2024

Directiva que regula el uso de la firma digital en las entidades públicas

DIRECTIVA N° 002-2024-PCM/SGTD

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

CONTROL DE VERSIONES

Versión	Fecha	Título	Elaborado por
1.0	DIC2024	Directiva que regula el uso de la firma digital en las entidades públicas	Secretaría de Gobierno y Transformación Digital

CONTENIDO

DIRECTIVA QUE REGULA EL USO DE LA FIRMA DIGITAL EN LAS ENTIDADES PÚBLICAS

1. Objeto

Establecer disposiciones para el uso adecuado de la firma digital y electrónica en las entidades públicas, de conformidad con lo establecido en la Ley N° 27269, Ley de Firmas y Certificados Digitales, y su Reglamento, aprobado mediante Decreto Supremo N°052-2008-PCM, así como, dar cumplimiento a lo dispuesto en 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, aprobado mediante Decreto Supremo N° 029-2021-PCM.

2. Finalidad

Contribuir en la prestación segura de servicios digitales y procesos de gestión interna de las entidades públicas mediante el uso adecuado de la firma digital y electrónica.

3. Marco legal

La presente Directiva se sustenta en las siguientes normas:

a) Ley N° 29158, Ley Orgánica del Poder Ejecutivo.
b) Ley N° 27269, Ley de Firmas y Certificados Digitales.
c) Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
d) Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
e) Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
f) Decreto Supremo N° 052-2008-PCM, Decreto Supremo que aprueba el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, en adelante el Reglamento de la Ley N° 27269.
g) Decreto Supremo N° 026-2016-PCM, Decreto Supremo 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.
h) Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General.
i) 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.
j) 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.
k) Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2022-PCM/SGTD, que aprueba la Guía para el uso e integración de la Plataforma Nacional de Firma Digital en las entidades de la Administración Pública.
l) Resolución Ministerial N° 224-2023-PCM, que aprueba el Texto Integrado del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros.
m) Resolución de la Comisión para la Gestión de la Infraestructura Oficial de Firma Electrónica N° 075-2019/CFE-INDECOPI, que aprueba la Guía de Acreditación de Entidad de Certificación versión 4.1.

n) Resolución de la Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica N° 010-2016/CFE-INDECOPI, que aprueba la nueva versión de Guía de Acreditación de Aplicaciones de Software.

4. Alcance

4.1. La presente Directiva es de aplicación obligatoria a:

a) Las entidades de la Administración Pública señaladas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 004-2019-JUS, con excepción de las personas jurídicas señaladas en el numeral 8 del citado artículo.

b) Las empresas que realizan actividad empresarial del Estado que se encuentran en el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE) y de los gobiernos regionales y locales, en lo que corresponde.

4.2. Quedan exceptuadas aquellas entidades públicas que por norma expresa con rango de Ley cuenten con disposiciones específicas para el uso de la firma digital y/o electrónica en un ámbito específico. Sin perjuicio de ello, en todo lo no previsto en dichas normas se aplica supletoriamente lo establecido en la presente Directiva.

4.3. Cuando en la presente Directiva se mencione a entidades públicas, deberá entenderse a aquellas referidas en los literales a) y b) del numeral 4.1 precedente.

5. Acrónimos

En la presente Directiva se utilizan los siguientes acrónimos:

a) AAC: Autoridad Administrativa Competente
b) CAdES: CMS Advanced Electronic Signatures
c) CMS: Cryptographic Message Syntax
d) CRL: Certificate Revocation List
e) DNIe: Documento Nacional de Identidad electrónico
f) DNId: Documento Nacional de Identidad digital
g) ETSI: European Telecommunications Standards Institute
h) FIPS: Federal Information Processing Standard
i) IOFE: Infraestructura Oficial de Firma Electrónica
j) OCSP: Online Certificate Status Protocol
k) PAdES: PDF Advanced Electronic Signatures
l) PKI: Public Key Infrastructure
m) PDF: Portable Document Format (ISO 32000)
n) TSA: Time Stamping Authority
o) TSL: Lista de Servicios de Confianza
p) XAdES: XML Advanced Electronic Signatures
q) XML: Extensible Markup Language

6. Definiciones

Para los efectos de la presente Directiva resultan de aplicación las definiciones establecidas en el Reglamento de la Ley N°27269, además de las siguientes:

a) **Código QR** (o "*Quick Response Code*" por su denominación en inglés)**:** Es un tipo de código de barras bidimensional que contiene datos codificados en la forma de cuadrados negros organizados en una grilla cuadrada de fondo blanco, que pueden ser decodificados por dispositivos electrónicos tales como

un teléfono inteligente. El uso de códigos QR es libre de licencias y su especificación se encuentra estandarizada en el ISO/IEC 18004:2006.

b) **Datos de validación de largo plazo:** Son aquellos datos que permiten verificar que una firma digital fue generada en un determinado momento en el tiempo y que en ese momento era válida. Entre los datos de validación de largo plazo tenemos a las CRL, las respuestas OCSP, los sellos de tiempo y los certificados digitales.
c) **Dato a ser firmado:** Secuencia de bytes que serán firmados digitalmente y pueden tener como origen un fichero PDF, un fichero XML, una foto, un audio, un video, un plano, un mapa, etc.
d) **Firmante:** Es quien crea una firma electrónica en cualquiera de sus modalidades (simple, avanzada o firma digital).
e) **Firma digital de agente automatizado:** Es aquella firma digital generada sin intervención humana utilizando una clave privada asociada a un certificado digital de agente automatizado emitido en el marco de la IOFE.
f) **PIN o contraseña:** Es una secuencia de dígitos y/o letras que permite controlar el acceso y el uso de una clave privada; es mantenida en secreto, confidencial y bajo responsabilidad del firmante.
g) **Sello de Tiempo:** Es un dato que contiene una fecha y hora cierta para evidenciar que un dato ha existido en un momento determinado en el tiempo, y que no ha sido alterado desde entonces. El sello de tiempo es generado por un Prestador de Servicios de Valor Añadido en la modalidad de Sistema de Sellado de Tiempo, acreditado en el marco de la IOFE.
h) **Verificador:** Es quién requiere verificar la validez de una firma electrónica en cualquiera de sus modalidades (simple, avanzada o firma digital).

7. Uso de la firma digital y otras modalidades de firma electrónica

7.1. Las entidades públicas deben utilizar la firma digital:

a) Aplicando las disposiciones establecidas en la presente Directiva.
b) Para la emisión, publicación o intercambio de datos, información o documentos electrónicos con otras entidades públicas, ciudadanos o personas en general.
c) En escenarios con alto riesgo de que su autoría pueda ser cuestionada o desconocida.

7.2. Las entidades públicas pueden utilizar las modalidades de firma electrónica simple o avanzada, para lo cual deben:

a) Realizar una evaluación previa del riesgo del uso de dicha modalidad para determinar el nivel de riesgo (bajo, medio o alto), haciendo uso de normas técnicas o estándares internacionales en gestión de riesgos ampliamente reconocidos.
b) Documentar el resultado de la evaluación de riesgo realizada.
c) Utilizar la firma electrónica simple en escenarios con bajo riesgo de que su autoría pueda ser cuestionada o desconocida.
d) Utilizar la firma electrónica avanzada en escenarios con mediano riesgo de que su autoría pueda ser cuestionada o desconocida.
e) Elaborar y aprobar procedimientos específicos que permitan el uso adecuado de cada modalidad utilizada.

7.3. En caso de controversia sobre la autoría de una firma digital o electrónica, la carga de la prueba varía según la modalidad utilizada, de conformidad con lo establecido en el artículo 2A del Reglamento de la Ley N°27269, que señala lo siguiente:

a) Para la firma electrónica simple o avanzada, la carga de la prueba recae en quien la invoque como auténtica.
b) Para la firma digital, la carga de la prueba recae en quien la señala como apócrifa.

7.4. Para los efectos de la presente Directiva toda vez que se haga mención a la firma digital debe entenderse que se refiere a la firma electrónica cualificada establecida en el artículo 1A del Reglamento de la Ley N° 27269.

8. Formatos de la firma digital

8.1. Los formatos[1] de la firma digital que deben ser utilizados por las entidades públicas son los siguientes: CAdES, XAdES y PAdES.

8.2. El formato CAdES, se encuentra descrito en la especificación técnica ETSI TS 101 733. Es apropiado para firmar ficheros de cualquier tipo o tamaño, y cuando se requiere que la firma digital se guarde en formato binario.

8.3. El formato XAdES, se encuentra descrito en la especificación técnica ETSI TS 101 903. Es apropiado para firmar ficheros de cualquier tipo y cuando se requiere que la firma digital se guarde en formato XML.

8.4. El formato PAdES, se encuentra descrito en la especificación técnica ETSI TS 102 778-3. Es apropiado para firmar ficheros en formato PDF y cuando se requiere que la firma digital quede embebida dentro del fichero firmado. Puede ser creado en uno de los siguientes modos:
a) **Visible:** En este modo, una representación gráfica (elemento visual conformado por texto y/o imagen) es asociada a la firma digital.
b) **Invisible:** En este modo, no se asocia ninguna representación gráfica (elemento visual) a la firma digital, por lo tanto, su existencia no es visible al ojo humano.

9. Niveles de la firma digital

9.1. Los niveles de la firma digital que deben ser utilizados por las entidades públicas son los siguientes:
a) **Básico (nivel B)**: Una firma digital de nivel básico protege la integridad del dato firmado y evidencia la autoría de la firma; no obstante, su verificabilidad es posible mientras el certificado digital del firmante se mantenga vigente (es decir, que no se encuentre ni revocado, ni expirado). Asimismo, una firma digital de este nivel incorpora la fecha y hora del computador donde ésta es creada, por lo que debe ser adoptada en situaciones donde la precisión de la fecha y hora del momento de su creación no es determinante y/o cuando no requiera ser verificada en una fecha posterior a la vigencia del certificado digital del firmante.
b) **Con sello de tiempo (nivel T)**: Es una firma digital de nivel B que incluye una fecha y hora cierta provista por un tercero en el rol de Prestador de Servicios de Valor Añadido, en la modalidad de Sistema de Sellado de Tiempo. Este nivel de firma digital debe elegirse cuando la consignación de la fecha y hora del momento de su creación es determinante.
c) **Con disponibilidad de datos de validación en el largo plazo (nivel LT)**: Es una firma digital de nivel T que contiene, además, los datos de validación de largo plazo o sus referencias. En particular, busca asegurar

[1] Los formatos de firma digital CAdES, XAdES y PAdES han sido desarrollados por el Instituto de Estándares de Telecomunicaciones Europeo (ETSI). Asimismo, se encuentran referidos en la Guía de Acreditación de Aplicaciones de Software.

la disponibilidad de los datos de validación, incluso si sus fuentes de origen ya no se encuentran disponibles. Este nivel de firma debe elegirse cuando se requiere que la firma digital sea verificable en el largo plazo, es decir, más allá de la vigencia del certificado digital del firmante.

d) **Con disponibilidad e integridad de datos de validación en el largo plazo (nivel LTV)**: Es una firma digital de nivel LT que contiene, además, una fecha y hora cierta provista por un tercero en el rol de Prestador de Servicios de Valor Añadido, en la modalidad de Sistema de Sellado de Tiempo. En particular, busca asegurar la disponibilidad e integridad de los datos de validación de largo plazo y, si se implementan las medidas adecuadas (por ejemplo, la aplicación de sellos de tiempo periódicamente), una firma digital en este nivel aún puede ser verificable mucho después de que los algoritmos criptográficos utilizados para su creación ya no se consideren seguros, o posterior a la expiración de los datos de validación de largo plazo. Este nivel de firma debe elegirse cuando se requiere que la firma digital sea verificable en el largo plazo, es decir, más allá de la vigencia de los algoritmos y de los datos de validación de largo plazo.

9.2. Las entidades públicas pueden, posterior a la creación de una firma digital en un determinado nivel, promoverla a un nivel superior a través de una operación de extensión de firma digital (ver numeral 14 de la presente Directiva).

10. Empaquetamiento de la firma digital

Las formas de empaquetamiento de la firma digital que deben ser utilizadas por las entidades públicas son las siguientes:

a) **Embebido** (o "*Enveloped"* por su denominación en inglés): La firma digital es embebida dentro del fichero que contiene el dato firmado. En este caso, una operación de creación de firma digital genera un nuevo fichero conteniendo el dato firmado y la firma.

b) **Envolvente** (o "*Enveloping"* por su denominación en inglés): El dato firmado es embebido dentro de la firma digital como un sub-elemento. En este caso, una operación de creación de firma digital genera un nuevo fichero conteniendo la firma y ésta al dato firmado.

c) **Desacoplado** (o "*Detached"* por su denominación en inglés): La firma digital y el dato firmado se encuentran en ficheros diferentes. En este caso, una operación de creación de firma digital genera un nuevo fichero que contiene solamente a la firma, por lo cual, se requiere gestionar ambos ficheros de manera independiente.

d) **Internamente desacoplado** (o "*Internally-detached"* por su denominación en inglés): La firma digital y el dato firmado se encuentran en un mismo fichero XML. En este caso, una operación de creación de firma digital genera un nuevo fichero XML conteniendo la firma y el dato firmado como elementos desacoplados.

11. Operaciones de la firma digital

11.1. Las operaciones de la firma digital que deben ser realizadas por las entidades públicas son la creación, validación y extensión, de acuerdo con lo establecido en los numerales 12, 13 y 14 de la presente Directiva, respectivamente.

11.2. Para la realización de las operaciones de firma digital, las entidades públicas deben utilizar los formatos, niveles y empaquetamientos definidos en los numerales 8, 9 y 10 de la presente Directiva.

12. Operación de creación de la firma digital

12.1. La creación de una firma digital es la operación mediante la cual un firmante crea una firma utilizando un software de creación de firmas digitales acreditado dentro del marco de la IOFE. Para la creación de una firma digital se debe utilizar el servicio de creación de firmas digitales de la Plataforma Nacional de Firma Digital (FIRMA PERÚ), aplicando lo establecido en la Guía para el uso e integración de la Plataforma Nacional de Firma Digital en las entidades de la Administración Pública, aprobada mediante Resolución N°002-2022-PCM/SGTD o norma vigente.

12.2. Para la creación de una firma digital, un firmante utiliza los siguientes elementos:

a) Un certificado digital vigente emitido en el marco de la IOFE, junto con su clave privada correspondiente (obligatorio).
b) Un PIN o contraseña (obligatorio).
c) El documento a ser firmado (obligatorio).
d) El software de creación de firmas digitales (obligatorio).
e) Un servicio de sellado de tiempo (opcional).

12.3. La creación de la firma digital se desarrolla en dos escenarios:

a) **Con intervención humana**: Este escenario se da cuando el firmante es titular de un certificado digital de persona natural o es suscriptor de un certificado digital de persona jurídica emitido en el marco de la IOFE.
b) **Sin intervención humana**. Este escenario se da cuando el firmante es titular de un certificado digital de persona jurídica de tipo agente automatizado emitido en el marco de la IOFE.

12.4. Un firmante puede crear múltiples firmas digitales de dos maneras:

a) **Interactivamente:** Se efectúa una operación de creación de firma digital a la vez y, en cada una, el firmante introduce el PIN o contraseña y/o elige parámetros diferentes por cada firma digital.
b) **En lote:** Se efectúan múltiples operaciones de creación de firma digital de manera continua en múltiples datos. No se requiere que el firmante introduzca el PIN o contraseña para cada firma digital y todas éstas utilizan los mismos parámetros de firma. La necesidad o no de introducir el PIN o contraseña por cada operación de creación de firma digital depende de las capacidades del módulo criptográfico portador que está siendo utilizado.

13. Operación de validación de la firma digital

13.1. La validación de la firma digital es la operación mediante la cual un verificador comprueba su validez utilizando un software de validación de firmas digitales, de acuerdo con lo establecido en el artículo 4 del Reglamento de la Ley N°27269. Para la validación de una firma digital se debe utilizar el servicio de validación de firmas digitales de la Plataforma Nacional de Firma Digital (FIRMA PERÚ), aplicando lo establecido en la Guía para el uso e integración de la Plataforma Nacional de Firma Digital en las entidades de la Administración Pública, aprobada mediante Resolución N°002-2022-PCM/SGTD o norma vigente.

13.2. Para la validación de una firma digital, un verificador utiliza los siguientes elementos de forma obligatoria:

a) El dato firmado.

b) La firma digital.
c) El software de validación de firmas digitales.

13.3. La verificación de la validez de una firma digital se desarrolla en dos escenarios:
a) **Con intervención humana**. Este escenario se da cuando el verificador es una persona natural, pudiendo ser el firmante o un tercero.
b) **Sin intervención humana**. Este escenario se da cuando el verificador es un sistema de información que invoca de manera automatizada a un software de validación de firmas digitales.

13.4. Un verificador puede validar firmas digitales de dos maneras:
a) **Interactivamente.** Se caracteriza porque se efectúa la operación de validación de un único dato firmado.
b) **En lote.** Se caracteriza porque se efectúa la operación de validación de múltiples datos firmados, de manera continua.

13.5. La validación de una firma digital puede generar como resultado una de las siguientes respuestas:
a) **VÁLIDA.** Significa que, en el momento de la validación, la firma digital ha superado satisfactoriamente todos los criterios de validez establecidos en el estándar ETSI EN 319 102-1 y en la Guía de Acreditación de Aplicaciones de Software, en su versión vigente, aprobada por la AAC de la IOFE.
b) **NO VÁLIDA.** Significa que, en el momento de la validación, la firma digital no cumple con alguno o algunos de los criterios de validez establecidos en el estándar ETSI EN 319 102-1 y en la Guía de Acreditación de Aplicaciones de Software, en su versión vigente, aprobada por la AAC de la IOFE. Algunos de estos criterios de validez pueden ser, por ejemplo: conformidad de la firma digital (formato, hash, cifrado) y/o conformidad del certificado digital (cancelado, expirado, aún no válido).
c) **INDETERMINADA.** Significa que, en el momento de la validación, no es posible afirmar si una firma digital es VÁLIDA o es NO VÁLIDA.

14. Operación de extensión de la firma digital

14.1. La extensión de la firma digital es la operación mediante la cual se promueve su nivel a uno superior, utilizando un software de extensión de firmas digitales. La promoción de una firma digital de nivel B o T a los niveles LT o LTV permiten extender su verificabilidad en el tiempo mediante la incorporación de datos de validación de largo plazo en la misma.

14.2. Para la extensión de una firma digital, se utilizan los siguientes elementos de forma obligatoria:
a) El dato firmado.
b) La firma digital válida.
c) El software de extensión de firmas digitales.
d) El sistema de sellado de tiempo.
e) Los servicios de CRL y OCSP.

14.3. La persona que promueve el nivel de la firma digital puede ser un tercero, no es necesario que sea el firmante.

14.4. La extensión de una firma digital se desarrolla en dos escenarios:

a) **Con intervención humana**. Este escenario es utilizado cuando quién realiza la operación de extensión de la firma digital es una persona natural.
b) **Sin intervención humana**. Este escenario es utilizado cuando quién realiza la operación de extensión de la firma digital es un sistema de información que invoca de manera automatizada a un software de extensión de firmas digitales.

14.5. Se puede extender la verificabilidad de múltiples firmas digitales de dos maneras:
a) **Interactivamente.** Se caracteriza porque se efectúa la operación de extensión de la firma digital de un único dato firmado.
b) **En lote.** Se caracteriza porque se efectúan la operación de extensión de la firma digital en múltiples datos firmados de manera continua.

15. Clasificación de los certificados digitales

15.1. Los certificados digitales emitidos en el marco de la IOFE pueden clasificarse por: su titularidad, su posición en la Estructura Jerárquica de Certificación del Estado Peruano, y su propósito para el que fue emitido.

15.2. De acuerdo con su titularidad, un certificado digital puede ser:
a) **De persona natural.** Es aquel cuya titularidad recae en una persona física.
b) **De persona jurídica.** Es aquel cuya titularidad recae en una persona jurídica. En el marco de la presente Directiva, vienen a ser las entidades públicas. Pueden ser de dos tipos: para agente automatizado o para servidor civil.

15.3. De acuerdo con su posición en la Estructura Jerárquica de Certificación del Estado Peruano, un certificado digital puede ser:
a) **Certificado digital raíz.** Son certificados digitales autofirmados, utilizados exclusivamente para la emisión de certificados digitales de nivel intermedio. En el marco de la presente Directiva, vienen a ser los certificados digitales de la Entidad de Certificación Nacional para el Estado (ECERNEP).
b) **Certificado digital intermedio.** Son certificados digitales que jerárquicamente se encuentran entre los certificados digitales de nivel raíz y los de usuario final, y son utilizados para emitir certificados digitales de usuario final. En el marco de la presente Directiva, vienen a ser los certificados digitales de las Entidades de Certificación Nacional para el Estado (ECEP).
c) **Certificado digital de usuario final.** Son certificados digitales emitidos exclusivamente para realizar operaciones de firma, autenticación o cifrado.

15.4. De acuerdo con el propósito para el que fue emitido, un certificado digital puede ser:
a) **De firma.** Es aquel certificado digital emitido para el firmado protegido contra el no repudio. En este caso, el valor del bit no repudio (*nonRepudiation*) de su atributo uso de la clave (*KeyUsage*) está marcado con el valor verdadero (*true*).
b) **De autenticación.** Es aquel certificado digital emitido para la autenticación de la identidad del titular o suscriptor. En este caso, el valor del bit firma digital (*digitalSignature*) de su atributo uso de la clave

(*KeyUsage*) está marcado con el valor verdadero (*true*).

c) **De cifrado.** Es aquel certificado digital emitido para el cifrado de datos. En este caso, el valor del bit cifrado de datos (*dataEncipherment*) de su atributo uso de la clave (*KeyUsage*) está marcado con el valor verdadero (*true*).

d) **De entidad de certificación.** Es aquel certificado digital utilizado para emitir certificados digitales.

16. Titular y/o suscriptor de un certificado digital

16.1. El titular y/o suscriptor de un certificado digital puede ser una persona natural o jurídica:

a) **Una persona natural.** Se puede constituir en:

- El titular y el suscriptor de un certificado digital de usuario final. Por ejemplo, este caso se configura cuando un ciudadano obtiene su DNIe o DNId, constituyéndose en titular y suscriptor de los certificados digitales contenidos en estos.
- El suscriptor de un certificado de usuario final. Este caso ocurre cuando un servidor civil ha recibido un certificado digital de usuario final como parte de sus herramientas de trabajo para llevar a cabo sus labores en una entidad pública. En este caso, el servidor civil se constituye en el suscriptor del referido certificado digital, y la entidad pública se constituye en el titular.

b) **Una persona jurídica.** Se constituye como el titular y el suscriptor de un certificado digital raíz, intermedio o de usuario final. El último caso corresponde cuando el certificado digital es de agente automatizado.

16.2. Las obligaciones del titular y/o suscriptor de un certificado digital son aquellas establecidas en los artículos 10 y 15 del Reglamento de la Ley N°27269.

16.3. La responsabilidad sobre los efectos jurídicos generados por la utilización de una firma digital corresponde al titular del certificado digital[2].

16.4. Las entidades públicas deben definir y aprobar un procedimiento para gestionar la emisión, renovación y cancelación de certificados digitales de persona jurídica para sus servidores civiles.

17. Usos de un certificado digital

17.1. Los usos permitidos de un certificado digital de persona natural se encuentran establecidos en el contrato o acuerdo suscrito entre su titular y la Entidad de Certificación; y, en el caso de un certificado digital de persona jurídica se encuentran establecidos en el contrato o acuerdo suscrito entre el suscriptor y/o el titular y/o la Entidad de Certificación.

17.2. Los certificados digitales de persona natural contenidos en el DNIe o DNId pueden ser utilizados por los servidores civiles para la creación de firmas digitales que requieran generar en el ejercicio de sus funciones en una entidad pública, en los actos de administración interna, actos administrativos, durante la tramitación de procedimientos administrativos, procedimientos de gestión interna y prestación de servicios digitales; de conformidad con lo establecido en el artículo 17 la Ley de Gobierno Digital. Las entidades públicas deben establecer los casos de uso de estos certificados digitales, así como las responsabilidades del servidor civil y la entidad respecto de la firma digital

[2] Artículo 9 del Reglamento de la N° 27269"

creada.

17.3. Los certificados digitales de persona jurídica entregados a servidores civiles como parte de sus herramientas de trabajo en una entidad pública deben ser utilizados por éste únicamente para la creación de firmas digitales que requieran generar en el ejercicio de sus funciones en la referida entidad, en los actos de administración interna, actos administrativos, durante la tramitación de procedimientos administrativos, procedimientos de gestión interna y/o prestación de servicios digitales autorizados, salvo disposición en contrario que determine la entidad pública como el titular del certificado digital.

18. Módulo criptográfico portador

18.1. Los certificados digitales de usuario final para la firma digital, y sus claves privadas correspondientes, deben ser almacenados en módulos criptográficos portador, tales como:

a) Módulos criptográficos que cuenten con certificación de seguridad FIPS 140-2 nivel 1, o certificación equivalente *Common Criteria*, los cuales son utilizados para certificados digitales emitidos por Entidades de Certificación acreditadas con nivel de seguridad medio.
b) Módulos criptográficos con certificación de seguridad FIPS 140-2 nivel 2, o certificación equivalente *Common Criteria*, los cuales son utilizados para certificados digitales emitidos por Entidades de Certificación acreditadas con nivel de seguridad medio - alto.
c) Módulos criptográficos con certificación de seguridad FIPS 140-2 nivel 3, o certificación equivalente *Common Criteria*, los cuales son utilizados para certificados digitales emitidos por Entidades de Certificación acreditadas con nivel de seguridad alto.

18.2. Un módulo criptográfico portador debe permitir la exportación del certificado digital, mas no la exportación de su clave privada.

18.3. Es permitido el uso de certificados digitales para firma digital almacenadas, junto con sus correspondientes claves privadas, en módulos criptográficos portadores remotos, y administrados por un Prestador de Servicios de Valor Añadido acreditado en la modalidad de Sistema de Creación de Firma Remota.