Resolución Directoral Regional

Nº 2410 -2018-DRELM

Lima, 06 Abr. 2018

VISTO: El expediente DRELM **Nº EAUGD2018-INT-0009856,** el Informe N° 013-2018-MINEDU/VMGI-DRELM-OPP-ERMC y el Informe Legal Nº 953-2018-MINEDU/VMGI-DRELM-OAJ;

CONSIDERANDO:

Que, la Ley N° 27658, Ley Marco 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 pública y construir un Estado democrático, descentralizado y al servicio del ciudadano;

Que, el artículo 76 de la Ley N° 28044, Ley General de Educación, dispone que la Dirección Regional de Educación es un Órgano especializado del Gobierno Regional responsable del Servicio Educativo en el ámbito de su respectiva circunscripción territorial, teniendo como finalidad promover la educación, la cultura, el deporte, la recreación, la ciencia y la tecnología. Asegura los servicios educativos y los programas de atención integral con calidad y equidad en su ámbito jurisdiccional, para lo cual coordina con las Unidades de Gestión Educativa Local y convoca a la participación de los diferentes actores sociales;

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

Que, el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, aprobado mediante Decreto Supremo Nº 052-2008-PCM, regula, para los sectores público y privado, la utilización de las firmas digitales y el régimen de la Infraestructura Oficial de Firma Electrónica, que comprende la acreditación y supervisión de las Entidades de Certificación, las Entidades de Registro o Verificación, y los Prestadores de Servicios de Valor Añadido;

Que, el artículo 191 del Reglamento de Organización y Funciones del Ministerio de Educación, aprobado por Decreto Supremo N° 001-2015-MINEDU, establece que la

Dirección Regional de Educación de Lima Metropolitana es un órgano desconcentrado del Ministerio de Educación, a través del Despacho Viceministerial de Gestión Institucional, responsable del servicio educativo y de los programas de atención integral en el ámbito de su jurisdicción, así como de evaluar y supervisar a las Unidades de Gestión Educativa Local de Lima Metropolitana;

Que, de conformidad con los artículos 7 y 8 del Manual de Operaciones de la Dirección Regional de Educación de Lima Metropolitana, aprobado por Resolución Ministerial N° 215-2015-MINEDU, la Dirección Regional es la máxima autoridad administrativa de la DRELM, responsable de brindar disposiciones, así como de expedir actos resolutivos en materia de su competencia;

Que, el artículo 8 del Decreto Legislativo N° 1310 dispone que, las entidades del Poder Ejecutivo deben adecuar sus sistemas de trámite documentario o equivalentes para el envío automático de documentos electrónicos con otras entidades, así como dentro de sus áreas, órganos y unidades, hasta el 31 de diciembre de 2018;

Que, con Informe N° 008-2018-MINEDU/VMGI-DRELM/DIR/OAC/EAUGD adjunto al Memorandum N° 62-2018-MINEDU/VMGI-DRELM/DIR/OAC-EAUGD, la Oficina de Atención al Usuario y Comunicaciones propuso la aprobación de las "Orientaciones para el uso de la Firma Digital en la Dirección Regional de Educación de Lima Metropolitana";

Que, mediante Informe N° 013-2018-MINEDU/VMGI-DRELM-OPP-ERMC e Informe Legal N° 953-2018-MINEDU/VMGI-DRELM-OAJ, la Oficina de Planificación y Presupuesto y la Oficina de Asesoría Jurídica de la Dirección Regional de Educación de Lima Metropolitana, respectivamente, emitieron opinión favorable con relación al proyecto de Orientaciones propuesto;

Que, según lo mencionado, dichas Orientaciones se ciñen a lo establecido en la Resolución Directoral Regional N° 1639-2017-DRELM, de fecha 23 de marzo de 2017, que aprueba las Orientaciones para la formulación y aprobación de Orientaciones en la Dirección Regional de Educación de Lima Metropolitana y sus Unidades de Gestión Educativa Local;

Contando con la visación de la Oficina de Planificación y Presupuesto, la Oficina de Asesoría Jurídica, y de conformidad con lo dispuesto en la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, la Ley N° 27269, Ley de Firmas y Certificados Digitales, el Decreto Legislativo N° 1310, el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 006-2017-JUS, las facultades conferidas por el Reglamento de Organización y Funciones del Ministerio de Educación, aprobado por Decreto Supremo N° 001-2015-MINEDU, la Resolución Ministerial N° 215-2015-MINEDU, que aprueba el Manual de Operaciones de la Dirección Regional de Educación de Lima Metropolitana.

SE RESUELVE:

ARTÍCULO 1.- APROBAR las Orientaciones N° 04-2018/MINEDU/VMGI-DRELM/OAC-EAUGD denominada "Orientaciones para el uso de la Firma y Certificados Digitales en la Dirección Regional de Educación de Lima Metropolitana", así como sus cuatro (04) anexos que forman parte integrante de la presente Resolución en dieciséis (16) folios.

ARTÍCULO 2.- ENCARGAR a la Oficina de Planificación y Presupuesto de esta Sede Regional, la supervisión del estricto cumplimiento de las Orientaciones aprobadas en el artículo 1 de la presente Resolución.

ARTÍCULO 3.- DISPONER la publicación de la presente Resolución en la página web de la Dirección Regional de Educación de Lima Metropolitana: www.drelm.gob.pe para su difusión correspondiente.

Regístrese y Comuníquese,

Documento firmado digitalmente

KILLA SUMAC SUSANA MIRANDA TRONCOS
Directora Regional de Educación de
Lima Metropolitana

ORIENTACIONES N° 04 -2018/MINEDU/VMGI-DRELM/OPP-ETI

"ORIENTACIONES PARA EL USO DE LA FIRMA Y CERTIFICADOS DIGITALES EN LA DIRECCIÓN REGIONAL DE EDUCACIÓN DE LIMA METROPOLITANA"

1. FINALIDAD

Implementar el uso de la Firma Digital en los documentos que emite la Dirección Regional de Educación de Lima Metropolitana - DRELM, con la finalidad de contribuir al Proyecto Cero Papel como parte de la política y aporte al gobierno electrónico.

2. OBJETIVO

Establecer las orientaciones que regulen el uso de certificados digitales, tokens, y la firma digital a nivel de funcionarios y servidores públicos de la DRELM.

3. ALCANCES

La presente Orientación es de cumplimiento obligatorio para los funcionarios y servidores públicos de la DRELM que cuentan con certificado digital, y que en el ejercicio de sus funciones deban firmar digitalmente documentos electrónicos en el marco de los procesos de los órganos y/o unidades orgánicas a las que pertenecen.

4. BASE NORMATIVA

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 27269, Ley de Firmas y Certificados Digitales y sus Modificatorias.
- Decreto Supremo N° 006-2017-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444 – Ley del Procedimiento Administrativo General.
- Decreto Supremo N° 001-2015-MINEDU, que aprueba el Reglamento de Organización y Funciones del Ministerio de Educación.
- Decreto Supremo N° 081-2013-PCM, que aprueba la Política de Gobierno Electrónico 2013-2017.
- Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.
- Decreto Supremo N° 105-2012-PCM, que establece disposiciones para facilitar la puesta en marcha de la firma digital y modifica el Decreto Supremo N° 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales.
- Decreto Supremo N° 070-2011-PCM, que modifica el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados y establece normas aplicables al procedimiento registral en virtud del Decreto Legislativo N° 681 y Ampliatorias.
- Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales

- Resolución Ministerial N°215-2015-MINEDU, Manual de Operaciones de la Dirección Regional de Educación de Lima Metropolitana.

5. ORIENTACIONES GENERALES

5.1 Siglas

DRELM	Dirección Regional de Educación de Lima Metropolitana
MINEDU	Ministerio de Educación del Perú
PCM	Presidencia de Consejo de Ministros del Perú
INDECOPI	Instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual
EREP-RENIEC	Registro Nacional de Identificación y Estado Civil
FIPS	Estándares Federales de Procesamiento de la Información
DNI	Documento Nacional de Identidad

5.2 Definiciones

Administrador del Certificado Digital: Servidor designado por la Dirección Regional, encargado de gestionar ante el Registro Nacional de Identificación y Estado Civil - RENIEC, los Certificados Digitales para el personal de la entidad.

Autenticación: Proceso que permite determinar la identidad del firmante, en función del documento electrónico firmado digitalmente por éste, garantizando su vinculación e integridad.

Autoridad Administrativa Competente: Es el organismo público responsable de acreditar las Entidades de Certificación, a las Entidades de Registro o Verificación y a los Prestadores de Servicios de Valor Añadido, públicos y privados, encargadas de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura y de cumplir las demás funciones señaladas en el reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales aprobado con Decreto Supremo N° 052-2008-PCM, o aquellas que requiera en el transcurso de sus operaciones, conforme a la normativa que le resulte aplicable. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI.

Certificado Digital: Es un documento electrónico usado como credencial, que ha sido generado y firmado digitalmente por una Entidad de Certificación y que permite identificar a la persona natural o jurídica que emitirá la firma digital.

Contraseña: Código o combinación de caracteres, utilizado como medida de seguridad y cuyo objeto es el de proteger el "acceso no autorizado" a un recurso determinado.

Clave privada: Es una de las claves de un sistema de criptografía asimétrica que es usada para generar una firma digital en un documento electrónico para firmar un documento. La clave privada sólo debe permanecer en propiedad del suscriptor.

Clave pública: Es la otra clave en un sistema de criptografía asimétrica que es usada por el destinatario de un documento electrónico para verificar la firma digital puesta en dicho documento. La clave pública puede ser conocida por cualquier persona.

Documentos: Son los escritos públicos o privados, los impresos, fotocopias, facsímil o fax, planos, cuadros, dibujos, fotografías, radiografías, cintas cinematográficas microformas tanto en la modalidad de microfilm como en la modalidad de soportes informáticos y otras reproducciones de audio, video, la telemática en general y demás objetos que recojan contengan o representen algún hecho, o una actividad humana o su resultado.

Documento electrónico: Es la unidad básica documentaria cuyo soporte material es algún tipo de dispositivo electrónico o magnético, susceptible de ser generada, clasificada, gestionada, transmitida, procesada o conservada por una persona natural o jurídica utilizando sistemas informáticos.

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 verificación. Para el Estado Peruano es el Registro Nacional de Identificación y Estado Civil – RENIEC.

Entidad de Registro o Verificación (EREP): Es la 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 y cancelación. 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.

Equivalencia Funcional: Principio por el cual los actos jurídicos realizados por medios electrónicos que cumplan con las disposiciones legales vigentes poseen la misma validez y eficacia jurídica que los actos realizados por medios convencionales, pudiéndoles sustituir para todos los efectos legales. De conformidad con lo establecido en la Ley y su Reglamento, los documentos firmados digitalmente pueden ser presentados y admitidos como prueba en toda clase de procesos judiciales y procedimientos administrativos.

Expediente: Conjunto de documentos que acumulan toda la actividad procedimental de un mismo asunto originado de oficio o a solicitud de los administrados

Firma Digital: Es aquella firma electrónica que utilizando una técnica de criptografía asimétrica, permite la identificación del 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.

Firma Principal: Es la firma digital del autor del documento o del funcionario que suscribe el documento electrónico.

Firma visto bueno: Es la firma digital del asesor, especialista, asistente, colaborador, servidor o funcionario, quien elaboró, verificó, controló o revisó el documento. Puede incluir también la firma digital del llamado por procedimiento a dar confianza administrativa a quién suscribe la firma principal del documento electrónico.

Infraestructura Oficial de Firma Electrónica: Es un sistema confiable acreditado, regulado y supervisado por la autoridad administrativa competente, provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de 1) La integridad de los documentos electrónicos 2) La identidad de su autor, lo que es regulado conforme a Ley. El sistema incluye la generación de firmas digitales, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la Autoridad Administrativa Competente, incluyendo a la Entidad de Certificación Nacional para el Estado Peruano, las Entidades de Registro o Verificación para el Estado Peruano y los Prestadores de Servicios de Valor Añadido para el Estado Peruano.

Integridad: Presunción legal por la cual un documento electrónico no ha sido alterado desde su emisión hasta su recepción. Es decir, se presume que el mensaje de datos recibido corresponde al enviado. Por esta presunción, un documento electrónico firmado digitalmente

conforme a las normas vigentes, conserva la integridad del mensaje de datos, por el hecho de haber sido firmadas digitalmente, sin importar en que medio quede almacenado.

No repudio: Cuando una persona firma digitalmente un documento electrónico (al igual que cuando lo hace con una firma manuscrita) materializa en este acto la expresión de su voluntad, vinculando a la persona con el contenido del documento. De esta forma la persona no puede repudiar posteriormente la manifestación de su voluntad. El documento es veraz y sus efectos plenos.

Pin: Es un número de identificación personal utilizado como contraseña para acceder de manera segura a ciertos sistemas informáticos.

Presunción de Veracidad: Todos los documentos generados en los sistemas con firma digital integrada en todas las formas y formalidades prescritas, responden a la verdad de los hechos que ellos afirman.

Representante del Titular: Persona natural que cuenta con facultades para representar a la persona jurídica en los trámites de certificado digital ante la EREP-RENIEC.

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.

Token: Es un dispositivo de almacenamiento criptográfico que contiene el Certificado Digital asignado a la persona titular del mismo, que le permite firmar digitalmente.

El token u otro dispositivo de almacenamiento de certificado digital cumplen con el estándar FIPS 140-2, según convenio suscrito con el RENIEC.

5.3 De Las Firmas Y Certificados Digitales

La suscripción de un documento electrónico con firma digital generado desde un certificado digital vigente, es un mecanismo tecnológico que posee validez y eficacia jurídica.

La firma digital electrónica tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita; aplicando un software de firma digital acreditado ante la autoridad administrativa competente.

La implementación de la firma digital tendrá los siguientes beneficios:

- Simplificación administrativa
- Aportar el aumento de la confianza electrónica
- Aportar el desarrollo del gobierno electrónico

- Otorgar mayor seguridad e integridad a los documentos

La firma digital se basa en la propiedad sobre un mensaje o documento cifrado (resumen hash) utilizando la clave privada de un suscriptor de certificado digital y ésta sólo puede ser descifrado utilizando la clave pública asociada. De tal manera, se tiene la seguridad de que el mensaje o documento que ha podido descifrarse utilizando la clave pública sólo pudo cifrarse utilizando la clave privada.

6. ORIENTACIONES ESPECÍFICAS

6.1 Emisión Del Certificado Digital

6.1.1 El trámite de certificado digital se inicia con la manifestación de necesidad de la oficina de firmar digitalmente los documentos, lo cual se solicita mediante formato de Solicitud de Firma Digital según Anexo N° 1, la que es alcanzada al Administrador de Certificados Digitales, para su trámite correspondiente.

6.1.2 La Dirección Regional, designa al Administrador del Certificado Digital, quién es el responsable de solicitar ante EREP-RENIEC los certificados correspondientes para el personal de la entidad.

Esta designación la realiza la Dirección Regional a través de una delegación de facultades la misma que tiene que ser informada a RENIEC.

6.1.3 Una vez emitido el certificado digital a favor de la DRELM y entregado al Administrador del Certificado Digital, se inicia el trámite para la emisión y gestión de certificados digitales para los suscriptores. Para dicho efecto, el Administrador del Certificado Digital debe:

- Registrar los datos de los suscriptores en el formulario “Autorización para la emisión de Certificados Digitales a los Suscriptores” a través de su Cuenta de usuario en el portal de la EREP-RENIEC.

- Generar el reporte “Lista de Autorizaciones Generadas”. Este documento se firma en forma manuscrita y se envía en físico a la EREP-RENIEC.

- El Administrador del Certificado Digital deberá comunicar vía correo electrónico a los servidores a los que se les ha generado la Autorización, se acerquen a la EREP-RENIEC con su DNI vigente para recabar su certificado digital.

- Cuando el servidor se acerca a la EREP-RENIEC para recibir su certificado digital, pero no firma los formatos debido a que se ha incluido información incorrecta o inexacta en el certificado digital,

deberá comunicarse con el Administrador del Certificado Digital para que genere una solicitud a la EREP-RENIEC

- El suscriptor recibirá una clave y la ruta para descargar el Certificado Digital emitido por la EREP-RENIEC en un plazo máximo de cinco (05) días hábiles en su correo electrónico institucional. El suscriptor será responsable de revisar su correo tanto en la bandeja de entrada como en la bandeja de correo no deseado, la emisión de dicho certificado y sus instrucciones correspondiente por la EREP-RENIEC.

- Una vez recibido el correo electrónico del EREP-RENIEC, el suscriptor deberá comunicarse con el Equipo de Tecnologías de la Información de la Oficina de Planificación y Presupuesto, para que procedan a la instalación del certificado digital en su equipo de cómputo. En el proceso de instalación del Certificado Digital se solicitará que el suscriptor ingrese una contraseña, la cual servirá, para que pueda firmar a partir de ese momento los documentos electrónicos.

  En caso que la Dirección considere conveniente, determinará quién o quienes podrán hacer uso de la instalación del certificado digital mediante un token u otro dispositivo de almacenamiento del certificado digital. Se solicitará que el suscriptor ingrese un Pin, el cual servirá, para que pueda firmar a partir de ese momento los documentos electrónicos

6.2 Del Uso Del Certificado Digital Para La Firma Digital De Los Suscriptores

6.2.1 Los Jefes de Oficina, deberán de velar por el correcto uso de la firma digital en sus unidades y Equipos funcionales de la DRELM.

6.2.2 Para que un suscriptor pueda utilizar la firma digital en los documentos electrónicos, debe contar con el Certificado Digital, un dispositivo electrónico de seguridad que almacena su clave privada (token criptográfico y computador.) y el Software de Firma Digital.

6.2.3 Los suscriptores harán uso de los certificados digitales para firmar digitalmente documentos electrónicos de acuerdo a las funciones y procedimientos de su competencia. El uso de la contraseña de su certificado digital es intransferible, siendo responsabilidad y no repudiado del suscriptor la firma de cualquier documento electrónico usando su usuario contraseña.

6.2.4 Con relación al uso de la clave privada y del certificado digital por parte del suscriptor, este deberá cumplir con lo siguiente:

a) Emplear adecuadamente su certificado digital conforme a lo dispuesto en la Ley N° 27269 – Ley de Firmas y Certificados Digitales y su Reglamento y sus modificatorias.

b) Mantener el control y absoluta reserva de la clave privada bajo su responsabilidad y debe ser conocida únicamente por él.

c) En caso de extravío o pérdida de la tarjeta inteligente o token criptográfico se estaría garantizando que nadie que no conozca dicha contraseña o PIN de acceso podrá hacer uso de su firma digital

d) Custodiar su contraseña o PIN de acceso de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado.

e) En caso de que la clave privada quede comprometida en su seguridad, el suscriptor debe notificarlo de inmediato al Administrador del Certificado Digital de la DRELM; para que proceda a la cancelación del certificado digital.

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

6.2.6 El suscriptor debe elaborar el documento y convertirlo a formato PDF para firmarlo digitalmente. En caso no se haya efectuado la firma digital, podrá modificar el documento las veces que sea necesario para su posterior firma.

6.2.7 Para firmar digitalmente un documento electrónico, se deberá seleccionar y cargar el documento electrónico a firmar mediante el Software de Firma.

En caso se requiere firmar documentos de forma masiva se deberá realizar la firma en bloque.

6.3 Del Procedimiento De Suspensión De La Solicitud De Los Certificados Digitales

6.3.1 Cuando por error de la Oficina solicitante y/o del Administrador del Certificado Digital se han consignado información inexacta en la solicitud.

6.3.2 El Administrador del Certificado Digital deberá remitir mediante oficio al EREP-RENIEC la solicitud de suspensión del proceso de atención de una autorización de certificado digital, indicando el número de solicitud, así como los nombres y apellidos y el DNI del suscriptor.

6.3.3 Para proceder con la suspensión del Certificado se deberá completar el Formato según Anexo N° 2.

6.4 Del Procedimiento De Anulación De Certificados Digitales

6.4.1 Superado el plazo máximo de cinco días hábiles para el envío de su certificado digital en su correo electrónico, el suscriptor deberá verificar la información plasmada en la copia de los formatos remitidos por la EREP-RENIEC que se encuentren correctos, de no ser así solicitará su anulación de su certificado digital. Para ello el suscriptor deberá de completar el Formato según Anexo 2.

6.4.2 El Administrador del Certificado Digital deberá remitir mediante oficio la solicitud de anulación del proceso de atención de un autorización de certificado digital al EREP-RENIEC, indicando el número de solicitud, así como lo nombres y apellidos y el DNI del suscriptor.

6.5 Del Procedimiento De Cancelación De Certificados Digitales

6.5.1 Procede en los siguientes casos:

a) Por deterioro, alteración o cualquier otro hecho que afecte la clave privada o la contraseña de acceso a su clave privada.

b) Por la pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada (computador o token criptográfico)

c) Cada vez que haya desvinculación o rotación de personal el jefe de la Oficina al que se encuentre asignado el personal, remitirá al Administrador del Certificado Digital la relación de personal con su DNI.

d) Cuando el suscriptor del certificado digital solicite mediatamente al Administrador del Certificado Digital la cancelación de su certificado, cuando sospeche el compromiso potencial de su clave privada, debido a la pérdida de su contraseña o sospecha de que un tercero conozca o pueda deducir dicha contraseña.

6.6 La Administración De Los Token Criptográfico

6.6.1 El Administrador del Certificado Digital, asignarán un token a cada una de las Jefaturas de las Oficinas de la DRELM.

6.6.2 En el caso de solicitud de token para otras posiciones que no sean Jefaturas, el responsable de la oficina remitirá al Administrador del Certificado Digital, la relación de servidores

que visarán y/o firmarán los documentos, debiendo llenar el Formato de Requerimiento de Dispositivo Criptográfico – Token, según Anexo N° 3.

6.6.3 La asignación del token la realiza el Administrador del Certificado Digital, se efectúa mediante el formato de Asignación de Dispositivo Criptográfico según Anexo N° 4.

6.6.4 El Administrador de Certificado Digital, instruye a los suscriptores, respecto al almacenamiento del certificado en el token.

6.6.5 En caso de bloqueo de password o PIN del token, el suscriptor está en la obligación de comunicar al Administrador del Certificado Digital, quién verifica si se trata de un bloqueo momentáneo o permanente. Si fuera un bloqueo permanente, el Administrador del Certificado Digital, se comunica con la EREP-RENIEC para la revocación del certificado digital y generación de uno nuevo.

6.6.6 El suscriptor es responsable del token criptográfico asignado. En caso este haya sido perdido, sustraído, deteriorado, averiado o robado, éste deberá ser sustituido con otro token con características iguales o mejores, el cual debe ser aprobado.

6.6.7 En el caso de cese de labores, el suscriptor deberá devolver el Dispositivo Electrónico como parte de la entrega de cargo al Administrador del Certificado Digital.

7. ORIENTACIONES COMPLEMENTARIAS

7.1 Los documentos electrónicos firmados digitalmente se almacenan en el repositorio de datos de la DRELM, destinado además para el procesamiento, clasificación y consulta, con las medidas de seguridad correspondientes, garantizando el principio de equivalencia funcional y la integridad de su contenido.

7.2 Para realizar la consulta de verificación de autenticidad de un documento con firma digital se deberá acceder al siguiente link http://drelm-consulta.signfast.pe/

7.3 La clave privada es almacenada de manera segura en un dispositivo criptográfico que cumpla con el Estándar FIPS 140-2 sección 4.7.2 o Common Criteria EAL4+, y está en posesión del suscriptor del certificado digital (tarjeta inteligente, token o disco duro de la computadora).

8. RESPONSABILIDADES

8.1. Del Administrador del Certificado Digital

a) Entregar información veraz durante la solicitud de emisión de certificados y demás procesos: suspensión, anulación, cancelación ante

RENIEC.

b) Cumplir permanentemente las condiciones establecidas por la Entidad de Certificación para la utilización del Certificado.

c) Solicitar la generación, renovación, actualización o cancelación de los certificados digitales ante la EREP-RENIEC.

d) El Administrador del Certificado Digital solicita a la EREP-RENIEC la emisión y cancelación de los certificados digitales del/ la suscriptor/a, asumiendo las obligaciones del Titular, estipuladas en el artículo 15 del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado con Decreto Supremo N° 052- 2008-PCM.

8.2. Del Equipo de Tecnología de la Información

a) Brindar capacitación y asistencia técnica en el uso del dispositivo de almacenamiento de certificado digital o token.

b) En caso de ser necesario, el Equipo de Tecnología deberá atender las incidencias técnicas de los suscriptores con respecto a la instalación de los certificados digitales y uso de las firmas digitales.

c) Incorporar las medidas técnicas orientadas a mantener la integridad del documento electrónico con firma digital y que la información que contenga sea accesible para su posterior consulta.

8.3 Del Suscriptor

a) Todo/ a suscriptor/a que tiene asignado un token u otro dispositivo de almacenamiento de certificado digital es responsable de cambiar el PIN para su uso. Puede realizar los cambios de PIN que considere convenientes a través de la opción de gestión de dispositivo, pudiendo solicitar el apoyo del Equipo de TI, siendo responsable de mantener la confidencialidad de la misma.

b) Emplear adecuadamente su certificado digital, conforme a la normativa vigente.

c) Dejar de utilizar la clave privada, transcurrido el plazo de vigencia del certificado digital.

d) Notificará a la EREP- RENIEC, a través del Administrador de los Certificados Digitales sin retrasos las inexactitudes o cambios en el contenido del certificado digital.

e) Proteger el acceso al repositorio del certificado digital (computador, tarjeta inteligente, token criptográfico).

9. ANEXOS

Anexo N°1 – Solicitud de Firma Digital
Anexo N° 2 – Anulación, suspensión y/o Cancelación de Certificado Digital
Anexo N° 3 – Requerimiento de Token
Anexo N° 4 – Asignación de Token

ANEXO N° 1

SOLICITUD DE FIRMA DIGITAL

PERÚ Ministerio de Educación — Dirección Regional de Educación de Lima Metropolitana		**USO DE LA FIRMA DIGITAL**
Nombres:	Apellidos:	N° DNI/CE:
Cargo:	Oficina - Unidad/Equipo:	Correo Institucional:
Observaciones:		

Firma

Jefe de Oficina

N° de DNI:

ANEXO N° 2

ANULACION, SUSPENSION Y/O CANCELACIÓN DE CERTIFICADO DIGITAL

PERÚ Ministerio de Educación / Dirección Regional de Educación de Lima Metropolitana	ANULACIÓN, SUSPENSIÓN O CANCELACIÓN DEL CERTIFICADO DIGITAL	Lugar:
		Fecha:

APELLIDOS	NOMBRES	N° DE DNI/CE	OFICINA - UNIDAD/EQUIPO	CARGO	CORREO INSTITUCIONAL	ANEXO DE OFICINA	CELULAR

Firma

Jefe de Oficina

N° de DNI:

ANEXO N° 3

REQUERIMIENTO DE TOKEN

PERÚ Ministerio de Educación — Dirección Regional de Educación de Lima Metropolitana	REQUERIMIENTO DE TOKEN

N° DNI / CE	APELLIDOS	NOMBRES	OFICINA	UNIDAD / EQUIPO	CARGO	CORREO INSTITUCIONAL	ANEXO DE OFICINA	CELULAR

(*) Consigne DNI o Carné de Extranjería

Firma

Jefe de Oficina

N° de DNI:

ANEXO N° 4

ASIGNACIÓN DE TOKEN

PERÚ Ministerio de Educación — Dirección Regional de Educación de Lima Metropolitana	**ASIGNACIÓN DE TOKEN**

SUSCRIPTOR/A		
Nombres y Apellidos:		
Cargo:		
Oficina:		
Unidad / Equipo:		
DNI/CE:	Correo Inst.:	*@drelm.gob.pe*
Celular:	Anexo:	

DISPOSITIVO DE ALMACENAMIENTO DE CERTIFICADO DIGITAL		
Marca	Modelo	N° de Serie

La Victoria, ____ de _____ del 20__

_____	_____
Entrega	Recibí Conforme
Administrador de Certificado Digital	Suscriptor