AUTORIDAD NACIONAL DEL SERVICIO CIVIL

MANUAL DE SEGURIDAD DEL SISTEMA DE PRODUCCIÓN DE MICROFORMAS DIGITALES DEL ARCHIVO CENTRAL DE SERVIR

Manual: SJSC-MN-02

Versión: 03

SUBJEFATURA DE SERVICIO AL CIUDADANO

Elaborado por: Julio César Gutiérrez Gómez **Cargo:** Analista de Gestión Documentaria y Archivo **Fecha:**	**Firma:**
Revisado por: Susana Arenas Estela **Cargo:** Sub Jefe de Servicio al Ciudadano **Fecha:**	**Firma:**
Revisado por: Luis Antonio Delgado Alva **Cargo:** Ejecutivo de la Subjefatura de Tecnologías de la Información (e) **Fecha:**	**Firma**
Revisado por: Jesús Hilario Ramos **Cargo:** Especialista en Racionalización **Fecha:**	**Firma:**
Revisado por: Luz Marina Grandez Ibérico De Bejarano **Cargo:** Jefe de la Oficina General de Administración y Finanzas **Fecha:**	**Firma:** Firmado digitalmente por GRANDEZ IBERICO DE BEJARANO Lúz Marina FAU 20477906461 soft Motivo: Soy el autor del documento Fecha: 2020/08/20 17:26:52-0500

ÍNDICE

I. OBJETIVO

Hacer de conocimiento los aspectos de seguridad que debe cumplir el Sistema de Producción de Microformas Digitales (SPMD) para mantener la confidencialidad, integridad y disponibilidad de la información que es convertida a microformas.

II. CAMPO DE APLICACIÓN

El presente documento se aplica en la producción de microformas digitales que se realiza en la Línea de Producción de Microformas Digitales (LPMD) del Archivo Central.

En todo lo no previsto en él, se aplican las reglas generales que cumple el Archivo Central sobre seguridad de la información y tecnología informática.

III. BASE NORMATIVA

3.1. Decreto Legislativo N° 681, que dicta normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la información elaborada en forma convencional cuanto la producida por procedimientos informáticos en computadoras.

3.2. Decreto Legislativo Nº 827, que amplía los alcances del Decreto Legislativo N° 681 a las entidades públicas a fin de modernizar el sistema de archivos oficiales.

3.3. Decreto Supremo N° 009-92-JUS, que aprueba el Reglamento del Decreto Legislativo Nº 681, sobre el uso de tecnologías de avanzada en materia de archivos de las empresas, y sus normas ampliatorias, modificatorias y reglamentarias.

3.4. Resolución Directoral N° 016-2015-INACAL/DN, que aprueba la 3ra. edición de la Norma Técnica Peruana NTP 392.030-2:2015 Microformas. Requisitos para las organizaciones que administran sistemas de producción y almacenamiento. Parte 2: Medios de Archivo Electrónico.

3.5. Resolución Ministerial Nº 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". Resulta aplicable en virtud del numeral 3.1.2 de la NTP 392.030-2:2015.

3.6. Resolución de Presidencia Ejecutiva N° 167-2019-SERVIR-PE, que aprueba la actualización de los documentos normativos del Sistema de Gestión de Seguridad de la Información, entre otros documentos la Política de Seguridad de la Información.

IV. DEFINICIONES

4.1. Archivo

Conjunto de documentos conservados por cualquier técnica, en cualquier medio actualmente conocido o recientemente desarrollado. (Numeral 4.1 del Artículo 4º de la NTP 392.030-2:2015).

4.2. Comité asesor

Está conformado según el numeral 8.3.2 del Manual SJSC-MN-01 del Sistema de producción de microformas digitales. Sus integrantes son personal calificado, según numeral 5.3 de la NTP 392.030-2: 2015. Es designado por el Sub Jefe de Servicio al Ciudadano.

4.3. Depositario de la fe pública

Según el numeral 8.4 del Manual de SJSC-MN-01 El Depositario de la fe pública puede ser uno o más notarios autorizados o fedatarios juramentados con especialización en informática. Deben tener certificado de idoneidad técnica y certificado digital vigente.

4.4. Línea de Producción de Microformas Digitales (LPMD)

Conjunto de procesos, procedimientos y recursos de software y hardware integrados como una unidad de producción para elaborar microformas. (Numeral 4.16 del Artículo 4º de la NTP 392.030-2:2015).

4.5. Microarchivo

Conjunto ordenado, codificado y sistematizado de los elementos materiales de soporte o almacenamiento portadores de microformas grabados, provistos de sistemas de índice y medios de recuperación que permiten encontrar, examinar visualmente y reproducir en copias exactas los documentos almacenados como microformas. (Artículo 1 del Decreto Legislativo N° 681 modificado por el Artículo 1 de la Ley N° 26612).

4.6. Microforma

Un término genérico para cualquier medio que contiene imágenes. (Numeral 4.19 del Artículo 4º de la NTP 392.030-2:2015).

4.7. Serie documental

Es el conjunto de documentos que poseen características comunes, producidos por una unidad de organización en el ejercicio de sus actividades o funciones, regulado por una norma jurídica o procedimiento y que, por consiguiente, son archivados, clasificados, y evaluados como unidad. (IX. Inciso h. Glosario de términos de la Directiva N° 012-2019-AGN/DDPA “Norma para la Valoración Documental en la Entidad Pública”, aprobada por Resolución Jefatural N° 214-2019-AGN/J).

4.8. Sistema informático

Conjunto de elementos relacionados compuesto por uno o más de los procesos, hardware, software, instalaciones y personal que proporcionan la capacidad de satisfacer una necesidad u objetivo definido. (Numeral 4.30 del Artículo 4º de la NTP 392.030-2:2015).

4.9. Supervisor

El Analista en gestión documentaría y archivo de la Subjefatura de Servicio al Ciudadano desempeña el cargo de Supervisor. Dirige el funcionamiento del SPMD y realiza el monitoreo de la Línea de Producción de Microformas.

4.10. Operador

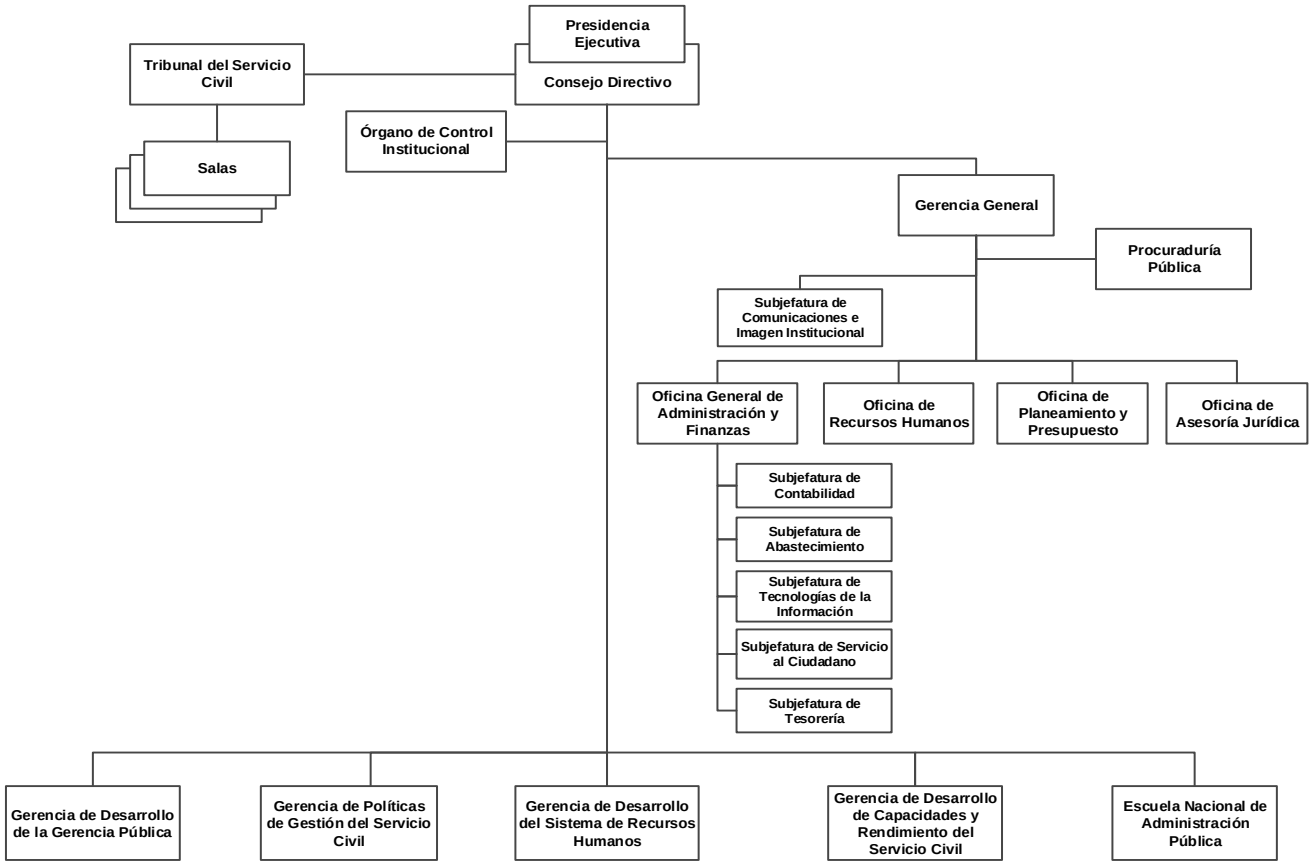
Personal designado por la SJSC para realizar labores operativas en el SPMD.

V. PRESENTACIÓN DE LA ORGANIZACIÓN

SERVIR es el organismo técnico especializado, rector del Sistema Administrativo de Gestión de Recursos Humanos del Estado, creado con el fin de contribuir a la mejora continua de la administración del Estado a través del fortalecimiento del servicio civil. Su existencia, organización y funciones se sujetan a lo establecido en el Decreto Legislativo Nº 1023.

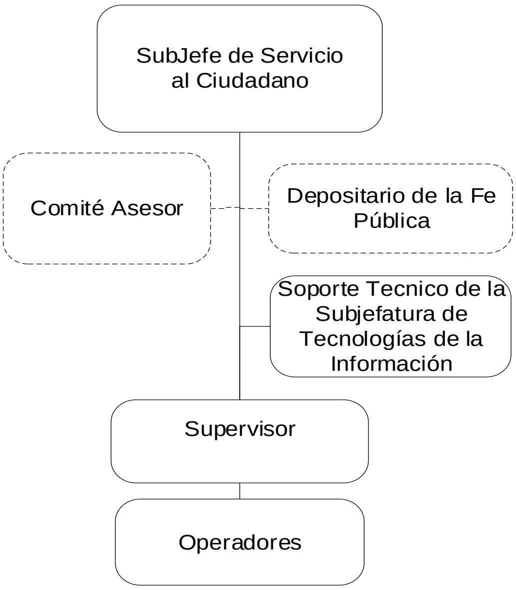
VI. ESTRUCTURA DE LA ORGANIZACIÓN

La estructura organizacional de SERVIR, se muestra en el siguiente organigrama:



VII. ESTRUCTURA DE LA ORGANIZACIÓN DEL SISTEMA

La estructura organizacional específica del SPMD contempla al cargo de Subjefe de Servicio al Ciudadano como autoridad máxima. El siguiente organigrama lo muestra con los demás colaboradores:



VIII. FUNCIONES DE LOS RESPONSABLES DEL SISTEMA

8.1 El Subjefe de Servicio al Ciudadano es responsable de hacer cumplir el presente manual, asegurando su implementación y control respectivo.

8.2 El Supervisor, los operadores designados para el SPMD, el Depositario de la fe pública y el personal de soporte técnico de la Subjefatura de Tecnologías de la Información (SJTI) son responsables de cumplir lo indicado en el presente manual según aplique.

IX. DESCRIPCIÓN GENERAL

9.1. Política de Seguridad de la Información

9.1.1 SERVIR, como ente rector del Sistema Administrativo de Gestión de Recursos Humanos del Estado, reconoce la importancia de la información como activo valioso para sus procesos, por lo tanto, se compromete a preservar su confidencialidad, integridad y disponibilidad mediante la gestión de riesgos, la promoción de una cultura en seguridad de la información, la implementación de infraestructura y tecnología acorde con las necesidades de la Entidad, el cumplimiento del marco legal y regulatorio aplicable a seguridad de la información y mejorar continuamente el Sistema de Gestión de Seguridad de la Información.

9.1.2 La política de seguridad de la información tiene como objetivos:

9.1.1.1. Reducir la probabilidad de materialización de los riesgos de seguridad de la información con el fin de asegurar su confidencialidad, integridad, disponibilidad.

9.1.1.2. Concientizar a todos los servidores civiles sobre la importancia y la comprensión de sus responsabilidades individuales sobre la seguridad de la información.

9.1.1.3. Cumplir con los requisitos legales y regulatorios de seguridad de la información.

9.1.1.4. Evaluar y mejorar el sistema de gestión de seguridad de la información

9.1.3 El Archivo Central de SERVIR protege el activo consistente en la información contenida en las microformas y en los documentos que dieron origen a éstas. Preserva su confidencialidad,

integridad y disponibilidad a fin de ofrecer información confiable a sus usuarios internos, a los ciudadanos y a las entidades públicas.

9.2. Disposiciones Generales

9.2.1 La SJSC ejerce sus funciones de conformidad con lo dispuesto en el Reglamento de Organización y Funciones de SERVIR. En concordancia con tal marco normativo, tiene a su cargo la gestión de los documentos y archivos relacionados a los procedimientos administrativos y servicios que desarrolla SERVIR, correspondiéndole entre otras funciones la gestión del Archivo Central.

9.2.2 La Oficina General de Administración y Finanzas, a través de la SJTI, administra los procesos de seguridad de la información y brinda soporte técnico a los usuarios finales. Asimismo, gestiona la operatividad de los equipos de cómputo, aplicativos informáticos y redes de comunicación de la institución.

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 en coordinación con soporte técnico de la SJSC bajo la supervisión del Supervisor.

9.2.3 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).

9.2.4 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.

9.2.5 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.

9.3. Desarrollo e implementación del Sistema de Producción de Microformas

9.3.1 En el desarrollo e implementación del sistema de producción de microformas se prevén las medidas de seguridad necesarias para su adecuado desempeño, contempladas en la NTP 392.030-2-2015.

9.3.2 El proceso de producción de microformas cuenta con los controles de calidad establecidos en el respectivo manual SJSC-MN-01 Manual del Sistema de Producción de Microformas Digitales del Archivo Central de SERVIR.

9.3.3 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.

9.4. Mantenimiento y actualización del Sistema de Producción de Microformas

9.4.1 Se debe considerar 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 y busca reducir la brecha existente entre lo que quieren los usuarios (necesidades de información) y lo que tienen (información proporcionada por los medios portadores).

9.5. Seguridad de la gestión del Sistema de Producción de Microformas

9.5.1 Los operadores del SPMD deberán proporcionar las facilidades necesarias al momento de producirse una auditoria o evaluación del sistema de producción de microformas.

9.5.2 El backup de la información del SPMD se realiza de manera diaria y está a cargo de la SJTI según lo demanden las necesidades de la producción de microformas. (Procedimiento backup y protección de la información (SJTI-PR-01).

9.5.3 El SPMD debe contar con controles 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.

9.5.4 Es de responsabilidad del soporte técnico de la SJTI mantener los antivirus actualizados.

9.5.5 Todo archivo que sea bajado de Internet deberá ser examinado por el antivirus antes de su ejecución; las consecuencias de ésta (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.

9.5.6 Es responsabilidad del usuario cumplir y acatar todas las normas descritas en este apartado Nº 9.5 referente a la Seguridad de la Gestión del Sistema de Producción de Microformas.

9.6. Recursos humanos

9.6.1 En lo que atañe a los recursos humanos, se siguen las disposiciones de la cláusula A7, seguridad de los recursos Humanos de la NTP ISO/IEC 27001:2014, en los aspectos y modo mencionados en los numerales 9.6.2 a 9.6.5 del presente documento.

9.6.2 Todo el personal, antes de prestar servicios en la institución firma una declaración jurada que le obliga a mantener una conducta que asegure la integridad y confidencialidad de la información a la cual accede.

9.6.3 El personal que opera el SPMD 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 SJSC dispone las coordinaciones y demás medidas necesarias para tal capacitación, la misma que incluye la capacitación correctiva luego de producida alguna contingencia.

9.6.4 En caso de un evento o incidencia que comprometa la seguridad de la información y que sea imputable a un integrante del personal, el supervisor deberá informar en forma inmediata a la autoridad competente.

9.6.5 El Supervisor toma las medidas necesarias para que al cese de la prestación del servicio por parte de un empleado o proveedor, éstos devuelvan a la institución 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.

9.7. Seguridad física y del entorno

9.7.1 En lo que atañe a la seguridad física y del entorno, se siguen las disposiciones de la cláusula A9 Seguridad Física y Ambiental de la NTP ISO/IEC 27001:2014, en los aspectos y modo mencionados en los numerales 8.7.2 a 8.7.6 del presente documento.

9.7.2 La LPMD se encuentra ubicada en el primer piso del inmueble ocupado por el Archivo Central de SERVIR sito en Av. Arequipa N° 934, Cercado de Lima, el cual está construido de material noble. El acceso al área está protegido con paneles de vidrio pavonado y vigilado con cámara de video. El

acceso al inmueble está protegido con reja, puerta externa, guardianía y puerta de acceso interna electrónica biométrica. El local cuenta con señalización y extintor contra incendios.

Asimismo, la LPMD posee una estación remota en la mesa de partes situada en el inmueble ubicado en el pasaje Francisco de Zela N° 150 del distrito de Jesús María, el cual también está construido de material noble. El acceso al área está protegido con paredes de drywall, lunas de atención al público y vigilado con cámara de video. El acceso al inmueble está protegido con reja, puerta externa, guardianía, detector de metales y puerta de acceso interna a la mesa de partes. El local cuenta con señalización y extintor contra incendios.

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

9.7.4 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 institución. 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 Sub Jefatura de Tecnología de la Información autoriza el uso de equipos fuera del local de la institución, en cuyo caso el lugar del uso debe contar con medidas de seguridad contra acceso no autorizado.

9.7.5 Las estaciones de la LPMD, deberán tener rótulos con los datos de los operadores.

9.7.6 El cableado eléctrico y de datos está ordenado y protegido por fundas organizadoras.

9.8. Gestión de comunicaciones y operaciones

9.8.1 En lo que atañe a la gestión de comunicaciones y operaciones, la institución sigue las disposiciones de la cláusula A12 Seguridad de las Operaciones de la NTP ISO/IEC 27001:2014, en los aspectos y modo mencionados en los numerales 8.5 y 8.8.2 a 8.8.5 del presente documento.

9.8.2 Para la protección contra software malicioso, todos los equipos informáticos y dispositivos móviles de propiedad de SERVIR cuentan con la protección de antivirus corporativo el cual se actualiza diariamente de manera automática. Los usuarios a quienes se les ha otorgado un equipo informático están prohibidos de desactivar o desinstalar el software antivirus instalado.

9.8.3 Para gestionar la seguridad de las redes, la SJTI establece los lineamientos en la red informática y asigna un identificador (cuenta) único y exclusivo a toda persona que haga uso de los activos de información ya sea de forma temporal o permanente y que le permita contar con el mínimo acceso autorizado para el normal desarrollo de sus actividades.

9.8.4 Para gestionar el correo electrónico, la SJTI establece los lineamientos para el otorgamiento y buen uso del correo electrónico. Cada usuario es responsable por el contenido de todas las comunicaciones que almacene o envíe utilizando su cuenta de correo electrónico.

9.9. Control de accesos

9.9.1 La SJTI establece los lineamientos para la gestión de accesos en la entidad. Todos los accesos a los activos de información de SERVIR se basan en la necesidad y rol del usuario.

9.9.2 Los responsables de las áreas usuarias son los encargados de autorizar y solicitar el otorgamiento o cancelación de accesos a los recursos de tecnología de información de los usuarios a su cargo mediante solicitud formal a la SJTI.

9.10. Utilización de claves de acceso

9.10.1 La utilización de claves secretas constituye un mecanismo de seguridad lógica relacionado con la protección de los sistemas computarizados. Cada usuario de los sistemas de información de SERVIR debe contar con (i) Identificador o Nombre de usuario: que corresponde a la identidad de la persona y es único dentro de la red y de la aplicación. (ii) Password o contraseña: que debe ser conocido sólo por el usuario.

9.10.2 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.

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

9.10.3.1 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.

9.10.3.2 El operador de la LPMD debe evitar abandonar su computador dejando activa su clave de acceso. Al menos debe usar un protector de pantalla.

9.10.3.3 Cuando un operador 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, debe 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.

9.10.3.4 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.

9.10.4 Los usuarios de la red deben tomar en cuenta las siguientes consideraciones para el manejo de clave de accesos:

9.10.4.1 El usuario debe cambiar su contraseña regularmente o cada vez que el sistema se lo solicite. Está prohibido compartir las contraseñas asignadas.

9.10.4.2 Evitar anotar la clave de acceso en medios visibles.

9.11. Directorios compartidos

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

9.11.2 Toda información de uso de la LPMD 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.

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

9.12. Software utilizado

9.12.1 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 personal de soporte de la Subjefatura de Tecnología de la Información, debidamente autorizados por el

Supervisor, es la única persona que pueden instalar software de cualquier tipo en las computadoras: desktops, laptops, notebooks, servidor.

9.12.2 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.

9.12.3 Se realizan 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.

9.13. Actualización de equipos

9.13.1 Para realizar la actualización de un equipo de cómputo, el Supervisor elabora un informe dirigido al Subjefe de Servicio al Ciudadano explicando las mejoras necesarias, tomando en cuenta la prioridad y el impacto en el servicio al cliente interno y externo.

9.13.2 La adquisición de repuestos o componentes necesarios para el proceso de actualización y reparación, requiere la autorización del Subjefe de Servicio al Ciudadano.

9.13.3 Finalizada la actualización de los equipos, el Supervisor debe informar los cambios y/o reemplazos de equipos y/o componentes al área de Control Patrimonial para su revalorización.

9.14. Plan de contingencia

9.14.1 El Plan de contingencia del SPMD del Archivo Central de SERVIR 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 con la política de seguridad de la entidad.

X. CUADRO DE CONTROL DE CAMBIOS

ITEM	TEXTO VIGENTE	TEXTO ACTUALIZADO	VERSIÓN	FECHA	RESPONSABLE
1	Elaboración inicial del documento	--	1	31/07/19	Subjefatura de Servicio al Ciudadano
2	--	Se actualiza el numeral 8.1 relacionado a la Política y objetivos de seguridad de la información	2	27/01/20	Subjefatura de Servicio al Ciudadano
3	1. Introducción	Se elimina	3	10/08/20	Subjefatura de Servicio al Ciudadano
4	2. Objetivo	I. OBJETIVO	3	10/08/20	Subjefatura de Servicio al Ciudadano
5	3. Alcance	II. CAMPO DE APLICACIÓN	3	10/08/20	Subjefatura de Servicio al Ciudadano
6	4. Definiciones y abreviaturas	IV. DEFINICIONES	3	10/08/20	Subjefatura de Servicio al Ciudadano
7	4.1. NTP	4.1. Archivo	3	10/08/20	Subjefatura de Servicio al Ciudadano
8	4.2. SERVIR	4.2. Comité Asesor	3	10/08/20	Subjefatura de Servicio al Ciudadano
9	4.3. SJSC	4.3. Depositario de la Fe Pública	3	10/08/20	Subjefatura de Servicio al Ciudadano
10	4.4. SPMD	4.4. Línea de Producción de Microformas Digitales (LPMD)	3	10/08/20	Subjefatura de Servicio al Ciudadano
11	4.5. LPMD	4.5. Microarchivo	3	10/08/20	Subjefatura de Servicio al Ciudadano
12	Se agrega	4.6. Microforma, 4.7. Serie documental, 4.8. Sistema informático, 4.9. Supervisor, 4.10. Operador	3	10/08/20	Subjefatura de Servicio al Ciudadano
13	5. Base normativa	III. BASE NORMATIVA	3	10/08/20	Subjefatura de Servicio al Ciudadano

14	5.6. Resolución de Presidencia Ejecutiva Nº 221-2017-SERVIR-PE, que aprueba: i) la Política de Seguridad de la Información, ii) Manual del Sistema de Seguridad de la Información de SERVIR, iii) Manual de Lineamientos de Seguridad de la Información, iv) Procedimiento Inventario, Etiquetado y tratamiento de activos de información del Sistema de Gestión de la Seguridad de la Información; y, v) Procedimiento de identificación, análisis y evaluación de riesgos del Sistema de Gestión de la Seguridad de la Información.	3.6. Resolución de Presidencia Ejecutiva N° 167-2019-SERVIR-PE, que aprueba la actualización de los documentos normativos del Sistema de Gestión de Segur8idad de la Información.	3	10/08/20	Subjefatura de Servicio al Ciudadano
15	6. Referencias	Se elimina	3	10/08/20	Subjefatura de Servicio al Ciudadano
16	Se agrega	V. PRESENTACIÓN DE LA ORGANIZACIÓN	3	10/08/20	Subjefatura de Servicio al Ciudadano
17	Se agrega	VI. ESTRUCTURA DE LA ORGANIZACIÓN	3	10/08/20	Subjefatura de Servicio al Ciudadano
18	Se agrega	VII. ESTRUCTURA DE LA ORGANIZACIÓN DEL SISTEMA	3	10/08/20	Subjefatura de Servicio al Ciudadano
19	7. Responsables	VIII. FUNCIONES DE LOS RESPONSABLES DEL SISTEMA	3	10/08/20	Subjefatura de Servicio al Ciudadano
20	8. Contenido	IX. DESCRIPCIÓN GENERAL	3	10/08/20	Subjefatura de Servicio al Ciudadano
21	8.1. Política de seguridad de la información	En el numeral 9.1 se ordena las ideas reemplazando y agregando textos.	3	10/08/20	Subjefatura de Servicio al Ciudadano