DIRECTIVA N. ° 004-2023-MDCH/GM

Anexo N° 01
MATRIZ DE APROBACIÓN

"DIRECTIVA PARA LA GESTIÓN Y USO DE FIRMA Y CERTIFICADO DIGITAL EN LOS SISTEMAS DE INFORMACIÓN DE LA MUNICIPALIDAD DE CHORRILLOS"

2023

ELABORADO POR:	
MUNICIPALIDAD DE CHORRILLOS MG. DAVID EUGENIO VALLADARES ALVAREZ GERENTE DE INFORMÁTICA Y TECNOLOGÍA GERENCIA DE INFORMATICA Y TECNOLOGIA	
REVISADO POR:	
MUNICIPALIDAD DE CHORRILLOS ECON. YEHUDI NATALIO CHIRINOS BERROCAL Gerente de Planeamiento y Presupuesto GERENCIA DE PLANEAMIENTO Y PRESUPUESTO	MUNICIPALIDAD DE CHORRILLOS ABOG. ANA KATHERINE ESPINOZA OKAMOTO Gerente de Asesoría Jurídica GERENCIA DE ASESORIA JURIDICA
APROBADO POR:	
MUNICIPALIDAD DE CHORRILLOS LIC. CESAR AUGUSTO AGUILAR VILLEGAS GERENTE MUNICIPAL GERENCIA MUNICIPAL	

DIRECTIVA N. ° 004-2023-MDCH/GM

Anexo N° 02
ESTRUCTURA DE LA DIRECTIVA

INDICE

I. OBJETIVO 3
II. FINALIDAD 3
III. BASE LEGAL 3
IV. ALCANCE 4
V. DEFINICIÓN 4
VI. DISPOSICIONES GENERALES 8
VII. DISPOSICIONES ESPECÍFICAS 12
VIII. DISPOSICIONES COMPLEMENTARIAS 15
IX. ANEXOS 15

DIRECTIVA PARA LA GESTIÓN Y USO DE LA FIRMA Y CERTIFICADO DIGITAL EN LOS SISTEMAS DE INFORMACIÓN DE LA MUNICIPALIDAD DE CHORRILLOS

I. OBJETIVO:

1.1. Establecer lineamientos que permitan regular la implementación y el uso de la firmas y certificados digitales en la Municipalidad de Chorrillos, a fin de impulsar el proceso de modernización de la gestión pública, reduciendo el tiempo de atención y trámite, tanto de la ciudadanía como de los usuarios internos que hacen uso de los servicios que se brindan dentro de nuestra Entidad, asegurando la integridad, validez jurídica y autenticidad de los actos administrativos, considerados dentro del marco del desarrollo de 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 optimización en tiempo y costo, 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 públicos de la Municipalidad de Chorrillos, firmar digitalmente los documentos electrónicos que generen, en los diferentes sistemas de información administrados por la Gerencia de Informática y Tecnología, como parte de sus funciones, haciendo uso del respectivo lector de tarjeta inteligente y/o dispositivo criptográfico, 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 implementación de estrategias Cero Papel en la documentación interna y externa, a través del empleo de documentos electrónicos, que garanticen la seguridad de la información y que generen una óptima administración de recursos al Estado.

III. BASE LEGAL:

3.1. Constitución Política del Perú.

3.2. Ley N° 27972, Ley Orgánica de Municipalidades y modificatorias.

3.3. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.

3.4. Ley N° 27269, Ley de Firmas y Certificados Digitales.

3.5. Ley N° 29733, Ley de Protección de Datos Personales.

3.6. Decreto Legislativo N° 1310, que aprueba medidas adicionales de Simplificación Administrativa y su modificatoria.

3.7. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.

3.8. Ordenanza Municipal N° 413-2021-MDCH, que aprueba el Nuevo Reglamento de Organización y Funciones (ROF) y la Estructura Orgánica de la Municipalidad Distrital de Chorrillos, y sus modificatorias.

3.9. Ordenanza Municipal N° 423-2021-MDCH, que aprueba la modificación del Reglamento de Organización y Funciones - ROF y la Estructura Orgánica de la Municipalidad Distrital de Chorrillos.

3.10. Decreto Supremo N° 030-2002-PCM, que aprueba el Reglamento de la Ley Marco de Modernización de la Gestión del Estado.

3.11. Decreto Supremo N° 052-2008-PCM, que el Reglamento de la Ley de Firmas y certificados Digitales, del 19 de julio de 2008.

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

3.13. Decreto Supremo Nº 081-2013-PCM, que aprueba la Política Nacional de Gobierno Electrónico 2013-2017.

3.14. Decreto Supremo N° 026-2016-PCM, que aprueba las 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.

3.15. Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General.

3.16. Resolución Ministerial Nº 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición, en todas las entidades integrantes del Sistema Nacional de Informática".

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

3.18. Resolución de Gerencia Municipal N° 064-2020-MDCH/GM, que aprueba la Directiva N° 005-2020-MDCH/GM, "Directiva que aprueba los Lineamientos para la Formulación, Aprobación, Modificación y Difusión de las Directivas de la Municipalidad de Chorrillos".

3.19. Contrato de Contraprestación de Servicios de Certificación Digital Certificado Clase III - Persona Jurídica, entre la Municipalidad de Chorrillos y el Registro Nacional de Identificación y Estado Civil, suscrito el 15 de agosto de 2019.

3.20. Contrato de Prestación de Servicios de Certificación Digital Certificado Clase IV - Agente Automatizado – Persona Jurídica, entre la Municipalidad de Chorrillos y el Registro Nacional de Identificación y Estado Civil, suscrito el 31 de enero de 2023.

IV. ALCANCE:

La presente Directiva aplica a todos los Órganos y Unidades Orgánicas pertenecientes a la Municipalidad de Chorrillos, que cuenten con la autorización y/o uso obligatorio de firma y certificado digital en los procesos administrativos.

V. DEFINICIÓN:

Para la siguiente Directiva se considerará lo siguiente:

5.1. **Certificado digital:** Es un documento digital emitido por una entidad autorizada o Entidad de Certificación (EC). El certificado digital vincula un par de claves (una pública y otra privada) con una persona y asegura su identidad digital. Con esta identidad digital la persona podrá ejecutar acciones de comercio y gobierno electrónico con seguridad, confianza y pleno valor legal. Los certificados digitales emitidos por las entidades de certificación deben contener al menos:

- Datos que identifiquen indubitablemente al suscriptor.
- Datos que identifiquen a la Entidad de Certificación.
- La clave pública.
- La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos.
- Número de serie del certificado.
- Vigencia del certificado.
- Firma digital de la Entidad de Certificación.

5.2. **Ciclo de vida del certificado digital**: son los estados por el que puede pasar un certificado digital. Los estados son:

5.2.1. **Emisión**: cuando se solicita por primera vez, el anterior expiró o fue revocado.

5.2.2. **Renovación**: cuando se solicita una renovación antes de que el certificado digital cumpla su período de vigencia. Este procedimiento es válido por única vez para certificados de período de vigencia de un año.

5.2.3. **Suspensión**: es una medida que modifica la validez de un certificado digital y hace que las firmas realizadas a posteriori de la fecha de suspensión sean inválidas. También se puede solicitar una suspensión temporal a la Prestador de servicios electrónicos de confianza; Una vez que finaliza el período de suspensión, el certificado se reactiva.

5.2.4. **Revocación:** Revocar un certificado es anular su validez antes de la fecha de caducidad que consta en el mismo. La revocación puede ser solicitada en cualquier momento, y en especial, cuando el titular crea que sus claves privadas son conocidas por otros.

5.2.5. **Cancelación:** El robo, pérdida o extravío del medio portador del certificado digital podría generar escenarios de suplantación y/o fraude que menoscabaría la confianza en el ecosistema digital. Los suscriptores de certificados digitales pueden dejar sin efecto la validez de su certificado digital (robado, perdido, extraviado, etc.) mediante el uso del servicio de cancelación. Para cancelar un certificado digital el suscriptor debe ingresar a la plataforma web o acudir a una oficina de atención para realizar el respectivo trámite, donde brindará los datos asociados a su certificado digital para proceder con la cancelación. La cancelación de certificados digitales es realizada en forma automática. Esta solicitud genera una petición de cancelación de certificado digital que implica el cambio de estado de este, dejando sin efecto, a partir de ese momento, las facultades que se le otorgaron al suscriptor del certificado digital.

MUNICIPALIDAD DE CHORRILLOS VºBº GERENCIA MUNICIPAL

MUNICIPALIDAD DE CHORRILLOS VºBº Ger. Planeam. y presupuesto

MUNICIPALIDAD DE CHORRILLOS VºBº Gerencia de Informática y Tecnología

MUNICIPALIDAD DE CHORRILLOS GERENCIA DE ASESORIA JURIDICA VºBº

5.3. **Clase de certificado - Clase III - Persona Jurídica:** Son los certificados digitales para funcionarios y servidores civiles de la administración pública como entidad final emitidos para Persona Jurídica con periodo de validez de 1 y 2 años.

5.4. **Clave privada:** Es una cadena de caracteres (números y letras) que, en un sistema de criptografía asimétrica, se mantiene en reserva por parte del titular de la firma digital.

5.5. **Clave pública:** Es una cadena de caracteres (números y letras) que, en un sistema de criptografía asimétrica, puede y debe ser difundida abiertamente para facilitar y promover la comunicación.

5.6. **Contraseña de acceso a la clave privada:** es una secuencia corta de caracteres alfanuméricos y es de conocimiento únicamente del firmante.

5.7. **Correo Electrónico:** Es el conjunto de palabras que identifican a una persona que puede enviar y recibir correo. Cada dirección es única y pertenece siempre a la misma persona.

5.8. **Documento Electrónico:** Es la unidad básica estructurada de información registrada, publicada o no, susceptible de ser generada, clasificada, gestionada, transmitida, procesada o conservada por una persona o una organización de acuerdo con sus requisitos funcionales, utilizando sistemas informáticos.

5.9. **Entidad de certificación:** Es la 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.

5.10. **Entidad de Registro o Verificación para el Estado Peruano (EREP):** Cumple con las funciones y obligaciones de una Entidad de Registro o Verificación (ER) según lo indicado en el Reglamento de Firmas y Certificados Digitales.

5.11. **Entidad final:** Es el suscriptor de un certificado digital.

5.12. **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, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública, relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada. 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 IOFE.

5.13. **Firma electrónica:** se trata de cualquier símbolo o carácter o conjunto de símbolos o caracteres basados en medios electrónicos que cumple con alguna de las funciones de la firma manuscrita.

5.14. **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.

5.15. **Identidad digital:** Es el reconocimiento de la identidad de una persona en un medio digital (como por ejemplo Internet) a través de mecanismos tecnológicos seguros y confiables, sin necesidad de que la persona esté presente físicamente.

5.16. **Infraestructura Oficial de Firma Electrónica (IOFE):** Es el sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente (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.

5.17. **PIN:** El número de identificación personal, pin o PIN (de las siglas en inglés, Personal Identification Number) es un tipo de contraseña utilizado en ciertos sistemas, como la tarjeta SIM, el teléfono móvil o el cajero automático, para identificarse y obtener acceso al sistema.

5.18. **Plataforma Integrada de la Entidad de Registro (PIER):** Es una herramienta que permitirá una gestión eficiente y eficaz gestión de los Certificados Digitales de las Entidades de la administración pública, los cuales son solicitados a la Entidad de Registro y Verificación para el Estado Peruano (EREP) permitiendo brindar un servicio de calidad y seguridad. Además, permite garantizar la integridad, autenticidad y confidencialidad de la información, siguiendo para ello los lineamientos de la Política de Seguridad y Plan de Seguridad de la EREP, asimismo los Lineamientos de Seguridad de la Información del RENIEC; respetando las normas de privacidad para el manejo de toda la información.

5.19. **Registro Nacional de Identificación y Estado Civil – RENIEC:** Es la Entidad de Certificación Nacional para el Estado Peruano - ECERNEP, Entidad de Certificación para el Estado Peruano - ECEP y Entidad de Registro o Verificación para el Estado Peruano – EREP de la Infraestructura Oficial de Firma Electrónica – IOFE. Tiene la facultad de emitir certificados digitales para personas naturales y jurídicas que lo soliciten, prestando los servicios de Certificación Digital, para el uso de autenticación y firma digital, los cuales serán emitidos al personal autorizado y designado por cada entidad del sector público, quienes se constituirán en suscriptores.

5.20. **Suscriptor:** Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor. En caso de que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

5.21. **Dispositivo criptográfico:** En el contexto del presente documento, un dispositivo criptográfico es un smartcard (con interfaz de contacto y/o proximidad) y/o token (con interfaz USB) con capacidad de realizar operaciones criptográficas.

5.22. **Tarjeta inteligente (smartcard):** Es un dispositivo físico, muy similar a una tarjeta de crédito convencional. Sin embargo, este pequeño dispositivo contiene un chip criptográfico donde se almacena la clave privada del certificado digital de manera segura.

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

5.24. **Titular de la firma digital:** es la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos.

5.25. **Titular:** Es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

VI. DISPOSICIONES GENERALES:

6.1. Responsabilidad General

6.1.1. La Gerencia Municipal, es la responsable de autorizar y/o aprobar el uso de la firma digital en el(los) proceso(s), actividad(es) o tarea(s) de las funciones y/o competencias de los Órganos y Unidades Orgánicas de la Entidad.

6.1.2. La Gerencia Municipal, es la responsable de autorizar y/o aprobar la relación de los/las suscriptores/as que aplicarán la firma digital en los documentos electrónicos generados por la Entidad.

6.1.3. La Gerencia de Informática y Tecnología, es la responsable de la implementación de la firma en los sistemas de información de la Municipalidad de Chorrillos; así como, de brindar la asistencia técnica y capacitaciones a todos los/las suscriptores/as.

6.1.4. La Gerencia de Informática y Tecnología, es la responsable de incorporar y tomar las medidas técnicas necesarias destinadas a mantener inalterado el documento electrónico con firma digital, conservarlo y asegurar la confidencialidad, disponibilidad e integridad de dichos documentos.

6.1.5. Los Órganos y Unidades Orgánicas, así como los/las suscriptores/as de la Municipalidad de Chorrillos, son los responsables de velar por el cumplimiento de las disposiciones para el uso de la firma y/o certificado digital en los sistemas de información que se brindan en la Entidad.

6.1.6. La Gerencia de Informática y Tecnología, es la responsable de brindar la asistencia técnica en el uso de los dispositivos criptográficos y/o lector de tarjeta inteligente, así como garantizar la integridad del documento electrónico con firma digital almacenado en los servidores del Centro de Datos de la Municipalidad de Chorrillos.

6.1.7. La Gerencia de Informática y Tecnología, será el responsable de asignar a los servidores públicos autorizados, las lectoras de tarjetas inteligentes para DNI electrónico y tokens criptográficos, con el **Formato de Asignación de Dispositivo Criptográfico (FADC) – Anexo N° 04**.

6.1.8. Cuando se le entregue el dispositivo criptográfico al/la suscriptor/a, este será el/la responsable de mantenerlo en custodia y ante cualquier pérdida o robo, tendrá que reponerlo.

6.2. Responsabilidad de la Municipalidad de Chorrillos

6.2.1. Designar mediante acto resolutivo correspondiente, al responsable de la administración de los certificados digitales de la Municipalidad de Chorrillos, para el desarrollo de sus funciones.

6.3. Responsabilidad del Administrador de Certificado Digital de la Municipalidad de Chorrillos

6.3.1. Administrar la lista de los/las suscriptores/as con certificados digitales.

6.3.2. Verificar y entregar a la RENIEC la información consignada por los/las suscripciones/as para la solicitud de emisión de certificados y demás procesos relacionados a los certificados digitales (cancelación, suspensión, revocación, reemisión y modificación).

6.3.3. Coordinar con los/las suscriptores/as respecto de las actividades de operación, uso y control de los certificados digitales.

6.3.4. Actualizar, de ser necesario, la información remitida tanto a la entidad de certificación como a la entidad de registro o verificación, previa coordinación con los/las suscriptores/as sobre la veracidad y exactitud de esta.

6.3.5. Solicitar la cancelación del certificado digital asignado en caso de que la reserva sobre la clave privada se haya visto comprometida.

6.3.6. Llevar el control de la fecha de emisión y caducidad de los certificados digitales asignados a los/las suscriptores/as.

6.3.7. Cumplir con las condiciones establecidas por la entidad de certificación para la utilización del certificado.

6.3.8. Proporcionar a los/las suscriptores/as las disposiciones, normas y guías de uso de firma y certificación digitales.

6.4. Responsabilidad de la Gerencia de Informática y Tecnología

6.4.1. Instalar y configurar los certificados digitales.

6.4.2. Brindar capacitación y asistencia técnica en el uso de dispositivos criptográficos de almacenamiento de certificado digital y DNI electrónico.

6.4.3. Brindar asistencia técnica en la atención de incidentes y requerimientos referidos al uso de dispositivos criptográficos, uso y aplicación de la firma digital u otros dispositivos.

6.4.4. Incorporar y recomendar medidas y/o controles técnicos orientados a mantener la integridad, disponibilidad y confidencialidad de los documentos electrónicos con firma digital.

6.5. Responsabilidad de los Gerentes, Subgerentes y Jefes

6.5.1. Solicitar a través de la Gerencia Municipal el uso de la firma digital en el/los proceso(s), actividad(es) o tarea(s) de su función y/o competencia, mediante el **Formato de Uso de la Firma Digital (FUFID) – Anexo N° 02**.

6.5.2. Remitir a el/la Administrador/a del Certificado Digital, a través de la Gerencia Municipal, la relación de los/las suscriptores/as responsables de firmar los documentos que requieren certificados digitales, mediante el llenado del **Formato de Requerimiento Firma Digital (FREFID) – Anexo N° 03**.

6.5.3. Remitir a el/la Administrador/a del Certificado Digital, a través de la Gerencia Municipal la lista de renovación de los/las suscriptores/as, mediante el llenado del **Formato de Requerimiento Firma Digital (FREFID) – Anexo N° 03.**

6.6. Responsabilidad de los/las suscriptores/as

6.6.1. El/La suscriptor/a que tiene asignado un dispositivo criptográfico y/o lector de tarjeta inteligente para DNI electrónico, es el/la único/a responsable de todas las acciones que derivan del uso de estos.

6.6.2. El/La suscriptor/a que tiene asignado un dispositivo criptográfico de almacenamiento de certificado digital, es el/la único/a responsable de cambiar el PIN para su uso y mantener la confidencialidad de esta.

6.6.3. Solicitar la cancelación del certificado digital, en caso de que la reserva sobre la clave privada se haya visto comprometida, remitiendo al correo electrónico certificadosdigitales@munichorrillos.gob.pe, con copia al correo electrónico del Gerente de Informática y Tecnología, con el asunto "CANCELACIÓN DE CERTIFICADO DIGITAL".

6.6.4. Emplear adecuadamente su certificado digital, conforme a la normativa e instructivos vigentes.

6.6.5. Ser diligentes en la custodia de su clave privada y su contraseña, con el fin de evitar usos no autorizados.

6.7. De la Firma y Certificado Digital

6.7.1. El Artículo 3 del DECRETO SUPREMO Nº 052-2008-PCM - REGLAMENTO DE LA LEY DE FIRMAS Y CERTIFICADOS DIGITALES, indica textualmente 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. En tal sentido, cuando la ley exija la firma de una persona, ese requisito se entenderá cumplido en relación con un documento electrónico, si se utiliza una firma digital generada en el marco de la Infraestructura Oficial de la Firma Electrónica.

6.7.2. La delegación de firma establecida en el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General aprobado mediante Decreto Supremo N° 004-2019-JUS, es aplicable solo al uso de la firma manuscrita.

6.8. Del Modelo de Gestión Documental (MGD)

6.8.1. En concordancia al artículo 8 del Decreto Legislativo Nº 1310, que aprueba medidas adicionales de simplificación administrativa, señala que las entidades de la Administración Pública deben interconectar sus sistemas de trámite documentario o equivalentes para el envío automático de documentos electrónicos entre dichas entidades.

6.8.2. La resolución de la Secretaría Resolución de la Secretaría de Gobierno Digital Nº 001-2017-PCM/SEGDI aprueba el Modelo de Gestión Documental (MGD), mediante el cual se establece un marco de referencia que permite a las Entidades de la Administración Pública, intercambiar documentos a través de la Plataforma de Interoperabilidad del Estado. Para los efectos del referido Modelo de

los documentos electrónicos que las Entidades de la Administración Pública intercambien comprenderán de información básica sobre el documento, representación de la firma digital, documentos anexos y metadatos asociados a este, todo ello en concordancia con lo establecido en el artículo 8 del Decreto Legislativo N° 1310.

6.8.3. Los lineamientos documentados del MGD, establecen que la Entidad debe elaborar, revisar y aprobar los lineamientos de gestión y formalidad que son documentos normativos internos que regulan la gestión documental en la Entidad, asimismo debe incluir los lineamientos para el uso de certificados y firmas digitales.

6.8.4. Los documentos electrónicos firmados digitalmente se almacenarán en un repositorio de documentos (equipo servidor de datos) de la Municipalidad de Chorrillos, destinado para el procesamiento, clasificación y consulta, con las medidas de seguridad correspondiente, garantizando el principio de equivalencia funcional y la integridad de su contenido.

VII. DISPOSICIONES ESPECÍFICAS:

7.1. DE LA IMPLEMENTACIÓN DE LA FIRMA Y CERTIFICADO DIGITAL

7.1.1. El uso efectivo de la firma digital en los documentos de la entidad se implementará de manera progresiva, siendo necesario que los Órganos y Unidades Orgánicas de la Municipalidad de Chorrillos identifiquen los procesos que generan documentos, en los cuales resulte justificable y oportuna el uso de la firma y/o certificado digital, en concordancia con los lineamientos de simplificación administrativa del Estado Peruano.

7.1.2. La Municipalidad de Chorrillos, como persona jurídica, solicita el contrato de prestación de servicios de certificación digital ante la RENIEC mediante su representante legal, antes de dar inicio al uso de la firma y certificado digital en la Entidad.

7.1.3. Los Órganos y Unidades Orgánicas que requieran hacer uso de la firma y/o certificado digital en los sistemas de información, lo tendrá que solicitar y coordinar con la Gerencia de Informática y Tecnología a través de la Gerencia Municipal, mediante el **Formato de uso de la Firma Digital (FUFID) – Anexo N° 02**, indicando los documentos electrónicos que serán firmados digitalmente, el diagrama de flujo del proceso actual y el propuesto, la identificación de la etapa del proceso en que se firma digitalmente, los mismos que serán implementados de forma gradual y progresiva.

7.1.4. La Gerencia de Informática y Tecnología, en coordinación con el área usuaria, evaluarán el formato de la propuesta presentada y en caso esta sea aprobada, se realizarán las coordinaciones necesarias y se establecerá el flujo de trabajo, junto con los modelos de documentos electrónicos en los sistemas de información, para su posterior implementación.

7.1.5. La Gerencia de Informática y Tecnología, realiza el despliegue de la arquitectura tecnológica y sistemas de información, para el uso y aplicación de los certificados y firmas digitales en los documentos electrónicos generados por los servidores públicos de la Municipalidad de Chorrillos, con el uso de sus respectivos DNI electrónico y/o token criptográfico; con la finalidad de brindar a los servidores públicos la disponibilidad de realizar la firma digital fuera de los ambientes físicos de la Municipalidad de Chorrillos.

7.1.6. Los Órganos y Unidades Orgánicas deberán remitir a la Gerencia de Informática y Tecnología, a través de la Gerencia Municipal, la relación de los servidores públicos que cuentan con autorización de acceso para firmar digitalmente con el uso de DNI electrónico y/o token criptográfico, desde los sistemas de información institucionales, indicando su número de DNI, el nombre completo, unidad orgánica, cargo, correo electrónico, teléfono fijo, celular del servidor público.

7.1.7. Los sistemas de información que vienen soportando los procesos funcionales, administrativos y de apoyo de la Municipalidad de Chorrillos, serán actualizados de manera progresiva, incorporándolos en aquellos que resulten justificables y oportunos.

MUNICIPALIDAD DE CHORRILLOS V°B° GERENCIA MUNICIPAL

MUNICIPALIDAD DE CHORRILLOS V°B° Ger.Planeam. y presupuesto

MUNICIPALIDAD DE CHORRILLOS V°B° Gerencia de Informática y Tecnología

MUNICIPALIDAD DE CHORRILLOS GERENCIA DE ASESORÍA JURÍDICA V°B°

7.1.8. Para que un suscriptor pueda aplicar la firma digital, es necesario que cuente con certificado digital vigente en un dispositivo criptográfico o DNI electrónico y un aplicativo acreditado que permita firmar digitalmente.

7.2. DEL PROCEDIMIENTO PARA LA CANCELACIÓN DE LA FIRMA Y/O CERTIFICADO DIGITAL

7.2.1. Las áreas usuarias solicitan la cancelación del certificado digital de los servidores públicos, a la Gerencia de Informática y Tecnología a través de la Gerencia Municipal, cuya relación laboral ha concluido; haciendo entrega de los lectores de tarjetas inteligentes para DNI electrónico y/o tokens criptográficos.

7.2.2. La Gerencia de Informática y Tecnología a través del administrador del certificado digital, gestionará la cancelación del certificado digital, cuando el servidor público no tenga relación laboral con la Entidad.

7.2.3. Se debe solicitar la cancelación del certificado digital cuando exista:

- Exposición, puesta en peligro o uso indebido de la clave privada.
- Deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
- Cuando la información contenida en el certificado ya no resulte correcta.
- Cuando el/la suscriptor/a deja de laborar en la Municipalidad de Chorrillos.

7.3. DE LA ADMINISTRACIÓN DEL CERTIFICADO DIGITAL

7.3.1. El representante legal de la Municipalidad de Chorrillos es quien debe solicitar a través de la RENIEC la suscripción del contrato de prestación de servicios de certificación digital de persona jurídica para la Municipalidad.

7.3.2. Una vez suscrito el contrato de prestación de servicios de certificación digital el certificado digital de persona jurídica a favor de la Municipalidad de Chorrillos, se inicia el trámite para la emisión de certificados digitales para los/las suscriptores/as de la Entidad.

7.4. DE LOS/LAS SUSCRIPTORES/AS DE LA ENTIDAD

7.4.1. Los/las servidores/as de confianza de la Municipalidad de Chorrillos remiten la solicitud formal mediante el llenado del **Formato de Requerimiento de Firma Digital (FREFID) – Anexo N° 03**, para suscriptores/as a la Gerencia de Informática y Tecnología, a través de la Gerencia Municipal, la relación de los/las suscriptores/as responsables de firmar digitalmente los documentos.

7.4.2. La Gerencia Municipal es quien autoriza la relación de los/las suscriptores/as de la Entidad.

7.5. DEL USO DE LA FIRMA DIGITAL

7.5.1. Los/Las suscriptores/as de los Órganos y Unidades Orgánicas de la Municipalidad de Chorrillos, deben hacer uso de la firma y certificado digital en todos los documentos electrónicos que se emitan dentro del marco administrativo de la Municipalidad de Chorrillos.

7.5.2. Los/Las suscriptores/as de los Órganos y Unidades Orgánicas de la Municipalidad de Chorrillos son responsables del contenido del documento electrónico en el que firmen digitalmente a través de los sistemas de información de la Municipalidad de Chorrillos o a través de un componente de firma digital.

7.5.3. Excepcionalmente, cuando por razones técnicas del sistema informático, el/la suscriptor/a 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.

7.5.4. El documento electrónico firmado digitalmente debe ser almacenado en la base de datos de los sistemas de información de la Municipalidad de Chorrillos, en archivo digital con formato PDF o similar y almacenado con las firmas digitales y sellos de tiempo correspondiente.

7.5.5. El/La suscriptor/a para firmar digitalmente un documento electrónico debe ejecutar los pasos siguientes:

- Seleccionar el documento electrónico en formato PDF almacenado en una carpeta de su computadora o en el repositorio establecido para tal fin.
- Utilizar su certificado digital almacenado en el dispositivo criptográfico asignado o su DNI electrónico.
- Usar el aplicativo acreditado para firma digital instalado en la computadora.
- Consignar su PIN solicitado por el software y proceder a firmar el documento electrónico.

7.6. DEL USO DE LOS DISPOSITIVOS CRIPTOGRÁFICOS DE ALMACENAMIENTO

Para el almacenamiento de los certificados digitales de los/las suscriptores/as en dispositivos criptográficos, se debe tener en cuenta lo siguiente:

7.6.1. La designación del dispositivo criptográfico o lector de tarjeta inteligente para DNI electrónico se efectúa mediante el **Formato de Asignación de Dispositivos Criptográfico (FADC) – Anexo N° 04** y firma de el/la suscriptor/a en señal de conformidad.

7.6.2. La Gerencia de Informática y Tecnología, es la encargada de instruir y/o capacitar a el/la suscriptor/a, respecto del uso, manejo y/o almacenamiento del certificado digital en el dispositivo criptográfico.

7.6.3. En caso de bloqueo de la contraseña o PIN del dispositivo criptográfico, el/la suscriptor/a está en la obligación de comunicar a la Gerencia de Informática y Tecnología, quien verifica si se trata de un bloqueo temporal o permanente.

7.6.4. El/La suscriptor/a es responsable del dispositivo criptográfico asignado; ante la pérdida de este, se toma en cuenta las disposiciones que establezca la Gerencia de Informática y Tecnología, respecto a su reposición.

VIII. DISPOSICIONES COMPLEMENTARIAS:

Los/Las suscriptores/as deben observar lo siguiente:

8.1. **Autenticidad:** Esta característica asegura que la firma digital del documento fue realizada efectivamente por el/la suscriptor/a.

8.2. **Integridad:** Un documento electrónico íntegro es aquel que llega a su destino completo y sin alteraciones. Una Infraestructura de Clave Pública (PKI), preserva la integridad de los documentos permitiendo saber si han sido alterados en el trayecto entre el emisor y el receptor.

8.3. **Neutralidad Tecnológica:** Se pueden emplear todas aquellas tecnologías que cumplan con los requisitos y resultados que las leyes exigen. El procedimiento para la firma digital usando certificados digitales y dispositivos criptográficos, es aplicado de tal forma que, no favorezca, excluya o restrinja alguna tecnología en particular.

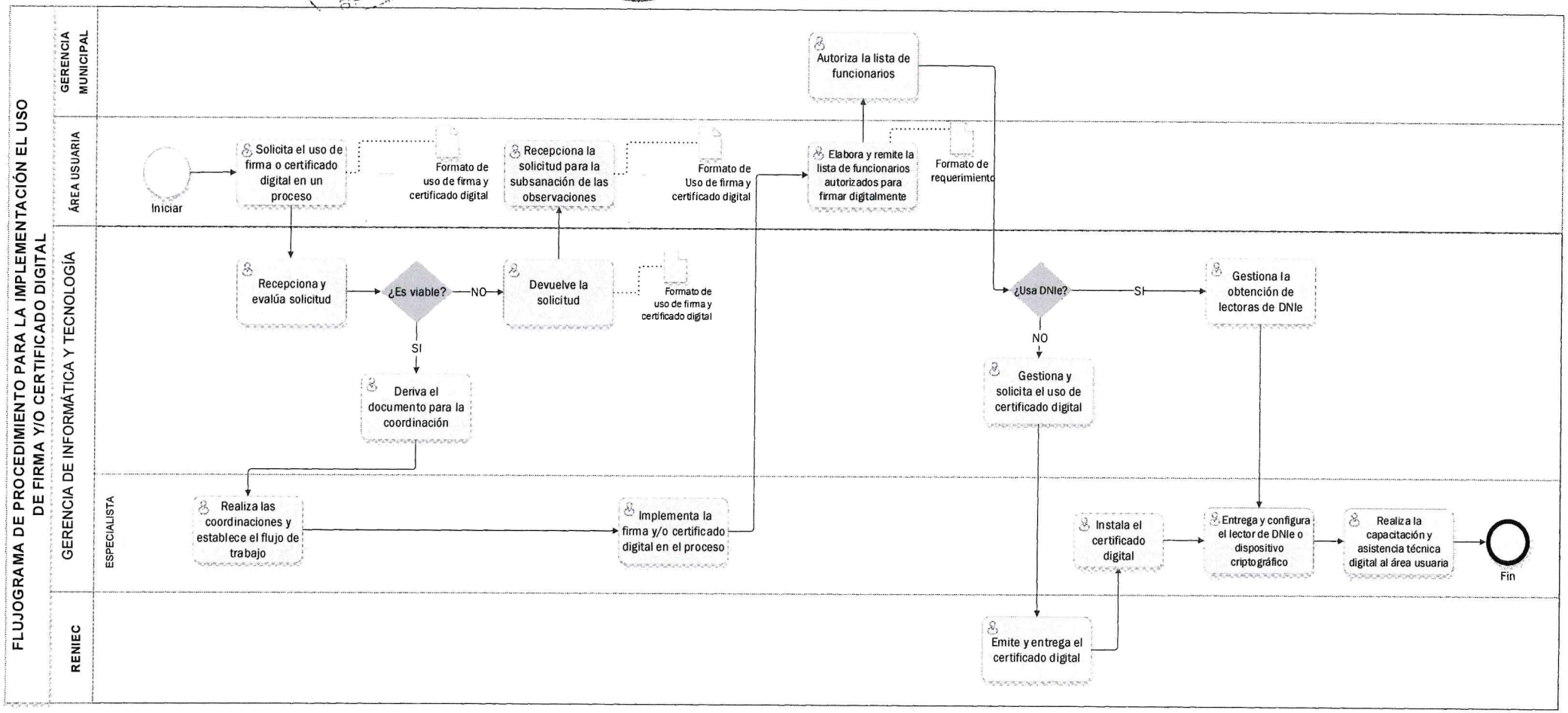
8.4. **Presunción de veracidad:** Todos los documentos generados en los sistemas de información con firma digital integrada en todas las formas y formalidades prescritas responden a la verdad de los hechos que ellos firman.

IX. ANEXOS:

9.1. **Anexo N° 01:** Flujograma de Procedimiento para la implementación del uso de firma y/o certificado digital.
9.2. **Anexo N° 02:** Formato de Uso de Firma Digital (FUFID).
9.3. **Anexo N° 03:** Formato de Requerimiento de Firma Digital (FREFID)
9.4. **Anexo N° 04:** Formato de Asignación de Dispositivo Criptográfico (FADC).

ANEXO N.º 01: FLUJOGRAMA DE PROCEDIMIENTO PARA LA IMPLEMENTACIÓN DEL USO DE FIRMA Y/O CERTIFICADO DIGITAL

Municipalidad de Chorrillos



ANEXO N.º 02: FORMATO DE USO DE FIRMA DIGITAL (FUFID)

Municipalidad de Chorrillos

USO DE FIRMA DIGITAL EN LA MUNICIPALIDAD DE CHORRILLOS		
INFORMACIÓN GENERAL		
Gerencia/Dirección/Oficina/Área:	**Cargo:**	**Correo:**
Nombres:	**Apellidos:**	**Teléfono/ Celular:**
INFORMACIÓN DEL PROCESO		
Nombre del Proceso:		
Actividades o Tareas que se Realizarán en el Proceso:		
Descripción breve del Uso de Firma o Certificado Digital:		

ANEXO N.º 03: FORMATO DE REQUERIMIENTO DE FIRMA DIGITAL (FREFID)

Municipalidad de Chorrillos

Nº	Nº DE DNI	APELLIDO PATERNO	APELLIDO MATERNO	NOMBRES	ÓRGANO Y/O UNIDAD ORGÁNICA	CARGO	CORREO	TELÉFONO	CELULAR

ANEXO N.º 04: FORMATO DE ASIGNACIÓN DE DISPOSITIVO CRIPTOGRÁFICO (FADC)

Municipalidad de Chorrillos

DATOS DEL SUSCRIPTOR/A	
Fecha de entrega:	
Sede:	
Gerencia/Dirección/Oficina/Área:	
Cargo:	
Nombre completo del suscriptor:	
DNI:	
Correo electrónico:	
Teléfono:	
Celular:	
DATOS DEL DISPOSITIVO DE FIRMA Y/O	
□ Lector de tarjeta inteligente	□ Dispositivo criptográfico
Marca:	Marca:
Modelo:	Modelo:
Nº de serie:	Nº de serie:

Administrador de Certificado Digital

El/La Suscriptor/a

Anexo
INFORME DE SUSTENTO DE NECESIDAD

Municipalidad de Chorrillos
GERENCIA DE INFORMATICA Y TECNOLOGIA

"Año de la unidad, la paz y el desarrollo"

MUNICIPALIDAD DE CHORRILLOS
GERENCIA MUNICIPAL
02 FEB 2023
RECIBIDO
HORA 8:35 FIRMA

INFORME Nº 0021-2023 MDCH-GIT

Para	:	**Abg. ANATOLY RENAN BEDRIÑANA CORDOVA** GERENTE MUNICIPAL
De	:	**Ing. ROBERTO CARLOS ROMAN ANAYA** GERENTE DE INFORMÁTICA Y TECNOLOGÍA
Asunto	:	ELABORACIÓN DE DIRECTIVA PARA LA GESTIÓN Y USO DE FIRMA Y CERTIFICADO DIGITAL EN LOS SISTEMAS DE INFORMACIÓN DE LA MUNICIPALIDAD DE CHORRILLOS
Referencia	:	PROVEÍDO N°200-2023-MDCH-GM
Fecha	:	Chorrillos, 1 de febrero de 2023

Tengo el agrado de dirigirme a usted, en atención al asunto del rubro, para informar que esta gerencia ha elaborado la DIRECTIVA PARA LA GESTIÓN Y USO DE FIRMA Y CERTIFICADO DIGITAL EN LOS SISTEMAS DE INFORMACIÓN DE LA MUNICIPALIDAD DE CHORRILLOS, en el marco del gobierno y transformación digital; de acuerdo al siguiente sustento técnico:

I. ANTECEDENTES

1.1 Contrato de Contraprestación de Servicios de Certificación Digital Certificado Clase III - Persona Jurídica, entre la RENIEC y la Municipalidad de Chorrillos de fecha 15 de agosto de 2019.

1.2 Contrato de Prestación de Servicios de Certificación Digital Certificado Clase IV - Agente Automatizado - Persona Jurídica, entre la RENIEC y la Municipalidad de Chorrillos de fecha 31 de enero de 2023.

1.3 Desplegar el Modelo de Gestión Documental, en cumplimiento al artículo 8 del Decreto Legislativo N° 1310, la Resolución de Secretaría de Gobierno Digital N°001-2017-PCM/SEGDI y modificatoria.

II. BASE LEGAL

2.1 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.

2.2 En el marco de lo dispuesto por la Ley N° 27269 - Ley de Firmas y Certificados Digitales y por disposición expresa del respectivo Reglamento de la Ley, EL RENIEC ha sido designado como Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), Entidad de Certificación para el Estado Peruano (ECEP) y Entidad de Registro o Verificación para el Estado Peruano (EREP). Mediante

Municipalidad de Chorrillos
GERENCIA DE INFORMATICA Y TECNOLOGIA

2023-0021

"Año de la unidad, la paz y el desarrollo"

Resolución N° 098-2018/CFE-INDECOPI de la Comisión para la Gestión de la Infraestructura Oficial de Firma Electrónica de fecha 28 de junio del año 2018, se acredita a EREP-RENIEC (Persona Jurídica).

2.3 El Registro Nacional de Identificación y Estado Civil - RENIEC es un organismo constitucional autónomo, con personería jurídica de derecho público interno, creado por mandato de la Constitución Política del Perú mediante la Ley N° 26497, goza de atribuciones en materia registral, técnica, administrativa, económica y financiera. Está encargado de organizar y mantener el Registro Único de Identificación de las Personas Naturales e inscribir los hechos y actos relativos a su capacidad y estado civil.

2.4 Ley N° 27658 - Ley de Modernización de la Gestión del Estado, declara al Estado Peruano en proceso de modernización en sus diferentes instancias, dependencias entidades, organizaciones y procedimientos con la finalidad de mejorar la gestión publica y construir un estado democrático, descentralizado y al servicio del ciudadano.

2.5 Decreto Supremo N° 052-2008-PCM - Reglamento de la Ley de Firmas y Certificados Digitales.

2.6 Decreto Supremo N.° 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

2.7 Resolución de Secretaría de Gobierno y Transformación Digital N.° 002-2021-PCM/SGTD, que aprueba la Directiva Nº 002-2021-PCM/ SGTD, Directiva que regula la generación y el uso del Código de Verificación Digital en las entidades de la Administración Pública.

2.8 Resolución de Secretaría de Gobierno Digital N.° 001-2021-PCM/SGD, que aprueba la Directiva N° 001-2021-PCM/SGD, "Directiva que establece los Lineamientos para la Conversión Integral de Procedimientos Administrativos a Plataformas o Servicios Digitales"
<https://www.gob.pe/institucion/pcm/normas-legales/1976362-001-2021-pcm-sgd>.

2.9 Decreto de Urgencia N° 006-2020, que crea el Sistema Nacional de Transformación Digital.

2.10 Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 004-2019-JUS, del 25 de enero de 2019.

Municipalidad de Chorrillos
GERENCIA DE INFORMATICA Y TECNOLOGIA

2023-0021

"Año de la unidad, la paz y el desarrollo"

2.11 Ley N° 27269 - Ley de Firmas y Certificados Digitales, del 28 de mayo de 2000.

2.12 Decreto Supremo N° 052-2008-PCM - Reglamento de la Ley de Firmas y Certificados Digitales, del 19 de julio de 2008.

2.13 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".

III. ANÁLISIS

3.1 En búsqueda de lograr un Gobierno Digital y del proceso de transformación digital en la Municipalidad de Chorrillos, resulta necesario fortalecer competencias para el despliegue de proyectos e iniciativas en gestión documental, interoperabilidad, identidad digital, gobernanza de datos y seguridad digital.

3.2 Asimismo, resulta necesario fortalecer el proceso de modernización y la simplificación administrativa, mediante el uso estratégico de las tecnologías digitales, como mecanismo de optimización en tiempo y costo, durante la tramitación de solicitudes y emisión de actos administrativos, que permitan la prestación de servicios públicos de calidad al ciudadano.

3.3 Del mismo modo, resulta necesario permitir a los servidores de confianza de la Municipalidad de Chorrillos, firmar digitalmente los documentos electrónicos que generen, en los diferentes sistemas de información administrados por la Gerencia de Informática y Tecnología, como parte de sus funciones, haciendo uso del respectivo lector de tarjeta inteligente y/o dispositivo criptográfico, 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.

3.4 También, resulta necesario promover la eco eficiencia y el uso racional de los recursos, mediante la implementación de estrategias Cero Papel en la documentación interna y externa, a través del empleo de documentos electrónicos, que garanticen la seguridad de la información y que generen una óptima administración de recursos al Estado.

3.5 La Municipalidad de Chorrillos suscribió con el Registro Nacional de Identificación y Estado Civil con fecha 15 de agosto de 2019, el Contrato de Contraprestación de Servicios de Certificación Digital Certificado Clase III - Persona Jurídica, en el marco de la Ley N° 27269 - Ley de Firmas y Certificados

Municipalidad de Chorrillos
GERENCIA DE INFORMATICA Y TECNOLOGIA

2023-0021

"Año de la unidad, la paz y el desarrollo"

Digitales modificado por la Ley N° 27310 y su reglamento aprobado por el Decreto Supremo N° 052-2008-PCM y modificaciones, y Decreto Supremo N° 026-2016-PCM donde se 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.

3.6 La Municipalidad de Chorrillos suscribió con el Registro Nacional de Identificación y Estado Civil con fecha 31 de enero de 2023, Contrato de Prestación de Servicios de Certificación Digital Certificado Clase IV - Agente Automatizado - Persona Jurídica, en el marco de la Ley N° 27269 - Ley de Firmas y Certificados Digitales modificado por la Ley N° 27310 y su reglamento aprobado por el Decreto Supremo N° 052-2008-PCM y modificaciones, y Decreto Supremo N° 026-2016-PCM donde se 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.

3.7 En cumplimiento al artículo 8 del Decreto Legislativo No 1310, la Resolución de Secretaría de Gobierno Digital N°001-2017-PCM/SEGDI y modificatoria, esta gerencia se encuentra en fase de despliegue del Modelo de Gestión Documental, cuyo plazo estimado es de 90 días calendario.

IV. CONCLUSIONES

4.1 A fin de fortalecer el proceso de modernización y la simplificación administrativa, mediante el uso estratégico de las tecnologías digitales, en el marco de gobierno y transformación digital; se concluye que, resulta necesario la elaboración y aprobación de la DIRECTIVA PARA LA GESTIÓN Y USO DE FIRMA Y CERTIFICADO DIGITAL EN LOS SISTEMAS DE INFORMACIÓN DE LA MUNICIPALIDAD DE CHORRILLOS.

4.2 A fin de permitir a los servidores de confianza de la Municipalidad de Chorrillos, firmar digitalmente los documentos electrónicos que generen, en los diferentes sistemas de información administrados por la Gerencia de Informática y Tecnología; se concluye que, resulta necesario la elaboración y aprobación de la DIRECTIVA PARA LA GESTIÓN Y USO DE FIRMA Y CERTIFICADO DIGITAL EN LOS SISTEMAS DE INFORMACIÓN DE LA MUNICIPALIDAD DE CHORRILLOS.

4.3 A fin de promover la eco eficiencia y el uso racional de los recursos, mediante la implementación de estrategias Cero Papel en la documentación interna y externa, a través del empleo de documentos electrónicos, que garanticen la seguridad de la información y que generen una óptima administración de recursos al Estado; se concluye que, resulta necesario la elaboración y aprobación de la DIRECTIVA PARA LA GESTIÓN Y USO DE FIRMA Y CERTIFICADO DIGITAL EN LOS SISTEMAS DE INFORMACIÓN DE LA MUNICIPALIDAD DE CHORRILLOS.

Municipalidad de Chorrillos
GERENCIA DE INFORMATICA Y TECNOLOGIA

2023-0021

"Año de la unidad, la paz y el desarrollo"

V. **RECOMENDACIONES**

5.1 Dar continuidad al trámite, hasta la aprobación y publicación de la DIRECTIVA PARA LA GESTIÓN Y USO DE FIRMA Y CERTIFICADO DIGITAL EN LOS SISTEMAS DE INFORMACIÓN DE LA MUNICIPALIDAD DE CHORRILLOS.

En ese sentido, se solicita que su despacho continúe con el trámite correspondiente hasta su aprobación con acto resolutivo y pueda ser publicado en nuestro portal web institucional.

Se adjunta tres (03) juegos de la mencionada directiva.

Atentamente,

MUNICIPALIDAD DE CHORRILLOS
ING. ROBERTO C. ROMAN ANAYA
GERENTE DE INFORMATICA Y TECNOLOGIA