REPUBLICA DEL PERU

Resolución de Secretaría General

N° 017-2013-PCM

VISTO: 20 JUN. 2013

El Memorando N° 339-2013-PCM/OS de fecha 10 de Junio de 2013, mediante el cual la Oficina de Sistemas de la Oficina de General de Administración remite el proyecto de directiva para el "*Uso de firmas y certificados digitales generados en documentos electrónicos oficiales, en el Sistema* de Información Trámite Documentario de la Presidencia del Consejo de Ministros", para su consideración en el marco del cumplimiento de Política Nacional de Modernización de la Gestión Pública aprobada por el Decreto Supremo N° 004-2013-PCM.

CONSIDERANDO:

Que, el artículo 1° de la Ley N° 27444, Ley del Procedimiento Administrativo General establece que los actos de administración interna de las entidades, destinados a organizar o hacer funcionar sus propias actividades o servicios, son regulados por cada entidad, con sujeción a las disposiciones del Título Preliminar y de aquellas normas que expresamente así lo establezcan;

Que, el Decreto Supremo N° 004-2013-PCM que aprueba la Política Nacional de Modernización de la Gestión Pública, señala como uno de sus principios orientadores de la política de modernización de la Gestión Pública, la innovación y el aprovechamiento de las tecnologías, a fin de revisar y renovar los procesos y procedimientos mediante los cuales implementan sus acciones;

Que, el artículo 4° del Decreto Supremo N° 009-2009-MINAM, que aprueba Medidas de Ecoeficiencia para el Sector Público, establece como medidas, la utilización con mayor frecuencia de la comunicación electrónica en reemplazo de la escrita, sobre todo en documentos preliminares y el evitar la impresión innecesaria de comunicaciones electrónicas;

Que, el artículo 3°del Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales, señala que 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;

Estando a lo previsto en el artículo 11° numeral 11.7 del Decreto Supremo que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por Decreto Supremo Nº 063-2007-PCM;

SE RESUELVE:

Artículo 1.- Aprobar la Directiva N°002 -2013-PCM/SG, denominada "*Uso de firmas y certificados digitales generados en documentos electrónicos oficiales, en el Sistema* de Información Trámite Documentario de la Presidencia del Consejo de Ministros".

Artículo 2.- La Directiva entrará en vigencia desde el día siguiente de su publicación en el portal institucional de la Presidencia del Consejo de Ministros.

Regístrese y comuníquese.

MANUEL ANGEL CLAUSEN OLIVARES
Secretario General
PRESIDENCIA DEL CONSEJO DE MINISTROS

DIRECTIVA N°002-2013-PCM/SG

"USO DE FIRMAS Y CERTIFICADOS DIGITALESGENERADOS EN DOCUMENTOS ELECTRÓNICOS OFICIALES, EN EL SISTEMA DE INFORMACIÓN TRÁMITE DOCUMENTARIO DE LA PRESIDENCIA DEL CONSEJO DE MINISTROS"

I. OBJETIVO

Normalizar el uso de firmas y certificados digitales en la emisión de documentos electrónicos oficiales, generados por funcionarios y servidores de la Alta Dirección y de los diversos Órganos de la Presidencia del Consejo de Ministros, haciendo uso del sistema de trámite documentario.

II. FINALIDAD

Conceder eficacia, y validez jurídica y administrativa a los documentos electrónicos firmados digitalmente y gestionados en el Sistema Información de Trámite Documentario (en adelante SITD) de la Presidencia del Consejo de Ministros, reconociéndoles las propiedades de equivalencia funcional, integridad, inalterabilidad, autenticidad y no repudio.

III. BASE LEGAL

3.1. Ley N° 29158, Ley Orgánica del Poder Ejecutivo
3.2. Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado
3.3. Ley Nº 27269, Ley de Firmas y Certificados Digitales
3.4. Ley N° 27444, Ley del Procedimiento Administrativo General
3.5. Ley N° 29060, Ley del Silencio Administrativo
3.6. Ley Nº 25323, Ley del Sistema Nacional de Archivos
3.7. Ley Nº 28716, Ley de Control Interno de las Entidades del Estado
3.8. Decreto Legislativo N° 681, que dictó normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborada en forma convencional cuanto la producida por procedimientos informáticos en computadoras
3.9. Decreto Legislativo N° 827, que amplía los alcances del Decreto Legislativo Nº 681 a las entidades públicas a fin de modernizar el sistema de archivos oficiales
3.10. Decreto Supremo N°005-2009-PCM que aprobó el Texto Único de Procedimientos Administrativos de la Presidencia del Consejo de Ministros
3.11. Decreto Supremo Nº 052-2008-PCM, que aprobó el Reglamento de la Ley de Firmas y Certificados Digitales
3.12. Decreto Supremo Nº 070-2012-PCM, que modificó el Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, y establece normas aplicables al procedimiento registral en virtud del Decreto Legislativo Nº 681 y ampliatorias

3.13. Decreto Supremo Nº 105-2012-PCM, que estableció disposiciones para facilitar la puesta en marcha de la firma digital y modifican el Decreto Supremo Nº 052-2008-PCM Reglamento de la Ley de Firmas y Certificados Digitales

3.14. Decreto Supremo N° 009-2009-MINAM, que aprueba Medidas de Ecoeficiencia para el Sector Público.

3.15. Decreto Supremo Nº 009-92-JUS, que aprobó el Reglamento del Decreto Legislativo Nº 681, sobre el uso de tecnologías de avanzada en materia de archivos de las empresas Decreto Ley Nº 19414, Ley de Defensa, Conservación e Incremento del Patrimonio Documental de la Nación, del 16 de Mayo de 1972

3.16. Decreto Supremo Nº 043-2003-PCM que aprueba el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública

3.17. Decreto Supremo Nº 072-2003-PCM, que aprueba el Reglamento de la Ley de Transparencia y Acceso a la Información Pública, del 07 de Agosto del 2003

3.18. Decreto Supremo Nº 015-2006-MIMDES, que declara los años 2007 al 2016 como el "Decenio de las Personas con Discapacidad en el Perú".

3.19. Decreto Supremo N° 002-98-ITINCI por el que aprueban requisitos y procedimiento para otorgamiento de Certificado de Idoneidad Técnica para la confección de microformas.

3.20. Decreto Supremo Nº 063-2007-PCM, que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros

3.21. Resolución de Secretaría General N° 018-2009-PCM que aprueba la Directiva General N° 003-2009-PCM/SG "Normas para la Generación de Documentos Oficiales en la Presidencia del Consejo de Ministros"

3.22. Resolución de Secretaría General N° 033-2011-PCM que aprueba la Directiva N° 003-2009-PCM/SG "Procedimiento para la Atención de las solicitudes de información formuladas por los Congresistas de la República".

3.23. Norma Técnica Peruana "NTP 392.030-1 1997 Microformas. Requisitos para las Organizaciones que operan sistemas de producción de microformas. Parte 1: Micropelícula y microfichas"

3.24. Norma Técnica Peruana "NTP 392.030-2 2005 Microformas. Requisitos para las organizaciones que operan sistemas de producción de microformas. Parte 2: Medios de archivo electrónico"

3.25. Norma Técnica Peruana "NTP-ISO 15489 -1. Información y Documentación. Gestión de registros. Parte 1: Generalidades".

3.26. Norma Técnica Peruana "NTP-ISO/TR 15489 -2. Información y Documentación. Gestión de registros. Parte 2: Directrices"

3.27. Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información

3.28. Norma Técnica Peruana "NTP ISO/IEC 12207:2006 Procesos del ciclo de vida del software"

3.29. Decreto Supremo N° 004-2013-PCM – Política Nacional de Modernización de la Gestión Pública.

IV. DEFINICIONES

- **Autoridad Administrativa Competente**.- Es el organismo público responsable de acreditar a las Entidades de Certificación, a las Entidades de Registro o Verificación y a los Prestadores de Servicios de Valor Añadido, públicos y privados, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, y las otras funciones señaladas en el presente Reglamento o aquellas que requiera en el transcurso de sus operaciones. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI.
- **Certificado Digital**.-Es un documento electrónico, usado como credencial, que ha sido generado y firmado digitalmente por una Entidad de Certificación. Es el documento credencial electrónico generado y firmado digitalmente por una Entidad de Certificación que vincula un par de claves con una persona natural o jurídica confirmando su identidad.
- **Documento electrónico**.- Es un documento contenido en un medio electrónico o magnético, cuya información se encuentra codificada.
- **Firma Electrónica**.- Es cualquier sonido, símbolo o proceso electrónico que permite al receptor de un documento electrónico identificar formalmente a su autor. También es conocida como firma electrónica básica.
- **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 a una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no pueden derivar de ella la clave privada –PKI, de conformidad a las normas vigentes sobre firmas y certificados digitales
- **Firma Principal**.- Es la firma Digital del autor del documento o del funcionario que suscribe el documento electrónico.
- **Firma Visto Bueno**.- Es la firma Digital del asesor, especialista, asistente, o servidor o funcionario, quien elaboró el informe o revisó el documento, o el llamado por procedimiento a dar confianza administrativa a quien suscribe la firma principal del documento electrónico.
- **Infraestructura Oficial de Firma Electrónica**.- Es un sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de: 1) La integridad de los documentos electrónicos; 2) La identidad de su autor, lo que es regulado conforme a Ley. El sistema incluye la generación de firmas digitales, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la Autoridad Administrativa Competente incluyendo a la Entidad de Certificación Nacional para el Estado Peruano, las Entidades de Certificación para el Estado Peruano, las Entidades de Registro o Verificación para el Estado Peruano y los Prestadores de Servicios de Valor Añadido para el Estado Peruano.

- **Medios electrónicos**.- Son sistemas de información que hacen uso de tecnología, y a través de los cuales se puede generar, procesar, transmitir y archivar documentos electrónicos.
- **Medio electrónico seguro**.- Es el medio electrónico que emplea firmas y certificados digitales emitidos por prestadores acreditados, haciendo que el intercambio de información se realice a través de canales seguros.
- **Principio de Equivalencia Funcional**.- Los actos jurídicos realizados haciendo uso de medios electrónicos poseen la misma validez y eficacia jurídica que los actos jurídicos realizados por medios convencionales.

  La condición es que en su realización se cumplan con las disposiciones legales vigentes.

  El efecto es que los "actos jurídicos electrónicos" equivalen a los actos jurídicos materiales, para todo efecto legal.

  En ese sentido, los documentos electrónicos que han sido firmados digitalmente constituyen prueba idónea en toda clase de procesos judiciales y procedimientos administrativos
- **Principio de Integridad.**- Presunción legal por la cual un documento electrónico no ha sido alterado desde su emisión hasta su recepción . Es decir, se presume que el mensaje de datos recibido corresponde al enviado.

  Por esta presunción, un documento electrónico firmado digitalmente conforme a las normas vigentes conserva la integridad del mensaje de datos, por el hecho de haber sido firmado digitalmente, sin importar en qué medio quede almacenado.
- **Principio de Inalterabilidad**.- Un documento electrónico puede ser alterado.

  Pero si este es firmado digitalmente, haciendo uso de un certificado digital, dentro de una estructura tecnológica de confianza, es posible demostrar la alteración o la no alteración de su contenido.

  Si ha sido alterado, pierde valor legal. Pero si el documento permanece íntegro, su valor probatorio es pleno.
- **Principio de Autenticidad**.- Se presume que una firma electrónica ha sido "escrita" por la persona a quien le ha sido asignado el certificado digital emitido por la Entidad autorizada.

  Esta firma electrónica permite al tercero presumir su certeza y la aprobación del contenido del documento sobre el cual está suscrita.

  Para suscribir la firma electrónica, la persona vinculada a esta, ha hecho uso de un esquema de seguridad, bajo alguna de las modalidades "algo que yo sé", "algo que yo tengo", "algo que yo soy".
- **Principio de No Repudio**.- Cuando una persona firma digitalmente un documento electrónico (al igual que cuando lo hace con una firma física), materializa en este acto la expresión de su voluntad, vinculando a la persona con el contenido del documento.

De esta forma la persona no puede repudiar posteriormente la manifestación de su voluntad. El documento es veraz y sus efectos, plenos.

- **PIN (*Personal Identification Number*)**.- Número de identificación personal.
- **Token.-** Dispositivo de almacenamiento critográfico que contiene el Certificado Digital asignado a la persona titular del mismo, que le permite firmar digitalmente.
- **Usuario.-** D.S. N° 002-98-ITINCI / NTP 302.030-2:2005. Individuo u organización que utiliza el sistema en operación para llevar a cabo una función especifica. Nota: El usuario puede llevar a cabo otros papeles, tales como el de adquiriente o responsable de mantenimiento. (3.36 NTP ISO/IEC 12207).
- **Sello de Tiempo (*Time Stamping*).-** Es el valor de fecha y hora firmados digitalmente, regulado de acuerdo al estándar RFC 3161 y las normas vigentes sobre firmas y certificados digitales.
- **PKI (*Public Key Infraestructure*).-** Sistema criptográfico asimétrico en el que se basan los certificados digitales.
- **SITD.-** Sistema de Información de Trámite Documentario de la Presidencia del Consejo de Ministros

V. ALCANCE

La presente Directiva es de aplicación obligatoria para los diversos Órganos de la Presidencia del Consejo de Ministros.

VI. RESPONSABILIDAD

6.1. La Secretaría General es responsable de la supervisión y aseguramiento del cumplimiento de las disposiciones establecidas en la presente Directiva.

6.2. La Secretaría General es responsable de notificar al interior de la Presidencia del Consejo de Ministros el inicio y gradualidad del uso de la Firma Digital.

6.3. Los funcionarios a cargo de los Órganos y de las Unidades Orgánicas comprendidas en el alcance de la presente Directiva son responsables de velar por el cumplimiento de las disposiciones para uso de la firma digital en documentos electrónicos oficiales.

6.4. Es responsabilidad de los funcionarios y servidores de la Presidencia del Consejo de Ministros el cumplimiento de las disposiciones impartidas en la presente.

VII. NORMAS GENERALES

7.1. La documentación electrónica oficial emitida bajo el alcance de la presente Directiva es aquella que cuenta con firma digital bajo la Infraestructura Oficial de Firma Electrónica.

7.2. El software de firma electrónica de la Presidencia del Consejo de Ministros para la emisión de documentos electrónicos seguros será el que la Oficina de Sistemas de la Oficina General de Administración recomiende a la Secretaría General, y esta apruebe. El mismo que puede ser propio o suministrado por terceros, a título gratuito u oneroso.

La validación de la integridad, y su no repudio, del documento electrónico con firma digital se hará a través del software que escoja la Secretaría General bajo el mismo procedimiento.

7.3. Los documentos electrónicos oficiales firmados digitalmente por los diversos Órganos y Unidades Orgánicas usarán el SITD de la Presidencia del Consejo de Ministros como medio de almacenamiento y gestión.

7.4. Los documentos electrónicos a ser firmados digitalmente deberán cumplir con las formalidades previstas para la generación de documentos oficiales en la Presidencia del Consejo de Ministros.

7.5. Los documentos firmados digitalmente deberán ser accesibles para su posterior consulta; ser conservados en su formato original de generación, envío, recepción u otro formato que reproduzca en forma demostrable la exactitud e integridad del contenido electrónico; y ser conservado toda la data que permita determinar el origen, destino, fecha y hora del envío y recepción.

7.6. Un documento electrónico podrá contar con una o varias firmas digitales.

7.7. Para los efectos de la presente Directiva, las firmas digitales comprenderán tanto "firmas" o "vistos" digitales en el documento electrónico emitido.

7.8. El documento electrónico con firma digital, almacenado en el sistema de la Presidencia del Consejo de Ministros, podrá ser impreso en papel a través de los fedatarios institucionales autorizados o fedatarios juramentados con especialización en informática, conforme a las normas de procedimiento administrativo general y a las especiales de la materia.

VIII. DISPOSICIONES GENERALES

8.1. Todo documento que se intercambie en el SITD, será transformado a formato PDF/A con el software de conversión a dicho formato que será instalado por personal de soporte técnico de la Oficina de Sistemas, en las computadoras de los usuarios autorizados a utilizar el SITD.

8.2. A través del SITD se podrán enviar o recibir documentos las 24 horas del día los 365 días. El régimen de horas hábiles en el horario de atención de la Presidencia del Consejo de Ministros se rige por lo dispuesto en la legislación vigente sobre el procedimiento administrativo general. El horario de atención estará publicado en el portal y en la intranet de la Presidencia del Consejo de Ministros www.pcm.gob.pe

Todo documento enviado con posterioridad al horario de atención establecido o en días feriados o feriados no laborables, se reputará

ingresado en el primer segundo siguiente, en el horario hábil de atención mencionado en el párrafo anterior.

8.3. La Secretaria General en coordinación con la Oficina de Sistemas de la Oficina General de Administración coordinará y gestionará la generación de los certificados y firmas digitales del personal de la PCM que le corresponda firmar digitalmente.

8.4. Los funcionarios y servidores a quienes se les asigne firma y certificado digital tienen la obligación de mantener la confidencialidad de sus claves de acceso, debiendo hacer uso personalísimo de ésta al momento de generarlas en los documentos electrónicos oficinales.

8.5. La administración de la bandeja principal de recepción de los documentos electrónicos del SITD estará a cargo del área de Trámite Documentario, quien a su vez será la encargada de distribuir dichos documentos a través del SITD para que las áreas responsables emitan respuesta.

8.6. La recepción de los documentos emitidos es obligatoria por el SITD para todos sus usuarios.

8.7. Se presume la recepción de los documentos electrónicos por parte de los destinatarios en el SITD, en el momento en que son emitidos, si estos cuentan con la prioridad Muy Urgente.

8.8. En caso de no recepción expresa por el usuario del SITD, se presumirá la recepción interna de los documentos en su bandeja de entrada a las 17:00:00 horas del mismo día en que fueron emitidos; o a las 09:00:01 horas del día hábil siguiente, si el documento fue remitido con posterioridad a las 17:00:00 horas.

8.9. Es constancia y prueba suficiente de recepción, la que emitirá el SITD, en razón de las presunciones administrativas internas consignadas en los tres numerales anteriores.

8.10. El personal autorizado de las diferentes áreas de PCM, podrán crear, firmar y enviar Documentos Electrónicos, haciendo uso del SITD, conteniendo la información que elaboren en cumplimiento de sus funciones.

8.11. Luego de firmado digitalmente un documento, este deberá ser impreso, con los respectivos anexos, para que sea enviado físicamente al destinatario, esto prevalecerá mientras se efectúe la transición entre la firma de documentos tradicional y la firma digital.

IX. DISPOSICIONES ESPECÍFICAS

9.1. Una vez elaborado el documento electrónico, deberá quedar listo para la firma o visto digital por el titular del certificado digital.

9.2. El SITD genera el número y fecha del documento electrónico, al mismo tiempo que se firmará digitalmente el documento.

9.3. El documento electrónico firmado digitalmente se remitirá a su destino por el SITD.

9.4. El documento electrónico con firma digital se conservará en el servidor de la Presidencia del Consejo de Ministros, bajo las normas y disposiciones de seguridad de la información vigentes.

9.5. Los jefes de oficina, jefes de secretarías, directores y jefes de comisión de la PCM, deben efectuar la solicitud, ante la Oficina de Sistemas de la PCM, para la obtención de la Firma y Certificado Digital.

9.6. La Oficina de Sistemas configurará lo correspondiente en los equipos de cómputo o los tokens, para almacenar e iniciar el uso, por parte de los solicitantes.

9.7. La Oficina de Sistemas instalará en los equipos de cómputo, y capacitará a los jefes de oficina, jefes de secretarías, directores y jefes de comisión de la PCM, en el uso del software de firma digital acreditado por el INDECOPI. Dicho sistema se utilizará para firmar digitalmente y con valor legal los documentos en la Presidencia del Consejo de Ministros.

X. PROCEDIMIENTO

10.1. Cada solicitante tendrá que utilizar un PIN asociado a la Firma Digital que le asigne. El solicitante debe cumplir con las políticas de seguridad de la información que correspondan.

10.2. El personal de soporte administrativo y/o secretarias, deberán generar los oficios, memorandos y otros documentos que serán firmados digitalmente por los jefes de oficina, jefes de secretarías, directores y jefes de comisión de la PCM cumpliendo con siguientes puntos:

a) El registro de documentos de la PCM debe ser mediante el uso SITD de la PCM.
b) La numeración de los documentos debe generarse haciendo uso del SITD de la PCM.
c) Los proyectos de documentos deben tener registrado el número de documento, generado previamente en el SITD, y la fecha de emisión, además de colocar el gráfico de la firma manuscrita de los jefes de oficina, jefes de secretarías, director y jefes de comisión de la PCM. Estos documentos deberán entregarse en formato PDF/A para que sean despachados y firmados digitalmente por los jefes de oficina, jefes de secretarías, directores y jefes de comisión de la PCM.

10.3. Los jefes de oficina, jefes de secretarías, director y jefes de comisión de la PCM deberán despachar los documentos que les corresponden, firmándolos o visándolos digitalmente haciendo uso del software de firma digital, mediante el cual se utiliza la firma digital y clave de acceso (PIN) para firmar digitalmente los documentos.

10.4. Los anexos que forman parte del documento principal deben ser almacenados en el SITD junto con el documento principal.

10.5. El personal de soporte administrativo y secretarias, luego de la firma digital de los documentos por parte de los jefes de oficina, jefes de secretarías, director y jefes de comisión de la PCM, deberán almacenar y derivar el documento firmado digitalmente hacia las áreas que correspondan, para ello, el SITD registrará la fecha, hora y destinatario.

10.6. Los jefes de oficina, jefes de secretarías, directores y jefes de comisión de la PCM, con el apoyo del personal administrativo y/o secretarias, deberán ingresar al SITD de la PCM para que efectúen la recepción lógica de los documentos derivados por las diferentes áreas, y gestionar posteriormente su atención.

10.7. Las preparación de nuevos documentos o respuesta a otros documentos internos deben seguir lo indicado en los numerales 10.2, 10.3, 10.4 y 10.5.

10.8. La validez del documento electrónico con firma digital puede verificarse haciendo uso del software autorizado.

XI. VIGENCIA

La presente Directiva entra en vigencia a su aprobación por la respectiva Resolución de Secretaría General.