

Guía para el uso e integración de la Plataforma Nacional de Firma Digital en la Administración Pública

Resolución de Secretaría de Gobierno y Transformación Digital N°
002-2022-PCM/SGTD



CONTROL DE VERSIONES

Versión	Fecha	Título	Elaborado por
1.0.0	2022/09	Guía para el uso e integración de la Plataforma Nacional de Firma Digital en la Administración Pública	Secretaría de Gobierno y Transformación Digital

Documento electrónico firmado digitalmente en el marco de la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias. La integridad del documento y la autenticidad de la(s) firma(s) pueden ser verificadas en <https://apps.firmaperu.gob.pe/web/validador.xhtml>



CONTENIDO

1. Objeto	2
2. Finalidad	2
3. Marco legal	3
4. Acrónimos	3
5. Definiciones	3
6. Plataforma Nacional de Firma Digital	4
7. Actores de la Plataforma FIRMA PERÚ	5
8. Características de la Plataforma FIRMA PERÚ	6
9. Servicio de Creación de firma digital	7
10. Servicio de Validación de firma digital	9
11. Formatos de firma digital	10
12. Cardinalidad de un documento firmado digitalmente	11
13. Niveles de firma digital	12
15. Firma digital en lote	13
16. Credenciales para la integración con la Plataforma FIRMA PERÚ	13



GUÍA PARA EL USO E INTEGRACIÓN DE LA PLATAFORMA NACIONAL DE FIRMA DIGITAL EN LA ADMINISTRACIÓN PÚBLICA

1. Objeto

Establecer los criterios para el uso e integración de la Plataforma Nacional de Firma Digital (en adelante Plataforma FIRMA PERÚ), así como para estandarizar las operaciones de creación y validación de firmas digitales mediante dicha Plataforma, de conformidad con lo establecido en el artículo 91 del 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, aprobado mediante Decreto Supremo N° 029-2021-PCM, y, la Ley N° 27269, Ley de Firmas y Certificados Digitales, y su Reglamento, aprobado mediante Decreto Supremo N° 052-2008-PCM y modificatorias.

2. Finalidad

La presente Guía tiene por finalidad:

- Contribuir con el proceso de transformación digital de las entidades públicas.
- Fortalecer la prestación de servicios digitales de calidad de manera segura e interoperable, mediante la adecuada creación y validación de firmas digitales creadas en el marco de la Infraestructura Oficial de Firma Electrónica - IOFE, que coadyuven a la satisfacción plena de las necesidades de la ciudadanía en el entorno digital.
- Impulsar el uso y despliegue de la firma digital en el país de conformidad con el marco normativo vigente.

3. Marco legal

- Ley N° 29158, Ley Orgánica del Poder Ejecutivo.
- Ley N° 27269, Ley de Firmas y Certificados Digitales.
- Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Decreto Supremo N° 052-2008-PCM, Decreto Supremo que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales y modificatorias.
- Decreto Supremo N° 026-2016-PCM, que aprueba medidas para el fortalecimiento de la infraestructura oficial de firma electrónica y la implementación progresiva de la firma digital en el sector público y privado.
- Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- Decreto Supremo N° 157-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Resolución Ministerial N° 156-2021-PCM, que aprueba el Texto Integrado del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros.



4. Acrónimos

En la presente Guía se utilizan los siguientes acrónimos:

- a) AAC : Autoridad Administrativa Competente.
- b) CRL : Lista de Certificados Cancelados.
- c) CADES : CMS Advanced Electronic Signatures.
- d) CMS : Cryptographic Message Syntax.
- e) ECERNEP : Entidad de Certificación Nacional para el Estado Peruano.
- f) ECEP : Entidades de Certificación para el Estado Peruano.
- g) IOFE : Infraestructura Oficial de Firma Electrónica.
- h) OCSP : Protocolo en línea del estado de los certificados.
- i) PAdES : PDF Advanced Electronic Signatures.
- j) PDF : Portable Document Format (ISO 32000).
- k) PIN : Personal Identification Number.
- l) PSVA-TSA : Prestador de Servicios de Valor Añadido en la modalidad de sistema de sellado de tiempo.
- m) RUC : Registro Único de Contribuyente.
- n) TSA : Time Stamping Authority.
- o) TSL : Trust Service Status List.
- p) XAdES : XML Advanced Electronic Signatures.
- q) XML : Extensible Markup Language.

5. Definiciones

Para efectos de la presente Guía se entiende como:

- a) **Firma digital:** Es aquella firma electrónica que utilizando una técnica de criptografía asimétrica, permite la identificación del signatario y 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 se 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 del Código Civil¹.
- b) **Firma digital de agente automatizado:** Es aquella firma digital generada sin intervención humana utilizando una llave privada asociada a un certificado digital de agente automatizado emitido en el marco de la IOFE.
- c) **Certificado digital:** Es el documento credencial electrónico generado y firmado digitalmente por una Entidad de Certificación que vincula un par de llaves con una persona natural o jurídica². El ciclo de vida de un certificado digital comprende: la emisión, la cancelación, y la renovación³.

¹ De conformidad con el artículo 6 del Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo N° 052-2008-PCM y modificatorias.

² Toma como base la definición establecida en el Glosario de Términos del Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo N° 052-2008-PCM y modificatorias.

³ De conformidad con la Décima Cuarta Disposición Complementaria Final del Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo N° 052-2008-PCM y modificatorias. Disponible en: https://cdn.www.gob.pe/uploads/document/file/357172/DS_052-2008-PCM.pdf.



- d) **Sello de tiempo:** Es el dato que consigna la fecha y hora cierta para evidenciar que un dato u objeto digital ha existido en un momento determinado en el tiempo, y que no ha sido alterado desde entonces⁴.
- e) **Documento electrónico:** Es la unidad básica estructurada de información, es susceptible de ser clasificada, transmitida, procesada o conservada utilizando medios electrónicos, sistemas de información o similares. Contiene información de cualquier naturaleza, es registrado en un soporte electrónico o digital, en formato abierto y de aceptación general, a fin de facilitar su recuperación y conservación en el largo plazo⁵.
- f) **Flujo de firma:** Es la secuencia ordenada de operaciones de creación de firma digital, aplicadas a un documento electrónico, y efectuadas por múltiples firmantes.
- g) **Flujo documental:** Es la secuencia de pasos o recorrido de un documento electrónico a lo largo de su tramitación en una entidad.

6. Plataforma Nacional de Firma Digital

6.1 La Plataforma FIRMA PERÚ es la plataforma digital que permite la creación y validación de firmas digitales dentro del marco de la IOFE, para la provisión de los servicios digitales prestados por las entidades de la Administración Pública.

6.2 La Plataforma FIRMA PERÚ está conformada por los siguientes servicios:

- a) **Servicio de creación de firma digital:** Este servicio permite realizar las siguientes operaciones:
- Crear firmas digitales de usuario final, independiente de un flujo documental.
 - Crear firmas digitales de usuario final, de manera integrada a un flujo documental.
 - Crear firmas digitales de agente automatizado, de manera integrada a un flujo documental.
- b) **Servicio de validación de firma digital:** Este servicio permite realizar las siguientes operaciones:
- Verificar la validez de una firma digital independiente de un flujo documental.
 - Verificar la validez de una firma digital de manera integrada a un flujo documental.
- c) **Servicio de creación de flujos de firma digital.** Este servicio permite realizar las siguientes operaciones:
- Crear flujos de firma digital de usuario final con la participación de múltiples firmantes.
 - Crear firmas digitales de usuario final en el orden establecido por el flujo de firma.

7. Actores de la Plataforma FIRMA PERÚ

Los actores involucrados en las operaciones de creación y validación de firmas digitales en la Plataforma FIRMA PERÚ son los siguientes:

⁴ De conformidad con la Décima Cuarta Disposición Complementaria Final del Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo N° 052-2008-PCM y modificatorias.

⁵ Artículo 36 del 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, aprobado mediante Decreto Supremo N° 029-2021-PCM.



- a) **Firmante:** Persona natural o jurídica titular o suscriptor de un certificado digital, emitido dentro del marco de la IOFE, y vinculado a una llave privada contenida en un módulo criptográfico de creación de firma digital y que actúa en nombre propio o en nombre de una persona natural o jurídica a la que representa.
- b) **Verificador:** Persona natural o jurídica que verifica la validez de una firma digital, habiendo tenido o no el rol de firmante.
- c) **Creador del flujo de firma:** En una operación de creación de firma digital de usuario final dentro de un flujo de firma, es la persona natural o servidor civil que: (i) prepara y/o selecciona el documento a ser firmado; (ii) define quienes serán los firmantes; (iii) establece el orden del firmado; y, (iv) define los parámetros de la firma digital.
- d) **Servicios de la Plataforma FIRMA PERÚ:** Son los servicios definidos en el numeral 6.2 de la presente Guía.
- e) **Sistema de información:** Es el sistema de información de una entidad pública que puede invocar los servicios de creación y/o validación de firma digital provisto por la Plataforma FIRMA PERÚ.
- f) **Entidad pública:** Es la entidad de la Administración Pública comprendida en el alcance de la presente norma.
- g) **Módulo criptográfico de creación de firma digital:** Es el módulo criptográfico que resguarda de manera segura la llave privada del suscriptor de un certificado digital. El módulo criptográfico puede ser de hardware o de software. Para este último caso, se debe contar con certificación de seguridad al menos FIPS 140-2 nivel 1 o equivalente, de acuerdo con lo exigido en el marco de la IOFE.
- h) **Sistema de sellado de tiempo:** Es el sistema que provee el servicio que consigna la fecha y hora cierta para evidenciar que un dato u objeto digital ha existido en un momento determinado del tiempo, y que no ha sido alterado desde entonces⁶. El uso de un sello de tiempo en una firma digital debe ser proveído por un PSVA-TSA, acreditado en el marco de la IOFE, de acuerdo con lo establecido en el literal c) del numeral 8 de la presente norma.

8. Características de la Plataforma FIRMA PERÚ

Las características principales de la Plataforma FIRMA PERÚ son las siguientes:

- a) Soporta la firma digital de todo tipo de objeto digital. Sin embargo, para garantizar la interoperabilidad de los objetos firmados, se recomienda utilizar los siguientes formatos estandarizados:

Tipo de Dato	Formatos
Texto	XML (W3C XML Specification), JSON (ISO/IEC 21778:2017), PDF (ISO 32000-2).
Imagen	JPEG (ISO/IEC 10918),

⁶ Artículo 36 del Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales.



Tipo de Dato	Formatos
	PNG (ISO/IEC 15948), SVG (W3C SVG).
Audio	MP3 (ISO/IEC 11172-3, ISO/IEC 13818-3).
Video	MPEG-4 (ISO/IEC 14496).
Cartografía vectorial	GML (ISO 19136:2007).
Comprimidos	ZIP (ISO/IEC 21320-1:2015).

Se pueden utilizar formatos diferentes a los listados en la tabla anterior cuando existan particularidades que lo justifiquen y garanticen su interoperabilidad, o en el caso de documentos electrónicos que pudieran perder valor probatorio como resultado de una conversión a otro formato.

- b) Admite certificados digitales emitidos por las ECEP, subordinadas a la ECERNEP, así como los certificados emitidos por Entidades de Certificación privadas que están registradas en la TSL administrada por la AAC de la IOFE y que cumplen lo dispuesto en la Política General de Certificación de la ECERNEP.
- c) Cuando se requiera crear una firma digital con sello de tiempo, las personas naturales o entidades públicas usuarias deben adquirir este servicio a un PSVA-TSA acreditado ante la AAC. Es responsabilidad del firmante o entidad pública registrar en la plataforma FIRMA PERÚ los datos del sistema de sellado de tiempo (URL, usuario, y contraseña).

9. Servicio de Creación de firma digital

9.1 Es el servicio utilizado por un procedimiento en el cual un firmante crea una firma digital con la Plataforma FIRMA PERÚ.

9.2 El servicio de creación de firma digital, de acuerdo con su integración o no en un flujo documental, puede desarrollar tres (03) operaciones de creación de una firma digital:

a) Creación de firma digital de usuario final independiente de un flujo documental

Es utilizada cuando el firmante es una persona natural y la operación de firma se realiza de manera independiente a cualquier flujo documental. En este caso, el firmante es titular de un certificado digital de persona natural o es suscriptor⁷ de un certificado digital de persona jurídica. Los pasos para la creación de una firma digital en esta operación son los siguientes:

- **Paso 1:** Se prepara el documento electrónico a ser firmado, en el formato definido por el usuario.

⁷ De acuerdo con el Glosario de Términos del Reglamento de la Ley de Firmas y Certificados Digitales se entiende por suscriptor:

"Suscriptor. - Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad del suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica."



- **Paso 2:** El firmante accede a la plataforma FIRMA PERÚ y ejecuta el aplicativo de creación de firma digital.
- **Paso 3:** El firmante procede a seleccionar el documento a firmar. Opcionalmente, puede configurar un servicio de sello de tiempo y puede definir opciones de firma, p.ej. formato de firma (ver numeral 11 de la Guía), nivel de firma (ver numeral 13 de la Guía), entre otros.
- **Paso 4:** El aplicativo de creación de firma digital le solicita al firmante seleccionar un certificado digital.
- **Paso 5:** El aplicativo de creación de firma digital valida el certificado del firmante y de toda su ruta de certificación (CRL, OCSP, TSL).
- **Paso 6:** En el caso de firmas en formato PAdES, el aplicativo de creación de firma digital, le solicita al firmante definir los parámetros de la firma (motivo de firma, una representación gráfica, posición de la representación gráfica de la firma, entre otros).
- **Paso 7:** El aplicativo de creación de firma digital obtiene el hash del documento y lo envía al módulo criptográfico de creación de firma digital.
- **Paso 8:** El módulo criptográfico de creación de firma digital solicita al firmante su PIN o contraseña.
- **Paso 9:** El módulo criptográfico de creación de firma digital genera la firma digital y la devuelve al servicio de creación de firma digital.
- **Paso 10:** De ser el caso, el aplicativo de creación de firma digital solicita un sello de tiempo a un sistema de sellado de tiempo y lo empaqueta con la firma digital.
- **Paso 11:** La firma digital generada es devuelta al firmante, ya sea incrustada al documento o de manera independiente, de acuerdo con lo definido por el firmante.

El servicio de creación de firma digital de usuario final, independiente de un flujo documental, se encuentra disponible en el siguiente enlace:

- Enlace: <https://apps.firmaperu.gob.pe/web/firmador.xhtml>

b) Creación de firma digital de usuario final de manera integrada a un flujo documental

Es utilizada cuando el firmante es una persona natural y la operación de firma se realiza como parte de un flujo documental dentro de un sistema de información de una entidad pública. En este caso, el firmante es titular de un certificado digital de persona natural o es suscriptor de un certificado digital de persona jurídica. Los pasos para la creación de una firma digital en esta operación son los siguientes:

- **Paso 1:** Se prepara el documento electrónico a ser firmado por uno o varios firmantes. Esto puede ser realizado: (i) a iniciativa del personal que labora en la entidad pública (p.ej. secretaria, analista, el propio firmante, otros); (ii) de manera automatizada por el propio sistema de información; o, (iii) de una combinación de las dos anteriores. Asimismo, el creador del flujo de firma define los parámetros de la firma (formato de firma, nivel de firma, representación gráfica, posición, motivo de firma etc.) y el orden en el que van a firmar los firmantes (secuencial o paralelo).
- **Paso 2:** Los firmantes acceden al sistema de información e inician el acto de firma, conforme el orden de firma establecido en el paso anterior.



- **Paso 3:** Por cada firma, el sistema de información invoca al servicio de creación de firma digital de la Plataforma FIRMA PERÚ. En la invocación, el sistema de información envía los parámetros de firma definidos por el creador del flujo de firma (p.ej., el motivo de la firma, cargo del funcionario o servidor público, otros).
- **Paso 4:** El servicio de creación de firma digital le solicita al firmante seleccionar un certificado digital.
- **Paso 5:** El servicio de creación de firma digital valida el certificado del firmante y de toda su ruta de certificación (CRL, OCSP, TSL).
- **Paso 6:** De ser el caso, el servicio de creación de firma digital muestra al firmante el documento a firmar para que posicione manualmente la representación gráfica de la firma.
- **Paso 7:** El servicio de creación de firma digital obtiene el hash del documento y lo envía al módulo criptográfico de creación de firma digital.
- **Paso 8:** El módulo criptográfico de creación de firma digital solicita al firmante su PIN o contraseña.
- **Paso 9:** El módulo criptográfico de creación de firma digital genera la firma digital y la devuelve al servicio de creación de firma digital.
- **Paso 10:** De ser el caso, el servicio de creación de firma digital solicita un sello de tiempo a un sistema de sello de tiempo y, lo empaqueta con la firma digital.
- **Paso 11:** La firma digital generada es devuelta al sistema de información, ya sea incrustada al documento o de manera independiente, de acuerdo con lo definido por el mismo.

La documentación de integración entre un sistema de información y la Plataforma FIRMA PERÚ para la creación de firmas digitales dentro de un flujo documental se encuentra disponible en el siguiente enlace:

- Enlace: <https://resources.firmaperu.gob.pe/documentos/firmador-componente-web.pdf>

c) Creación de firma digital de agente automatizado de manera integrada a un flujo documental

Es utilizada cuando el firmante es titular de un certificado digital de agente automatizado y la operación de firma se realiza como parte de un flujo documental dentro de un sistema de información de una entidad pública. Los pasos para la creación de una firma digital en esta operación son los siguientes:

- **Paso 1:** La entidad pública prepara el documento electrónico y lo carga en el sistema de información.
- **Paso 2:** El sistema de información envía el documento al servicio de creación de firma digital de agente automatizado junto con los parámetros de firma.
- **Paso 3:** El servicio de creación de firma digital de agente automatizado valida el certificado de firma de agente automatizado y de toda su ruta de certificación (CRL, OCSP, TSL).
- **Paso 4:** El servicio de creación de firma digital de agente automatizado obtiene el hash del documento y lo envía al módulo criptográfico de creación de firma digital.
- **Paso 5:** El módulo criptográfico de creación de firma digital genera la firma digital y la devuelve al servicio de creación de firma digital de agente automatizado.



- **Paso 6:** De ser el caso, el servicio de creación de firma digital de agente automatizado solicita un sello de tiempo a un sistema de sellado de tiempo y, lo empaqueta con la firma digital.
- **Paso 7:** La firma digital generada es devuelta al sistema de información, ya sea incrustada al documento o de manera independiente, de acuerdo con lo definido por el mismo.
- **Paso 8:** El sistema de información, según lo definido por la entidad pública, asocia el documento electrónico con la firma digital creada y lo entrega al solicitante.

La documentación de integración entre un sistema de información y la Plataforma FIRMA PERÚ para la creación de firmas digitales de agente automatizado se encuentra disponible en el siguiente enlace:

- Enlace: <https://resources.firmaperu.gob.pe/documentos/agente-servicio-web.pdf>

10. Servicio de Validación de firma digital

10.1 Es el servicio de la Plataforma FIRMA PERÚ utilizado por un verificador para comprobar la validez de una firma digital y puede desarrollarse en dos (02) escenarios:

a) Validación de firma digital independiente de un flujo documental

Este escenario es utilizado cuando la validación la realiza una persona natural, quien elige el documento a ser validado y recibe el resultado de la validación. Los pasos para la validación de una firma digital son los siguientes:

- **Paso 1:** Un verificador carga en la Plataforma FIRMA PERÚ el documento electrónico firmado digitalmente. En el caso de tratarse de una firma desacoplada, carga el documento y la firma digital asociada.
- **Paso 2:** La Plataforma FIRMA PERÚ envía la información remitida por el verificador hacia el servicio de validación de firma digital.
- **Paso 3:** El servicio de validación de firma digital genera un reporte detallado del resultado y lo envía a la Plataforma FIRMA PERÚ.
- **Paso 4:** La plataforma FIRMA PERÚ presenta el reporte de validación al verificador.

El servicio de validación de firma digital independiente de un flujo documental se encuentra disponible en el siguiente enlace:

- Enlace: <https://apps.firmaperu.gob.pe/web/validador.xhtml>

b) Validación de firma digital integrada a un flujo documental

Este escenario es utilizado cuando la validación se hace como parte de un flujo documental. Los pasos para la validación de una firma digital son los siguientes:

- **Paso 1:** El sistema de información que soporta el flujo documental envía el documento electrónico firmado digitalmente (en caso se encuentren en un único fichero) o el documento y la firma digital asociada (en el caso que se encuentren en ficheros diferentes) hacia el servicio de validación de firma digital.



- **Paso 2:** El servicio de validación de firma digital efectúa la validación y genera un reporte detallado y lo envía al sistema de información.
- **Paso 3:** Si el resultado de la validación de la firma digital es "**VÁLIDO**", entonces el sistema de información continúa con el flujo documental.
- **Paso 4:** Si el resultado de la validación de la firma digital es "**NO VÁLIDO**" o "**INDETERMINADO**", entonces el sistema de información no continúa con el flujo documental.

La documentación de integración entre un sistema de información y la Plataforma FIRMA PERÚ para la validación de firmas digitales integrada a un flujo documental se encuentra disponible en el siguiente enlace:

- Enlace: <https://resources.firmaperu.gob.pe/documentos/validador-servicio-web.pdf>

10.2 Los resultados de la validación de una firma digital con la Plataforma FIRMA PERÚ, independientemente si se encuentra o no integrada a un flujo documental, son los siguientes:

- a) **VÁLIDO:** Este resultado se presenta cuando se pasaron con éxito todas las validaciones criptográficas de la firma digital, los requisitos de las guías de acreditación vigentes⁸ y la validación de la cadena de certificados.
- b) **NO VÁLIDO:** Este resultado se presenta cuando no se tuvo éxito en alguna de las validaciones criptográficas de la firma digital y/o en algún requisito de las guías de acreditación y/o en la validación de la cadena de certificados.
- c) **INDETERMINADO:** Este resultado se presenta cuando el software de validación no puede concluir que la firma digital es válida o es no válida.

11. Formatos de firma digital

Los formatos de firma digital admitidos en la Plataforma FIRMA PERÚ son los siguientes:

- a) **CADES** (*CMS Advanced Electronic Signatures*), según la especificación técnica ETSI TS 101 733, es la evolución del primer formato de firma estandarizado denominado CMS (*Cryptographic Message Syntax*). Es apropiado para firmar ficheros grandes, especialmente si la firma contiene el documento original porque optimiza el espacio de la información. Tras firmar, el ojo humano no puede ver la información firmada con un editor de texto, porque la información se guarda en formato binario.
- b) **XAdES** (*XML Advanced Electronic Signatures*), según la especificación técnica ETSI TS 101 903, es un fichero de texto XML, un formato de texto muy similar al HTML que utiliza etiquetas. Las firmas obtenidas suelen ser más grandes que en el caso del formato CADES, por eso no es adecuado cuando la prioridad es el espacio de almacenamiento.
- c) **PAdES** (*PDF Advanced Electronic Signatures*), según la especificación técnica ETSI TS 102 778-3, es el formato más adecuado cuando el documento original se encuentra en formato PDF. Opcionalmente, con este formato de firma se puede tener asociado una representación gráfica de la firma digital en alguna página del documento.

⁸ Guías de Acreditación aprobadas por la AAC.

12. Cardinalidad de un documento firmado digitalmente

12.1 La cardinalidad de un documento electrónico firmado digitalmente se refiere al número de firmas digitales asociadas al mismo, pudiendo ser una o múltiples firmas. Mientras que, en una sola firma digital interviene un único firmante, en una firma digital múltiple participan varios firmantes siguiendo un orden en secuencia o en paralelo.

12.2 La firma digital en secuencia es la firma digital múltiple en la que el orden en el que se firma el documento es la característica principal, ya que cada firma refrenda la firma del firmante anterior. Este orden de firmado se utiliza especialmente en escenarios en los que se debe seguir un flujo ordenado y específico en la creación de las firmas digitales. Los formatos de firma digital que soportan la firma digital en secuencia son el PAdES y el XAdES (embebido).

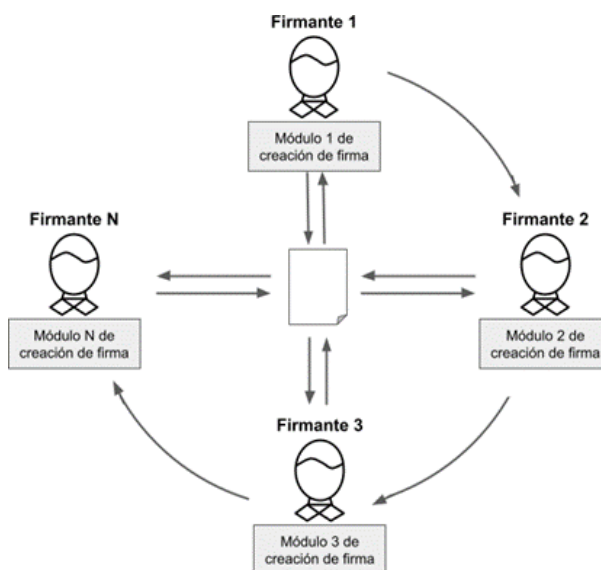


Figura 1. Orden de los firmantes para la creación de una firma digital en secuencia

12.3 La firma digital en paralelo es la firma múltiple en la que todos los firmantes pueden firmar el documento, de manera simultánea o no, sin importar el orden en el que se firma. Este tipo de firma múltiple se puede utilizar en situaciones donde los firmantes tienen el mismo rango o responsabilidad en la firma del documento. Los formatos de firma digital que soportan la firma digital en paralelo son el CADES y el XAdES.

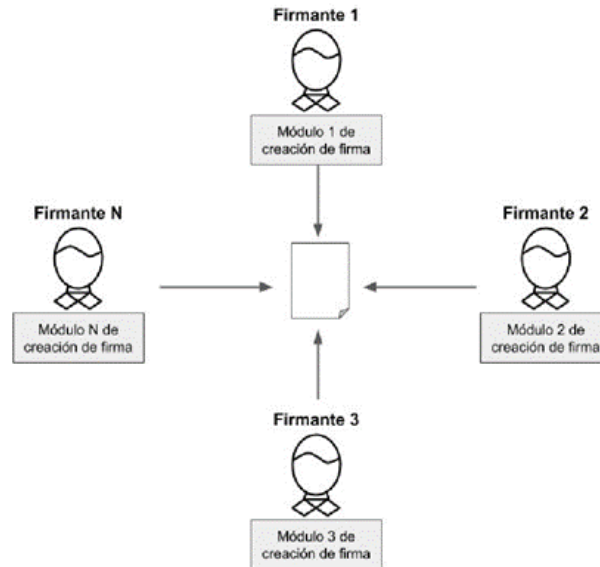


Figura 2. Firma digital en paralelo

12.4 El servicio de creación de flujos de firma digital de la Plataforma FIRMA PERÚ permite definir flujos de firma digital en secuencia o en paralelo de manera independiente a un flujo documental. Aquellas entidades públicas que requieran implementar flujos de firma digital en secuencia o en paralelo dentro de un flujo documental (por ejemplo: un sistema de gestión documental, sistema de trámite documentario, entre otros) deben desarrollar estas funcionalidades como parte de sus sistemas de información de gestión documental.

13. Niveles de firma digital

Dependiendo de la naturaleza del documento electrónico a firmar digitalmente y, de ser el caso, de las políticas de seguridad y gestión documental, la Plataforma FIRMA PERÚ permite que el firmante o el creador del flujo de firma elijan uno de los siguientes niveles de firma digital:

- Firma digital básica (*B level*)**. Esta firma digital no incluye el uso de un sello de tiempo, sino, utiliza la fecha y hora del reloj del computador local donde se efectúa la operación de firma.
- Firma digital con sello de tiempo (*T level*)**. Esta firma digital utiliza un servicio de sellado de tiempo proporcionado por un PSVA-TSA acreditado en el marco de la IOFE, para obtener una fecha y hora confiable, la cual es incrustada en la firma digital.
- Firma digital con datos de validación a largo plazo (*LTA level*)**. Esta firma digital incluye datos de validación a largo plazo que permiten la validación de una firma digital posterior a la expiración de los objetos criptográficos utilizados en la firma digital, incluso sin necesidad de estar conectado al Internet. Asimismo, utiliza un servicio de sellado de tiempo proporcionado por un PSVA-TSA acreditado en el marco de la IOFE, para obtener una fecha y hora confiable, la cual es incrustada en la firma digital.

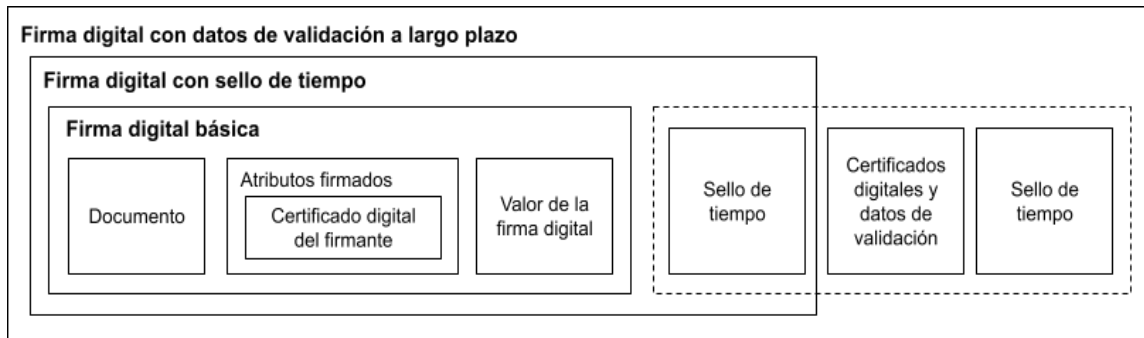


Figura 3. Diagrama ilustrativo de los niveles de firma digital

14. Firma digital en lote

- 14.1 La firma digital en lote es aquella operación de creación de firma digital en la cual múltiples documentos son firmados por un único firmante. La Plataforma FIRMA PERÚ permite la creación de firmas digitales en lote.
- 14.2 Dependiendo del módulo criptográfico utilizado, el firmante debe ingresar su PIN o contraseña una única vez por todo el lote o una vez por cada documento del lote. Es potestad del firmante contar con un módulo criptográfico de creación de firma digital que satisfaga el caso de uso exigido por su sistema de información y la IOFE.

15. Credenciales para la integración con la Plataforma FIRMA PERÚ

- 15.1 La Plataforma FIRMA PERU, para su integración a los sistemas de información de las entidades públicas, requiere la generación de credenciales asociadas a la entidad.
- 15.2 La credencial es generada por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, para lo cual las entidades públicas, a través de un correo electrónico institucional del Responsable de la unidad de organización de tecnologías de la información o la que haga sus veces en las entidades públicas, deben solicitarla al correo firmaperu@pcm.gob.pe, indicando en el asunto "**Solicitud de Credenciales FIRMA PERÚ**", y consignando la siguiente información según el servicio que desean integrar:

- Para la solicitud de la credencial:

Datos de la entidad pública	N° de RUC
	Nombre
	Siglas
	Dirección completa (Incluir departamento, provincia y distrito)
Datos de contacto técnico	N° de DNI
	Nombres y apellidos
	Correo institucional
	N° de celular



- Para el servicio de creación de firma digital:

Datos del sistema de información	Nombre del sistema de información que se integrará al servicio de firma digital.
	URL del sistema de información que se integrará al servicio (producción y/o pruebas y desarrollo separado por ";").

- Para el servicio de creación de firma digital de agente automatizado:

Datos de uso y servidor	Uso: Descripción del uso que se dará al servicio solicitado.
	IP del servidor: producción y/o pruebas y desarrollo separado por ";".

- Para el servicio de validación de firma:

Datos de uso y servidor	Uso: Descripción del uso que se dará al servicio solicitado.
	IP del servidor: Producción y/o pruebas y desarrollo separado por ";".

- 15.3 Las credenciales generadas son enviadas únicamente al correo institucional del contacto técnico. De preferencia, el contacto técnico es un profesional de la unidad de organización de tecnologías de la información o la que haga sus veces en la entidad pública. El contacto técnico es responsable de salvaguardar esta información.
- 15.4 El Responsable de la unidad de organización de tecnologías de la información o la que haga sus veces puede solicitar que se regeneren las credenciales de un determinado servicio, para ello solicita dicha acción al correo electrónico firmaperu@pcm.gob.pe, consignando el número de RUC de la entidad pública, número de celular del contacto técnico y el ID de cliente (dato contenido dentro de la credencial). Recibida dicha solicitud se enviará la nueva credencial generada al correo electrónico del contacto técnico.
- 15.5 La entidad pública es responsable de utilizar certificados digitales que satisfacen lo descrito en el literal b) del numeral 8 de la presente norma, así como, de utilizar módulos criptográficos de creación de firma digital que satisfacen lo exigido por la IOFE.