CÓDIGO DE VERIFICACIÓN
11768714312535

FIRMADO POR:

OBLITAS MENDEZ DE DIAZ Jessica Violeta (FAU20556097055)

GALLEGOS RONDON Jaime Adhemir (FIR09564692)

MOREAU HEREDIA Ricardo Arturo FAU 20556097055 soft

LEON SORIA Alex Rodolfo FAU 20556097055 hard

QUENALLATA MAMANI Ana Lucia (FIR25707424)

senace	SERVICIO NACIONAL DE CERTIFICACIÓN AMBIENTAL PARA LAS INVERSIONES SOSTENIBLES	Código: **MAN-SPMD-MS-01/01**

MANUAL DE SEGURIDAD DEL SISTEMA DE PRODUCCIÓN DE MICROFORMAS DIGITALES

senace | Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles

*Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: "**https://www.senace.gob.pe/verificacion**" ingresando el código de verificación que aparece en la parte superior izquierda de este documento.*

INDICE

1. INTRODUCCIÓN
2. OBJETIVO GENERAL
3. ÁMBITO DE APLICACIÓN
4. POLÍTICAS DE SEGURIDAD DEL SISTEMA DE PRODUCCIÓN DE MICROFORMAS DIGITALES
5. DISPOSICIONES GENERALES
6. DESARROLLO E IMPLEMENTACIÓN DEL SISTEMA DE PRODUCCIÓN DE MICROFORMAS
7. MANTENIMIENTO Y ACTUALIZACIÓN DEL SISTEMA DE PRODUCCIÓN DE MICROFORMAS
8. SEGURIDAD DE LA GESTIÓN DEL SISTEMA DE PRODUCCIÓN DE MICROFORMAS
9. RECURSOS HUMANOS
10. SEGURIDAD FÍSICA Y EL ENTORNO
11. GESTIÓN DE COMUNICACIONES Y OPERACIONES
12. CONTROL DE ACCESOS
13. UTILIZACIÓN DE CLAVES DE ACCESO
14. DIRECTORIOS COMPARTIDOS
15. SOFTWARE UTILIZADO
16. ACTUALIZACIÓN DE EQUIPOS
17. PLAN DE CONTINGENCIA
18. CONTROL DE CAMBIOS DEL DOCUMENTO

*Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: "**https://www.senace.gob.pe/verificacion**" ingresando el código de verificación que aparece en la parte superior izquierda de este documento.*

1. INTRODUCCIÓN

La información es el patrimonio principal de toda organización, por lo que se deben aplicar medidas de seguridad para protegerla y estar preparados para afrontar contingencias y desastres de diversos tipos.

Con el fin de orientar y facilitar la toma de decisiones se establece en este documento una serie de disposiciones y responsabilidades, que pretenden otorgar viabilidad y seguridad a la administración de la información en el contexto de la producción de microformas digitales realizada por la Oficina de Atención a la Ciudadanía y Gestión Documentaria del Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles - Senace.

2. OBJETIVO GENERAL

Establecer disposiciones y responsabilidades para que el Senace sea capaz de formalizar y mejorar los servicios de producción de microformas, garantizando la máxima seguridad para la información.

3. ÁMBITO DE APLICACIÒN

El presente documento es aplicable a la producción de microformas digitales. En todo lo no previsto en él, se aplican las reglas generales que cumple el Senace sobre seguridad de la información y tecnología informática.

4. NORMATIVA DE SEGURIDAD DEL SISTEMA DE PRODUCCIÓN DE MICROFORMAS DIGITALES

4.1. La normativa de seguridad del sistema de producción de microformas digitales es formulada y aprobada por los órganos correspondientes del Senace observando las competencias y funciones previstas en el Reglamento de Organización y Funciones vigente y demás documentos normativos pertinentes.

4.2. La normativa de seguridad del sistema de producción de microformas digitales aprobada es difundida entre el personal de la entidad mediante la entrega de un ejemplar en papel o en documento electrónico, de lo cual queda constancia. Asimismo, se capacita al personal cuando se incorpora a la entidad y cada vez que haya una modificación de dichas normas. La evaluación de la comprensión de lo enseñado se realiza mediante exámenes al interior de las sesiones de capacitación y además una vez al año.

4.3. Los cambios al sistema de seguridad de la información deben ser evaluados y aprobados por el Comité de Gestión de Seguridad de la Información del Senace.

4.4. La normativa de seguridad del sistema de producción de microformas digitales es evaluada periódicamente por personal de la entidad o terceros contratados para ese efecto.

5. DISPOSICIONES GENERALES

5.1. La Oficina de Atención a la Ciudadanía y Gestión Documentaria – OAC, ejerce sus funciones de conformidad con lo dispuesto en el Reglamento de Organización y Funciones – ROF del Senace, aporbado por Decreto Supremo N° 009-2017-

*Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: "**https://www.senace.gob.pe/verificacion**" ingresando el código de verificación que aparece en la parte superior izquierda de este documento.*

MINAM. En concordancia con los literales e) y f) del artículo 45 del ROF del Senace, la OAC tiene por función:

"…
e) Conducir y ejecutar las actividades de recepción, registro, despacho, control y seguimiento de la documentación interna y externa.

f) Organizar, conducir y ejecutar las acciones para la gestión de los archivos y centro de documentación del SENACE.
…"

5.2. La Oficina de Tecnologías de la Información - OTI, en el marco de los literales c) y h) del artículo 43 del ROF del Senace, tiene las siguientes funciones:

"…
c) Diseñar, implementar y administrar la infraestructura tecnológica informática y de comunicaciones del SENACE, realizando las mejoras y actualizaciones que correspondan.
…"

"…
h) Administrar la infraestructura de equipos, sistemas, servicios de red, bases de datos y aplicaciones en producción, garantizando su disponibilidad e implementando mecanismos de respaldo y controles de seguridad.
…"

Sin perjuicio de lo mencionado, en lo que respecta a la producción de microformas digitales, los aspectos operativos y el soporte técnico inmediatos están a cargo del Operador Informático de la línea de producción de microformas bajo la supervisión del Supervisor.

5.3. Las medidas de seguridad incluyen el uso de firewall y de firmas digitales. En la línea de producción de microformas la firma digital es aplicada por el depositario de la fe pública (fedatario juramentado con especialización en informática). Si el proceso de producción específico lo requiere, un operador también puede aplicar previamente una firma digital.

5.4. Las personas responsables de la recepción y digitalización de los documentos, así como de la revisión de los documentos electrónicos en medios portadores físicos, guardan reserva absoluta sobre los contenidos de la información que se maneje.

5.5. Las personas responsables de cada proceso de producción de microformas deben vigilar la participación efectiva de los equipos de trabajo en el desarrollo de dicho proceso, la inclusión de los métodos de evaluación, de control y de las pistas de auditoría.

6. DESARROLLO E IMPLEMENTACIÓN DEL SISTEMA DE PRODUCCIÓN DE MICROFORMAS

6.1. En el desarrollo e implementación del sistema de producción de microformas se prevén las medidas de seguridad necesarias para su adecuado desempeño.

*Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: "**https://www.senace.gob.pe/verificacion**" ingresando el código de verificación que aparece en la parte superior izquierda de este documento.*

6.2. El proceso de producción de microformas cuenta con los controles de calidad establecidos en el respectivo manual.

6.3. Una vez concluido el proceso de producción de microformas, se debe emitir el Acta correspondiente con la respectiva conformidad por parte de los intervinientes del proceso.

7. MANTENIMIENTO Y ACTUALIZACIÓN DEL SISTEMA DE PRODUCCIÓN DE MICROFORMAS

7.1. Se debe canalizar las sugerencias y observaciones propuestas por los usuarios a la digitalización y/o indización de las imágenes. Esta actividad constituye un elemento de retro-alimentación que permite medir, buscando reducir la brecha existente entre lo que quieren los usuarios (necesidades de información) y lo que tienen (información proporcionada por los medios portadores).

7.2. Con la finalidad de proporcionar un servicio personalizado y ágil, se comunicará a los usuarios la relación de personas responsables de su atención, así como el medio para contactarlos.

7.3. Finalmente, se llevará un registro detallado de las correcciones y actualizaciones solicitadas por los usuarios, con el fin de tomar las acciones correctivas.

8. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL SISTEMA DE PRODUCCIÓN DE MICROFORMAS

8.1. Los usuarios deberán proporcionar las facilidades necesarias al momento de producirse una auditoría.

8.2. Los responsables de cada proceso de producción de microformas, deben mantener respaldos (backups) actualizados de los archivos, con el propósito de asegurar la continuidad de su trabajo.

8.3. El backup de la información se realizará de manera diaria en la computadora destinada para el Backup. Así mismo, de manera semanal en los medios que defina la OTI.

8.4. Los usuarios deberán tener agrupados y almacenados todos los documentos y archivos lógicos. Si el Supervisor lo cree conveniente, dispone que los usuarios copien su información a una unidad lógica en la red, o inclusive almacenen sus archivos y documentos en dicha unidad.

8.5. Los sistemas de producción de microformas deben contar con mecanismos que aseguren que los datos a procesar cumplan con los requerimientos establecidos y la información se distribuya adecuadamente, así como garantizar que únicamente el personal autorizado tenga acceso al sistema. El compartir la clave de acceso a un sistema se considera falta grave. El usuario es responsable de mantener secreta su clave de acceso.

8.6. Es de responsabilidad exclusiva de los usuarios el ejecutar los archivos de actualización de antivirus que sean indicados por el Operador Informático o por la OTI en el momento mismo en que sean notificados de la necesidad de la ejecución de dicha actualización.

*Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: "**https://www.senace.gob.pe/verificacion**" ingresando el código de verificación que aparece en la parte superior izquierda de este documento.*

8.7. El uso del correo electrónico (no público o gratuito) debe ser destinado sólo para fines laborales, es decir de acuerdo con las funciones propias del usuario.

8.8. En caso de recibir un correo de un destinatario no frecuente o desconocido, con el asunto vago, en un idioma diferente al nuestro o características que susciten desconfianza respecto de la procedencia o motivo del mismo, se deberá proceder a eliminar dicho correo de la Bandeja de Entrada y posteriormente de Elementos Eliminados.

8.9. Todo archivo que sea bajado de Internet deberá ser examinado por el antivirus antes de su ejecución; las consecuencias de la ejecución del archivo son responsabilidad únicamente del usuario. Está totalmente prohibido el download o el bajar desde Internet programas freeware, shareware, trial, o de cualquier otro tipo de distribución.

8.10. Es responsabilidad del usuario cumplir y acatar todas las normas descritas en este numeral 8, referente a la Gestión de Seguridad de la Información en el Sistema de Producción de Microformas.

9. RECURSOS HUMANOS

9.1. Respecto a los recursos humanos, se siguen las disposiciones de la sección A.7 “Seguridad de los recursos humanos” de la tabla A.1 “Objetivos de Control y controles” del Anexo A de la NTP ISO/IEC 27001:2014, en los aspectos y modo mencionados en los numerales 9.2 a 9.5 del presente documento.

9.2. Todo el personal, antes de prestar servicios en la entidad, firma una declaración jurada que le obliga a mantener una conducta que asegure la integridad y confidencialidad de la información a la cual accede. Sin perjuicio de ello, una declaración en tal sentido se incluye en el texto de los contratos de servicio del personal.

9.3. El personal que opera el sistema de producción de microformas y los sistemas informáticos en general, es capacitado en lo referido a sus responsabilidades y demás temas de seguridad que le permitan minimizar los riesgos asociados con el manejo de la información. La OAC dispone las coordinaciones y demás medidas necesarias para tal capacitación, la misma que incluye la capacitación correctiva luego de producida alguna contingencia.

9.4. En caso de un evento o incidencia que comprometa la seguridad de la información y que sea imputable a un integrante del personal, se observará el procedimiento disciplinario establecido en la legislación laboral vigente o en el contrato de prestación de servicios correspondiente.

9.5. El Supervisor toma las medidas necesarias para que al cese de la prestación del servicio por parte de un servidor o proveedor, éstos devuelvan a la entidad el hardware, software, claves, información y demás activos que hubieren recibido de ella. También dispone lo necesario para que se retiren los derechos de acceso a la red informática.

10. SEGURIDAD FÍSICA Y DEL ENTORNO

10.1. Respecto a la seguridad física y del entorno, se siguen las disposiciones de la sección A.11 “Seguridad física y ambiental” de la tabla A.1 “Objetivos de Control y

*Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: “**https://www.senace.gob.pe/verificacion**” ingresando el código de verificación que aparece en la parte superior izquierda de este documento.*

controles” del Anexo A de la NTP ISO/IEC 27001:2014, en los aspectos y modo mencionados en los numerales 10.2 a 10.3 del presente documento.

10.2. Las áreas seguras de procesamiento de la información en la línea central de producción de microformas están ubicadas en el inmueble ocupado por la entidad sito en Av. Ernesto Diez Canseco N° 351, Miraflores, ciudad de Lima y están construidas de material idóneo. El acceso al área está protegido. El acceso al inmueble está protegido con puerta externa, guardianía y puerta de acceso interna con cerradura biométrica. El local cuenta con señalización y extinguidor de incendios.

10.3. Se debe gestionar las autorizaciones de ingreso en base a un listado visado por la OAC que menciona a las personas con permisos de acceso. Asimismo, se debe contar con un registro de ingreso de visitas a cargo del Supervisor.

10.4. Para la seguridad de los equipos del sistema de producción de microformas, se sitúan los mismos en un lugar alejado de la zona de ingreso a las oficinas de la entidad. Dichos equipos están conectados a una red eléctrica estabilizada que los protege contra fluctuaciones del suministro eléctrico. El Supervisor vela por su oportuno mantenimiento. Se prohíbe comer, beber y fumar cerca de los equipos. Sólo la OTI autoriza el uso de equipos fuera del local de la entidad, en cuyo caso el lugar del uso debe contar con medidas de seguridad contra acceso no autorizado.

10.5. Todo el personal de la línea de producción de microformas deberá portar en todo momento su identificación en un lugar visible.

10.6. El cableado eléctrico y de datos está separado y protegido por canaletas de pared o piso según corresponda.

11. GESTIÓN DE COMUNICACIONES Y OPERACIONES

11.1. Respecto a la gestión de comunicaciones y operaciones, se siguen las disposiciones de las secciones A.12 “Seguridad de las operaciones” y A.13 “Seguridad de las comunicaciones” de la tabla A.1 “Objetivos de Control y controles” del Anexo A de la NTP ISO/IEC 27001:2014, en los aspectos y modo mencionados en los numerales 8 y 11.2 a 11.5 del presente documento.

11.2. Para la protección contra software malicioso, se usa software antivirus de conformidad con lo indicado en los numerales 8.6, 8.9 y se aplican las restricciones en la instalación y uso del software según lo indicado en los numerales 13.1 y 14 del presente documento.

11.3. Para gestionar el respaldo y recuperación, se realizan copias de respaldo, de conformidad con lo indicado en los numerales 8.2 y 8.3 del presente documento.

11.4. Para gestionar la seguridad de las redes, se hace uso de equipos de seguridad informática configurados apropiadamente.

11.5. Para gestionar el correo electrónico, se siguen las disposiciones de los numerales 8.7 y 8.8 del presente documento.

12. CONTROL DE ACCESOS

*Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: “**https://www.senace.gob.pe/verificacion**” ingresando el código de verificación que aparece en la parte superior izquierda de este documento.*

12.1. Respecto al control de accesos, se siguen las disposiciones de la sección A.9 “Control de acceso” de la tabla A.1 “Objetivos de Control y controles” del Anexo A de la NTP ISO/IEC 27001:2014, en los aspectos y modo mencionados en el numeral 12.2 del presente documento.

12.2. Para controlar el acceso a la información y a los procesos, se utilizan claves de acceso conforme a lo dispuesto en los numerales 8.5 y 13, se registran los usuarios y se les asigna privilegios según los numerales 14.2, 14.3, y 15.2 del presente documento.

13. UTILIZACIÓN DE CLAVES DE ACCESO

13.1. La utilización de claves secretas constituye un mecanismo de seguridad lógica relacionado con la protección de los sistemas computarizados.

13.2. A través de solicitudes de clave de acceso formuladas al administrador del sistema informático se establecen restricciones de acceso a los archivos y programas, para evitar que personas no autorizadas puedan violar la confidencialidad de la información o realizar actos no deseados que impidan la continuidad del proceso.

13.3. Los usuarios de la red local deberán tener en consideración los siguientes lineamientos que deberán aplicar en el manejo de claves secretas:

13.3.1. Las claves de acceso son de manejo exclusivo y confidencial del usuario, no debiendo ser comunicadas a otras personas. Todas las transacciones registradas con su clave de acceso serán de su exclusiva responsabilidad.

13.3.2. El usuario deberá evitar abandonar su computador dejando activa su clave de acceso. Al menos debe usar un protector de pantalla.

13.3.3. Cuando un usuario con acceso al sistema o a los recursos de red se ausente por motivo de vacaciones, enfermedad o permiso por un periodo mayor a 5 días, deberá comunicar este hecho al Supervisor dentro de las 24 horas siguientes de ocurrido el hecho, vía correo electrónico para realizar el bloqueo de su clave de acceso, la que será restituida a su retorno.

13.3.4. Para el caso de cese o ingreso de un nuevo personal, también se debe comunicar el hecho dentro de las 24 horas siguientes con la finalidad de desactivar o activar un usuario.

13.4. Los usuarios de la red deberán tomar en cuenta las siguientes consideraciones para el manejo de clave de accesos:

13.4.1. La longitud mínima de clave de acceso no debe ser menor a 10 caracteres alfanuméricos.

13.4.2. Al escoger una clave de acceso, el usuario deberá evitar asociaciones obvias, como nombres de familiares y/o mascotas, números telefónicos, PIN de tarjeta de crédito, marca de su auto, sea en orden directo (directo) o inverso (osrevni).

13.4.3. Evitar anotar la clave de acceso en medios visibles.

*Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: “**https://www.senace.gob.pe/verificacion**” ingresando el código de verificación que aparece en la parte superior izquierda de este documento.*

14. DIRECTORIOS COMPARTIDOS

14.1. Está prohibido que cualquier usuario haga uso de software ajeno a la entidad con el fin de acceder a información no autorizada. Este hecho será considerado como falta grave, siendo sujeto a sanción.

14.2. Toda información de uso de la línea de producción de microformas debe ser almacenada en los recursos compartidos que cada usuario tiene a su disposición en el servidor, salvo aquella de carácter confidencial, la cual puede almacenarse localmente con su respectiva clave de acceso.

14.3. Los permisos y usos de los recursos compartidos, son coordinados con el Supervisor.

15. SOFTWARE UTILIZADO

15.1. Está prohibido instalar software no licenciado. En consecuencia, no se deben instalar programas que no sean originales o que no cuenten con su correspondiente licencia de uso. El operador informático o el personal de la OTI, debidamente autorizados por el Supervisor, son las únicas personas que pueden instalar software de cualquier tipo en las computadoras: desktops, laptops, notebooks, servidor.

15.2. El software que el usuario debe utilizar en la computadora que tiene asignada ha sido definido en función del análisis de las actividades que desempeña. El usuario es responsable del software instalado en la PC que tiene asignada. No todos los usuarios pueden llegar a tener el mismo software instalado en sus computadoras.

15.3. Se realizarán auditorías internas periódica y aleatoriamente, para garantizar que sólo se esté utilizando el software designado. De encontrar algo no autorizado (ya sea software original o pirata), será considerado como falta grave.

16. ACTUALIZACIÓN DE EQUIPOS

16.1. Para realizar la actualización de un equipo de cómputo, el Supervisor elaborará un informe dirigido a la OAC explicando las mejoras necesarias, tomando en cuenta la prioridad y el impacto en el servicio al cliente interno y externo.

16.2. Para la adquisición de equipos, la OAC realiza las gestiones de planificación y asignación de presupuesto en coordinación con la Oficina de Tecnologías de la Información y la Oficina de Planeamiento y Presupuesto, en el marco de su competencia.

16.3. La adquisición de repuestos o componentes necesarios para el proceso de actualización y reparación requiere la autorización de la OAC.

16.4. Finalizada la actualización de los equipos, el Supervisor debe informar los cambios y/o reemplazos de equipos y/o componentes al órgano encargado de la contabilidad (activos) para su revalorización.

*Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: "**https://www.senace.gob.pe/verificacion**" ingresando el código de verificación que aparece en la parte superior izquierda de este documento.*

17. PLAN DE CONTIGENCIA

El Plan de Contingencia permite salvaguardar la información y la integridad de los datos digitalizados y/o medios portadores frente a cualquier eventualidad, así como recuperar los servicios tecnológicos en el menor tiempo posible. Se desarrolla en concordancia al Plan de Continuidad Operativa del Senace.

18. CONTROL DE CAMBIOS DEL DOCUMENTO

VERSIÓN ANTERIOR		VERSIÓN ACTUAL	
Número, capítulo o ítem del párrafo	Descripción del número, capítulo o ítem del párrafo	Descripción del cambio efectuado	Motivo del cambio efectuado
No aplica.			

*Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: "**https://www.senace.gob.pe/verificacion**" ingresando el código de verificación que aparece en la parte superior izquierda de este documento.*

ANEXO I

INFORMACIÓN SOBRE LAS FIRMAS DIGITALES EN LA PRODUCCIÓN DE MICROFORMAS DIGITALES

1. FINALIDAD

El presente documento es de aplicación al Sistema de Producción de Microformas Digitales - SPMD del Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles – Senace y tiene por finalidad dar cumplimiento a las exigencias de documentación que los siguientes numerales de la NTP 392.030-2: 2015 establecen respecto de la tecnología de firma digital usada en el Sistema de Producción de Microformas:

NTP 392.030-2: 2015:

- Numeral 6.3.3:

  "6.3.3 Cuando en la línea de producción de microformas se determine el uso de las firmas electrónicas o digitales se debe documentar la manera en la que la organización aplica y cumple las disposiciones legales y reglamentarias vigentes".

- Numeral 6.7.6:

  "6.7.6 Para el caso del software utilizado en la aplicación de la firma digital la organización debe adoptar las medidas y controles contra software malicioso especificadas en la NTP ISO/IEC 17799, NTP-ISO/IEC 27002:2017 o ISO/IEC 27002, permitir la autenticación aplicando el modelo especificado en la norma ISO/IEC 9798-1, registrar la fecha y hora referida al Tiempo Universal Coordinado (UTC) y permitir asegurar el no repudio aplicando el mecanismo especificado en la norma ISO/IEC 13888-3".

El presente documento complementa las disposiciones que sobre la materia estén incluidas en los documentos normativos sobre aspectos de seguridad de la información que aplica Senace.

Para el mejor cumplimiento de las citadas disposiciones, se recomienda que:

a. La línea de producción de microformas, a través de la Oficina de Atención a la Ciudadanía y Gestión Documentaria – OAC, coordine con la Oficina de Asesoría Jurídica para mantener actualizados los requisitos legales de aplicación de la firma digital.
b. La OAC coordine con la Oficina de Tecnologías de la Información para abordar los detalles tecnológicos operativos y la comprensión de los estándares.
c. Antes de la etapa de aplicación de firma digital por el depositario de la fe pública en el proceso de producción de microformas, se consulte el Registro Nacional de Fedatarios Juramentados con Especialización en Informática[1],

[1] También llamados Fedatarios Informáticos.

*Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: "**https://www.senace.gob.pe/verificacion**" ingresando el código de verificación que aparece en la parte superior izquierda de este documento.*

disponible en el sitio web del Ministerio de Justicia, para verificar la vigencia de su certificado de idoneidad técnica.

d. Antes de la etapa de aplicación de firma digital por el depositario de la fe pública en el proceso de producción de microformas, se verifique que su certificado digital y el software de firma digital estén considerados dentro de la Infraestructura Oficial de Firma Electrónica IOFE. Al efecto, consultar la Trusted Service List "Registro Oficial de Prestadores de Servicio de Certificación" (ROPS) disponible en el sitio web de la autoridad administrativa competente en la materia (INDECOPI).
e. Se verifique que las funcionalidades del hardware y software de firma digital se adecúen a las necesidades de producción específicas del Senace.

2. APLICACIÓN Y CUMPLIMIENTO DE LAS DISPOSICIONES LEGALES Y REGLAMENTARIAS SOBRE FIRMA DIGITAL, Y DISPONIBILIDAD DE LOS CERTIFICADOS DIGITALES

El presente apartado tiene por finalidad dar cumplimiento a la exigencia de documentación establecida en el numeral 6.3.3 de la NTP 392.030-2-2015 sobre producción de microformas.

2.1. Aplicación y cumplimiento de las disposiciones legales y reglamentarias

A fin de cumplir lo establecido con la Ley N° 27269, Ley de firmas y certificados digitales y su Reglamento aprobado con Decreto Supremo N° 052-2008-JUS, Senace contempla el uso de certificados digitales basados en tecnología PKI, emitidos a nombre de los fedatarios informáticos con quienes trabaja, y que permiten a éstos aplicar sus firmas digitales a los documentos electrónicos.

En tal sentido, la entidad exige a todo fedatario informático contar con un certificado digital para la aplicación de su firma digital en los documentos que sean pertinentes (de acuerdo a la NTP 392.030-2-2015).

2.2. Relación de certificados digitales vigentes

Los certificados con que se cuenta actualmente se detallan en el siguiente cuadro:

Proveedor: Zytrust		
Emitido por: WISeKey Certify ID Advanced Services CA 4		**Versión:** V3
Titular del Certificado	**Vigencia**	**Número de Serie**
Fedatario Informático Henry Suárez Marquina	Del 06-12-2017 al 06-12-2018	2a df 96 3b 00 00 00 00 1b 55

Proveedor: Zytrust		
Emitido por: WISeKey Certify ID Advanced Services CA 4		**Versión:** V3
Titular del Certificado	**Vigencia**	**Número de Serie**
Fedataria Informática María Victoria Navarro Crespo	Del 02-10-2017 al 02-10-2018	3b hr 81 4c 00 00 00 00 1b 79

*Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: "**https://www.senace.gob.pe/verificacion**" ingresando el código de verificación que aparece en la parte superior izquierda de este documento.*

La aplicación de la firma digital como parte del proceso de producción de microformas corresponde a los fedatarios informáticos titulares de los mencionados certificados digitales detallados en los cuadros precedentes. El Senace puede contratar a fedatarios informáticos distintos a los mencionados, los cuales igualmente deben ser titulares de certificados digitales vigentes.

La actualización de los certificados digitales de los fedatarios informáticos es de cuenta y responsabilidad exclusiva de estos últimos. Al efecto, siguen el procedimiento de renovación o de emisión de nuevo certificado establecido por la entidad de certificación con la cual contraten.

3. ESPECIFICACIONES PARA EL CASO DEL SOFTWARE DE FIRMA DIGITAL

El presente apartado tiene por finalidad documentar la manera en que se cumplen las especificaciones para el caso del software utilizado en la aplicación de la firma digital, establecidas en el punto 6.7.6 de la NTP 392.030-2-2015 sobre producción de microformas.

3.1. Protección contra software malicioso

Como medida de protección contra la injerencia de cualquier software malicioso en la red, la entidad cuenta con un sistema de seguridad o “firewall” para impedir el acceso no autorizado hacia o desde una red privada conectada a Internet.

Así mismo, cada computadora se encuentra debidamente protegida por software antivirus diariamente actualizado, así como con el uso de claves para salvaguardar la información contenida dentro de cada PC. El sistema operativo está configurado para impedir la instalación de software no autorizado.

A nivel de hardware, los puertos USB de las PC se encuentran deshabilitados. La excepción es la PC destinada para la aplicación de la firma digital del fedatario informático, a fin de posibilitarle el uso del token que contiene su certificado digital y clave privada.

3.2. Posibilidad de autenticación

En la actividad de firma digital, la autenticación del firmante se produce primero al conectarse vía internet con la entidad de certificación que emitió el certificado. Mediante el protocolo OCSP (Online Certification Service Provider) se realiza la verificación de la autenticidad y vigencia del certificado digital, lo cual habilita para la aplicación de la firma digital sobre el documento electrónico.

Para la verificación de la autenticidad de documentos electrónicos firmados digitalmente, se ejecuta el software verificador de firma digital, el cual permite comprobar la autenticidad del certificado digital usado y la integridad del documento electrónico.

*Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: “**https://www.senace.gob.pe/verificacion**” ingresando el código de verificación que aparece en la parte superior izquierda de este documento.*

Las funcionalidades descritas son posibilitadas por la tecnología PKI (Public Key Infraestructure) que permite la autenticación de la entidad de certificación emisora de los certificados digitales.

3.3. Registro de hora y fecha referido al tiempo universal coordinado

En la producción de microformas se aplica el sellado de tiempo (Time Stamping) para incorporar en las mismas la información cierta sobre el momento de su producción.

El sellado de tiempo es aplicado complementariamente por el software de firma digital, al incluir en el documento electrónico firmado digitalmente los datos del momento del firmado. Se aplica pues, junto con el acto de aplicación de la firma digital del fedatario informático.

El servicio de Sellado Digital de Tiempo es brindado por un prestador de servicios de valor añadido (TSA -Time Stamping Authority) que dispone de una fuente segura de tiempo sincronizada con la Escala de Tiempo Universal (UTC), y con ella se puede firmar todos aquellos documentos o resúmenes (valores hash) que se envíe.

3.4. Aseguramiento del no repudio

La tecnología PKI que se usa en la producción de microformas permite el aseguramiento del no repudio de los documentos electrónicos firmados digitalmente, mediante mecanismos que usan técnicas de criptografía asimétrica con la intervención de una tercera parte confiable consistente en una autoridad de certificación.

Concretamente, las técnicas asimétricas usadas por la tecnología PKI permiten que la verificación posterior de la identidad del firmante y de la integridad del documento electrónico impida el repudio. En el proceso de producción de microformas esto se comprueba ejecutando el software verificador de firma digital luego de la etapa de aplicación de firma digital por el fedatario informático.

*Esta es una copia auténtica imprimible de un documento electrónico archivado en el Senace, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: "**https://www.senace.gob.pe/verificacion**" ingresando el código de verificación que aparece en la parte superior izquierda de este documento.*