senace	SERVICIO NACIONAL DE CERTIFICACIÓN AMBIENTAL PARA LAS INVERSIONES SOSTENIBLES	Código: DIR-OTI-01/01	
		Fecha de aprobación:	07/07/2016

DIRECTIVA
USO DE LA FIRMA DIGITAL EN EL SENACE

ROL	NOMBRE	CARGO	FECHA	FIRMA
Elaborado por:	Roodwin Eduardo Bahamonde Melendrez	Especialista en Soporte Técnico I	02/06/2016	
	Zico Alexis Yacila Espinoza	Especialista en Desarrollo de Sistemas II	02/06/2016	
Revisado por:	Roberto Puyó Valladares	Jefe de la Oficina de Tecnologías de la Información	02/06/2016	
	María Eulalia Olcese Herrera	Jefa de la Oficina de Planeamiento y Presupuesto	03/06/2016	
	Aldo Renato Ramírez Palet	Jefe de la Oficina de Asesoría Jurídica	22/06/2016	
Aprobado por:	Alfredo Xavier Neyra Gavilano	Secretario General	07/07/2016	

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - SENACE
V°B°
R. BAHAMONDE M.
Especialista de Soporte Técnico I

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - SENACE
V°B°
Z. YACILA E.
Especialista de Desarrollo de Sistemas II

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - SENACE
V°B°
R. PUYÓ V.
JEFE

OFICINA DE PLANEAMIENTO Y PRESUPUESTO - SENACE
María Eulalia Olcese Herrera
JEFA

OFICINA DE ASESORÍA JURÍDICA - SENACE
V°B°
ALDO RENATO RAMIREZ PALET
JEFE

SECRETARÍA GENERAL
Alfredo Xavier Neyra Gavilano
SENACE

1. OBJETIVO

Establecer las normas y procedimientos que regulen el uso de certificados digitales, tokens y la firma digital en el Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles- Senace, con la finalidad de impulsar el proceso de modernización de la gestión pública en la entidad.

2. ALCANCE

Las disposiciones de la presente Directiva son de obligatorio cumplimiento de los órganos y unidades orgánicas del Senace, en cuyos procesos se haya establecido el uso obligatorio de la firma digital, certificados digitales y tokens.

3. BASE NORMATIVA

3.1 Constitución Política del Perú.
3.2 Ley N° 25323, Ley del Sistema Nacional de Archivos.
3.3 Ley N° 27269, Ley de Firmas y Certificados Digitales.
3.4 Ley N° 27444, Ley del Procedimiento Administrativo General.
3.5 Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
3.6 Ley N° 29733, Ley de Protección de Datos Personales.
3.7 Ley N° 29968, Ley de Creación del Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles - Senace.
3.8 Decreto Supremo N° 002-98-ITINCI, que aprueba requisitos y procedimiento para otorgamiento de Certificado de Idoneidad Técnica para la confección de Microformas.
3.9 Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de la Ley N° 27269 de Firmas y Certificados Digitales, y modificatoria/s.
3.10 Decreto Supremo N° 009-2009-MINAM, que aprueba Medidas de Ecoeficiencia para el Sector Público.
3.11 Decreto Supremo N° 105-2012-PCM, establecen disposiciones para facilitar la puesta en marcha de la firma digital y modifican el Decreto Supremo N° 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales.
3.12 Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.
3.13 Decreto Supremo N° 081-2013-PCM, que aprueba la Política Nacional de Gobierno Electrónico 2013-2017.
3.14 Decreto Supremo N° 026-2016-PCM, que aprueba 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 Resolución Ministerial N° 179-2004-PCM, que aprueba uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2004 Tecnología de la Información. Procesos del Ciclo de Vida del Software, 1ª Edición, en entidades del Sistema Nacional de Informática".
3.16 Resolución Ministerial N° 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 Jefatural N° 368-2002-INEI, aprueba la Directiva, Normas Técnicas para el Almacenamiento y Respaldo de la Información procesada por las entidades de la Administración Pública.

4. RESPONSABILIDAD

Los órganos y unidades orgánicas del Senace son responsables de velar por el cumplimiento de las disposiciones para el uso de la firma digital en documentos electrónicos de la entidad.

La Oficina de Tecnologías de la Información es responsable de brindar la asistencia técnica en el uso de los tokens y asegurar la integridad del documento electrónico con firma digital almacenado en el Sistema de Gestión Documental del Senace.

5. DEFINICIONES

5.1 Administrador/a del Certificado Digital
Servidor/a designado/a por la Secretaría General, con el objeto de gestionar ante la EREP-RENIEC, los certificados digitales para los/las suscriptores/as de la entidad.

5.2 Autenticación
Proceso que permite determinar la identidad de la persona que firma digitalmente, en función del documento electrónico firmado por éste y al cual se le vincula, asegurando que frente a un trámite realizado vía electrónica, ambas partes tengan certeza que la persona que emite el documento electrónico es la persona quien dice ser.

5.3 Autoridad Administrativa Competente
Es el organismo público responsable de acreditar a 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.

5.4 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.

5.5 Contraseña
Código secreto que se introduce en un equipo de cómputo para poder accionar un mecanismo o para acceder a ciertas funciones informáticas.

5.6 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, vídeo, la telemática en general y demás objetos que recojan, contengan o representen algún

hecho, o una actividad humana o su resultado, de acuerdo al artículo 234 del Código Procesal Civil.

5.7 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.

5.8 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. Para el Estado Peruano es el Registro Nacional de Identificación y Estado Civil- RENIEC.

5.9 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 de un certificado digital, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales. De acuerdo al Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales aprobado con Decreto Supremo N° 052-2008-PCM, el RENIEC es la única entidad de certificación, verificación y registro en nuestro país.

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

5.11 Expediente Electrónico
Conjunto de documentos digitalizados y generados electrónicamente respecto de un trámite iniciado en la entidad.

5.12 FIPS 140-2
Es un estándar de seguridad de ordenadores para la acreditación de módulos criptográficos, cuyas siglas responden al acrónimo de Federal Information Processing Standard (estándares federales de procesamiento de la información) publicación 140-2.

5.13 Firma Digital
Es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, mediante la cual se vincula una clave privada y una clave pública para identificar a la persona natural o jurídica que hace uso de la misma.

5.14 Firma Electrónica
Es cualquier sonido, símbolo o proceso electrónico que permite al receptor de un documento electrónico identificar formalmente a su autor. También es conocida como firma electrónica básica.

5.15 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: 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, 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.

5.16 Medios electrónicos
Son sistemas de información que hacen uso de tecnología, a través de los cuales se puede generar, procesar, transmitir y archivar documentos electrónicos.

5.17 PDF/A
Es un formato de archivo para el guardado a largo plazo de documentos electrónicos. Está basado en la versión de Referencia 1.4 de PDF de Adobe Systems Inc. (implementada en Adobe Acrobat 5 y versiones posteriores) y está definido por la ISO 19005-1:2005.

5.18 PIN: (Personal Identification Number)
Es un número de identificación personal utilizado como contraseña para acceder de manera segura a ciertos sistemas informáticos.

5.19 PKI (Public Key Infraestructure)
Sistema criptográfico asimétrico en el que se basan los certificados digitales.

5.20 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.

5.21 Sello de Tiempo (Time Stamping)
Es el valor de fecha y hora de firma digital de un documento, regulado de acuerdo al estándar RFC 3161 y las normas vigentes sobre firmas y certificados digitales.

5.22 Servicio de tercero neutral en intermediación electrónica
Es un servicio que proporciona el sello de tiempo externo tomado de una fuente confiable.

5.23 Suscriptor/a
Es el/la servidor/a autorizado/a para firmar digitalmente.

5.24 Titular
Persona natural o jurídica a quien se le atribuye de manera exclusiva un Certificado Digital. Para efectos de la presente Directiva, el Titular del Certificado Digital es el Senace.

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

5.26 Usuario
Es la persona natural u organización que utiliza un sistema en operación para llevar a cabo una función específica.

6. ABREVIATURAS

OTI	:	Oficina de Tecnologías de la Información.
Senace	:	Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles.
EREP-RENIEC	:	Entidad de Registro o Verificación para el Estado Peruano.

7. DISPOSICIONES GENERALES

7.1 El uso efectivo de la firma digital en documentos electrónicos de la entidad se implementa de manera progresiva, siendo necesario que los órganos y las unidades orgánicas del Senace identifiquen los procesos y actividad(es)/tarea(s) que generen documentos en los cuales resulte inexcusable y oportuna el uso de la firma digital, en concordancia con los lineamientos de simplificación administrativa que propone el Estado Peruano.

7.2 Los órganos que identifiquen determinados documentos que requieran el uso de la firma digital deben comunicar a la Secretaría General sobre los mismos mediante el formato: Uso de la Firma Digital en el Senace (DIR-OTI-01/01-A).

7.3 La Secretaría General tiene a su cargo:

a) Aprobar la lista priorizada de los documentos que deben disponer de la firma digital, en coordinación con la OTI.
b) Designar al/a la Administrador/a del Certificado Digital.
c) Aprobar la relación de suscriptores/as que contarán con certificados digitales y tokens.

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

7.5 Los documentos electrónicos firmados digitalmente se almacenan en el repositorio de datos del Senace, 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.

7.6 Los sistemas de información del Senace se diseñan para que de manera progresiva se implante la firma digital en los procesos idóneos para su aplicación.

7.7 El proceso de autenticación en los sistemas de información a los que los administrados tienen acceso (colocando su usuario y contraseña), tienden de

manera gradual a utilizar el DNI Electrónico o Certificado Digital, proporcionando mayor seguridad en el uso del sistema.

8. DISPOSICIONES ESPECÍFICAS

8.1 Firma Digital

8.1.1 Para que un/a suscriptor/a pueda aplicar la firma digital en los documentos electrónicos, es necesario contar con un certificado digital, un software firmador y un dispositivo de almacenamiento de certificado digital (que puede ser el token o la Pc).

8.1.2 Las consideraciones a tener en cuenta para firmar digitalmente un documento electrónico son las siguientes:

a) El/La suscriptor/a con su certificado digital emitido (el procedimiento para la emisión de un certificado digital se describe en el numeral 8.6-Para la emisión del Certificado Digital de la presente Directiva) debe tener disponible, en una carpeta dentro del computador o en cualquier unidad de almacenamiento, el documento electrónico que va a firmar (este documento debe estar en formato PDF).
b) El/La suscriptor/a debe utilizar el token asignado conforme a lo establecido en el numeral 8.5.2 de la presente Directiva, en el que se encuentra el certificado digital y además el software firmador.
c) El/La suscriptor/a debe usar el software firmador, luego debe seleccionar el documento electrónico a firmar. Una vez cargado el documento, el/la suscriptor/a debe colocar su clave PIN, y con esta acción, se firma digitalmente el documento.

8.2 Respecto a las obligaciones

8.2.1 Del/la Administrador/a del Certificado Digital:

a) Entregar información veraz durante la solicitud de emisión de certificados y demás procesos de certificación (cancelación, suspensión, re-emisión y modificación).
b) Actualizar, de ser necesario, la información remitida tanto a la Entidad de Certificación como a la Entidad de Registro o Verificación, asumiendo la responsabilidad por la veracidad y exactitud de ésta.
c) Solicitar la cancelación del certificado digital en caso de que la reserva sobre la clave privada se haya visto comprometida, bajo responsabilidad.
d) Cumplir permanentemente las condiciones establecidas por la Entidad de Certificación para la utilización del certificado.

8.2.2 De la Oficina de Tecnologías de la Información:

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

b) Brindar asistencia técnica a solicitud del/de la suscriptor/a en la atención de incidentes referidos al uso del token u otro dispositivo de almacenamiento de certificado digital.
c) Incorporar las medidas técnicas orientadas a mantener la integridad del documento electrónico con firma digital en el Sistema de Gestión Documental del Senace y que la información que contenga sea accesible para su posterior consulta.

8.2.3 De los/las Suscriptores/as:

a) El/la suscriptor/a que tiene asignado un certificado digital y un token, es el único y directo responsable de todas las acciones que derivan del uso de los mismos.
b) 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 a la OTI, siendo responsable de mantener la confidencialidad de la misma.
c) Efectuar la solicitud de cancelación del certificado digital, en caso de que la reserva sobre la clave privada se haya visto comprometida, dirigida al correo electrónico helpdesk@senace.gob.pe, con el asunto [Certificado Digital] Cancelación de Certificado Digital.
d) Emplear adecuadamente su certificado digital, conforme a la normativa vigente.
e) Ser diligente en la custodia de su clave privada y su contraseña, con el fin de evitar usos no autorizados.
f) Dejar de utilizar la clave privada, transcurrido el plazo de vigencia del certificado digital.
g) Notificar a la EREP-RENIEC, sin retrasos injustificables:
   - La pérdida, robo o extravío del token u otro dispositivo de almacenamiento de certificado digital.
   - El compromiso potencial de su clave privada o de su contraseña.
   - La pérdida de control sobre su clave privada, debido al compromiso de su contraseña (datos de activación) o por cualquier otra causa.
   - Las inexactitudes o cambios en el contenido del certificado digital.

8.3 Presunciones legales de la firma digital

Los/as suscriptores/as deben observar lo siguiente:

8.3.1 Autenticidad

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

8.3.2 Equivalencia funcional

De conformidad con lo establecido en la Ley de Firmas y Certificados Digitales y su Reglamento, los documentos firmados digitalmente pueden ser presentados y admitidos como prueba en toda clase de procesos judiciales y procedimientos administrativos.

8.3.3 Integridad

Se entiende que un documento con firma digital no ha sido alterado con el transcurso del tiempo, una vez que fue firmado digitalmente y transmitido vía web, correo electrónico, o copiado y/o movido a algún medio de almacenamiento masivo.

8.3.4 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 y tokens es aplicado de tal forma que no favorezca, excluya o restrinja alguna tecnología en particular.

8.3.5 No repudio

Una persona no puede desconocer que ha elaborado un documento en el cual se encuentre su firma digital.

8.3.6 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.

8.4 Certificado Digital

8.4.1 La Secretaría General del Senace, designa al/la Administrador/a del Certificado Digital, quien es el/la responsable de solicitar ante EREP-RENIEC los certificados correspondientes para el personal de la entidad.

8.4.2 Los órganos y unidades orgánicas que gestionen sistemas de información donde se incluya la firma digital, son responsables de:
a) Atender las consultas funcionales de los/as suscriptores/as.
b) Administrar los/as suscriptores/as con certificados digitales.
c) Llevar el control de la fecha de emisión y caducidad de los certificados digitales asignados a los/las suscriptores/as.
d) Remitir la lista de renovación de suscriptores/as al/la Administrador/a del Certificado Digital.

8.4.3 La Secretaría General aprueba la relación de suscriptores/as que cuentan con certificados digitales y tokens, quienes son responsables de visar y/o firmar los documentos.

8.4.4 Para la emisión del certificado digital:

a) El/La Administrador/a 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.
Para este fin, el Senace presenta a la EREP-RENIEC, el documento que evidencia la delegación de facultades referida en el párrafo precedente.

b) La instalación del certificado digital se realiza en un token u otro dispositivo de almacenamiento del certificado digital. Los/Las suscriptores/as conocen la contraseña de acceso a dichos dispositivos y son responsables de su resguardo (confidencialidad).

8.5 Tokens

8.5.1 Los/Las responsables de los órganos del Senace, remiten al/la Administrador/a del Certificado Digital, la relación de servidores/as responsables de visar y/o firmar los documentos y que requieran tokens, debiendo llenar el Formato de Requerimiento de Dispositivo Criptográfico – Token (DIR-OTI-01/01-B).

8.5.2 La asignación del token se efectúa mediante el Formato de Asignación de Dispositivo Criptográfico (DIR-OTI-01/01-C) y firma del/la suscriptor/a en señal de conformidad, previa aprobación de la relación de suscriptores/as por parte de la SG.

8.5.3 El/La Administrador/a del Certificado Digital instruye a los/las suscriptores/as, respecto al almacenamiento del certificado en el token.

8.5.4 En caso de bloqueo del password o PIN del token, el/la suscriptor/a está en la obligación de comunicarlo al/la Administrador/a del Certificado Digital, quien verifica si se trata de un bloqueo momentáneo o permanente. Si fuera un bloqueo permanente, el/la Administrador/a del Certificado Digital se comunica con la EREP-RENIEC para la revocación del certificado digital y generación de uno nuevo. En el supuesto que la revocación y generación de un nuevo certificado genere un costo, dicho costo será asumido por el Senace.

8.5.5 El/La suscriptor/a es responsable del token asignado. Ante la pérdida del mismo, se toma en cuenta las disposiciones que establezca la Unidad de Logística, respecto a la reposición.

8.6 Para la emisión del Certificado Digital

Una vez emitido el certificado digital a favor del Senace, éste puede iniciar el trámite para la emisión y/ gestión de certificados digitales para los/as suscriptores/as, a través del/la Administrador/a del Certificado Digital. Para dicho efecto, el/la Administrador/a del Certificado Digital debe:

8.6.1 Registrar los datos de los/las suscriptores/as en el formulario "Autorización de Suscriptores/as" a través de su cuenta de usuario en el portal de la EREP-RENIEC.

8.6.2 Generar el reporte "Listado de autorizaciones generadas". Este documento se firma en forma manuscrita y se envía en físico a la EREP-RENIEC.

8.6.3 Realizar la emisión de los certificados digitales para los/las suscriptores/as, luego de recibidas las autorizaciones de la EREP-RENIEC, bajo las siguientes dos modalidades:

8.6.3.1 No presencial, mediante la verificación con la base de datos.

a) La EREP-RENIEC recibe la autorización y procesa los formatos respectivos que serán remitidos al correo electrónico del/de la suscriptor/a o entregados al/la Administrador/a del Certificado Digital, mediante el envío a su correo electrónico o en USB a la persona que designe.

b) Los formatos son impresos y firmados por cada suscriptor/a y son remitidos físicamente a la EREP- RENIEC.

c) Una vez que se cuente con esta documentación y se realice la verificación, automáticamente el sistema envía de ser procedente, un correo electrónico a la dirección electrónica registrada del/de la suscriptor/a que contiene un enlace web para realizar la descarga de su certificado digital.

d) El/La suscriptor/a comunica a Mesa de Ayuda de la OTI, la recepción del correo para la descarga del certificado digital. El personal de la OTI descarga el certificado digital en el token, solicita que el/la suscriptor/a establezca el PIN o contraseña para la firma de documentos e instruye en el uso del token para firmar documentos.

8.6.3.2 Presencial.

a) El/La suscriptor/a, previa coordinación con el/la Administrador/a del Certificado Digital, se apersona a la EREP-RENIEC portando su documento de identidad vigente.

b) En la EREP-RENIEC se procede a la autenticación y el registro de los formatos para su firma respectiva.

c) Se realiza la entrega del certificado digital, instalándolo en su token.

8.6.4 Solicitar la generación, renovación, actualización, revocación o cancelación de los certificados digitales ante la EREP-RENIEC, para lo cual debe seguir los pasos definidos por el convenio de colaboración interinstitucional de certificación digital, en el marco del Decreto Supremo N° 070-2011-PCM y el Decreto Supremo N° 105-2012-PCM suscrito con el Registro Nacional de Identificación y Estado Civil (RENIEC).

8.6.5 Solicitar ante la EREP-RENIEC, la cancelación o revocatoria del certificado digital cuando el/la suscriptor/a o el/la Administrador/a del Certificado Digital tomen conocimiento de la ocurrencia de:

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 ser servidor/a del Senace.

8.7 Firma de documentos

8.7.1 Documentos generados electrónicamente

8.7.1.1 La firma digital es utilizada en la(s) actividad(es)/tarea(s) de los procesos definidos por los órganos y unidades orgánicas, en concordancia con el Formato Uso de la Firma Digital en el Senace (DIR-OTI-01/01-A), aprobado por la Secretaría General. El personal con la autorización correspondiente puede colocar la firma digital en el documento electrónico.

8.7.1.2 El documento emitido con firma digital tiene la característica de un archivo tipo PDF/A.

8.7.2 Documentos físicos digitalizados

8.7.2.1 La firma digital es utilizada en la(s) actividad(es)/tarea(s) de los procesos definidos por los órganos y unidades orgánicas. El personal con la autorización correspondiente puede colocar la firma digital en el documento electrónico.

8.7.2.2 La firma digital se aplica también a los documentos presentados por los administrados adjuntos a los formularios de registro vía web. El personal con la autorización correspondiente puede colocar la firma digital en el documento electrónico.

8.7.2.3 El documento emitido con firma digital tiene la característica de un archivo tipo PDF/A.

9. CAMBIOS A LA VERSIÓN ANTERIOR

No aplica.

10. FORMATOS

- DIR-OTI-01/01-A: Formato Uso de la Firma Digital en el Senace.
- DIR-OTI-01/01-B: Formato de Requerimiento de Dispositivo de Almacenamiento de Certificado Digital.
- DIR-OTI-01/01-C: Formato de Asignación de Dispositivo de Almacenamiento de Certificado Digital.

DIR-OTI-01/01-A: Formato Uso de la Firma Digital en el Senace

senace	USO DE LA FIRMA DIGITAL EN EL SENACE	DIR-OTI-01/01-A

Nombres:	Apellidos :	Cargo:
Órgano / Unidad Orgánica:	Correo Electrónico:	

Nombre del Proceso:	Actividades o tareas :	Orientación Orientado al Ciudadano ☐ Mejora de la gestión Interna ☐	Posibles documentos firmados digitalmente:

SECRETARIO GENERAL
Alfredo Xavier Neyra Gavilano
SENACE

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
V°B°
Z. YACILA E.
Especialista de Desarrollo de Sistemas II
SENACE

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
V°B°
R. BALMACEDA M.
Especialista de Soporte Técnico I
SENACE

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN SENACE
VB°
R. PUYO V.
JEFE

OFICINA DE PLANEAMIENTO Y PRESUPUESTO
María Eulalia Olcese Herrera
JEFA
SENACE

OFICINA DE ASESORÍA JURÍDICA - SENACE
V°B°
ALDO RENATO RAMIREZ PALET
JEFE

DIR-OTI-01/01-B: Formato de Requerimiento de Dispositivo de Almacenamiento de Certificado Digital

senace	REQUERIMIENTO DE DISPOSITIVO DE ALMACENAMIENTO DE CERTIFICADO DIGITAL	DIR-OTI-01/01-B

ORDEN	DNI/CE(*)	NUM DOCUMENTO	PRIMER APELLIDO	SEGUNDO APELLIDO	APELLIDO DE CASADA	NOMBRES	ÓRGANO	UNIDAD ORGÁNICA	CARGO	CORREO -E	TELÉFONO CONTACTO	CELULAR CONTACTO	ENTREGA(**)

(*) Consigne DNI o Carné de Extranjería.
(**) Consigne Presencial y No Presencial.

SECRETARIO GENERAL
Alfredo Xavier Neyra Gavilano
SENACE

Nota:
La entrega Presencial, consiste en que el/la servidor/a se apersona físicamente al EREP-RENIEC para que se le entregue el certificado digital en el dispositivo de almacenamiento (token).

La entrega No Presencial, consiste en enviar información al EREP-RENIEC, relativa a la autorización que debe tener el/la servidor/a para la habilitación de su correspondiente certificado digital. Luego de la validación por parte del EREP-RENIEC, se recibe un enlace vía web para descargar el certificado digital e instalarlo (que lo hace la OTI) en el token asignado al servidor.

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - SENACE
VºBº
Z. YACILA E.
Especialista de Desarrollo de Sistemas II

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - SENACE
VºBº
R. BARRAMONDE M.
Especialista de Soporte Técnico I

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN SENACE
VºBº
R. PUYÓ V.
JEFE

OFICINA DE PLANEAMIENTO Y PRESUPUESTO
María Eulalia Closs Herrera
JEFA
SENACE

OFICINA DE ASESORÍA JURÍDICA
VºBº
ALDO RENATO RAMÍREZ PALET
JEFE
SENACE

DIR-OTI-01/01-C: Formato de Asignación de Dispositivo de Almacenamiento de Certificado Digital

senace	ASIGNACIÓN DE DISPOSITIVO DE ALMACENAMIENTO DE CERTIFICADO DIGITAL	DIR-OTI-01/01-C

SUSCRIPTOR/A			
Órgano	<Órgano del/la suscriptor/a>		
Unidad orgánica	<Unidad orgánica del/la suscriptor/a>		
Cargo	<Cargo del/la suscriptor/a>		
Suscriptor/a	<Nombre del/la suscriptor/a>		
DNI	<DNI>	Correo electrónico	<correo@senace.gob.pe>
Teléfono Contacto	01-5000710	Celular Contacto	<móvil del/la suscriptor/a>

DISPOSITIVO DE ALMACENAMIENTO DE CERTIFICADO DIGITAL		
Marca	Modelo	N° de serie
Bit4Id	DS2048 (IAM)	<Número de Serie>

San Borja, <> de <> de 201_

SECRETARIO GENERAL – Alfredo Xavier Neyra Gavilano – SENACE

Entrega	Recibí conforme
<Administrador/a del Certificado Digital>	<Suscriptor/a>

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN SENACE – V°B° R. PUYO V. – JEFE

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN – V°B° Z. YACILA E. – Especialista de Desarrollo de Sistemas II – SENACE

OFICINA DE PLANEAMIENTO Y PRESUPUESTO – SENACE – JEFA

OFICINA DE ASESORÍA JURÍDICA – SENACE – V°B° ALDO RENZO – JEFE

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN – V°B° R. BARAMONDE M. – Especialista de Soporte Técnico I – SENACE