



UNIDAD DE GESTIÓN EDUCATIVA LOCAL N° 02
Rímac – Independencia - San Martín de Porres – Los Olivos

RESOLUCIÓN DIRECTORAL U.G.E.L.02 N° 06487

San Martín de Porres, 29 SET. 2020

Visto, el oficio N° 143-2020-MINEDU/VMGI/DRELM-UGEL.02-APP, con expediente N° MPT2020-INT-0047736, y demás documentos en nueve (09) folios útiles;

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 191° del Reglamento de Organización y Funciones (ROF) del Ministerio de Educación, aprobado por Decreto Supremo N° 001-2015-MINEDU, establece que las UGEL de Lima Metropolitana constituyen instancias de gestión educativa descentralizadas de la Dirección Regional de Educación de Lima Metropolitana – DRELM;

Que, mediante Resolución Ministerial N° 215-2015-MINEDU, se aprobó el Manual de Operaciones de la DRELM, documento de gestión de carácter técnico y normativo, que establece en su artículo 33° que las UGEL de Lima Metropolitana son responsables de ejecutar las acciones e implementar las acciones para garantizar la adecuada prestación del servicio educativo, en el ámbito de su jurisdicción; cuenta con autonomía administrativa, económica y presupuestal, conforme a la normativa aplicable, estableciendo además su estructura orgánica y sus funciones;

Que, la Ley N° 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 N° 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 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;

Que, el Decreto Legislativo N° 1497, establece medidas para promover y facilitar condiciones regulatorias que contribuyan a reducir el impacto en la economía peruana por la emergencia sanitaria producida por el COVID-19, en cuya Octava Disposición Complementaria Final otorga un plazo hasta el 31 de diciembre de 2020 para que las entidades del Poder Ejecutivo dispongan la conversión de los procedimientos administrativos a iniciativa de parte y servicios prestados en exclusividad que se encuentren aprobados a la entrada en vigencia del mencionado decreto legislativo, a fin de que puedan ser atendidos por canales no presenciales, con excepción de aquellos que demanden la realización de diligencias en las que se requiera de manera obligatoria la concurrencia del administrado;

Que, mediante Oficio N° 143-2020-MINEDU/VMGI/DRELM-UGEL.02 - APP, el Área de Planificación y Presupuesto ha propuesto un proyecto de "Orientaciones para el Uso de la Firma y Certificados Digitales en la Unidad de Gestión Educativa Local N° 02";

Estando a lo opinado por el Área de Planificación y Presupuesto, con el visto bueno del Área de Asesoría Jurídica y de conformidad con las Leyes N° 28044, 29944, los Decretos Supremos N°s. 011-2012-ED, 004-2013-ED, R.M. N° 220-2019-MINEDU, R.V.M. N° 307-2019-MINEDU, R.V.M. N° 142-2020, R.M. 037-2020-MINEDU y en uso de las facultades conferidas por la Resolución Directoral Regional N° 5244-2016-DRELM;

SE RESUELVE:

Artículo 1.- APROBAR las Orientaciones N° 001-2020-MINEDU/VMGI/DRELM-UGEL.02 denominada "Orientaciones para el uso de la Firma y Certificados Digitales en la Unidad de Gestión Educativa Local N° 02", documento que forma parte integrante de la presente Resolución, en ocho (08) folios.

Artículo 2.- ENCARGAR al Área de Planificación y Presupuesto de la UGEL 02, la supervisión del estricto cumplimiento de las Orientaciones aprobadas en el artículo 1 de la presente Resolución y al Equipo de Tecnologías de la Información – ETI, brindar el soporte necesario a las demás Áreas de la UGEL 02, para la óptima implementación y utilización de la misma.

ARTÍCULO 3.- DISPONER la publicación de la presente Resolución en la página web de la Unidad de Gestión Educativa Local N° 02 para su difusión correspondiente.

Regístrese y Comuníquese;



Lic. DORIS MARTHA MELGAREJO HERRERA
Directora de la Unidad de Gestión Educativa Local N° 02 - Rímac



ORIENTACIONES N.º 001-2020-MINEDU/VMGI/DRELM-UGEL.02**“ORIENTACIONES PARA EL USO DE LA FIRMA Y CERTIFICADOS DIGITALES EN LA UNIDAD DE GESTIÓN EDUCATIVA LOCAL N.º 02”****1. FINALIDAD**

Implementar el uso de la firma digital en los documentos que emite la Unidad de Gestión Educativa Local N.º 02, con el propósito de contribuir al Proyecto Cero Papel que forma parte de la política y aporte al gobierno electrónico.

2. OBJETIVO

Establecer las disposiciones y orientaciones que regulen el uso de certificados digitales, medios criptográficos y la firma digital, por los funcionarios y servidores públicos de la UGEL 02.

3. ALCANCES

Las orientaciones del presente documento son de cumplimiento obligatorio para los funcionarios y servidores públicos de la UGEL 02 que cuentan con certificado digital, y que en el ejercicio de sus funciones deban firmar digitalmente documentos electrónicos en el marco de los procesos que ejecutan en las unidades orgánicas a las que pertenecen.

4. BASE LEGAL

- Ley N.º 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley N.º 27269, Ley de Firmas y Certificados Digitales y sus Modificatorias.
- Decreto Legislativo N.º 1497, que establece medidas para promover y facilitar condiciones regulatorias que contribuyan a reducir el impacto en la economía peruana por la emergencia sanitaria producida por el COVID-19.
- Decreto Supremo N.º 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N.º 27444 – Ley del Procedimiento Administrativo General.
- Decreto Supremo N.º 001-2015-MINEDU, que aprueba el Reglamento de Organización y Funciones del Ministerio de Educación.
- Decreto Supremo N.º 081-2013-PCM, que aprueba la Política de Gobierno Electrónico 2013-2017.
- Decreto Supremo N.º 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.
- Decreto Supremo N.º 105-2012-PCM, que establece disposiciones para facilitar la puesta en marcha de la firma digital y modifica el Decreto Supremo N.º 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales.
- Decreto Supremo N.º 052-2008-PCM, que aprueba el Reglamento de la Ley N.º 27269, Ley de Firmas y Certificados Digitales
- Resolución Ministerial N.º 215-2015-MINEDU, Manual de Operaciones de la Dirección Regional de Educación de Lima Metropolitana.



5. ACRÓNIMOS

ECERNEP	Entidad de Certificación Nacional para el Estado Peruano, que se encarga de emitir los certificados raíz para las Entidades de Certificación para el Estado Peruano.
ECEP	Entidad de Certificación para el Estado Peruano. Cumple con las funciones y obligaciones de una Entidad de Certificación según lo indicado en el Reglamento de firmas y certificados digitales.
EREP	Entidad de Registro o verificación para el Estado Peruano. 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.
IOFE	Infraestructura Oficial de Firma Electrónica
PIER	Plataforma Integrada de la Entidad de Registro. Es el aplicativo WEB del RENIEC para uso de los representantes de la entidad para las solicitudes y cancelaciones de certificados digitales.
ReFirma	Aplicativo de RENIEC para uso de los suscriptores para firmar digitalmente los documentos electrónicos.
RENIEC	Registro Nacional de Identificación y Estado Civil
DNI-e	Documento Nacional de Identidad electrónico.

6. DEFINICIONES

- 6.1 Autenticación:** Proceso técnico que permite determinar la identidad de una persona que firma digitalmente un documento electrónico.
- 6.2 Certificado Digital:** Es un documento electrónico emitido por una entidad autorizada que vincula el par de claves (pública y privada), con el suscriptor de la firma digital.
- 6.3 Clave personal de acceso (PIN):** Secuencia de caracteres numéricos o alfa numéricos, que permiten el acceso a las claves privadas asociadas a los certificados digitales.
- 6.4 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 y es mantenida en reserva por el titular de la firma digital.
- 6.5 Clave pública:** En un sistema de criptografía asimétrica, es aquella usada por el destinatario de un mensaje de datos, para verificar la firma digital puesta en dicho mensaje y que puede ser conocida por cualquier persona.
- 6.6 Criptografía:** Técnica para cifrar (ocultar) los datos de tal manera que un mensaje u documento electrónico solo pueda ser entendido por las personas autorizadas.
- 6.7 Criptografía asimétrica:** Tipo de criptografía que utiliza dos claves, para cifrar y descifrar la información, una privada (que no es conocida) y otra pública (conocida por todos).
- 6.8 DNI electrónico (DNI-e):** Es el documento nacional de identidad que posee un dispositivo electrónico que permite acreditar, de manera presencial y no presencial, la identidad de su titular y lo puede usar para la firma digital en documentos electrónicos.



- 6.9 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.
- 6.10 Entidad de Registro o Verificación (EREP):** Es la persona jurídica, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de certificado digital, la aceptación y autorización de las solicitudes de emisión y cancelación de certificados digitales. De acuerdo al Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales aprobado con Decreto Supremo N° 052-2008-PCM, el RENIEC es la única entidad de certificación, verificación y registro en nuestro país.
- 6.11 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.
- 6.12 Firma Digital:** Es un tipo de firma electrónica que, utilizando técnicas de criptografía, permite la identificación del suscriptor y ha sido creada por medios que éste mantiene bajo su control, de manera que está vinculada únicamente al suscriptor 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, y cumple con el principio de equivalencia funcional.
- 6.13 Firma electrónica:** Conjunto de caracteres o símbolos que acompaña un documento electrónico y cumple con una o más funciones de la firma manuscrita.
- 6.14 Identidad digital:** Es el reconocimiento de la identidad de una persona en un medio digital (como por ejemplo en Internet), a través de mecanismos tecnológicos seguros y confiables, sin la necesidad de que la persona se encuentre presente físicamente.
- 6.15 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 la integridad de los documentos electrónicos y la identidad de su autor, lo que es regulado conforme a Ley.
- 6.16 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. Técnicamente la integridad es preservada mediante una infraestructura de clave pública PKI (*Public Key Infrastructure*).
- 6.17 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.
- 6.18 Representante del Titular:** Persona natural que cuenta con facultades para representar a la persona jurídica en los trámites de solicitudes de certificado digital ante la EREP (RENIEC).



6.19 Suscriptor: Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula un certificado digital, de manera exclusiva, para el uso de la firma digital en documentos electrónicos.

6.20 Token: Es un dispositivo de almacenamiento criptográfico que tiene una apariencia similar a un USB, en el que se puede almacenar las claves pública y privada del certificado digital asignado a la persona titular del mismo, y que le permite firmar digitalmente.

7. ORIENTACIONES GENERALES

7.1 Solicitudes de las áreas u oficinas

Para la utilización de la firma digital, los jefes de área de la UGEL 02 canalizarán sus solicitudes de Certificado Digital al Jefe del Área de Planificación y Presupuesto, quien actúa por delegación del Titular como representante legal de la entidad, debiendo adjuntarse a la solicitud la documentación de sustento que este le indique, por cada uno de los aspirantes a suscriptor.

7.2 Registro de solicitudes

El Jefe del Área de Planificación y Presupuesto, en su calidad de representante delegado por el Titular de la UGEL 02 para que actúe como representante ante la Entidad de Registro: RENIEC, revisa la información presentada por las áreas u oficinas de la UGEL 02, y de estar completa procede a registrar las solicitudes de aspirantes a suscriptor en la Plataforma Integrada de la Entidad de Registro (PIER).

7.3 Descarga del Certificado Digital

Una vez que el RENIEC comunique al correo de cada trabajador propuesto por las áreas, la aprobación de su solicitud de certificado digital, este es responsable de descargar el certificado digital dentro del plazo establecido por RENIEC. El Coordinador del Equipo de Tecnologías de la Información brindará el soporte necesario a los trabajadores de la UGEL 02, a quienes el RENIEC les haya comunicado la aprobación de sus solicitudes de certificado digital, a fin de que puedan descargar el mismo, sea en una PC, Laptop o en un Token, según corresponda.

7.4 Validez 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 firma digital se basa en la propiedad sobre un mensaje o documento cifrado, utilizando la clave privada de un suscriptor de certificado digital y ésta sólo puede ser descifrada 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.

7.5 Del Uso de la Firma digital

Los documentos que emita la entidad, como oficios, memorandos, informes u otros, serán suscritos preferentemente con firma digital, en tanto esta se implementa de manera progresiva en la UGEL 02, con excepción de aquellos que por su propia naturaleza o porque así lo requiere alguna norma, o cuando exista algún impedimento técnico; puede utilizarse excepcionalmente la firma manuscrita.



8. ORIENTACIONES ESPECÍFICAS

8.1 Solicitud del Certificado Digital

8.1.1 El trámite de certificado digital se inicia con la manifestación de necesidad del Área de firmar digitalmente los documentos, mediante solicitud que es presentada al Área de Planificación y Presupuesto, en la que se detalla la lista de nombres y apellidos completos, número de DNI, cargo, correo electrónico institucional y teléfono de contacto. En caso de contar el personal propuesto con un Token, deberá precisar en la solicitud si desea que su certificado pueda ser descargado en este tipo de dispositivo criptográfico.

8.1.2 Una vez emitido el certificado digital a favor de la UGEL 02 y descargado el Certificado Digital por el representante de la entidad, se inicia el trámite para la emisión y gestión de certificados digitales para los suscriptores. Para dicho efecto, el representante de la entidad debe:

- Registrar los datos de los suscriptores a través de su cuenta de usuario, en la Plataforma Integrada de la Entidad de Registro (PIER) de la RENIEC.
- Generar el reporte "Lista de Aspirantes a Suscriptor". Este documento se firma en forma digital y se envía mediante la plataforma PIER.
- En caso el trabajador reciba mediante correo de RENIEC que se ha incluido información incorrecta o inexacta en su documentación de sustento o en su Declaración Jurada, deberá canalizar por medio de la Jefatura del Área, una nueva documentación de sustento.
- De ser aprobado por RENIEC el suscriptor recibirá una clave y la ruta para descargar el Certificado Digital emitido por la EREP: RENIEC 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, las instrucciones y plazos establecidos por la EREP: RENIEC.
- Una vez recibido el correo electrónico de la RENIEC, el suscriptor podrá solicitar al Equipo de Tecnologías de la Información - ETI, el soporte para 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 de uso privado, la cual servirá, para que pueda firmar a partir de ese momento los documentos electrónicos.

En caso que el Jefe del Área lo considere conveniente, determinará y comunicará quién o quienes podrán solicitar la instalación del certificado digital mediante un Token u otro dispositivo de almacenamiento del certificado digital.



8.2 Del Uso del Certificado Digital para la Firma Digital de los Suscriptores

8.2.1 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 (Laptop, PC o Token) y el software de firma digital (ReFirma).

- 8.2.2 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. Cada trabajador es responsable de su clave privada, al generar la firma digital en los documentos electrónicos que le corresponden.
- 8.2.3 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, por lo que debe ser conocida únicamente por el suscriptor, y evitar su pérdida, revelación, modificación o uso no autorizado.
 - c) En caso de extravío o pérdida del Token criptográfico, deberá ser puesto en conocimiento de su jefe inmediato, siendo el suscriptor el responsable de la reposición del Token o de cualquier otro dispositivo criptográfico asignado.
 - d) En caso de que la clave privada quede comprometida en su seguridad, el suscriptor por intermedio de su Jefe de Área, debe notificarlo de inmediato al Área de Planificación y Presupuesto, para que proceda a la cancelación del certificado digital.
- 8.2.4 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.
- 8.2.5 Para firmar digitalmente un documento electrónico, se deberá seleccionar y cargar el documento electrónico a firmar mediante el software ReFirma, proporcionado por el EREP: RENIEC.
- 8.2.6 En caso se requiera firmar documentos de forma masiva se deberá realizar la firma en lote, mediante la opción correspondiente del software ReFirma, para lo cual se deberá indicar en el mencionado aplicativo los parámetros de firma digital en lote.

8.3 Del Procedimiento De Cancelación De Certificados Digitales

La cancelación de un Certificado Digital procede en los siguientes casos:

- 8.3.1 Por deterioro, alteración o cualquier otro hecho que afecte la clave privada o la contraseña de acceso a su clave privada.
- 8.3.2 Por la pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada (computador, laptop o token criptográfico).
- 8.3.3 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.
- 8.3.4 Cuando el suscriptor del certificado digital, a través de su Jefe de Área, solicite al Área de Planificación y Presupuesto la cancelación de su certificado, por existir el riesgo potencial de su clave privada, debido a la pérdida de su contraseña o sospecha de que un tercero conozca o pueda deducir dicha contraseña.



9. ORIENTACIONES COMPLEMENTARIAS

- 9.1 Los documentos electrónicos firmados digitalmente se almacenan en el repositorio de datos de la UGEL 02, destinado además para el procesamiento, clasificación y consulta, con las medidas de seguridad correspondientes, que garanticen la integridad de su contenido.
- 9.2 En el caso de firmar como visto en el documento electrónico, esta firma deberá colocarse preferentemente al lado izquierdo del documento a visar, o en su defecto en una de las esquinas del mismo.
- 9.3 La UGEL 02 a través del Equipo de Tecnologías de la Información - ETI, implementará un enlace en la página Web institucional, que permita al público realizar la consulta de verificación de la autenticidad de los documentos con firma digital que se emitan.
- 9.4 Para todo lo no previsto en las presentes orientaciones, se aplicarán las normas legales vigentes que regulan el uso de la firma digital, prevaleciendo estas últimas en caso de discrepancia o conflicto con la primera.

10. RESPONSABILIDADES

10.1 Del Representante Legal de la Entidad

- a) Cumplir permanentemente las condiciones establecidas por la Entidad de Certificación para la utilización del Certificado Digital de Persona Jurídica emitido a favor de la UGEL 02.
- b) Registrar la información de las solicitudes de emisión de certificados digitales y demás procesos: suspensión, anulación, cancelación ante RENIEC.
- c) Solicitar la generación, renovación, actualización o cancelación de los certificados digitales ante la EREP: RENIEC.
- d) El representante legal de la entidad solicita a la EREP: RENIEC la emisión y cancelación de los certificados digitales de los suscriptores, 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.

10.2 Del Equipo de Tecnologías de la Información

- a) Brindar capacitación y asistencia técnica en el uso del dispositivo de almacenamiento de certificado digital o Token, en caso el usuario cuente con este dispositivo.
- b) En caso de ser necesario, el Equipo de TI atenderá las incidencias técnicas de los suscriptores con respecto a la instalación de los certificados digitales y uso del aplicativo de firma digital (ReFirma).
- c) Implementar 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.



10.3 Del Suscriptor

- a) El suscriptor es responsable de emplear adecuadamente su certificado y su firma digital, conforme a la normativa vigente sobre Firmas y Certificados Digitales, así como a los fines y objetivos de la UGEL 02.
- b) Es responsabilidad del suscriptor la firma de cualquier documento electrónico usando su contraseña o clave privada, por lo que deberá mantenerla en reserva y evitar su uso indebido por terceras personas. Siéndole aplicable el principio de No Repudio, y teniendo validez el documento firmado para todos los efectos legales.
- c) El suscriptor dejará de utilizar la clave privada de firma digital, una vez transcurrido el plazo de vigencia del certificado digital.
- d) Todo suscriptor 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.
- e) Todo suscriptor debe proteger el acceso al repositorio del certificado digital (computador, tarjeta inteligente, token criptográfico); de cualquier persona no autorizada.

