REPORTE TEMÁTICO N.° 175/2024-2025

FIRMA DIGITAL

Legislación nacional

Lima, 27 de mayo de 2025

Plaza Bolívar, Av. Abancay s/n – Lima, Perú
Central Telefónica: 311-7777

www.congreso.gob.pe

PRESENTACIÓN

El Departamento de Investigación Parlamentaria, a través del Área de Servicios de Investigación y Seguimiento Presupuestal, ha elaborado el Reporte Temático N.º 175/2024-2025-ASISP/DIP, referido a la firma digital en nuestro ordenamiento jurídico vigente.

Para la elaboración se ha consultado la información disponible en fuentes oficiales sobre la materia; cuyas referencias se consignan en el documento.

Esperamos poder brindar información que contribuya a la labor parlamentaria.

1. CONSIDERACIONES GENERALES

La gobernanza digital "es la articulación y concreción de políticas de interés público con los diversos actores involucrados (Estado, Sociedad Civil y Sector Privado), con la finalidad de alcanzar competencias y cooperación para crear valor público y la optimización de los recursos de los involucrados, mediante el uso de tecnologías digitales[1]". Busca:

- Establecer las estructuras y procesos que aseguren que la estrategia de gobierno digital se alinea con los objetivos estratégicos de gobierno
- Articular y concretar políticas de interés público entre actores involucrados para crear valor público
- Que los riesgos y oportunidades sean adecuadamente administrados
- Optimizar los recursos disponibles a través del uso racional de las tecnologías digitales[2]

En dicho contexto, el gobierno digital debe entenderse como "el uso de las tecnologías digitales como parte integral de las estrategias de modernización de los gobiernos con el fin de crear valor público (…) un ecosistema de gobierno digital constituido por los actores estatales, organizaciones no gubernamentales, empresas, asociaciones de ciudadanos y personas encargadas de la producción y acceso a los datos, servicios y contenidos a través de interacciones con el gobierno[3]". Sus componentes estructurales son; (i) la identidad digital; (ii) el portal digital del Estado; (iii) la interoperabilidad gubernamental; (iv) la carpeta digital ciudadana; (v) la casilla digital del ciudadano; y (vi) la ciberseguridad.

1.1 Firma digital

La identidad digital es el uso de tecnología para asegurar y probar identidad[4] (la representación de la persona en el entorno digital); así como para acceder a determinados recursos de información o físicos, y realizar transacciones a través de Internet o redes privadas[5]. Y la herramienta por medio de la cual se valida dicha identidad y garantiza la autenticidad de los documentos digitales es la firma digital.

La *Guía para el uso e integración de la Plataforma Nacional de Firma Digital en la Administración Pública*[6], de la Secretaría de Gobierno y Transformación Digita, de la Presidencia del Consejo de Ministros, indica que la Plataforma FIRMA PERÚ permite la creación y validación de firmas digitales dentro del marco de la *Infraestructura Oficial de Firma Electrónica*, para la provisión de los servicios digitales prestados por las entidades de la Administración Pública. Y presenta las siguientes definiciones:

> **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

[1] NASER, Alejandra. Gobernanza digital e interoperabilidad gubernamental. Una guía para su implementación. CEPAL, 2021.p. 14. https://www.cepal.org/es/publicaciones/47018-gobernanza-digital-interoperabilidad-gubernamental-guia-su-implementacion
[2] https://biblioguias.cepal.org/gobierno-digital/concepto-gobernanza
[3] NASER, Alejandra, Op. cit, p. 15.
[4] FATF GUIDANCE ON DIGITAL IDENTITY IN BRIEF, 2020, https://www.fatf-gafi.org/content/dam/fatf-gafi/brochures/Digital-ID-in-brief.pdf
[5] https://biblioguias.cepal.org/gobierno-digital/identidad-digital
[6] https://cdn.www.gob.pe/uploads/document/file/3690615/Gu%C3%ADa%20para%20el%20uso%20e%20integraci%C3%B3n%20de%20la%20Plataforma%20Nacional%20de%20Firma%20Digital%20en%20la%20Administraci%C3%B3n%20P%C3%BAblica.pdf?v=1664204905

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 Civil.

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 jurídica. El ciclo de vida de un certificado digital comprende: la emisión, la cancelación, y la renovación.

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 entonces.

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 plazo.

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.

Firma Perú cuenta con servicios de:

Para la ciudadanía en general:

- Firmador de documentos: aplicación para PC que te permite generar tu firma digital.
- Validador de firmas digitales: servicio digital que te permite validar firmas digitales.

Para las entidades públicas:

- Firmador: componente que se integra a las aplicaciones web y de PC institucionales para generar firmas digitales a nombre de personas jurídicas o naturales (con DNIe).
- Validador: aplicación tipo servicio web para los servicios de las entidades públicas para la validación desatendida de firma digital.
- Agente: aplicación tipo servicio web para los servicios de las entidades públicas para la generación desatendida de firma digital.

CUADRO 1
LEGISLACIÓN NACIONAL

<table>
<tr><td rowspan="2">FIRMA DIGITAL</td><td>Firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.</td><td>Modalidades de firma electrónica:
a) Firma Electrónica Simple. Es un dato en formato electrónico anexo a otros datos electrónicos o asociado de manera lógica con ellos, que utiliza un firmante para firmar.
b) Firma Electrónica Avanzada. Es aquella firma electrónica simple que cumple con las siguientes características: (i) está vinculada al firmante de manera única, (ii) permite la identificación del firmante, (iii) ha sido creada utilizando datos de creación de firmas que el firmante puede utilizar bajo su control, y (iv) está vinculada con los datos firmados de modo tal que cualquier modificación posterior de los mismos es detectable.
c) Firma Electrónica Cualificada. La firma electrónica cualificada o firma digital es aquella firma electrónica avanzada que cumple con lo establecido en el capítulo II del presente Reglamento</td><td>No se restringe la utilización de las firmas digitales generadas fuera de la Infraestructura Oficial de Firma Electrónica, las cuales serán válidas en consideración a los pactos o convenios que acuerden las partes.</td><td>a) En caso de controversia sobre la autoría de la firma electrónica simple o avanzada, la carga de la prueba recae en quien la invoque como auténtica.
b) En caso de controversia, en la utilización de la firma electrónica cualificada, la carga de la prueba se invierte debiendo quien niegue la autoría, demostrar que la firma es apócrifa.</td></tr>
<tr><td colspan="2">La firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita.</td><td colspan="2">Los documentos electrónicos firmados digitalmente dentro del marco de la Infraestructura Oficial de Firma Electrónica deberán ser admitidos como prueba en los procesos judiciales y/o procedimientos administrativos, siempre y cuando la firma digital haya sido realizada utilizando un certificado emitido por una Entidad de Certificación acreditada en cooperación con una Entidad de Registro o Verificación acreditada.
La comprobación de la validez de un documento firmado digitalmente se realiza en un ambiente electrónico aplicando el Software de Verificación de la firma digital. En caso de controversia sobre la validez de la firma digital, el Juez podrá solicitar a la Autoridad Administrativa Competente el nombramiento de un perito especializado en firmas digitales.</td></tr>
</table>

CARACTERÍSTICAS DE LA FIRMA DIGITAL	a) Se genera al cifrar el código de verificación de un documento electrónico, usando la clave privada del titular del certificado. b) Es exclusiva del suscriptor y de cada documento electrónico firmado por éste. c) Es susceptible de ser verificada usando la clave pública del suscriptor. d) Su generación está bajo el control exclusivo del suscriptor. e) Está añadida o incorporada al documento electrónico mismo de tal manera que es posible detectar si la firma digital o el documento electrónico fue alterado.		
TITULAR DE LA FIRMA DIGITAL	La persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos.	Tiene la obligación de brindar a las entidades de certificación y a los terceros con quienes se relacione a través de la utilización de la firma digital, declaraciones o manifestaciones materiales exactas y completas	Las personas naturales deberán presentar una solicitud a la Entidad de Registro o Verificación; dicha solicitud deberá estar acompañada de toda la información requerida por la Declaración de Prácticas de Registro o Verificación, o en los procedimientos declarados. La Entidad de Registro o Verificación deberá comprobar la identidad del solicitante a través de su documento oficial de identidad. En el caso de personas jurídicas, la solicitud del certificado digital y el registro o verificación de su identidad deberán realizarse a través de un representante debidamente acreditado. La persona jurídica se constituirá en titular del certificado digital. Conjuntamente con la solicitud, debe indicarse la persona natural que será el suscriptor, señalando para tal efecto las atribuciones y los poderes de representación correspondientes. Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, las facultades de titular y suscriptor de dicho certificado corresponderán a la persona jurídica, quien asumirá la responsabilidad por el uso de dicho certificado digital.
CERTIFICADOS DIGITALES	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.	1. Datos que identifiquen indubitablemente al suscriptor. 2. Datos que identifiquen a la Entidad de Certificación. 3. La clave pública. 4. La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos. 5. Número de serie del certificado. 6. Vigencia del certificado. 7. Firma digital de la Entidad de Certificación.	Para la obtención de un certificado digital, el solicitante deberá acreditar lo siguiente: a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles. b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.
CANCELACIÓN CERTIFICADO DIGITAL	1. A solicitud del titular de la firma digital. 2. Por revocatoria de la entidad certificante. 3. Por expiración del plazo de vigencia. 4. Por cese de operaciones de la Entidad de Certificación.		

REVOCACIÓN DEL CERTIFICADO DIGITAL	1. Se determine que la información contenida en el certificado digital es inexacta o ha sido modificada. 2. Por muerte del titular de la firma digital. 3. Por incumplimiento derivado de la relación contractual con la Entidad de Certificación.
ENTIDAD DE CERTIFICACIÓN	Cumple con la función de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado o aquellos que brinden seguridad al sistema de certificados en particular o del comercio electrónico en general. Las Entidades de Certificación podrán igualmente asumir las funciones de Entidades de Registro o Verificación.
ENTIDAD DE REGISTRO O VERIFICACIÓN	Cumple con la función de levantamiento de datos y comprobación de la información de un solicitante de certificado digital; identificación y autenticación del suscriptor de firma digital; aceptación y autorización de solicitudes de emisión de certificados digitales; aceptación y autorización de las solicitudes de cancelación de certificados digitales.

Fuente: Sistema Peruano de Información Jurídica (SPIJ).
Elaboración: Área de Servicios de Información y Seguimiento Presupuestal (ASISP).

CUADRO 2
FIRMA DIGITAL

Norma	Texto
Ley 27269 Ley de Firmas y Certificados Digitales	**Artículo 1.- Objeto de la ley** La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad. Entiéndase por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita. **Artículo 2.- Ámbito de aplicación** La presente ley se aplica a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos. **DE LA FIRMA DIGITAL** **Artículo 3.- Firma digital** La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada. **DEL TITULAR DE LA FIRMA DIGITAL** **Artículo 4.- Titular de la firma digital** El titular de la firma digital es la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos. **Artículo 5.- Obligaciones del titular de la firma digital** El titular de la firma digital tiene la obligación de brindar a las entidades de certificación y a los terceros con quienes se relacione a través de la utilización de la firma digital, declaraciones o manifestaciones materiales exactas y completas. **DE LOS CERTIFICADOS DIGITALES** **Artículo 6.- Certificado digital** El 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.

	Artículo 7.- Contenido del certificado digital Los certificados digitales emitidos por las entidades de certificación deben contener al menos: 1. Datos que identifiquen indubitablemente al suscriptor. 2. Datos que identifiquen a la Entidad de Certificación. 3. La clave pública. 4. La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos. 5. Número de serie del certificado. 6. Vigencia del certificado. 7. Firma digital de la Entidad de Certificación. **Artículo 8.- Confidencialidad de la información** La entidad de registro recabará los datos personales del solicitante de la firma digital directamente de éste y para los fines señalados en la presente ley. Asimismo, la información relativa a las claves privadas y datos que no sean materia de certificación se mantiene bajo la reserva correspondiente. Sólo puede ser levantada por orden judicial o pedido expreso del suscriptor de la firma digital. **Artículo 9.- Cancelación del certificado digital** La cancelación del certificado digital puede darse: 1. A solicitud del titular de la firma digital. 2. Por revocatoria de la entidad certificante. 3. Por expiración del plazo de vigencia. 4. Por cese de operaciones de la Entidad de Certificación. **Artículo 10.- Revocación del certificado digital** La Entidad de Certificación revocará el certificado digital en los siguientes casos: 1. Se determine que la información contenida en el certificado digital es inexacta o ha sido modificada.

	2. Por muerte del titular de la firma digital. 3. Por incumplimiento derivado de la relación contractual con la Entidad de Certificación. **Artículo 11.-** Los Certificados de Firmas Digitales emitidos por Entidades Extranjeras tendrán la misma validez y eficacia jurídica reconocidas en la presente Ley, siempre y cuando tales certificados sean reconocidos por la autoridad administrativa competente. **DE LAS ENTIDADES DE CERTIFICACION Y DE REGISTRO** **Artículo 12.- Entidad de Certificación** La Entidad de Certificación cumple con la función de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado o aquellos que brinden seguridad al sistema de certificados en particular o del comercio electrónico en general. Las Entidades de Certificación podrán igualmente asumir las funciones de Entidades de Registro o Verificación. **Artículo 13.- Entidad de Registro o Verificación** La Entidad de Registro o Verificación cumple con la función de levantamiento de datos y comprobación de la información de un solicitante de certificado digital; identificación y autenticación del suscriptor de firma digital; aceptación y autorización de solicitudes de emisión de certificados digitales; aceptación y autorización de las solicitudes de cancelación de certificados digitales. **Artículo 14.- Depósito de los Certificados Digitales** Cada Entidad de Certificación debe contar con un Registro disponible en forma permanente, que servirá para constatar la clave pública de determinado certificado y no podrá ser usado para fines distintos a los estipulados en la presente ley. El Registro contará con una sección referida a los certificados digitales que hayan sido emitidos y figurarán las circunstancias que afecten la cancelación o vigencia de los mismos, debiendo constar la fecha y hora de inicio y fecha y hora de finalización. A dicho Registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten. **Artículo 15.- Inscripción de Entidades de Certificación y de Registro o Verificación** El Poder Ejecutivo, por Decreto Supremo, determinará la autoridad administrativa competente y señalará sus funciones y facultades. La autoridad competente se encargará del Registro de Entidades de Certificación y Entidades de Registro o Verificación, las mismas que deberán cumplir con los estándares técnicos internacionales. Los datos que contendrá el referido Registro deben cumplir principalmente con la función de identificar a las Entidades de Certificación y Entidades de Registro o Verificación. (…).

	DISPOSICIONES COMPLEMENTARIAS, TRANSITORIAS Y FINALES (…). **Tercera. -** La autoridad competente podrá aprobar la utilización de otras tecnologías de firmas electrónicas siempre que cumplan con los requisitos establecidos en la presente ley, debiendo establecer el Reglamento las disposiciones que sean necesarias para su adecuación. (…).
Decreto Supremo N°.052-2008-PCM Reglamento de la Ley de Firmas y Certificados Digitales	DISPOSICIONES GENERALES **Artículo 1.- Del objeto** El objeto de la presente norma es regular, para los sectores público y privado, la utilización de las firmas digitales y el régimen de la Infraestructura Oficial de Firma Electrónica, que comprende la acreditación y supervisión de las Entidades de Certificación, las Entidades de Registro o Verificación, y los Prestadores de Servicios de Valor Añadido; de acuerdo a lo establecido en la Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley Nº 27310, en adelante la Ley. Reconociendo la variedad de modalidades de firmas electrónicas, la diversidad de garantías que ofrecen, los diversos niveles de seguridad y la heterogeneidad de las necesidades de sus potenciales usuarios, la Infraestructura Oficial de Firma Electrónica no excluye ninguna modalidad, ni combinación de modalidades de firmas electrónicas, siempre que cumplan los requisitos establecidos en el artículo 2 de la Ley. **Artículo 1A.- Modalidades de la firma electrónica** Se reconocen las siguientes tres (03) modalidades de firma electrónica: a) Firma Electrónica Simple. Es un dato en formato electrónico anexo a otros datos electrónicos o asociado de manera lógica con ellos, que utiliza un firmante para firmar. b) Firma Electrónica Avanzada. Es aquella firma electrónica simple que cumple con las siguientes características: (i) está vinculada al firmante de manera única, (ii) permite la identificación del firmante, (iii) ha sido creada utilizando datos de creación de firmas que el firmante puede utilizar bajo su control, y (iv) está vinculada con los datos firmados de modo tal que cualquier modificación posterior de los mismos es detectable. c) Firma Electrónica Cualificada. La firma electrónica cualificada o firma digital es aquella firma electrónica avanzada que cumple con lo establecido en el capítulo II del presente Reglamento **Artículo 2.- De la utilización de las firmas digitales** Las disposiciones contenidas en el presente Reglamento no restringen la utilización de las firmas digitales generadas fuera de la Infraestructura Oficial de Firma Electrónica, las cuales serán válidas en consideración a los pactos o convenios que acuerden las partes. **Artículo 2A.- Carga de la prueba de la firma electrónica** Para cada modalidad de firma electrónica la aplicación de la carga de la prueba varía conforme a lo siguiente:

a) En caso de controversia sobre la autoría de la firma electrónica simple o avanzada, la carga de la prueba recae en quien la invoque como auténtica.

b) En caso de controversia, en la utilización de la firma electrónica cualificada, la carga de la prueba se invierte debiendo quien niegue la autoría, demostrar que la firma es apócrifa.

CAPÍTULO I
DE LA VALIDEZ Y EFICACIA JURÍDICA DE LAS FIRMAS DIGITALES Y DOCUMENTOS ELECTRÓNICOS

Artículo 3.- De la validez y eficacia de la firma digital
La firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita. En tal sentido, cuando la ley exija la firma de una persona, ese requisito se entenderá cumplido en relación con un documento electrónico si se utiliza una firma digital generada en el marco de la Infraestructura Oficial de la Firma Electrónica.

Lo establecido en el presente artículo y las demás disposiciones del presente Reglamento no excluyen el cumplimiento de las formalidades específicas requeridas para los actos jurídicos y el otorgamiento de fe pública.

Artículo 4.- De los documentos firmados digitalmente como medio de prueba
Los documentos electrónicos firmados digitalmente dentro del marco de la Infraestructura Oficial de Firma Electrónica deberán ser admitidos como prueba en los procesos judiciales y/o procedimientos administrativos, siempre y cuando la firma digital haya sido realizada utilizando un certificado emitido por una Entidad de Certificación acreditada en cooperación con una Entidad de Registro o Verificación acreditada, salvo que se tratara de la misma entidad con ambas calidades y con la correspondiente acreditación para brindar ambos servicios, asimismo deberá haberse aplicado un software de firmas digitales acreditado ante la Autoridad Administrativa Competente. Esto incluye la posibilidad de que a voluntad de las partes pueda haberse utilizado un servicio de intermediación digital.

La firma digital generada en el marco de la Infraestructura Oficial de Firma Electrónica garantiza el no repudio del documento electrónico original. Esta garantía no se extiende a los documentos individuales que conforman un documento compuesto, a menos que cada documento individual sea firmado digitalmente.

La comprobación de la validez de un documento firmado digitalmente se realiza en un ambiente electrónico aplicando el Software de Verificación de la firma digital. En caso de controversia sobre la validez de la firma digital, el Juez podrá solicitar a la Autoridad Administrativa Competente el nombramiento de un perito especializado en firmas digitales, sin perjuicio de lo dispuesto por los artículos 252, 264 y 268 del Código Procesal Civil.

Si el documento firmado digitalmente se ha convertido en una microforma o microarchivo, el notario o fedatario con Diploma de Idoneidad Técnica vigente cumplirá con las normas del Decreto Legislativo Nº 681 y cuidará de cumplir aquellas normas que sean pertinentes de la Ley y de este Reglamento.

Artículo 5.- De la conservación de documentos electrónicos
Cuando los documentos, registros o informaciones requieran de una formalidad para la conservación de documentos electrónicos firmados digitalmente, deberán:

	a) Ser accesibles para su posterior consulta. b) Ser conservados con su formato original de generación, envío, recepción u otro formato que reproduzca en forma demostrable la exactitud e integridad del contenido electrónico. c) Ser conservado todo dato que permita determinar el origen, destino, fecha y hora del envío y recepción. La firma digital vinculada a un certificado digital generada bajo la Infraestructura Oficial de Firma Electrónica no requiere mecanismos adicionales para conservar dicho documento a salvo de adulteraciones y asegurar el cumplimiento del principio de equivalencia funcional y la integridad del contenido del documento electrónico. CAPÍTULO II DE LA FIRMA DIGITAL **Artículo 6.- De la 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 Civil. Las firmas digitales son las generadas a partir de certificados digitales que son: a) Emitidos conforme a lo dispuesto en el presente Reglamento por entidades de certificación acreditadas ante la Autoridad Administrativa Competente. b) Incorporados a la Infraestructura Oficial de Firma Electrónica bajo acuerdos de certificación cruzada, conforme al artículo 73 del presente Reglamento. c) Reconocidos al amparo de acuerdos de reconocimiento mutuo suscritos por la Autoridad Administrativa Competente conforme al artículo 71 del presente Reglamento. d) Emitidos por Entidades de Certificación extranjeras que hayan sido incorporados por reconocimiento a la Infraestructura Oficial de Firma Electrónica conforme al artículo 72 del presente Reglamento. **Artículo 7.- De las características de la firma digital** Las características mínimas de la firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica son: a) Se genera al cifrar el código de verificación de un documento electrónico, usando la clave privada del titular del certificado. b) Es exclusiva del suscriptor y de cada documento electrónico firmado por éste.

	c) Es susceptible de ser verificada usando la clave pública del suscriptor. d) Su generación está bajo el control exclusivo del suscriptor. e) Está añadida o incorporada al documento electrónico mismo de tal manera que es posible detectar si la firma digital o el documento electrónico fue alterado. **Artículo 8.- De las presunciones** Tratándose de documentos electrónicos firmados digitalmente a partir de certificados digitales generados dentro de la Infraestructura Oficial de Firma Electrónica, se aplican las siguientes presunciones: a) Que el suscriptor del certificado digital tiene el control de la clave privada asociada, con un elevado grado de confianza, incluso cuando la misma es gestionada por un Prestador de Servicios de Valor Añadido acreditado en la modalidad de sistema de creación de firma remota. b) Que el documento electrónico fue firmado empleando la clave privada del suscriptor del certificado digital. c) Que el documento electrónico no ha sido alterado con posterioridad al momento de la firma. Como consecuencia de los literales previos, el suscriptor no podrá repudiar o desconocer un documento electrónico que ha sido firmado digitalmente usando su clave privada, siempre que no medie ninguno de los vicios de la voluntad previstos en el Título VIII del Libro II del Código Civil. **Artículo 9.- Del suscriptor** Dentro de la Infraestructura Oficial de Firma Electrónica, la responsabilidad sobre los efectos jurídicos generados por la utilización de una firma digital corresponde al titular del certificado. Tratándose de personas naturales, éstas son titulares y suscriptores del certificado digital. En el caso de personas jurídicas, éstas son titulares del certificado digital. Los suscriptores son las personas naturales responsables de la generación y uso de la clave privada, con excepción de los certificados digitales para su utilización a través agentes automatizados, situación en la cual las personas jurídicas asumen las facultades de titulares y suscriptores del certificado digital. **Artículo 10.- De las obligaciones del suscriptor** Las obligaciones del suscriptor son: a) Entregar información veraz bajo su responsabilidad. b) Generar por sí mismo la clave privada, o autorizar su generación a distancia por parte de un Prestador de Servicios de Valor Añadido acreditado en la modalidad de sistema de creación de firma remota, y firmar digitalmente mediante los procedimientos señalados por la Entidad de Certificación.

	c) Mantener el control y la reserva de la clave privada bajo su responsabilidad, sin perjuicio de la responsabilidad del Prestador de Servicios de Valor Añadido acreditado en la modalidad de sistema de creación de firma remota que genere la clave privada para el servicio de firma remota. d) Observar las condiciones establecidas por la Entidad de Certificación para la utilización del certificado digital y la generación de firmas digitales. e) En caso de que la clave privada quede comprometida en su seguridad, el suscriptor debe notificarlo de inmediato a la Entidad de Registro o Verificación o a la Entidad de Certificación que participó en su emisión para que proceda a la cancelación del certificado digital. **Artículo 11.- De la invalidez** Una firma digital generada bajo la Infraestructura Oficial de Firma Electrónica carece de validez, además de los supuestos que prevé la legislación civil, cuando: a) Es utilizada en fines distintos para los que fue extendido el certificado. b) El certificado haya sido cancelado conforme a lo establecido en el Capítulo III del presente Título. CAPÍTULO III DEL CERTIFICADO DIGITAL **Artículo 12.- De los requisitos** Para la obtención de un certificado digital, el solicitante deberá acreditar lo siguiente: a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles. b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos. **Artículo 13.- De las especificaciones adicionales para ser titular** Para ser titular de un certificado digital adicionalmente se deberá cumplir con entregar la información solicitada por la Entidad de Registro o Verificación, de acuerdo a lo estipulado por la Entidad de Certificación correspondiente, asumiendo el titular la responsabilidad por la veracidad y exactitud de la información proporcionada, sin perjuicio de la respectiva comprobación. En el caso de personas naturales, la solicitud del certificado digital y el registro o verificación de su identidad son estrictamente personales. La persona natural solicitante se constituirá en titular y suscriptor del certificado digital. **Artículo 14.- Del procedimiento para ser titular**

	Las personas naturales deberán presentar una solicitud a la Entidad de Registro o Verificación; dicha solicitud deberá estar acompañada de toda la información requerida por la Declaración de Prácticas de Registro o Verificación, o en los procedimientos declarados. La Entidad de Registro o Verificación deberá comprobar la identidad del solicitante a través de su documento oficial de identidad. En el caso de personas jurídicas, la solicitud del certificado digital y el registro o verificación de su identidad deberán realizarse a través de un representante debidamente acreditado. La persona jurídica se constituirá en titular del certificado digital. Conjuntamente con la solicitud, debe indicarse la persona natural que será el suscriptor, señalando para tal efecto las atribuciones y los poderes de representación correspondientes. Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, las facultades de titular y suscriptor de dicho certificado corresponderán a la persona jurídica, quien asumirá la responsabilidad por el uso de dicho certificado digital. **Artículo 15.- De las obligaciones del titular** Las obligaciones del titular son: a) Entregar información veraz durante la solicitud de emisión de certificados y demás procesos de certificación (cancelación, suspensión, re-emisión y modificación). b) Actualizar la información provista tanto a la Entidad de Certificación como a la Entidad de Registro o Verificación, asumiendo responsabilidad por la veracidad y exactitud de ésta. c) Solicitar la cancelación de su certificado digital en caso de que la reserva sobre la clave privada se haya visto comprometida, bajo responsabilidad, excepto cuando dicha clave sea gestionada por un Prestador de Servicios de Valor Añadido acreditado en la modalidad de sistema de creación de firma remota. d) Cumplir permanentemente las condiciones establecidas por la Entidad de Certificación para la utilización del certificado y, en su caso, por el Prestador de Servicios de Valor Añadido acreditado en la modalidad de sistema de creación de firma remota. **Artículo 16.- Contenido y vigencia** Los certificados emitidos dentro de la Infraestructura Oficial de Firma Electrónica contienen como mínimo, además de lo establecido en el artículo 7 de la Ley, lo siguiente: a) Para personas naturales: * Nombres y apellidos completos * Número de documento oficial de identidad * Tipo de documento * Dirección electrónica de los servicios donde consultar el estado de validez del certificado * Dirección electrónica del certificado de la entidad de certificación emisora * Identificador de la política de certificación bajo la cual fue emitido el certificado

b) Para personas jurídicas (suscriptor):

* Denominación o razón social
* Número del Registro Único de Contribuyentes (RUC) de la organización
* Nombres y apellidos completos del suscriptor
* Número de documento oficial de identidad del suscriptor
* Tipo de documento del suscriptor
* Dirección electrónica de los servicios donde consultar el estado de validez del certificado
* Dirección electrónica del certificado de la entidad de certificación emisora
* Identificador de la política de certificación bajo la cual fue emitido el certificado

c) Para personas jurídicas (titular):

* Denominación o razón social
* Número del Registro Único de Contribuyentes (RUC) de la organización
* Nombre del sistema de información o sistema de cómputo
* Dirección electrónica de los servicios donde consultar el estado de validez del certificado
* Dirección electrónica del certificado de la entidad de certificación emisora
* Identificador de la política de certificación bajo la cual fue emitido el certificado.

Artículo 17.- De las causales de cancelación
La cancelación del certificado digital puede darse:

a) A solicitud del titular del certificado digital o del suscriptor sin previa justificación, siendo necesario para tal efecto la aceptación y autorización de la Entidad de Certificación o la Entidad de Registro o Verificación, según sea el caso, dentro del plazo establecido por la Autoridad Administrativa Competente. Si una solicitud de cancelación es aprobada por la Entidad de Registro o Verificación, y luego tal entidad supere el plazo máximo en el cual debe comunicar dicha aprobación a la Entidad de Certificación correspondiente, dicha Entidad de Registro o Verificación será responsable por los daños ocasionados debido a la demora. De otro modo, habiendo sido notificada dentro del plazo establecido, la Entidad de Certificación será responsable de los daños que pueda ocasionar la demora en dicha cancelación. Del mismo modo ocurrirá en el caso que un suscriptor o titular solicite directamente a la Entidad de Certificación la cancelación de su certificado. Compete a la Autoridad Administrativa Competente establecer las sanciones respectivas.

b) Por decisión de la Entidad de Certificación (por revocación, según los supuestos contenidos en el artículo 10 de la Ley), con expresión de causa.

c) Por expiración del plazo de vigencia.

d) Por cese de operaciones de la Entidad de Certificación que emitió el certificado.

e) Por resolución administrativa o judicial que ordene la cancelación del certificado.

	f) Por interdicción civil judicialmente declarada o declaración de ausencia o de muerte presunta, del titular del certificado. g) Por extinción de la personería jurídica o declaración judicial de quiebra. h) Por muerte, o por inhabilitación o incapacidad declarada judicialmente de la persona natural suscriptor del certificado. i) Por solicitud de un tercero que informe y pruebe de manera fehaciente alguno de los supuestos de revocación contenidos en los incisos 1) y 2) del artículo 10 de la Ley. j) Otras causales que establezca la Autoridad Administrativa Competente. Las condiciones bajo las cuales un certificado digital pueda ser cancelado deben ser estipuladas en los contratos de los suscriptores y titulares. El uso de certificados digitales con posterioridad a su cancelación conlleva la inaplicabilidad de los artículos 3, 4 y 8 del presente Reglamento. En todos los casos la Entidad de Certificación debe indicar el momento desde el cual se aplica la cancelación, precisando la fecha, hora, minuto y segundo en la que se efectúa. La cancelación no puede ser aplicada retroactivamente y debe ser notificada al titular del certificado digital cuando corresponda. La Entidad de Certificación debe incluir el certificado digital cancelado en la siguiente publicación de la Lista de Certificados Digitales Cancelados. **Artículo 18.- De la cancelación del certificado a solicitud de su titular, suscriptor o representante.** La solicitud de cancelación de un certificado digital puede ser realizada por su titular, suscriptor o a través de un representante debidamente acreditado; tal solicitud podrá realizarse mediante documento electrónico firmado digitalmente, de acuerdo con los procedimientos definidos en cada caso por las Entidades de Certificación o las Entidades de Registro o Verificación. El titular y el suscriptor del certificado están obligados, bajo responsabilidad, a solicitar la cancelación del certificado al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias: a) Exposición, puesta en peligro o uso indebido de la clave privada. b) Deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada. c) Revocación de las facultades de representación y/o poderes de sus representantes legales o apoderados. d) Cuando la información contenida en el certificado ya no resulte correcta. e) Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la Entidad de Certificación.

	Artículo 19.- De la cancelación por revocación La revocación supone la cancelación de oficio de los certificados por parte de la Entidad de Certificación, quien debe contar, para tal efecto, con procedimientos detallados en su Declaración de Prácticas de Certificación. TÍTULO II DE LA INFRAESTRUCTURA OFICIAL DE FIRMA ELECTRÓNICA CAPÍTULO I ASPECTOS GENERALES **Artículo 20.- De los elementos** La Infraestructura Oficial de Firma Electrónica está constituida por: a) El conjunto de firmas digitales, certificados digitales y documentos electrónicos generados bajo la Infraestructura Oficial de Firma Electrónica. b) Las políticas y declaraciones de prácticas de los Prestadores de Servicios de Certificación Digital, basadas en estándares internacionales o compatibles con los internacionalmente vigentes, que aseguren la interoperabilidad entre dominios y las funciones exigidas, conforme a lo establecido por la Autoridad Administrativa Competente. c) El software, el hardware y demás componentes adecuados para las prácticas de certificación y las condiciones de seguridad adicionales comprendidas en los estándares señalados en el literal b). d) El sistema de gestión que permita el mantenimiento de las condiciones señaladas en los incisos anteriores, así como la seguridad, confidencialidad, transparencia y no discriminación en la prestación de sus servicios. e) La Autoridad Administrativa Competente, así como los Prestadores de Servicios de Certificación Digital acreditados o reconocidos. **Artículo 21.- De los estándares aplicables** La Autoridad Administrativa Competente determinará los estándares compatibles aplicando el principio de neutralidad tecnológica y los criterios que permitan lograr la interoperabilidad entre componentes, aplicaciones e infraestructuras de la firma digital análogas a la Infraestructura Oficial de Firma Electrónica. **Artículo 22.- De los niveles de seguridad** A fin de garantizar el cumplimiento de los requerimientos de seguridad necesarios para la implementación de los componentes y aplicaciones de la Infraestructura Oficial de Firma Electrónica, se establecen tres niveles: Medio, Medio Alto y Alto, cuyas precisiones adicionales a lo establecido en el presente Reglamento serán definidas por la Autoridad Administrativa Competente. El nivel de seguridad Alto se emplea en aplicaciones militares.

	CAPÍTULO II DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN DIGITAL **Artículo 23.- De las modalidades** Los Prestadores de Servicios de Certificación Digital (PSC) pueden adoptar cualquiera de las modalidades siguientes: a) Entidad de Certificación. b) Entidad de Registro o Verificación. c) Prestador de Servicios de Valor Añadido. Cuando la evolución tecnológica lo haga necesario, la AAC puede proponer las modificaciones que corresponda al Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, aprobado por Decreto Supremo Nº 052-2008-PCM, a fin de establecer modalidades adicionales para los Prestadores de Servicios de Certificación Digital, en base a estándares técnicos internacionales; servicios que contarán con la presunción de no repudio para las transacciones realizadas por los usuarios de dichos servicios. De conformidad con lo establecido en la Ley, resulta factible que una misma Entidad preste sus servicios en más de una de las modalidades establecidas anteriormente. No obstante, deberá contar con una acreditación independiente y particular para cada una de las modalidades de prestación de servicios de certificación que decida adoptar, a efectos de formar parte de la Infraestructura Oficial de Firma Electrónica. **Artículo 24.- De la acreditación** La acreditación del Prestador de Servicios de Certificación permite su ingreso a la Infraestructura Oficial de Firma Electrónica, gozando de las presunciones legales que rigen para tal supuesto. A tal efecto, el Prestador de Servicios de Certificación será inscrito en el correspondiente Registro de Prestadores de Servicios de Certificación Digital. De manera general el proceso de acreditación se rige por lo establecido en el presente Reglamento y de manera particular por lo establecido en los Reglamentos Específicos y Guías de Acreditación aprobados para tales efectos por la Autoridad Administrativa Competente. SECCIÓN I DE LAS ENTIDADES DE CERTIFICACIÓN **Artículo 25.- De las funciones** Las Entidades de Certificación tendrán las siguientes funciones: a) Emitir certificados digitales manteniendo una secuencia correlativa en el número de serie. b) Cancelar certificados digitales.

	c) Reconocer certificados digitales emitidos por entidades de certificación extranjeras que hayan sido incorporadas por reconocimiento a la Infraestructura Oficial de Firma Electrónica conforme al artículo 73 del presente Reglamento. Caso contrario, dichos certificados no gozarán del amparo de la Infraestructura Oficial de Firma Electrónica. d) Adicionalmente a las anteriores funciones, realizará las señaladas en los artículos 29 y 33 del presente Reglamento, en caso opten por asumir las funciones de Entidad de Registro o Verificación, o de Prestador de Servicios de Valor Añadido, respectivamente. **Artículo 26.- De las obligaciones** Las Entidades de Certificación registradas tienen las siguientes obligaciones: a) Cumplir con los requerimientos de la Autoridad Administrativa Competente en lo referente a la Política de Certificación, Declaración de Prácticas de Certificación, Política de Seguridad, Política de Privacidad y Plan de Privacidad. Estos documentos deberán ser aprobados por la Autoridad Administrativa Competente dentro del procedimiento de acreditación. b) Informar a los usuarios de todas las condiciones de emisión y de uso de sus certificados digitales, incluyendo las referidas a la cancelación de éstos. c) Mantener el control y la reserva de la clave privada que emplea para firmar digitalmente los certificados digitales que emite. Mantener la debida diligencia y cuidado respecto a la clave privada de la Entidad de Certificación, estando en la obligación de comunicar inmediatamente a la Autoridad Administrativa Competente cualquier potencial o real compromiso de la clave privada. d) Mantener depósito de los certificados digitales emitidos y cancelados, consignando su fecha de emisión y vigencia. No almacenar las claves privadas de los usuarios finales a menos que correspondan a certificados cuyo uso se limite al cifrado de datos. e) Cancelar el certificado digital al suscitarse alguna de las causales establecidas en el artículo 17 del presente Reglamento. Las causales y condiciones bajo las cuales deba efectuarse la cancelación del certificado deben ser estipuladas en los contratos de los titulares y suscriptores. f) Mantener la confidencialidad de la información relativa a los titulares y suscriptores de certificados digitales limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o pedido del titular o suscriptor del certificado digital (según sea el caso) realizado mediante un mecanismo que garantice el no repudio, debiendo respetar para tales efectos los lineamientos establecidos por la Autoridad Administrativa Competente y contenidos en la Norma Marco sobre Privacidad. g) Mantener la información relativa a los certificados digitales, por un período mínimo de diez (10) años a partir de su cancelación. h) Cumplir los términos bajo los cuales obtuvo la acreditación, así como los requerimientos adicionales que establezca la Autoridad Administrativa Competente conforme a lo establecido en el Reglamento. i) Informar y solicitar autorización a la Autoridad Administrativa Competente respecto de acuerdos de certificación cruzada que proyecte celebrar, así como los términos bajo los cuales dichos acuerdos se suscribirían.

	j) Informar y solicitar autorización a la Autoridad Administrativa Competente para efectos del reconocimiento de certificados emitidos por entidades extranjeras. k) Cumplir con las disposiciones de la Autoridad Administrativa Competente a que se refiere el artículo 27 del presente Reglamento. l) Brindar todas las facilidades al personal autorizado por la Autoridad Administrativa Competente para efectos de supervisión y auditoría. *m) Demostrar que los controles técnicos que emplea son adecuados y efectivos a través de la verificación independiente del cumplimiento de los requisitos especificados en el estándar WebTrust for Certification Authorities y la obtención del sello de Webtrust* n) Acreditar domicilio en el país. o) Cumplir lo dispuesto en las normas que regulan la protección de datos personales. Estas obligaciones podrán ser precisadas por la Autoridad Administrativa Competente, a excepción de las que señale expresamente la Ley Estas obligaciones podrán ser precisadas por la Autoridad Administrativa Competente, a excepción de las que señale expresamente la Ley. **Artículo 27.- Responsabilidad por riesgos** Para operar en el marco de la Infraestructura Oficial de Firma Electrónica y afrontar los riesgos que puedan surgir como resultado de sus actividades de certificación, las Entidades de Certificación acreditadas o reconocidas, de acuerdo con los niveles de seguridad establecidos, deben cumplir con mantener vigente la contratación de seguros o garantías bancarias que respalden sus certificados, así como con informar a los usuarios los montos contratados a tal efecto. Queda exenta de esta obligación la Entidad de Certificación Nacional para el Estado Peruano. La Autoridad Administrativa Competente establece la cuantía mínima de las pólizas de seguros o garantías bancarias, así como las medidas tecnológicas correspondientes al nivel de seguridad respectivo. Asimismo, la Autoridad Administrativa Competente determina los criterios para evaluar el cumplimiento de este requisito. **Artículo 28.- Del cese de operaciones** La Entidad de Certificación cesa sus operaciones en el marco de la Infraestructura Oficial de Firma Electrónica, en los siguientes casos: a) Por decisión unilateral comunicada a la Autoridad Administrativa Competente, asumiendo la responsabilidad del caso por dicha decisión. b) Por extinción de su personería jurídica. c) Por cancelación de su registro. d) Por sentencia judicial.

	e) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal, o resolución judicial de quiebra. f) Por decisión debidamente sustentada de la Autoridad Administrativa Competente frente al incumplimiento de los requerimientos exigidos en sus Reglamentos Específicos y Guías de Acreditación, observado en el proceso de evaluación técnica anual a que se refiere el artículo 71 del presente Reglamento. Para los supuestos contemplados en los incisos a) y b) la Entidad de Certificación tiene un plazo de treinta (30) días calendario para notificar el cese de sus operaciones tanto a la Autoridad Administrativa Competente como a los titulares de los certificados digitales que hubiera emitido. En tales supuestos, la Autoridad Administrativa Competente deberá adoptar las medidas necesarias para preservar las obligaciones contenidas en los incisos c), g) y h) del artículo 26 del presente Reglamento. La Autoridad Administrativa Competente establecerá los procedimientos para hacer público el cese de operaciones de las entidades de certificación. Los certificados digitales emitidos por una Entidad de Certificación cuyas operaciones han cesado deben ser cancelados a partir del día, hora, minuto y segundo en que se aplica el cese. (…).

Fuente: Sistema Peruano de Información Jurídica (SPIJ).
Elaboración: Área de Servicios de Información y Seguimiento Presupuestal (ASISP).