REPUBLICA DEL PERU

Resolución Secretarial

137-2018 MTC/04

Lima, 31 de octubre de 2018

VISTOS: El Informe N° 008-2018-MTC/10.06, el Memorándum N° 1538-2018-MTC/10.06 de la Oficina General de Administración; el Memorándum Nº 1901-2018-MTC/09 de la Oficina General de Planeamiento y Presupuesto; y el Informe N° 179-2018-MTC/04.02.JVZ de la Oficina de Atención al Ciudadano y Gestión Documental; y,

CONSIDERANDO:

Que, la Ley Nº 27269, Ley de Firmas y Certificados Digitales tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de la firma manuscrita u otra análoga que conlleve manifestación de voluntad;

Que, la Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado, prescribe que el proceso de modernización de la gestión del Estado tiene como finalidad fundamental la obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos, cuyo objetivo es alcanzar un Estado al servicio de la ciudadanía;

Oficina Gral. de Planeamiento y Presupuesto - MTC

Que, la Política Nacional de Modernización de la Gestión Pública aprobada por Decreto Supremo N° 004-2013-PCM, establece como uno de sus ejes transversales al gobierno electrónico, el mismo que comprende al uso de las Tecnologías de la Información y Comunicación (TIC) en los órganos de la administración pública para mejorar la información y los servicios ofrecidos a los ciudadanos, orientando la eficacia y eficiencia de la gestión pública e incrementar la transparencia del sector público;

Oficina Gral. Administración - Director General

Que, el Decreto Legislativo Nº 1310, Decreto Legislativo que aprueba medidas adicionales de simplificación administrativa, autoriza el uso de tecnologías de la digitalización, información y comunicación para la sustitución de documentos físicos y firmas ológrafas en la emisión, remisión y conservación de documentos en materia laboral;

OFICINA GENERAL DE ASESORÍA JURÍDICA - MTC

Que, mediante Decreto Legislativo N° 1412, Decreto Legislativo que Aprueba la Ley de Gobierno Digital, se establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

SECRETARÍA GENERAL - MTC - J. LÓPEZ

Que, por su parte el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS, establece que el procedimiento administrativo podrá realizarse total o parcialmente a través

de tecnologías y medios electrónicos, y que dichos actos administrativos realizados a través del medio electrónico, poseen la misma validez y eficacia jurídica que los actos realizados por medios físicos tradicionales;

Que, el Ministerio de Transportes y Comunicaciones ha definido como objetivo estratégico institucional en el Plan Operativo Institucional 2018, aprobado por Resolución Ministerial Nº 794-2017-MTC/01, "Fortalecer el uso intensivo de las tecnologías de la información y comunicación – TIC's, a fin de garantizar servicios integrales, seguros y competitivos;

Que, el literal c) del artículo 1 de la Resolución Ministerial N° 484-2017-MTC/01, delega en el/la Secretario/a General del Ministerio de Transportes y Comunicaciones, la facultad de aprobar Directivas de alcance a más de un órgano y/o proyecto de la Unidad Ejecutora 001: Ministerio de Transportes y Comunicaciones, sobre asuntos administrativos, de acuerdo a las normas legales vigentes;

Que, en ese contexto y dentro del marco legal antes citado, es necesario aprobar la Directiva que establece los lineamientos para la implementación y uso de firmas y certificados digitales en el Ministerio de Transportes y Comunicaciones;

De conformidad con lo establecido en la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo; la Ley Nº 29370, Ley de Organización y Funciones del Ministerio de Transportes y Comunicaciones, y su Reglamento de Organización y Funciones, aprobado por Decreto Supremo Nº 021-2007-MTC;

Ofic. Gral. de Planeamiento y Presupuesto - MTC -

Oficina Gral. Administración Director General

Oficina General de Asesoría Jurídica - MTC -

Secretaría General - MTC - J. LÓPEZ

SE RESUELVE:

Artículo 1.- Aprobar la Directiva N° 003 -2018-MTC/04, "Directiva que establece los lineamientos para la implementación y uso de firmas y certificados digitales en el Ministerio de Transportes y Comunicaciones", la misma que forma parte integrante de la presente Resolución Secretarial.

Artículo 2.- La implementación de firmas y certificados digitales en el Ministerio de Transportes y Comunicaciones se realiza en forma progresiva y conforme al cronograma que para tal efecto establecerá la Oficina de Tecnología de Información de la Oficina General de Administración.

Artículo 3.- Disponer la publicación de la presente Resolución Secretarial y la Directiva aprobada en el Portal Institucional del Ministerio de Transportes y Comunicaciones (www.mtc.gob.pe).

REPUBLICA DEL PERU

Resolución Secretarial

137-2018 MTC/04

Artículo 4.- Remitir copia de la presente Resolución Secretarial y de la Directiva aprobada a los órganos y unidades orgánicas del Ministerio de Transportes y Comunicaciones para su conocimiento y fines.

Regístrese y comuníquese

JUANA R. LÓPEZ ESCOBAR
Secretaria General
Ministerio de Transportes y Comunicaciones

Ofic. Gral. de Planeamiento y Presupuesto - MTC -

Oficina Gral. Administración
Director General

OFICINA GENERAL DE ASESORÍA JURÍDICA - MTC -

DIRECTIVA N° 003 -2018-MTC/04

DIRECTIVA QUE ESTABLECE LINEAMIENTOS PARA LA IMPLEMENTACIÓN Y USO DE FIRMAS Y CERTIFICADOS DIGITALES EN EL MINISTERIO DE TRANSPORTES Y COMUNICACIONES

I. OBJETIVO

Establecer lineamientos para la implementación y uso de firmas y certificados digitales en los actos administrativos y de administración interna del Ministerio de Transportes y Comunicaciones, en adelante MTC, a fin de reducir el tiempo de atención y trámite a las solicitudes de los usuarios de los servicios que brinda la entidad, asegurando la integridad, validez jurídica y la autenticidad de los actos administrativos, en el marco del desarrollo del gobierno digital.

II. FINALIDAD

2.1. Fortalecer el proceso de modernización y la simplificación administrativa, mediante el uso estratégico de las tecnologías digitales, como mecanismo de ahorro en tiempo y costos, durante la tramitación de solicitudes y emisión de actos administrativos, que permitan la prestación de servicios públicos de calidad al ciudadano.

2.2. Permitir a los servidores civiles del MTC, firmar digitalmente los documentos electrónicos que generen como parte de sus funciones, haciendo uso del respectivo Documento Nacional de Identidad Electrónico o de certificados digitales, con la misma validez y eficacia jurídica que el uso de una firma manuscrita, garantizando la autenticidad, integridad y el no repudio de los documentos electrónicos.

2.3. Promover la ecoeficiencia y el uso racional de los recursos, mediante la eliminación del uso del papel en la documentación interna y el empleo de documentos electrónicos que garanticen la seguridad de la información y que generen un ahorro significativo de recursos al Estado.

III. ALCANCE

La presente directiva es de aplicación para los servidores civiles del MTC que cuenten con la autorización para hacer uso de la firma digital en los documentos electrónicos; así como por los responsables de los órganos y unidades orgánicas a cargo de su implementación.

IV. BASE LEGAL

4.1 Ley Nº 27269, Ley de Firmas y Certificados Digitales.
4.2 Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado.
4.3 Ley N° 29370, Ley de Organización y Funciones del Ministerio de la Transportes y Comunicaciones.
4.4 Decreto Legislativo N° 1310, Decreto Legislativo que aprueba medidas adicionales de Simplificación Administrativa y su modificatoria.
4.5 Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.

4.6 Decreto Supremo Nº 021-2007-MTC, aprueba el Reglamento de Organización y Funciones del Ministerio de Transportes y Comunicaciones.

4.7 Decreto Supremo Nº 030-2002-PCM, Aprueban Reglamento de la Ley Marco de Modernización de la Gestión del Estado.

4.8 Decreto Supremo Nº 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales

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

4.10 Decreto Supremo Nº 026-2016-PCM, aprueban medidas para el fortalecimiento de la infraestructura oficial de firma electrónica y la implementación progresiva de la firma digital en el Sector Público y Privado.

4.11 Decreto Supremo Nº 006-2017-JUS, aprueba el Texto Único Ordenado de la Ley Nº 27444, Ley del Procedimiento Administrativo General.

4.12 Decreto Supremo N° 080-2018-PCM que dispone la presentación de Declaración Jurada de Intereses de los funcionarios y servidores públicos del Poder Ejecutivo.

4.13 Resolución Secretarial Nº 453-2010-MTC/04, aprueba la Directiva que establece Normas para la Formulación, Aprobación y Actualización de Directivas Internas que regulan materias de competencia del Ministerio de Transportes y Comunicaciones.

4.14 Resolución de Secretaría de Gobierno Digital Nº 001-2017-PCM/SEGDI, aprueba el Modelo de Gestión Documental en el marco del Decreto Legislativo Nº 1310.

V. DISPOSICIONES GENERALES

5.1 **Definición de términos:**

5.1.1 **Área usuaria:** Es la unidad de organización del MTC.

5.1.2 **Autenticación:** Es el proceso técnico que permite determinar la identidad de la persona que firma digitalmente, en función del documento electrónico firmado por éste y al cual se le vincula; este proceso no otorga certificación notarial ni fe pública.

5.1.3 **Autoridad Administrativa Competente (AAC):** Es la entidad que evalúa, acredita, supervisa, revoca o cancela la acreditación a las entidades prestadoras de servicios de certificación, así como la de dictar las normas complementarias y aprobar el uso de estándares. El INDECOPI es la entidad designada como AAC.

5.1.4 **CAdES (CMS Avanzado)**
Es la evolución del primer formato de firma estandarizado. Es apropiado para firmar ficheros grandes, especialmente si la firma contiene el documento original porque optimiza el espacio de la información. Tras firmar, no podrás ver la información firmada, porque la información se guarda de forma binaria.

5.1.5 **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.

5.1.6 **CMS:** Son plataformas web estandarizadas que permite a los usuarios crear contenido para su página desde un backend o gestor de contenidos sin necesidad de contar con conocimientos técnicos muy específicos.

5.1.7 **Certificado Digital de Agente Automatizado:** Software ReFirma Aga brindado por el Registro Nacional de Identificación y Estado Civil - RENIEC, debidamente

acreditado por la AAC de la IOFE (Infraestructura Oficial de Firma Electrónica), el cual ha sido diseñado para realizar las siguientes operaciones:

a) Creación de firmas digitales de documentos PDF (Sigla del inglés Portable Document Format - Formato de Documento Portátil), las firmas están envueltas en el documento (Firma en formato PAdES).

b) Creación de firmas digitales de cualquier tipo de documentos, la firma está separada del documento (Firma en formato CAdES).

c) Creación de firmas digitales de documentos XML, las firmas están envueltas en el documento (Firma en formato XAdES).

5.1.8 **Dispositivo criptográfico:** Elemento de hardware, tal como un token criptográfico o tarjeta inteligente que permite almacenar de manera segura el certificado digital y la clave privada de los usuarios o suscriptores que cuentan con un certificado digital. Deben cumplir con certificaciones y estándares de seguridad.

5.1.9 **Documento electrónico:** Es aquel documento administrativo en soporte electrónico que incorpora datos firmados electrónicamente mediante el certificado digital de un suscriptor y que cuenta con el mismo valor que los documentos administrativos firmados con firma manuscrita en papel.

5.1.10 **Documento de Identificación Nacional Electrónico (DNIe):** Es una credencial de identidad digital emitida por el RENIEC, que acredita presencial y no presencialmente la identidad de las personas.

5.1.11 **Entidad de Certificación:** Entidad que 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.

5.1.12 **Entidad de Registro o Verificación (EREP):** Entidad que 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.

5.1.13 **Expediente electrónico:** Es el conjunto de documentos electrónicos relacionados que podrían corresponder a un trámite o procedimiento administrativo en el MTC.

5.1.14 **Firma Digital:** Es aquella firma electrónica que cumple con todas las funciones de la firma manuscrita, en particular se trata de aquella firma electrónica basada en criptografía asimétrica. Permite la identificación del signatario, la integridad del contenido y tiene la misma validez que el uso de una firma manuscrita, siempre y cuando haya sido generada dentro de la Infraestructura Oficial de Firma Electrónica. La firma digital está vinculada únicamente al signatario.

5.1.15 **Firma manuscrita:** La firma manuscrita es aquella imagen que significa nuestro nombre, apellido o título realizada por nuestra propia mano y plasmada en un documento para darle autenticidad o para manifestar la aprobación de su contenido.

5.1.16 **HTML:** Lenguaje de marcado que se utiliza para el desarrollo de páginas de Internet. Se trata de la sigla que corresponde a HyperText Markup Language, es decir, Lenguaje de Marcas de Hipertexto, que podría ser traducido como Lenguaje de Formato de Documentos para Hipertexto.

5.1.17 **Identidad Digital:** Conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales. Los atributos de la identidad digital son otorgados por distintas entidades de la Administración Pública que, en su conjunto caracterizan al individuo.

5.1.18 **Infraestructura Oficial de Firma Electrónica (IOFE):** Es el sistema confiable, acreditado, regulado y supervisado por la AAC que cuenta con los instrumentos legales y técnicos para garantizar los procesos de certificación digital. Es decir, es la infraestructura dentro de la cual se generan las firmas y certificados digitales seguros y confiables, siempre y cuando se respeten sus disposiciones y normatividad.

5.1.19 **PAdES (PDF Avanzado):** Formato más adecuado cuando el documento original es un pdf. El destinatario de la firma puede comprobar fácilmente la firma y el documento firmado. Con los formatos anteriores esto no es posible si no se utilizan herramientas externas.

5.1.20 **Sello de tiempo:** Es un servicio que se brinda como valor añadido en las transacciones, sirve para autenticar la fecha y hora exacta (según relojes atómicos muy precisos) de una comunicación.

5.1.21 **Suscriptores:** Son aquellos servidores civiles que cuentan con autorización para firmar digitalmente documentos electrónicos, mediante la utilización de certificados digitales emitidos por una Entidad de Certificación debidamente acreditada.

5.1.22 **Tarjeta inteligente (smart card):** En el contexto de firmas y certificados digitales, es un dispositivo de almacenamiento, del tamaño y forma de una tarjeta de crédito convencional, que cuenta con un chip criptográfico para almacenar de manera segura y confiable las claves privada y pública, los certificados digitales y otros datos

5.1.23 **Token criptográfico:** Es un dispositivo físico del tamaño y forma de una memoria USB convencional. Este pequeño dispositivo contiene un chip criptográfico donde se almacena la clave privada de manera segura.

5.1.24 **No repudio:** Es la imposibilidad para una persona de desdecirse de sus actos cuando ha plasmado su voluntad en un documento y lo ha firmado en forma manuscrita o digitalmente con un certificado emitido por una Entidad de Certificación acreditada en cooperación de una Entidad de Registro o Verificación acreditada, salvo que la misma entidad tenga ambas calidades, empleando un software de firmas digitales acreditado, y siempre que cumpla con lo previsto en la legislación civil[1].

El no repudio hace referencia a la vinculación de un individuo (o institución) con el documento electrónico, de tal manera que no puede negar su vinculación con él ni reclamar supuestas modificaciones de tal documento (falsificación).

[1] Decima Cuarta Disposición Complementaria Final del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo Nº 052-2008-PCM, Glosario de Términos

5.1.25 **Visto bueno digital:** Firma(s) digital(es) del documento electrónico realizada por servidores civiles, previa(s) a la firma digital de la autoridad competente para suscribir digitalmente el acto administrativo o de administración. Significa que ha sido previamente examinado por los servidores civiles previa a la firma digital del titular que suscribe.

5.1.26 **XAdES (XML Avanzado):** El resultado es un fichero de texto XML, un formato de texto muy similar al HTML que utiliza etiquetas. Los documentos obtenidos suelen ser más grandes que en el caso de CAdES, por eso no es adecuado cuando el fichero original es muy grande.

5.1.27 **XML:** XML proviene de eXtensible Markup Language ("Lenguaje de Marcas Extensible"). Se trata de un metalenguaje (un lenguaje que se utiliza para decir algo acerca de otro) extensible de etiquetas que fue desarrollado por el Word Wide Web Consortium (W3C), una sociedad mercantil internacional que elabora recomendaciones para la World Wide Web.

5.2 **De la validez de la firma digital:**

5.2.1 La firma digital posee la misma validez y eficacia jurídica que el uso de una firma manuscrita.

5.2.2 La delegación de firma establecida en el Texto Único Ordenado de la Ley Nº 27444, Ley del Procedimiento Administrativo General aprobado mediante Decreto Supremo N° 006-2016-JUS, es aplicable solo al uso de la firma manuscrita.

5.3 **Conservación de los documentos electrónicos con firma digital**

Los documentos electrónicos con firma digital se encuentran conservados y almacenados con las medidas de seguridad y cumplimiento de normatividad correspondiente, garantizando su confidencialidad, disponibilidad e integridad.

VI. DISPOSICIONES ESPECIFICAS

6.1 **De la Implementación de la firma y certificado digital**

6.1.1 La Oficina de Organización y Racionalización de la Oficina General de Planeamiento y Presupuesto, en adelante ORA - OGPP en coordinación con la Oficina de Atención al Ciudadano y Gestión Documental - OACGD, identifican y priorizan los procesos donde se implementen de manera gradual y progresiva las firmas y certificados digitales, según lo establecido por las normas vigentes, sin perjuicio de la evaluación de las necesidades de las áreas usuarias del MTC que se pudieran realizar.

6.1.2 La ORA - OGPP envía a la Oficina de Tecnología de Información - OTI, el informe técnico solicitando la implementación de firmas y certificados digitales de los procesos priorizados, los cuales se implementan de manera gradual y progresiva. El informe debe contener lo siguiente:

a) Documentos electrónicos a ser firmados digitalmente.

b) Diagrama de flujo del proceso actual y propuesto.

c) Identificación de la etapa del proceso en que se firma digitalmente.

d) Sistemas o aplicativos administrados por la OTI que utilizan el componente de firma digital empleados en los procesos.

Los requerimientos solicitados están en función a las necesidades de las áreas usuarias y la normatividad vigente, los mismos que pueden ser ampliados.

6.1.3 La OTI evalúa la viabilidad de los sistemas o aplicativos que utilicen la firma y certificado digital, elabora y ejecuta el plan de implementación en coordinación con el área usuaria solicitante, previo cumplimiento de lo señalado en los párrafos 6.1.1 y 6.1.2.

6.1.4 La OTI realiza el despliegue de la arquitectura tecnológica y de sistemas para el uso y aplicación de los certificados y firmas digitales en los documentos electrónicos generados por los servidores civiles del MTC, con el uso de su respectivo DNIe. De manera excepcional, con la finalidad de brindar la disponibilidad de realizar a los funcionarios la firma digital fuera de las oficinas del MTC, la OTI puede asignar tokens criptográficos, los mismos que deben estar homologados por el RENIEC.

Para el caso utilización del DNIe se procede de la siguiente manera:

a) Los órganos y unidades orgánicas remiten a la OTI la relación de los funcionarios y servidores públicos que cuentan con autorización de acceso para firmar digitalmente con el uso de su DNIe, desde los sistemas de información institucionales, indicando la descripción de su cargo, rol, atribución o facultad que ostente el funcionario o servidor público.

b) La OTI asigna a los funcionarios y servidores públicos autorizados, los lectores de tarjeta inteligente para DNIe y configura los accesos correspondientes en los sistemas de información institucionales, desde donde se realiza la firma digital en los documentos electrónicos correspondientes a los actos de administración, actos administrativos, procedimientos administrativos y servicios digitales, entre otros.

Para el caso de utilización de token criptográfico, se procede de la siguiente manera:

c) La OTI gestiona con el RENIEC la obtención de los certificados digitales de los servidores civiles del MTC autorizados a firmar o visar digitalmente.

d) El servidor civil autorizado a firmar o visar digitalmente debe acercarse al RENIEC, previa comunicación por parte de la OTI, para la comprobación de la información, así como para la identificación y autenticación del titular y para la firma de los documentos exigibles, requeridos para la emisión del certificado digital correspondiente.

e) El servidor civil autorizado a firmar o visar digitalmente recibe del RENIEC por correo electrónico el enlace con el usuario y la clave para la descarga del certificado digital.

f) La OTI coordina con quien corresponda la instalación del certificado digital asignado a los servidores civiles del MTC, autorizados a firmar o visar

digitalmente.

g) La OTI para atender las necesidades de los usuarios podrá adquirir los tokens criptográficos configurar y entregar a los servidores civiles, previa firma del acta correspondiente, para luego.

6.1.5 La OACGD en coordinación con la ORA - OGPP realiza el seguimiento y control de la ejecución del plan de implementación mencionado en el párrafo precedente.

6.1.6 **Del Procedimiento para la cancelación del certificado digital**

a) Las áreas usuarias solicitan la cancelación del certificado de digital de los servidores cuya relación laboral ha concluido, a la OTI con copia a la OACGD, bajo responsabilidad.

b) La OTI gestiona la cancelación del certificado digital con la entidad de certificación y cuando el servidor civil no tenga relación laboral con la entidad.

c) De no ser necesario el uso de la firma digital en un proceso definido, el área usuaria debe comunicar dicha situación a la OTI con copia a la OACGD.

d) En tanto se implemente el módulo de administración del sistema de firmas y certificados digitales, el primer registro de datos es efectuado por la OTI, en coordinación con el área usuaria.

6.2 **Del uso de la firma y certificado digital**

6.2.1 Los suscriptores de las áreas usuarias del MTC deben hacer uso de la firma y certificado digital en todos los documentos electrónicos que emitan en el marco de su competencia funcional.

6.2.2 Los suscriptores de las áreas usuarias del MTC son responsables del contenido del documento electrónico en el que firmen digitalmente a través de los sistemas de información del MTC o a través de un componente de firma digital acreditado por IOFE.

6.2.3 Excepcionalmente, cuando por razones técnicas del sistema informático, el suscriptor no pueda firmar digitalmente el documento electrónico, puede usar la firma manuscrita, a fin de no paralizar las labores diarias en el cumplimiento de sus funciones.

6.2.4 El documento electrónico firmado digitalmente debe ser almacenado en la base de datos del sistema informático del MTC, en archivo digital con formato PDF o similar y almacenado con las firmas digitales y sellos de tiempo correspondiente, para futuras referencias de ser el caso y conforme a la normatividad vigente.

6.2.5 Los tipos documentales que deben ser considerados para la aplicación de la firma digital, son los siguientes: Oficios, cartas, actos administrativos, títulos habilitantes y otros que se vayan agregando al Modelo de Gestión Documental establecido en la normatividad vigente.

VII. DISPOSICIONES COMPLEMENTARIAS

7.1 Debe existir como mínimo un sistema de informático integrado al módulo de firma

digital que soporte el proceso donde se considere su uso.

7.2 La autenticidad del documento firmado digitalmente a través de los sistemas informáticos del MTC, debe ser validado mediante el módulo de firma digital del Ministerio.

7.3 La implementación de la firma y certificado digital se realiza de manera progresiva conforme las disposiciones indicadas en la Directiva.

7.4 Para el caso de los documentos electrónicos remitidos por otras entidades públicas y privadas, estos deben cumplir con las disposiciones del Modelo de Gestión Documental y la normatividad asociada.

VIII. RESPONSABILIDADES

8.1 Responsabilidades de las unidades orgánicas intervinientes

8.1.1 La OTI, es la responsable de implementar el módulo de firma digital a incorporarse en los sistemas y aplicaciones informáticas del MTC; así como de brindar asistencia técnica y capacitación a los servidores civiles autorizados en el uso de la misma.

8.1.2 La OTI es responsable de implementar el módulo de administración de firma digital que permite la asignación de las autorizaciones de acceso a los servidores civiles del MTC, autorizados a firmar digitalmente documentos electrónicos y la asignación de roles para el uso con el DNIe o el Token en los sistemas de información que hagan uso del mismo.

8.1.3 La OTI es responsable de incorporar las medidas técnicas destinadas a mantener inalterado el documento electrónico con firma digital, conservarlo y asegurar la confidencialidad, disponibilidad e integridad de dichos documentos.

8.1.4 La Oficina de Imagen Institucional es la responsable de difundir la presente directiva en coordinación con la OACGD.

8.1.5 La OACGD es el responsable operativo de la implementación del modelo de gestión documental, así como de los procesos asociados que consideren la firma digital de los servidores civiles en los sistemas de información.

8.1.6 La OACGD, como órgano especializado, establece los requisitos funcionales para la implementación de las firmas y certificados digitales en el MTC.

8.1.7 La ORA, es el órgano responsable de conducir y coordinar las acciones administrativas correspondientes al proceso de modernización de la gestión del estado en el ámbito sectorial, así como la de conducir las acciones de simplificación administrativa del Ministerio.

8.1.8 La ORA, conduce y facilita la labor del Equipo de Mejora Continua del MTC, el mismo que es responsable de planificar y gestionar el proceso de simplificación administrativa.

8.2 Responsabilidades del servidor civil autorizado

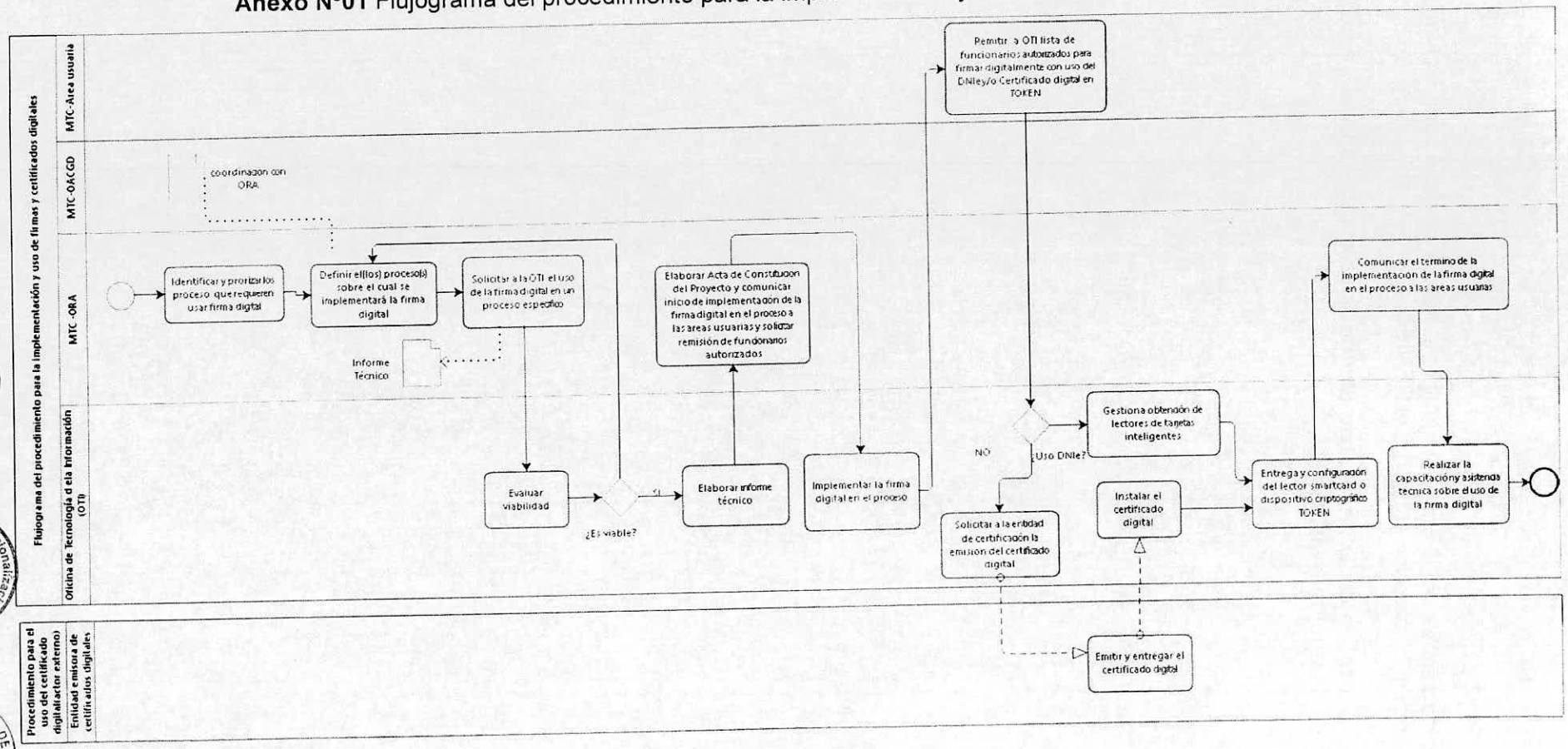
8.2.1 Los suscriptores son los responsables del adecuado uso de la firma digital.

8.2.2 En caso de pérdida del token criptográfico, el suscriptor debe comunicar a la OTI para la gestión correspondiente ante el RENIEC.

8.2.3 En caso de pérdida del DNIe, el suscriptor gestiona el duplicado con el RENIEC, de acuerdo a las normas vigentes.

IX. ANEXOS

Anexo N°01 Flujograma del procedimiento para la implementación y el uso del certificado digital.



Anexo Nº02 Flujograma del procedimiento para la cancelación del certificado digital.