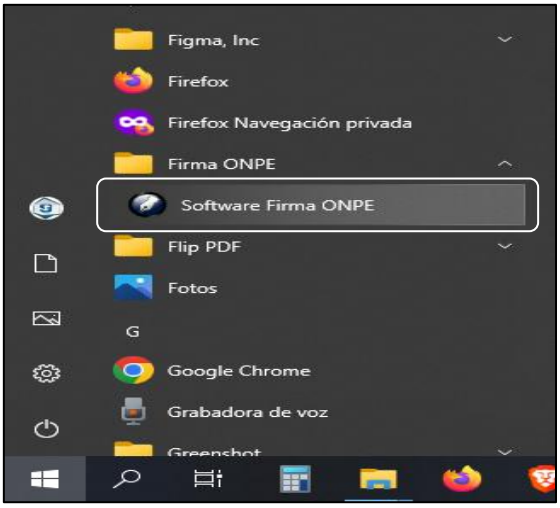
VIII. PROCEDIMIENTO

Para garantizar la correcta verificación y validación de firmas digitales en los documentos gestionados por FONDEPES, es necesario seguir un procedimiento estandarizado que asegure la autenticidad, integridad y validez legal de los mismos. Este procedimiento establece los pasos a seguir para validar las firmas digitales utilizando los aplicativos certificados por la Infraestructura Oficial de Firma Electrónica (IOFE): Firma ONPE, ReFirma y Firma Perú.

A continuación, se detallan las acciones a realizar para la verificación y validación de firmas digitales en documentos electrónicos, asegurando el cumplimiento de la normativa vigente y los estándares de seguridad requeridos.

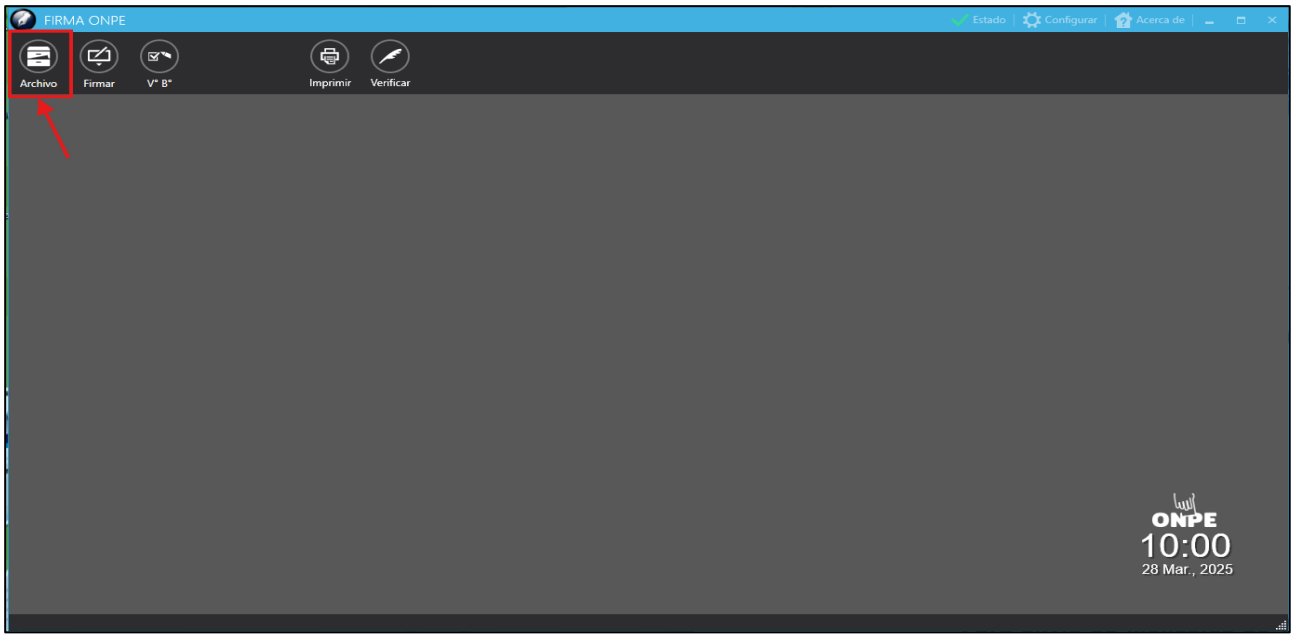
8.1. Firma ONPE

8.1.1. **Abrir el software Firma ONPE**.
Ubique y ejecute el aplicativo Firma ONPE desde la lista de programas instalados en su equipo.



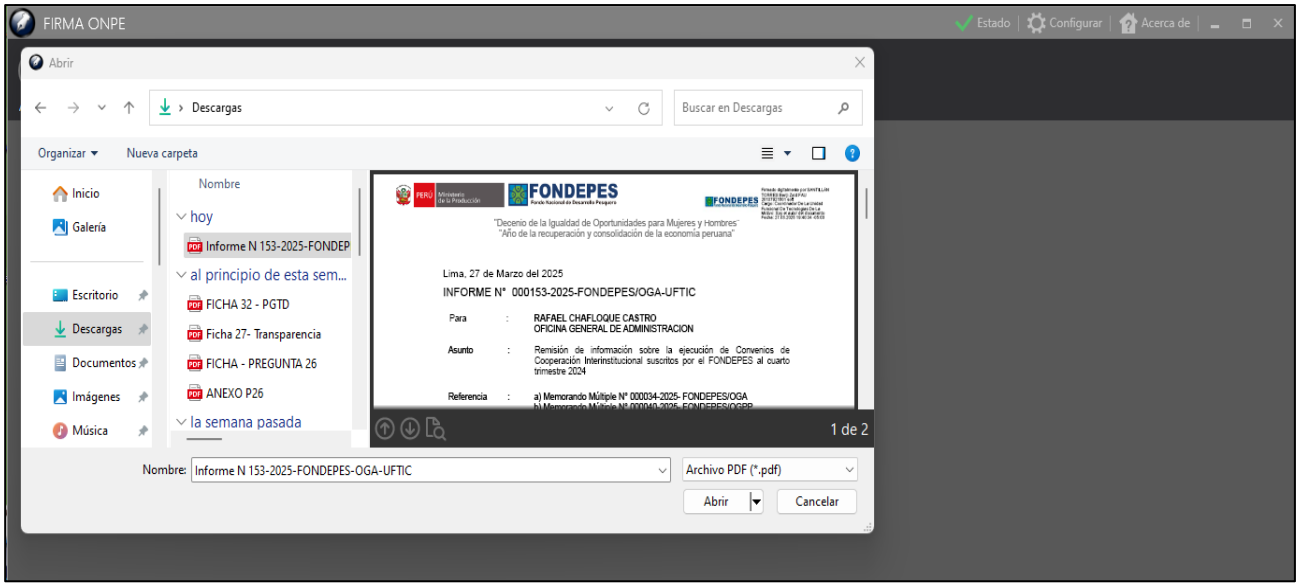
8.1.2. **Apertura del software Firma ONPE**
Una vez ejecutado, el software Firma ONPE se abrirá y estará listo para su uso.

8.1.3. **Interfaz principal de Firma ONPE**
Al abrir el software Firma ONPE, se mostrará la interfaz principal. Para comenzar el proceso, haga clic en el botón "**Archivo**" ubicado en la barra de opciones.



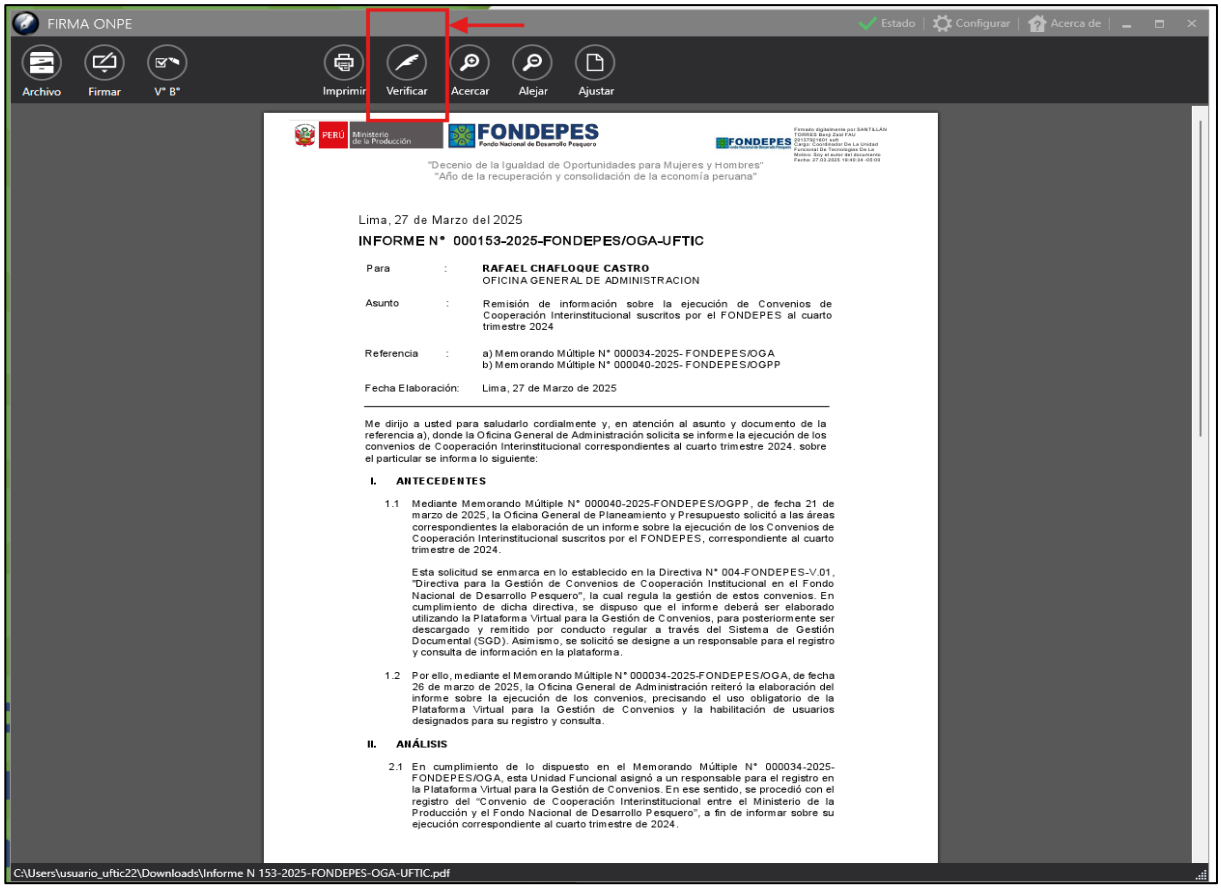
8.1.3. **Seleccionar el archivo a verificar**

Busque y seleccione el documento que desea verificar. Luego, haga clic en "**Abrir**" para cargarlo en el software Firma ONPE.



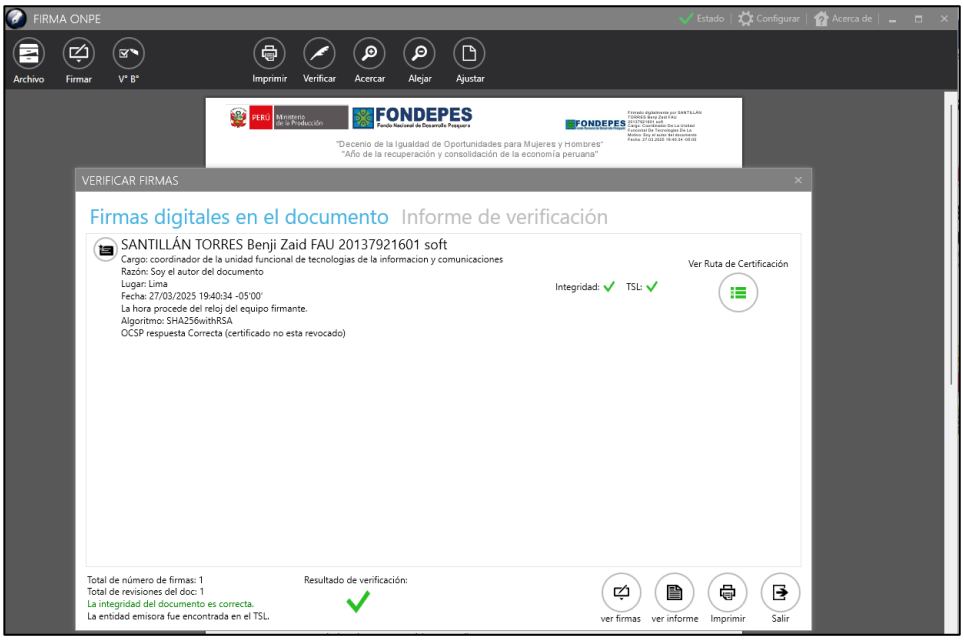
8.1.4. **Visualización del documento y verificación de la firma**

El documento PDF seleccionado se mostrará en el software Firma ONPE. A continuación, presione el botón "**Verificar**" para comprobar la validez de la firma digital.



8.1.5. **Visualización del resultado de la verificación**

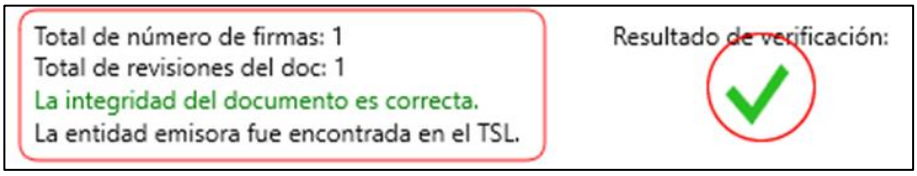
Después de unos segundos, el software Firma ONPE mostrará el resultado de la verificación de la firma digital, indicando si la firma es válida, si el certificado digital está vigente y si el documento no ha sido alterado.



- Identifica al usuario responsable de la firma.
- Se muestra el resultado de la verificación de la integridad del archivo.
- Se muestra el resultado de la verificación del estado de servicio de confianza del archivo.
- Se muestra el detalle de la Ruta de Certificación.
  El software va a escanear todos los parámetros necesarios para la verificación y autenticidad de la firma digital impresa en el documento.
- Se muestra a detalle el resumen de la verificación.
- Se muestra el resultado final de la Verificación.

8.1.6. **Documento con resultado VÁLIDO**

Si la firma digital es válida, el software **Firma ONPE** mostrará un mensaje indicando que la firma ha sido correctamente verificada con un “check” [✔] . y el siguiente mensaje.



Este resultado confirma que el documento es seguro y confiable para su uso dentro de los procesos institucionales.

8.1.7. **Documento con resultado NO VÁLIDO**

Un documento no cuenta con una firma digital valida cuando el resultado de la verificación del software muestra una “cruz” [✗] y el siguiente mensaje.

Se identifica al usuario responsable de la firma, pero:

- No aprueba la integridad del archivo.
- Alerta que el documento tiene cambios no firmados después de la última firma.

El resultado **TSL** es la licencia que certifica que el software cuenta con certificado de autenticación de firmas.

8.2. REFIRMA

8.2.1. Instalacion de ReFirma

Para utilizar ReFirma, es necesario instalar el software en su ordenador.

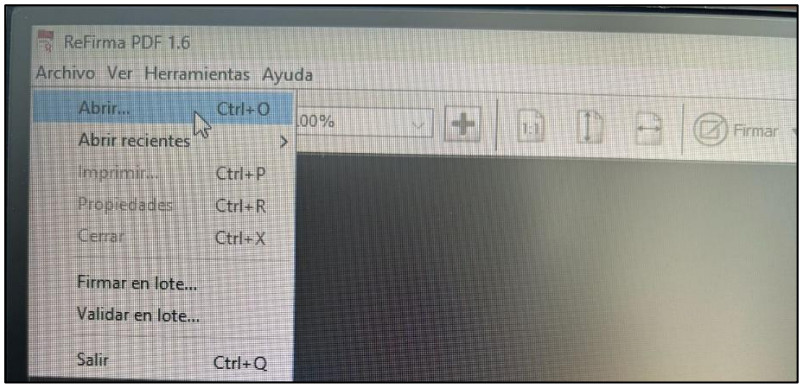
URL de descarga: **https://dsp.reniec.gob.pe/refirma_suite/pdf/web/main.jsf**

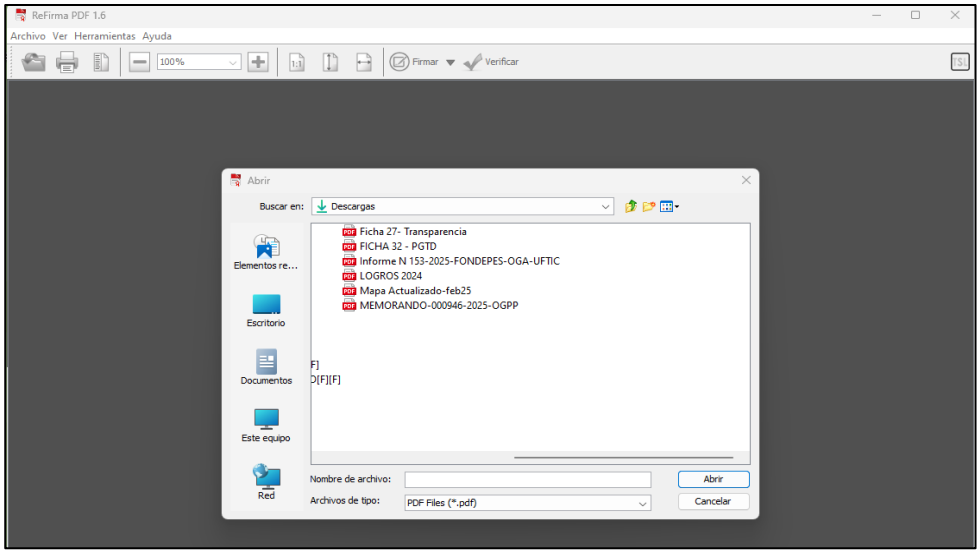
8.2.2. Ejecución del Software

Una vez instalado ReFirma, ábralo desde la lista de programas instalados en su ordenador para iniciar su uso.

8.2.3. Apertura del archivo a verificar

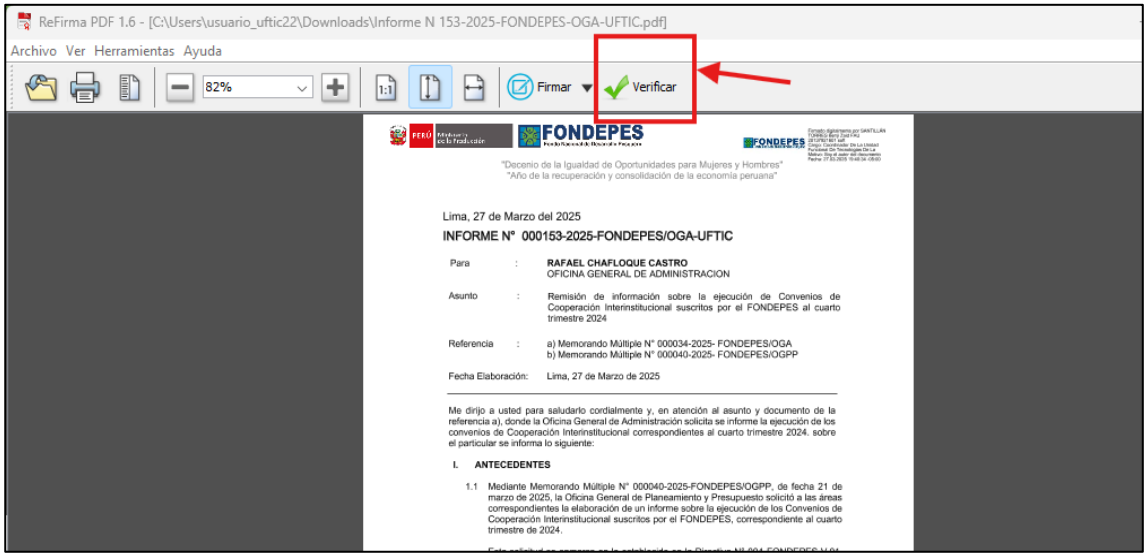
Seleccionar la opción "**Abrir**" un archivo dentro del software ReFirma y elija el documento que desea verificar.





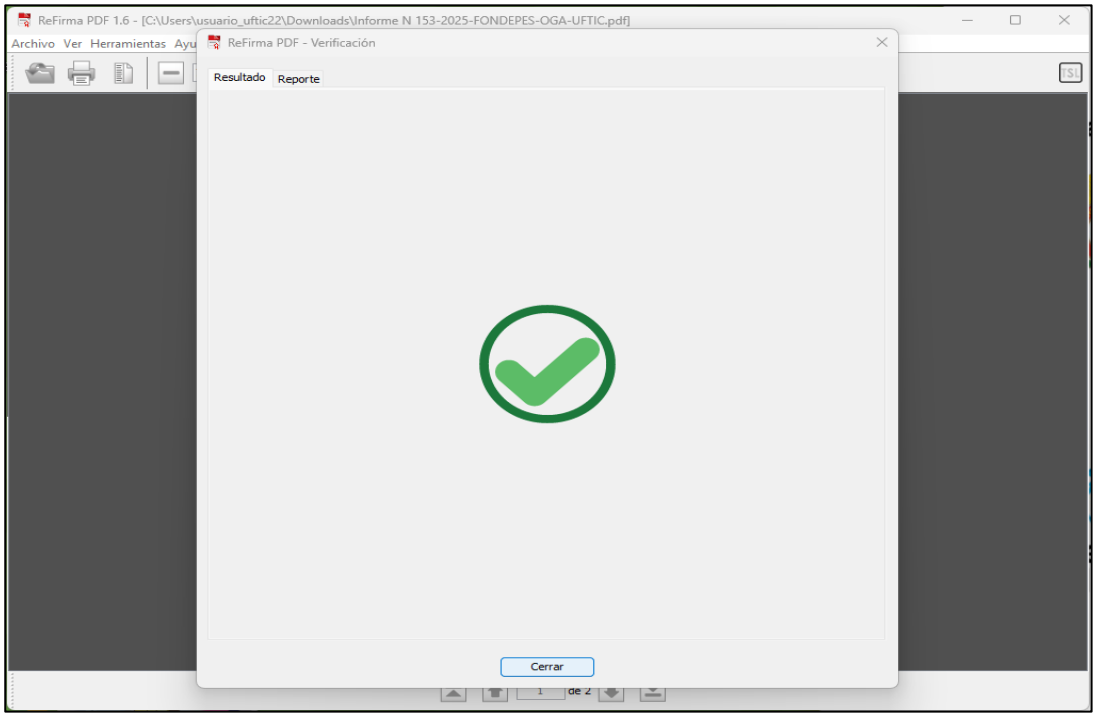
8.2.4. Iniciar verificación

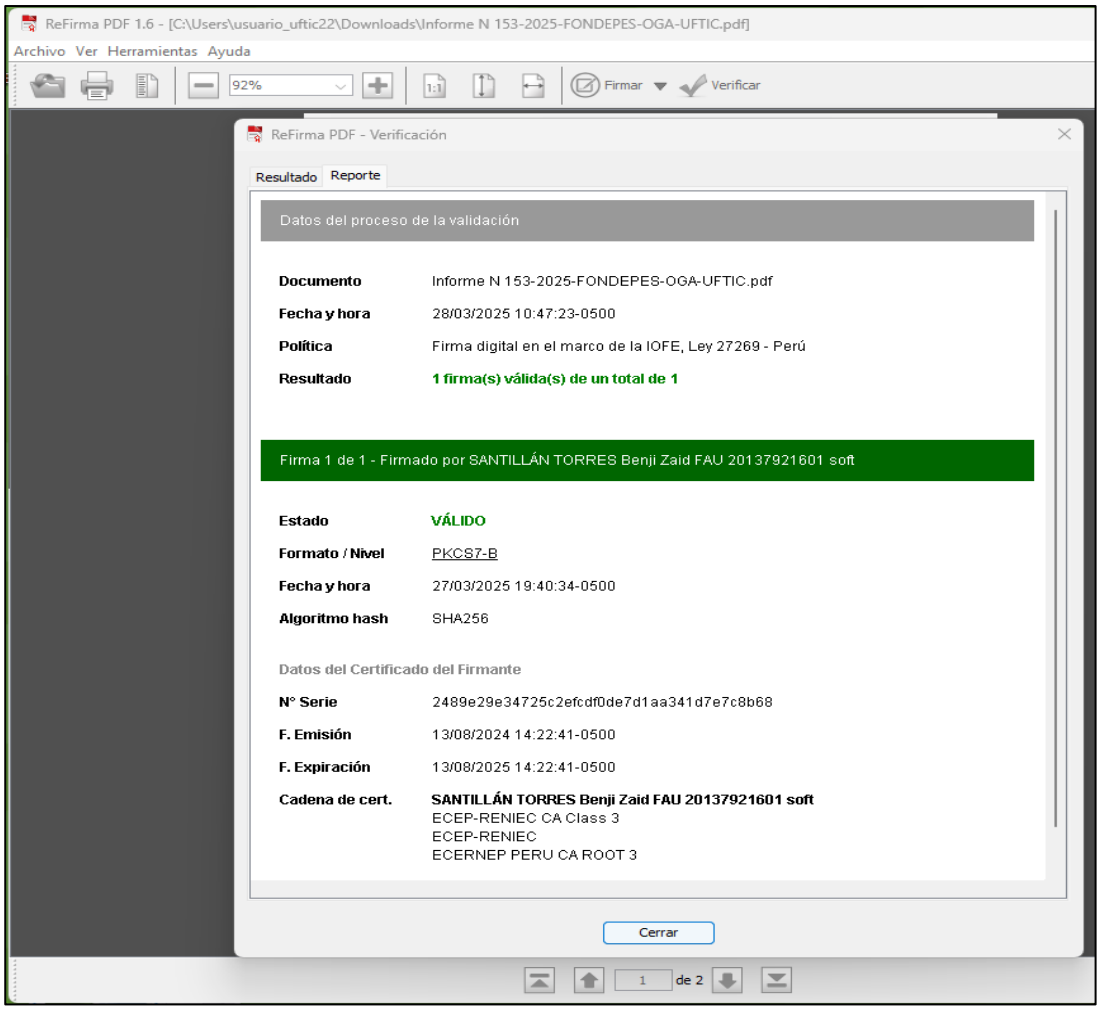
Haga clic en el botón "**Verificar**" para procesar la validación de la firma digital del documento.



8.2.5. Revisar el reporte de verificación

Verifique el reporte generado y asegúrese de que el estado del documento sea "**Válido**", lo que confirma la autenticidad e integridad de la firma digital.




ReFirma PDF 1.6 - [C:\Users\usuario_uftic22\Downloads\Informe N 153-2025-FONDEPES-OGA-UFTIC.pdf]
Archivo Ver Herramientas Ayuda
92%
Firmar
Verificar
ReFirma PDF - Verificación
Resultado
Reporte
Datos del proceso de la validación
Documento
Informe N 153-2025-FONDEPES-OGA-UFTIC.pdf
Fecha y hora
28/03/2025 10:47:23-0500
Política
Firma digital en el marco de la IOFE, Ley 27269 - Perú
Resultado
1 firma(s) válida(s) de un total de 1
Firma 1 de 1 - Firmado por SANTILLÁN TORRES Benji Zaid FAU 20137921601 soft
Estado
VÁLIDO
Formato / Nivel
PKCS7-B
Fecha y hora
27/03/2025 19:40:34-0500
Algoritmo hash
SHA256
Datos del Certificado del Firmante
N° Serie
2489e29e34725c2efcdf0de7d1aa341d7e7c8b68
F. Emisión
13/08/2024 14:22:41-0500
F. Expiración
13/08/2025 14:22:41-0500
Cadena de cert.
SANTILLÁN TORRES Benji Zaid FAU 20137921601 soft
ECEP-RENIEC CA Class 3
ECEP-RENIEC
ECERNEP PERU CA ROOT 3
Cerrar
1
de 2

8.3. FIRMA PERÚ

8.3.1. Acceder al validador de Firma Perú

Tienes dos medios para acceder al URL de consulta de validación de firma.

1. Directo de la página web de gob.pe: https://apps.firmaperu.gob.pe/web/validador.xhtml

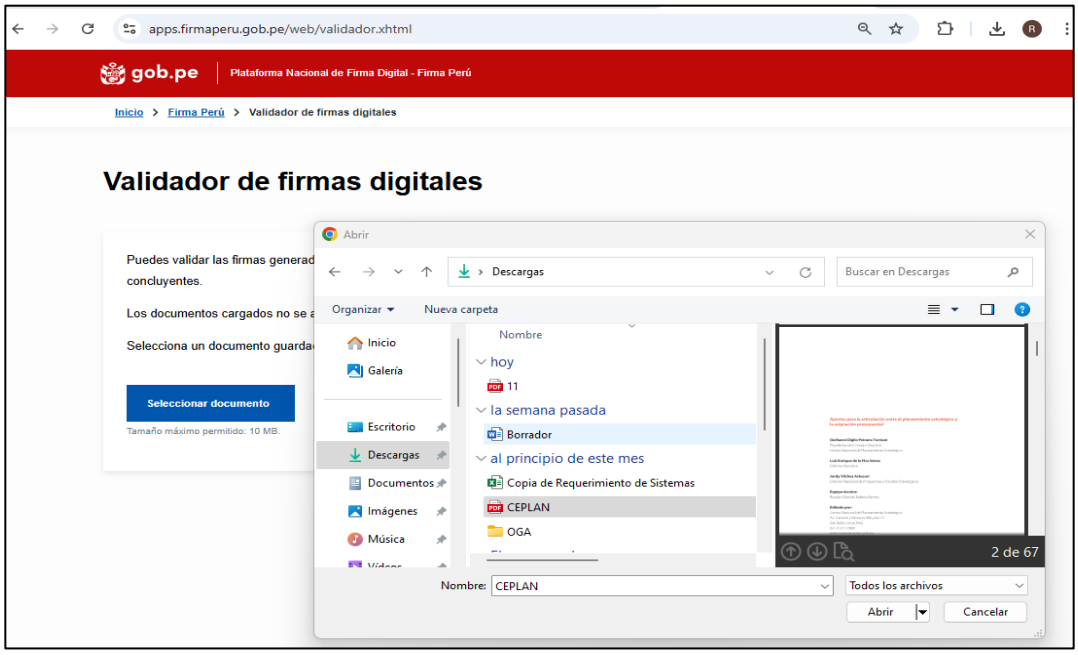
2. Desde la web del FONDEPES, a través del enlace de interés: Validar documentos firmados electrónicamente: https://www.gob.pe/14194-validar-documentos-firmados-digitalmente

Asegúrese de contar con el documento que desea verificar.

8.3.2. Seleccionar el documento a verificar

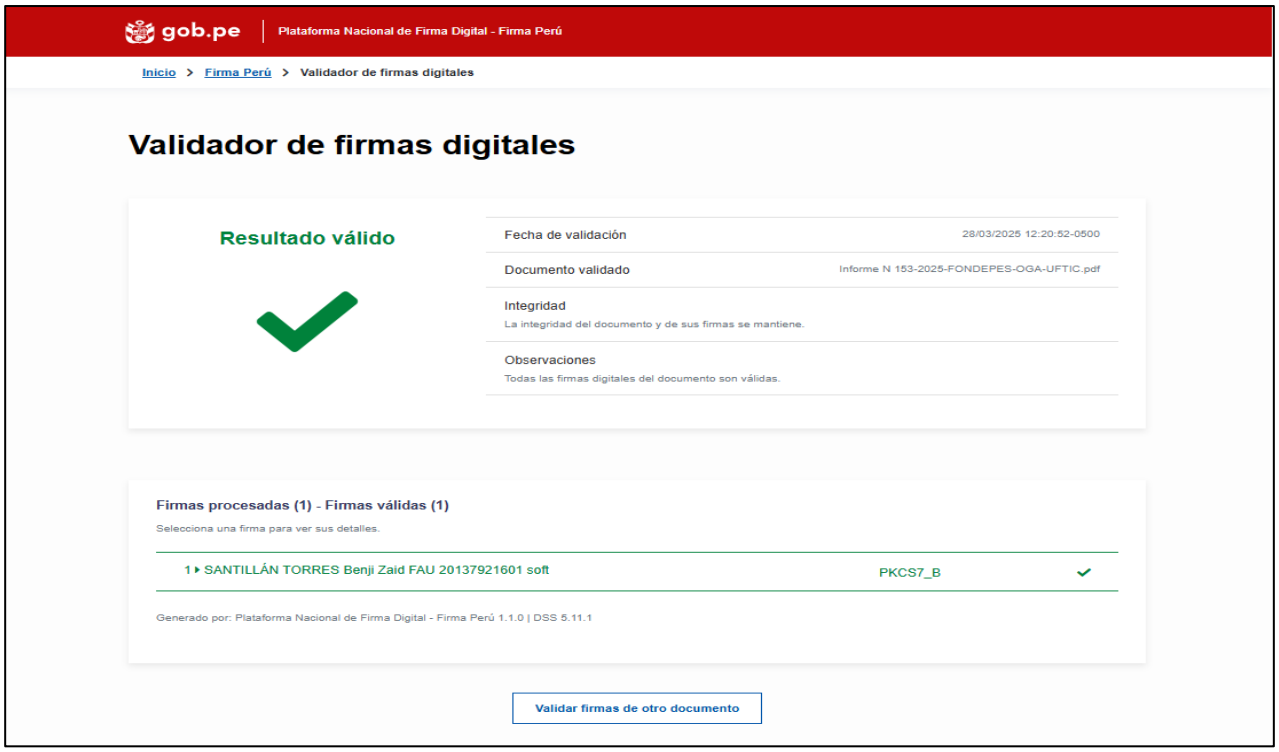
Haga clic en el botón **"Seleccionar Documento"** y, en la ventana emergente, busque el archivo que desea verificar.

Una vez seleccionado el documento, confirme su elección para proceder con la validación.



8.3.3. Visualizar el resultado de la verificación

Luego de seleccionar el documento, el sistema procesará la información y mostrará el resultado de la verificación de la firma digital.



IX. RESPONSABILIDADES

A efectos de garantizar una adecuada verificación y validación de las firmas digitales en los documentos se detallan las siguientes responsabilidades:

9.1. Usuario

- Validar y/o verificar que la firma digital en los documentos recibidos esté correctamente firmada. Para ello, el usuario deberá utilizar alguno de los siguientes aplicativos oficiales: Firma ONPE, ReFirma o Firma Perú, los cuales permiten validar firmas digitales de manera confiable y segura.
  Estas plataformas son interoperables y permiten verificar documentos firmados con certificados digitales emitidos por entidades acreditadas por Indecopi, como la ONPE, RENIEC y Firma Perú. Esto significa que un documento firmado con un certificado emitido por la ONPE puede ser verificado no solo en la plataforma de Firma ONPE, sino también en ReFirma o Firma Perú, y viceversa, siempre que el certificado digital sea reconocido por el aplicativo utilizado. La misma compatibilidad se aplica para los certificados emitidos por RENIEC (verificados a través de ReFirma) y por la entidad Firma Perú.
- En caso de presentarse dificultades técnicas durante el proceso de verificación o validación de firmas digitales —como errores en los aplicativos, certificados no reconocidos, firmas no válidas o documentos que no puedan ser verificados—, el usuario deberá reportar de inmediato la incidencia a la Unidad Funcional de Tecnología de la Información y Comunicación (UFTIC).
  Este reporte es obligatorio cuando el inconveniente impida validar correctamente un documento institucional o genere dudas sobre su autenticidad. La comunicación deberá realizarse a través del correo electrónico institucional (soporte.firmadigital@fondepes.gob.pe), adjuntando las capturas de pantalla correspondientes que evidencien el problema reportado.

9.2. Unidad Funcional de Tecnología de la Información y Comunicación (UFTIC)

- Brindar soporte técnico a los usuarios internos en el uso de los aplicativos oficiales: Firma ONPE, ReFirma y Firma Perú.
- Capacitar al personal institucional en el uso adecuado de la firma digital y en la verificación de documentos firmados digitalmente.
- Mantener y actualizar las herramientas tecnológicas necesarias para la verificación y validación de firmas digitales.
- Supervisar el cumplimiento de la normativa vigente relacionada con la gestión de documentos electrónicos firmados digitalmente. En ese marco, la UFTIC deberá reportar trimestralmente a la Oficina General de Administración sobre los hallazgos reportados por los usuarios del FONDEPES, mediante correo electrónico institucional (soporte.firmadigital@fondepes.gob.pe).

9.3. Oficina General de Administración (OGA)

- Gestionar la adquisición y renovación de certificados digitales para los funcionarios y servidores públicos que requieran firmar y validar digitalmente documentos oficiales.
- La OGA recibirá trimestralmente, vía correo electrónico institucional, el reporte elaborado por la UFTIC sobre los hallazgos reportados por los usuarios en el proceso de validación de firmas digitales.
- En caso que el reporte contenga incidencias relacionadas con **certificados no reconocidos, firmas no válidas o documentos no verificables** que no correspondan a fallas técnicas, la OGA deberá derivar el reporte a la Oficina General de Asesoría Jurídica para su evaluación y acciones correspondientes.
  Si las observaciones corresponden únicamente a aspectos técnicos, la OGA tomará conocimiento sin necesidad de derivar el caso.

9.4. Oficina de Asesoría Jurídica (OGAJ)

- Evaluar los reportes derivados por la Oficina General de Administración, con base en la información proporcionada por la UFTIC, a fin de determinar si corresponde iniciar acciones legales o administrativas según el marco normativo vigente.

X. CONTROL DE CAMBIOS

Versión	Fecha	Justificación	Descripción
01		Elaboración inicial del documento	No aplica