GOBIERNO REGIONAL
MADRE DE DIOS
Caminemos Juntos

DIRECTIVA Nº 002-2021-GRPPYAT/SGDIEI

"DIRECTIVA QUE ESTABLECE LINEAMIENTOS PARA LA IMPLEMENTACIÓN Y USO DE FIRMAS Y CERTIFICADOS DIGITALES EN EL GOBIERNO REGIONAL DE MADRE DE DIOS"

Puerto Maldonado, junio 2021

Firmado digitalmente por: HOLGADO CANAL Edwin Joel FAU 20527143200 hard
Motivo: Doy V° B°
Fecha: 21/06/2021 09:08:10-0500

Firmado digitalmente por: ACHIN LIMA Carlos FAU 20527143200 hard
Motivo: Doy V° B°
Fecha: 21/06/2021 10:17:49-0500

Firmado digitalmente por: ODAR YABAR Maria Angelica FAU 20527143200 hard
Motivo: Soy el autor del documento
Fecha: 28/06/2021 14:42:48-0500

DIRECTIVA Nº 002-2021-GRPYAT/SDIEI-UI

DIRECTIVA QUE ESTABLECE LINEAMIENTOS PARA LA IMPLEMENTACIÓN Y USO DE FIRMAS Y CERTIFICADOS DIGITALES EN EL GOBIERNO REGIONAL DE MADRE DE DIOS

ARTÍCULO 1. OBJETO

La Presente Directiva tiene como objetivo:

Establecer lineamientos para la implementación y uso de firmas y certificados digitales en los actos administrativos y de administración interna del Gobierno Regional de Madre de Dios, en adelante GOREMAD.

ARTÍCULO 2. FINALIDAD

2.1. Impulsar el proceso de modernización y de simplificación administrativa, a través del uso estratégico de las tecnologías digitales, como mecanismo de ahorro en tiempo y costos.

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

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

2.4. Definir el proceso de implementación, uso y cancelación de certificados digitales de suscriptores en el Gobierno Regional de Madre de Dios, para el uso de Firmas Digitales.

ARTÍCULO 3. MARCO LEGAL

a) Ley N° 29158, Ley Orgánica del Poder Ejecutivo.
b) Ley N° 27269, Ley de Firmas y Certificados Digitales.
c) Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
d) Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
e) Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
f) Decreto Supremo N° 052-2008-PCM, Decreto Supremo que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales y modificatorias.
g) Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.

h) Resolución de Secretaría de Gobierno Digital N° 001-2017-PCM/SEGDI, que aprueba el Modelo de Gestión Documental en el marco del Decreto Legislativo N° 1310.
i) Contrato de Prestación de Servicios de Certificación Digital, CERTIFICADO CLASE III - PERSONA JURIDICA suscrito entre el GOREMAD y el Registro Nacional de Identificación y Estado Civil (RENIEC).

ARTÍCULO 4. DEFINICIONES

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

4.2. Dispositivo criptográfico: Es el 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.

4.3. Documento electrónico: Es la 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.

4.4. 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.

4.5. Entidades de Registro o Verificación para el Estado Peruano (EREP-RENIEC): Es la persona jurídica, con excepción de los notarios públicos. encargada del levantamiento de datos. tal 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 Nº 27269, Ley de Firmas y Certificados Digitales aprobado con Decreto Supremo nº 052-2008-PCM, el RENIEC es la única entidad de certificación, verificación y registro en nuestro país.

4.6. 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 debidamente acreditado, que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica, y que no medie ninguno de los vicios de la voluntad previstos en el Código Civil.

4.7. 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.

4.8. PDF: Es un 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).

4.9. Responsable Técnico: Es el profesional que labora en la Sub Gerencia de Desarrollo Institucional e Informática, 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 dispositivo criptográfico y de capacitar a los Suscriptores para el uso de dicho Certificado.

4.10. Sistema Administrativo de Certificación Digital: Es aquel sistema informático que permite una gestión eficiente y eficaz de las funciones del Registro Nacional de Identificación y Estado Civil - RENIEC, en su 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.

4.11. Suscriptor: Funcionario o servidor público de la Entidad, que cuenta con certificado digital y token de ser el caso, será responsables de visar o firmar documentos electrónicos a través de un sistema informático.

4.12. Titular del Certificado Digital: Es la persona designada mediante Resolución, por el representante legal. la administración de los Certificados Digitales de la entidad, 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 ANA ante RENIEC; asimismo, realiza las altas y bajas de los certificados digitales de los suscriptores. Es el responsable de llevar un registro actualizado de los funcionarios y servidores de la entidad a quienes se les autoriza o cancela ante la RENIEC, los Certificados Digitales para la Firma Digital de los Suscriptores.

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

ARTÍCULO 5. ALCANCE

Las disposiciones contempladas en la presente Directiva son de aplicación y de obligatorio cumplimiento para todos los funcionarios y servidores que prestan servicio en la Unidad Ejecutora N.° 0875 del GOREMAD, independiente de su régimen laboral o

vinculo contractual según corresponda. Y tiene vigencia a partir del Dia Siguiente de su aprobación.

ARTÍCULO 6. CONSIDERACIONES SOBRE LA FIRMA DIGITAL

6.1. Validez legal de la Firma Digital

a) 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.

b) 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 o servidores públicos de la entidad.

c) En caso que 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 y deberá contar con un método de validación de la identidad digital del mismo (Formato Nº. 04), para lo cual el documento tiene que ser registrado en el sistema de Gestión Documental del GOREMAD, el cual se encargara de asignar la identidad del mismo.

6.2. Obligaciones del Suscriptor de la Firma Digital

a) Entregar información veraz bajo su responsabilidad.

b) Generar la clave privada y firmar digitalmente mediante los procedimientos señalados por la Entidad de Certificación.

c) La clave privada es intransferible. En tal sentido, el suscriptor es responsable de la misma, por to que deberá mantener su control y la reserva bajo responsabilidad.

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

e) En caso de que 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 RENIEC, la cancelación del certificado digital.

6.3. Emisión de Documentos con Firma Digital

a) Para la emisión de documentos con firma digital, el suscriptor debe contar con un certificado digital, ya sea por medio del certificado digital que se encuentran en el DNI electrónico o mediante certificado digital como persona jurídica tramitados por el representante legal del GOREMAD ante la RENIEC.

b) Los funcionarios y servidores, a quienes se les generó el certificado digital para la firma digital, registrarán una clave privada al momento de la instalación del certificado digital en el equipo informático institucional (laptop, PC o Token Criptográfico), es responsabilidad de estos emplear adecuadamente su certificado digital conforme a lo dispuesto en la Ley Nº 27269 – Ley de Firmas y Certificados Digitales y su Reglamento y sus modificatorias.

c) La Unidad de Informática de la Sub Gerencia de Desarrollo Institucional e Informática, presta apoyo técnico a los funcionarios y servidores en el uso del Certificado y Firma Digital. Una vez que los funcionarios y servidores obtengan su certificado digital, se procederá con la instalación del software y asignación de hardware, donde el suscriptor deberá firma el Formato Nº 02 "Acta de entrega – Recepción de Bienes para firma Digital". Además de instruir al personal operativo en el uso adecuado del software que producirá los documentos electrónicos firmados digitalmente

d) El Titular del Certificado Digital coordinará con la Oficina de Personal cualquier información adicional del suscriptor, necesaria para la autorización en el Sistema Administrativo de Certificación Digital.

e) Los funcionarios y servidores harán uso de los certificados digitales para firmar digitalmente documentos electrónicos de acuerdo a las funciones y procedimientos de su competencia, debiendo mantener el control y absoluta reserva sobre el certificado y clave privada bajo su responsabilidad.

f) El uso de la clave privada de su certificado digital es intransferible y debe ser conocida únicamente por el suscriptor, siendo responsabilidad y no repudio del suscriptor la firma de cualquier documento electrónico usando su certificado digital y clave privada.

g) Con respecto a los documento electrónicos firmados digitalmente, los certificados digitales pueden ser validados mediante el uso del Software Refirma, Refirma Validator y otros software de lectura de documentos en PDF con dicha funcionalidad.

Artículo 7. MECANICA OPERATIVA

7.1. Obtención del certificado digital para la firma digital de suscriptores

a) Los Suscriptores canalizarán sus pedidos a través de la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial, mediante el Formato N.º 01, "Listado de funcionarios Aspirantes a Suscriptores", la que debe ser remitida para su trámite correspondiente.

b) La Sub Gerencia de Desarrollo Institucional e Informática evaluará la viabilidad del requerimiento, considerando los recursos necesarios como el software y hardware que permitan su implementación, además se determinará si el

solicitante empleará DNI electrónico o certificado digital para la suscripción de firmas digitales.

c) Una vez aprobada la solicitud de firma digital, en caso de requerirse certificado digital el solicitante en coordinación con la Unidad de Informática llevara a cabo los procedimientos de la EREP-RENIEC para la "Autorización para la emisión de Certificados Digitales a los Suscriptores" según normatividad vigente.

d) Los suscriptores reciben un primer correo por parte del RENIEC, donde se le indica el inicio del proceso de solicitud de certificado digital.

e) Los suscriptores reciben un segundo correo del RENIEC el certificado digital / mediante el correo electrónico registrado, indicando la dirección URL para proceder a la descarga del certificado digital en la PC o Token de ser el caso.

f) El suscriptor deberá notificar a la Unidad de Informática para realizar la descarga 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.

g) El suscriptor no deberá olvidar la contraseña asignada para firmar los documentos digitalmente, en caso que suceda si el certificado se encontraba instalado en un equipo de cómputo 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, por otro lado en caso que el certificado digital se encuentre en un dispositivo token, el suscriptor tiene la opción de presentar el Formato N.º 05 "Solicitud de restauración de clave de certificado digital" a la Gerencia Regional de Planeamiento Presupuesto y Acondicionamiento territorial, debiendo sustentar detalladamente los motivos de su solicitud.

7.2. Uso del certificado digital para la firma digital por los suscriptores

a) El Responsable Técnico, previa coordinación con el Suscriptor, entrega el token con el Certificado Digital, instala el Software y realiza la capacitación técnica sobre el uso del Certificado Digital y la Firma Digital, una vez suscrito el Formato Nº 2 " Acta de Entrega – Recepción de bienes para firma Digital".

b) 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.

c) El uso del token es intransferible y de uso exclusivo para la firma de documentos electrónicos generados en la institución.

d) 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.

e) 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

7.3. Cancelación del certificado digital para la firma digital por los suscriptores

a) La Cancelación del certificado digital puede darse según lo establecido en el Contrato de prestación de servicios de Certificación Digital, CERTIFICADO CLASE III - PERSONA JURIDICA suscrito entre el registro Nacional de Identificación y Estado Civil (RENIEC) y el GOREMAD.

b) 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, confirmando posteriormente al Suscriptor, vía correo electrónico, dicha cancelación.

c) En caso que el suscriptor renuncie o cese de su cargo, adicionalmente al informe de entrega de cargo presentado a la Oficina de Personal deberá incluir la presentación del Formulario N° 3 "Solicitud de cancelación del Certificado Digital" debidamente llenado y firmado, el mismo que deberá ser remitido al titular del Certificado Digital para la cancelación ante el RENIEC. La cancelación del Certificado Digital del Suscriptor conlleva a la devolución del bien asignado (token o lector de DNI electrónico) que le fue entregado para el uso del mismo.

d) En caso de pérdida o robo del token se debe comunicar de la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial adjuntando el Formulario N.° 3 "Solicitud de cancelación del Certificado Digital" adjuntando copia de la denuncia policial con la finalidad de que a través del Titular del Certificado Digital se gestione ante el organismo correspondiente la cancelación del certificado digital. Cabe señalar que 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/servidor a quien se le asignó dicho dispositivo

Artículo 8. DISPOSICIONES COMPLEMENTARIAS

a) Los suscriptores son responsables del contenido de los documentos electrónicos firmados digitalmente.

b) En caso de que la clave privada quede comprometida en su seguridad, el suscriptor debe notificarlo de inmediato la Sub Gerencia de Desarrollo Institucional e Informática; para que se proceda a la cancelación del certificado digital.

c) En caso de bloqueo de clave privada o PIN del token, el suscriptor está en la obligación de comunicar a la Unidad de Informática, quién verifica si se trata de un bloqueo momentáneo o permanente. Si fuera un bloqueo permanente, la Unidad de Informática, se comunica con la EREP-RENIEC para la revocación del certificado digital y generación de uno nuevo.

d) Los documentos electrónicos, firmados digitalmente, deben ser admitidos como prueba en los procedimientos administrativos del Gobierno Regional de Madre de Dios, teniendo en cuenta que la firma digital ha sido consignada en mérito a un certificado emitido por una entidad de certificación debidamente acreditada, por lo que posee la misma validez y eficacia jurídica que el uso de firma manuscrita.

e) La implementación de la firma digital a través de los certificados digitales se realizará de forma progresiva, en coordinación con la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial y las áreas usuarias, debiéndose establecer los tipos de documentos y procedimientos administrativos a ser considerados para la aplicación de la firma digital, con las excepciones de aquellos que por su propia naturaleza o porque así lo requiera norma alguna, el uso de la firma manuscrita y medio físico para su entrega.

f) Todos los documentos internos y/o externos que emita la entidad firmados digitalmente deben ser registrados en el Sistema de Gestión Documental – SGD y/o almacenados en el repositorio de datos del GOREMAD para su resguardo e implementación de mecanismos de verificación de autenticidad vía enlace web.

g) Para todo lo no previsto en la presente directiva, será la aplicación de las normas legales vigentes que regulan el uso de las firmas digitales; prevaleciendo estas últimas en caso de discrepancia o conflicto con la primera.

h) Para realizar la consulta de verificación de autenticidad de un documento con firma digital se deberá acceder por medio del portal oficial del GOREMAD en el Gob.pe con el link https://www.gob.pe/regionmadrededios opción "verificar documento digital".

Artículo 9. ANEXOS

a) Formato Nº. 01: Lista de funcionarios Aspirantes a Suscriptores
b) Formato Nº. 02: Acta de Entrega – Recepción de Bienes para Firma Digital
c) Formato Nº. 03: Solicitud de Cancelación de Certificado Digital
d) Formato Nº. 04: Guía de Diseño de Documento para Firma Digital
e) Formato Nº. 05: Solicitud de Restauración de Clave de Certificado Digital

Artículo 10. FLUJOGRAMA