EMMSA
Empresa Municipal de Mercados S.A.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario del Perú: 200 años de Independencia"

RESOLUCIÓN DE GERENCIA GENERAL N° 131-2021-EMMSA-GG

Santa Anita, 21 de octubre de 2021

VISTOS:

El Memorando N° 444-2021-EMMSA-GAF (24SET2021) de la Gerencia de Administración y Finanzas; el Informe N° 043-2021-EMMSA-GAF-SGTI (23SET2021) de la Subgerencia de Tecnología de la Información; el Memorando N° 149-2021-EMMSA-GPPE (05OCT2021) de la Gerencia de Planeamiento, Presupuesto y Estadística; el Informe N° 031-2021-EMMSA-GPPE-SGPLM (05OCT2021) de la Subgerencia de Planeamiento y Modernización; y, el Informe N° 146-2021-EMMSA-GAJ (21OCT2021) de la Gerencia de Asesoría Jurídica;

CONSIDERANDO:

Que, mediante Acuerdo de Concejo N° 023, de fecha 26 de enero de 1989, el Concejo Provincial de Lima incorpora a la Empresa Municipal de Mercados S.A. (EMMSA) a la Municipalidad Metropolitana de Lima, como empresa municipal de derecho privado, organizada bajo la forma de sociedad anónima, con autonomía económica y administrativa, que se rige por su Estatuto Social, las disposiciones de carácter presupuestal emitidas por la Dirección General de Presupuesto Público y en forma supletoria por la Ley N° 26887, Ley General de Sociedades;

Que, mediante Resolución de Gerencia General N° 031-GG-EMMSA-2021, de fecha 28 de enero de 2021, se aprueba la Directiva DI-001-GPPE/001, **"Formulación de los Documentos Normativos de EMMSA"**, segunda versión (en adelante, la Directiva), por la cual se establecen los lineamientos que permiten normar y orientar a los órganos y unidades orgánicas de la entidad en el proceso de formulación, aprobación, publicación, difusión, implementación, revisión, actualización y derogación de los documentos normativos (DN) generados para normalizar sus procesos;

Que, los diversos órganos y unidades orgánicas de EMMSA, en su constante compromiso por la mejor continua, vienen revisando su normativa interna a fin de solicitar la aprobación de nuevos documentos normativos o en otros casos, estos se dejen sin efecto, con la finalidad de optimizar las labores de cada uno de ellas;

Que, en este contexto, mediante los documentos de vistos, la Gerencia de Planeamiento, Presupuesto y Estadística, a través de la Subgerencia de Planeamiento y Modernización emite opinión técnica favorable al proyecto de documento normativo denominado: Directiva DI-025-GAF/019, **"Uso de Firmas Digitales"**, primera versión, presentado por la Subgerencia de Tecnología de la Información por intermedio de la Gerencia de Administración y Finanzas; el

mismo que recomienda proseguir con el trámite para su aprobación, toda vez que establece los lineamientos para la autorización, uso y cancelación de certificados y firmas digitales de suscriptores en EMMSA;

Que, a través del documento de vistos, la Gerencia de Asesoría Jurídica opina que el proyecto de documento normativo cumple con los presupuestos establecidos en la Directiva; por lo que considera legalmente viable su aprobación;

Que, estando a los considerandos antes señalados y conforme a las facultades conferidas a la Gerencia General de EMMSA, en el literal u) del artículo 12 del Reglamento de Organización y Funciones (ROF), aprobado por Acuerdo de Directorio N° 18-2020; y con las visaciones de la Gerencia de Planeamiento, Presupuesto y Estadística; Subgerencia de Planeamiento y Modernización, Gerencia de Administración y Finanza; Subgerencia de Tecnología de la Información; y, Gerencia de Asesoría Jurídica;

SE RESUELVE:

ARTÍCULO PRIMERO.- APROBAR el documento normativo denominado: Directiva DI-025-GAF/019, **"Uso de Firmas Digitales"**, primera versión; que como anexo forma parte integrante de la presente resolución.

ARTÍCULO SEGUNDO.- DEJAR SIN EFECTO cualquier documento normativo que se oponga a la presente directiva.

ARTÍCULO TERCERO.- ENCARGAR a la Gerencia de Planeamiento, Presupuesto y Estadística publicar la presente Resolución de Gerencia General en el Portal Institucional de EMMSA: www.emmsa.com.pe y la difusión del documento normativo aprobado.

Regístrese, comuníquese y cúmplase

EMPRESA MUNICIPAL DE MERCADOS S.A.
JAIME ADHEMIR GALLEGOS RONDON
GERENTE GENERAL

DIRECTIVA

USO DE FIRMAS DIGITALES

Resolución de Gerencia General Nº 131 -2021-EMMSA-GG

Código: DI-025-GAF/019

Fecha de Aprobación:

Páginas: 1/16

Primera Versión

ÍNDICE

I. OBJETIVO

Establecer lineamientos para la autorización, uso y cancelación de certificados y firmas digitales de suscriptores en la Empresa Municipal de Mercados S.A. en adelante EMMSA.

II. ALCANCE

Las disposiciones contenidas en la presente directiva son de aplicación obligatoria para el/la Titular del Certificado Digital de la EMMSA o la persona facultada por éste(a) para asumir su representación ante las autoridades administrativas así como para los trabajadores de la entidad.

III. BASE LEGAL

3.1 **Ley N° 27269,** Ley de Firmas y Certificados Digitales y sus modificatorias., del 08 de mayo de 2000.

3.2 **Ley N° 27658,** Ley de Marco de Modernización de la Gestión del Estado del 30 de enero de 2002.

3.3 **Decreto Supremo N° 030-2002-PCM,** aprueban el Reglamento de la Ley Marco de la Gestión del Estado, del 02 de mayo de 2002.

3.4 **Decreto Supremo N° 052-2008-PCM,** aprueban el Reglamento de Ley de Firmas y Certificados Digitales y sus modificatorias, del 18 de julio de 2008.

3.5 **Decreto Supremo N° 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, del 28 de abril del 2016.

3.6 **Decreto Supremo N° 004-2019-JUS,** aprueban el Texto Único Ordenado de la Ley N° 27444, "Ley del Procedimiento Administrativo General", del 22 de enero del 2019.

3.7 **Decreto Supremo N° 16-2021-MINAM,** aprueban Disposiciones para la Gestión de la Ecoeficiencia en las Entidades de la Administración Pública, del 22 de Julio de 2021.

3.8 **Resolución de Secretaría de Gobierno Digital N° 001-2017-PCM/SEGDI,** aprueba el Modelo de Gestión Documental en el marco del Decreto Legislativo N° 1310, del 09 de agosto de 2017.

3.9 **Estatuto Social,** Constitución de la Empresa Municipal de Mercados Sociedad Anónima - EMMSA, y su modificatoria.

3.10 **Acuerdo de Concejo N° 023-1989,** el Concejo Provincial de Lima incorpora a la Empresa Municipal de Mercados S.A (EMMSA) a la Municipalidad

Metropolitana de Lima (MML) como empresa municipal de derecho privado, organizada bajo la forma de sociedad anónima, con autonomía económica y administrativa, del 26 de enero de 1989.

3.11 **Acuerdo de Directorio N° 18-2020,** aprueba la Estructura orgánica de EMMSA y el Reglamento de Organización y Funciones de EMMSA, del 03 de diciembre de 2020.

3.12 **Resolución de Gerencia General N° 061-2020-EMMSA**, aprueba el Cuadro de Codificación y Siglas de los Órganos y Unidades Orgánicas de la Empresa Municipal de Mercados S.A. – EMMSA, del 22 de diciembre de 2020.

3.13 **Resolución N° 031-GG-EMMSA-2021,** aprueba la Directiva 01-001GPPE/001. Formulación de los Documentos normativos en EMMSA, segunda versión, del 28 de enero de 2021.

3.14 **Resolución N° 061-GG-EMMSA-2021,** aprueba la Directiva DI-019-GAF/014, Elaboración y Generación de Documentos Oficiales en EMMSA, primera versión, del 16 de marzo de 2021.

IV. GLOSARIO DE TÉRMINOS

4.1 **Autorización**

Es el registro que se efectúa en el Sistema Administrativo de Certificación Digital, como consecuencia de la solicitud de emisión de Certificados Digitales para los suscriptores y el cumplimiento de requisitos.

4.2 **Autenticidad**

Proceso 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, asegurando que, frente a un trámite realizado vía electrónica, ambas partes tengan la certeza que la persona que emite el documento electrónico es la persona quien dice ser.

4.3 **Certificado Digital**

Documento electrónico generado y firmado digitalmente por una Entidad de Certificación, que vincula dos (02) claves con una persona natural o jurídica determinada (suscriptor), confirmando su identidad. Deberá ser almacenado en un Dispositivo criptográfico o en la computadora desde donde se firmarán los documentos electrónicos.

4.4 **Dispositivo criptográfico**

Contenedor físico que permite portar el Certificado Digital y protege las claves criptográficas, su uso es indispensable para entornos adecuados de protección de la clave privada del Certificado Digital y porque en su interior se procesa la firma digital del usuario.

4.5 **Documento electrónico**

Unidad básica estructurada de información registrada, publicada o no, susceptible de ser generada, clasificada, gestionada, transmitida, procesada o conversada por una persona o una organización de acuerdo a sus requisitos funcionales, utilizando sistemas informáticos. Deberán ser accesibles para su posterior consulta y 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 conservada la data que permita determinar el origen, destino, fecha y hora de envío.

4.6 **Entidad de Certificación**

Persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital; asimismo, puede asumir las funciones de registro o verificación.

4.7 **Entidades de Registro o Verificación para el Estado Peruano (EREP-RENIEC)**

Persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales. De acuerdo al reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales aprobado con Decreto Supremo n° 052-2008-PCM, el RENIEC es la única entidad de certificación, verificación y registro en nuestro país.

4.8 **Firma Digital**

Es aquella firma electrónica que, utilizando una técnica de criptografía asimétrica, permite identificar al signatario, y ha sido creada por medios que éste mantiene bajo su control, 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 (Suscriptor) debidamente acreditado, que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica – IOFE, y que no medie ninguno de los vicios de la voluntad previstos en el Código Civil.

4.9 **Infraestructura Oficial de Firma Electrónica – IOFE**

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, y 2) La identidad de su autor, regulado conforme a Ley. El sistema incluye la generación de firmas digitales.

4.10 **Integridad**

Presunción legal de que un documento, por el hecho de haber sido firmado digitalmente conforme a las normas vigentes, no ha sido alterado desde su emisión hasta su recepción, y de que conserva la integridad del mensaje de datos sin importar en que medio quede almacenado.

4.11 **No Repudio**

Esta expresión hace referencia a la vinculación de un individuo (o institución) con el documento electrónico, de tal manera que dicha persona no pueda negar 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 EREP – RENIEC, empleando un software de firma digital acreditado y siempre que cumpla con lo previsto en la legislación civil.

4.12 **PDF**

Formato de documento portátil, así como un formato de almacenamiento de documentos digitales independiente de la plataforma de software o hardware. Este formato es de tipo compuesto (imagen vectorial, mapa de bits y texto).

4.13 **Proceso de Certificado Digital**

Proceso a través del cual se gestiona el Certificado Digital ante la EREP-RENIEC, que contempla cuatro etapas: 1) La suscripción de la solicitud, 2) Emisión de la solicitud de suscripción, 3) Remisión del Certificado, y 4) Cancelación del Certificado Digital.

4.14 **Responsable Técnico**

Profesional que labora en la EMMSA en la Subgerencia de Tecnología de la Información, encargado de instalar los componentes para el Uso del Certificado Digital, de brindar el apoyo técnico para la descarga del certificado digital en la computador o entregar el dispositivo criptográfico y de capacitar a los Suscriptores para el uso de dicho Certificado.

4.15 **Sistema Administrativo de Certificación Digital**

Sistema informático que permite una gestión eficiente y eficaz de las funciones calidad de Entidad de Registro o Verificación para el Estado Peruano, permitiendo brindar un servicio de calidad y con seguridad a los solicitantes de la emisión de Certificados Digitales.

4.16 **Suscriptor**

Funcionario de la Entidad que cuenta con certificado digital y/o token, es responsable de visar o firmar documentos electrónicos a través de un sistema informático, vinculándolo con el documento electrónico firmado digitalmente.

4.17 **Titular del Certificado Digital**

Persona designada mediante Resolución por el representante legal de EMMSA para la administración de los Certificados Digitales de la entidad, es quien debe apersonarse a la Entidad de Registro o Verificación para el Estado Peruano (EREP - RENIEC) para la recepción de su Certificado Digital, así como la Cuenta de Usuario Titular y contraseña correspondiente, del Certificado Digital en la EMMSA ante RENIEC; asimismo, realiza las altas y bajas de los certificados digitales de los suscriptores.

4.18 **Token**

Dispositivo de almacenamiento criptográfico que contiene el Certificado Digital asignado al suscriptor que le permite firmar digitalmente. Se presenta como un dispositivo USB.

V. RESPONSABILIDADES

5.1 Los gerentes y subgerentes de la EMMSA, son responsables del debido y estricto cumplimiento de las disposiciones contenidas en la presente Directiva.

5.2 La Gerencia de Administración y Finanzas es responsable de la conducción y aplicación de la presente Directiva a través de la Subgerencia de Tecnología de la información, quien asignará un token a los funcionarios y/o trabajadores que cuenten con un certificado digital, de ser el caso. Asimismo, llevará un registro de los suscriptores autorizados por EMMSA para utilizar el Certificado Digital para firma digital, de igual forma deberá mantener en los equipos de cómputo de los suscritores las configuraciones necesarias con fines de uso y almacenamiento; por último, orientará a los suscritores en el uso del software correspondiente.

5.3 El Titular del Certificado Digital es el responsable de llevar un registro actualizado de los funcionarios de la entidad a quienes se les autoriza o cancela ante la RENIEC los Certificados Digitales para la Firma Digital de los Suscriptores.

VI. DISPOSICIONES GENERALES

Validez legal de la Firma Digital

6.1 La Firma Digital generada dentro de la Infraestructura Oficial de Firma Electrónica tiene la misma validez y eficacia jurídica que una firma manuscrita, siempre y cuando haya sido generada por un prestador de servicios de certificación digital debidamente acreditado.

Para la presente directiva, las firmas digitales comprenden tanto la firma principal o visto bueno efectuados en el documento electrónico emitido. Asimismo, un documento electrónico puede contar con una(o) o varias(os) firmas digitales o vistos de diferentes Funcionario de la entidad.

6.2 Cuando por la naturaleza del procedimiento se requiera un documento impreso en papel, generado con certificado y firma digital, esté se puede realizar, siendo el impreso una copia simple del mencionado documento electrónico.

6.3 Se deberá evitar imprimir los documentos electrónicos, como medida de ecoeficiencia y preservación de recursos naturales.

VII. DISPOSICIONES ESPECÍFICAS

7.1 **Obligaciones del Suscriptor de la Firma Digital**

7.1.1 Entregar información veraz bajo su responsabilidad.

7.1.2 Generar la clave privada y firmar digitalmente mediante los procedimientos señalados por la Entidad de Certificación. La clave privada es intransferible. En tal sentido, el suscriptor es responsable de la misma, por lo que deberá mantener su control y la reserva bajo responsabilidad.

7.1.3 Observar las condiciones establecidas por la Entidad de Certificación para la utilización del certificado digital y la generación de firmas digitales.

7.1.4 En caso, la clave privada quede comprometida en su seguridad, el suscriptor debe notificarlo de inmediato al Titular del Certificado Digital de la entidad para que éste solicite a la EREP-RENIEC o a la entidad de certificación que participó en su emisión, la cancelación del certificado digital.

7.2 **Emisión de Documentos con Firma Digital**

7.2.1 La documentación electrónica emitida bajo el alcance de la presente directiva es aquella que cuenta con firma digital bajo la infraestructura Oficial de Firma Electrónica - IOFE, por lo que es considerada con valor legal.

7.2.2 La entidad adecuará sus trámites y procedimientos aplicados en sus comunicaciones, tanto con los administrados como con las distintas entidades de la administración pública, a fin de llevarlos a cabo por medios electrónico; debiendo asegurar en todo momento la disponibilidad de acceso, la integridad, la autenticidad, el no repudio y la confidencialidad de las transacciones realizadas por estos medios, empleando para tales fines los certificados y firmas digitales emitidos dentro de la IOFE, así como canales seguros.

7.2.3 En caso los ciudadanos y las entidades de la administración pública requieran información de la entidad y no cuenten con servicios electrónicos seguros que le permitan el acceso a dicha información, se deberá remitir reproducción del documento digital en medio físico, conforme a lo dispuesto en el Decreto Supremo N° 026-2016-PCM.

7.3 **Condiciones técnicas para implementar la firma digital en los sistemas de información**

7.3.1 La SGTI establecerá las condiciones técnicas para implementar en los sistemas de información la firma de documentos electrónicos con certificado digital bajo los requisitos de la IOFE.

7.4 **Autorización del certificado digital para la firma digital de suscriptores**

7.4.1 Los responsables de cada Órgano y Unidad Orgánica que requieran utilizar firma digital solicitarán la autorización del Certificado Digital a la GAF, mediante el formulario "Solicitud de inscripción de Certificado Digital para uso de la Firma Digital" (Anexo N° 1), sustentando los motivos de su solicitud, quien a su vez lo derivará al Titular del Certificado Digital para el trámite respectivo.

7.4.2 El Titular del Certificado Digital coordinará con la SGRH cualquier información adicional del suscriptor, necesaria para la autorización en el Sistema Administrativo de Certificación Digital.

7.4.3 La SGTI, prestará apoyo técnico a los funcionarios y trabajadores en el uso del Certificado y Firma Digital. Una vez que los funcionarios y trabajadores obtengan su certificado digital, se procederá con la instalación del software, hardware y la capacitación, además de instruir al personal operativo en el uso adecuado del software que producirá los documentos electrónicos firmados digitalmente

7.5 **Obtención del certificado digital para la firma digital de suscriptores**

7.5.1 Los Suscriptores, previa coordinación con el Titular del Certificado Digital, se apersonan al RENIEC - EREP portando su Documento Nacional de Identidad vigente con la finalidad de proceder con la autenticación y registro de los Formatos para su firma manuscrita y la validación de sus huellas biométricas respectivas.

7.5.2 Los suscriptores reciben del RENIEC-EREP el Certificado Digital mediante el correo electrónico, indicando la dirección URL para proceder a la descarga del certificado digital en la PC o Token de ser el caso, para ello coordinará con la SGTI para el apoyo técnico correspondiente.

7.5.3 El suscriptor deberá descargar su Certificado Digital, teniendo un plazo máximo de 30 días calendario para dicho proceso, contabilizándose el plazo a partir de la autorización de la solicitud del Certificado Digital. De no realizar la descarga correspondiente de su Certificado Digital, luego de vencido el plazo dispuesto para dicho proceso, deberá asumir el costo para iniciar un nuevo trámite de ser el caso.

7.5.4 El suscriptor no deberá olvidar la contraseña asignada para firmar los documentos digitalmente, caso contrario se tendrá que gestionar un nuevo certificado digital ante los organismos competentes y deberá asumir el costo para iniciar un nuevo trámite de ser el caso.

7.6 **Uso del certificado digital para la firma digital por los suscriptores**

7.6.1 El Responsable Técnico de la SGTI, previa coordinación con el Suscriptor, entrega el Certificado Digital y/o token de requerirlo e instala el Software y realiza la capacitación técnica sobre el uso del Certificado Digital y la Firma Digital, para ello suscribirá el formulario " Acta de Entrega - Recepción" (Anexo N°2).

7.6.2 Los documentos suscritos con firma digital deben ser presentados en formato de archivo PDF, el mismo que permite almacenar la(s) firma(s) digital(es) correspondiente(s), para su uso posterior.

7.6.3 El uso de la clave asignada y/o token es intransferible y de uso exclusivo para la firma de documentos electrónicos generados en la institución a cargo del suscriptor.

7.6.4 Los suscriptores que cuenten con un certificado digital para la Firma Digital deberán efectuar la firma en los documentos autorizados, evitando que terceras personas utilicen las claves asignadas, bajo responsabilidad.

7.6.5 A partir de la recepción del Certificado Digital para la Firma Digital, los suscriptores reconocen como propios y auténticos los documentos que por su medio se generen, y aceptan las consecuencias derivadas del uso de la Firma Digital que expresa su voluntad para todo efecto legal, siendo responsables de la veracidad del contenido de la información registrada en todos los documentos autorizados.

7.6.6 El uso de la firma digital no exime a los Órganos y Unidades Orgánicas de EMMSA de adjuntar la documentación o sustento según corresponda; ni del cumplimiento de lo establecido por los dispositivos legales vigentes que regulan la firma digital.

7.7 **Cancelación del certificado digital para la firma digital por los suscriptores**

7.7.1 La cancelación del Certificado Digital de Suscriptor, se realiza a través del responsable del órgano de EMMSA al cual pertenece y comunicar dicha intención al Titular del Certificado Digital de EMMSA, para lo cual presentará el formulario "Solicitud de cancelación del Certificado Digital" (Anexo N° 4) debidamente llenado y firmado.

7.7.2 El Titular del Certificado Digital verifica la información recibida y cancela el Certificado Digital del Suscriptor en el Sistema Administrativo de Certificación Digital del RENIEC - EREP, confirmando posteriormente al Suscriptor, vía correo electrónico, dicha cancelación.

7.7.3 En caso el suscriptor cancele su certificado por renuncia o cese del contrato, adicionalmente al informe de entrega de cargo presentado a la SGRH deberá incluir la presentación del formulario "Solicitud de cancelación del Certificado Digital" (Anexo N° 4) debidamente llenado y firmado, el mismo que deberá ser remitido al Titular del Certificado Digital para la cancelación ante el RENIEC-EREP.

La cancelación del Certificado Digital del Suscriptor conlleva a la devolución del bien asignado que le fue entregado para el uso del mismo, con el formulario "Acta de Devolución" (Anexo N° 3).

7.7.4 En caso de pérdida o robo del token, el suscriptor debe comunicarlo a través de su responsable del órgano correspondiente al Titular del Certificado Digital de EMMSA, adjuntando el formulario "Solicitud de cancelación del Certificado Digital" (Anexo N° 4), adjuntando copia de la denuncia policial con la finalidad de que a través de éste se gestione ante el organismo correspondiente la cancelación del certificado digital.

7.7.5 El costo de reposición del token y cualquier pagó adicional que se ocasione por el trámite de un nuevo certificado digital es asumido por el funcionario/trabajador a quien se le asignó dicho dispositivo.

VIII. DISPOSICION FINAL

Los aspectos no contemplados en la presente Directiva, serán definidas por la Gerencia de Administración y Finanzas en coordinación con la Subgerencia de Tecnología de la Información de la EMMSA.

IX. VIGENCIA

La presente directiva entra en vigencia a partir del día siguiente de su aprobación.

X. APROBACIÓN

Será aprobada mediante Resolución de Gerencia General.

XI. ANEXOS

ANEXO N° 01

SOLICITUD DE INSCRIPCIÓN DE CERTIFICADO DIGITAL PARA USO DE LA FIRMA DIGITAL

ÓRGANO / UNIDAD ORGÁNICA SOLICITANTE: _____

FECHA: _____

N°	NOMBRES Y APELLIDOS	DNI

Sustento (motivos e impacto):

_____

_____

_____

_____

_____

_____

_____

Responsable del Órgano /Unidad Orgánica Solicitante

ANEXO N° 02

ACTA DE ENTREGA - RECEPCIÓN N° _____-20___

Santa Anita, ____ de_____ del 20____

Yo, _____, identificado con DNI N° _____ con cargo de_____ en la (Órgano / Unidad Orgánica) _____, procedo a recibir un (01) Certificado Digital TOKEN por la Subgerencia de Tecnología de la Información.

Así mismo, me comprometo a:

- Hacer uso adecuado del bien entregado, cuidarlo y consérvalo en buen estado.
- Asumir el costo que se genere por la emisión de un nuevo certificado digital.
- Asumir el costo por concepto de reposición del bien en caso de pérdida, robo, sustracción o destrucción de los bienes asignados.

Relación de bienes entregados para la generación de la firma digital:

BIEN	FECHA DE ENTREGA

_____	_____
Firma	Firma
Nombres y Apellidos:	Nombres y Apellidos:
DNI N°:	DNI N°:
ENTREGA RESPONSABLE	RECIBE SUSCRIPTOR

ANEXO N° 03

ACTA DE DEVOLUCIÓN N°____-20___

Lima, ___ de _____de 20___

Yo, _____, identificado con DNI N° _____ con cargo de_____ en la (Órgano / Unidad Orgánica) _____, procedo a la devolución del bien asignado para la generación de la Firma Digital, que fueron entregados por la Subgerencia de Tecnología de la Información de EMMSA.

Relación de bienes entregados para la generación de la firma digital:

BIEN ENTREGADO	FECHA DE DEVOLUCIÓN

_____ Firma

Nombres y Apellidos:

DNI N°:

DEVUELVE
SUSCRIPTOR

_____ Firma

Nombres y Apellidos:

DNI N°:

RECIBE
TITULAR DE CERTIFICADO DIGITAL

ANEXO N° 04

SOLICITUD DE CANCELACIÓN DEL CERTIFICADO DIGITAL

Lima, ____ de _____de 20____

Yo, _____, identificado con DNI N° _____ con cargo de_____ en la (Órgano / Unidad Orgánica) _____, solicito la cancelación de la firma digital asignada por los siguientes motivos:

_____

_____

_____

_____

_____

_____

Así mismo, me comprometo a devolver el TOKEN entregado por la Subgerencia de Tecnología de la Información de EMMSA, para la generación de la Firma Digital.

_____

Firma

Nombres y Apellidos:

DNI N°

ANEXO N° 05

FLUJOGRAMAS