AUTORIDAD NACIONAL DEL SERVICIO CIVIL

MANUAL DE SEGURIDAD DEL SISTEMA DE PRODUCCIÓN DE MICROFORMAS DIGITALES

Manual: TSC-MN-02

Versión: 05

TRIBUNAL DEL SERVICIO CIVIL

Elaborado por: Julio César Alarcón Paredes **Cargo:** Especialista en Gestión Documental y Archivo **Fecha:**	**Firma:**
Revisado por: Luis Antonio Delgado Alva **Cargo:** Especialista en Gestión de Proyectos de Tecnologías de la Información **Fecha:**	**Firma:**
Revisado por: Ana María Risi Quiñones **Cargo:** Secretaria Técnica del Tribunal del Servicio Civil **Fecha:**	**Firma:**
Revisado por: Fidel Flores Loayza **Cargo:** Coordinador de Modernización Institucional **Fecha:**	**Firma:**

Firmado digitalmente por ALARCON PAREDES Julio Cesar FAU 20477906461 soft
Motivo: Soy el autor del documento
Fecha: 2020/11/06 14:30:37-0500

Firmado digitalmente por DELGADO ALVA Luis Antonio FAU 20477906461 soft
Motivo: Soy el autor del documento
Fecha: 2020/11/16 13:36:57-0500

Firmado digitalmente por RISI QUIÑONES Ana Maria FAU 20477906461 hard
Motivo: Soy el autor del documento
Fecha: 2020/11/16 16:20:48-0500

Firmado digitalmente por FLORES LOAYZA Fidel FAU 20477906461 soft
Motivo: Soy el autor del documento
Fecha: 2020/11/11 14:42:15-0500

ÍNDICE

I. INTRODUCCIÓN

El Tribunal del Servicio Civil (TSC) de la Autoridad Nacional del Servicio Civil (SERVIR) requiere utilizar tecnologías avanzadas en materia de archivo de documentos e información, tanto respecto de la elaborada en forma convencional como de la producida por procedimientos informáticos, a fin de posibilitar el adecuado funcionamiento de sistemas de gestión documental que utilicen mecanismos de digitalización, de conformidad con la legislación sobre microformas, conformada principalmente por el Decreto Legislativo 681 y el Decreto Legislativo 827.

Con el fin de atender dicha necesidad, mediante Resolución de Presidencia Ejecutiva N° 004-2018-SERVIR - PE del 19 de enero de 2018 se autorizó la conversión de los documentos recibidos y generados por el TSC de SERVIR al sistema de microarchivos, contemplado en el Decreto Legislativo N° 681 y sus normas complementarias aplicables.

En dicho contexto, a fin de poder realizar la conversión de documentos a microformas, el TSC ha implementado un sistema de producción de microformas digitales, cuyos aspectos de seguridad deben ser documentados en aplicación del numeral 6.8.1 de la Norma Técnica Peruana *NTP* 392.030-2 3ra. Edición, año 2015 *Microformas. Requisitos para las organizaciones que administran sistemas de producción y almacenamiento. Parte 2: Medios de archivo electrónico*.

II. OBJETIVO

Hacer de conocimiento los aspectos de seguridad que debe cumplir el sistema de producción de microformas digitales para mantener la confidencialidad, integridad y disponibilidad de la información que es convertida a microformas.

III. ALCANCE

El presente documento se aplica en la producción de microformas digitales que se realiza en la línea de producción de microformas digitales del TSC.

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

IV. DEFINICIONES Y ABREVIATURAS

4.1. NTP
Norma Técnica Peruana

4.2. SERVIR
Autoridad Nacional del Servicio Civil

4.3. TSC
Tribunal del Servicio Civil

4.4. SPMD
Sistema de Producción de Microformas Digitales

4.5. LPMD
Línea de Producción de Microformas Digitales

V. BASE NORMATIVA

5.1. 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.

5.2. 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.

5.3. 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.

5.4. 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.

5.5. 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.

5.6. Resolución de Presidencia Ejecutiva N.º 004-2018-SERVIR-PE, que autoriza la conversión de los documentos recibidos y generados por el Tribunal del Servicio Civil de la Autoridad Nacional del Servicio Civil al Sistema de Microarchivos.

5.7. 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.

5.8. Resolución de Presidencia Ejecutiva N.º 167-2019-SERVIR-PE, que aprueba la actualización de los documentos normativos del Sistema de Gestión de Seguridad de la Información siguientes: i) Política de Seguridad de la Información de la Autoridad Nacional del Servicio Civil (versión 02), ii) Manual del Sistema de Seguridad de la Información (Código SJTI-MN01, versión 02), iii) Manual de Lineamientos de Seguridad de la Información (Código SJTI-MN02, versión 02).

VI. REFERENCIAS

6.1. TSC-MN-01 Manual del Sistema de Producción de Microformas Digitales

Nota: Los documentos mencionados son los vigentes incluyendo sus modificaciones.

VII. RESPONSABLES

7.1. El Secretario Técnico del TSC es responsable de hacer cumplir el presente manual, asegurando su implementación y control respectivo.

7.2. El Supervisor, los operadores designados para el sistema de producción de microformas digitales, el depositario de la fe pública y el personal de soporte tecnológico de la Sub jefatura de Tecnologías de la Información son responsables de cumplir lo indicado en el presente manual según aplique.

VIII. CONTENIDO

8.1. Política de seguridad de la información

8.1.1. El TSC 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.

8.1.2. La política de seguridad de la información tiene como objetivos:

8.1.2.1. Mantener capacitado al personal del sistema de producción de microformas digitales sobre las buenas prácticas de seguridad de la información (8.3.4 Conciencia, educación y capacitación sobre la seguridad de la información del SJTI-MN-02 Manual Lineamientos de Seguridad de la Información, versión 02).

8.1.2.2. Mitigar los riesgos de incidentes de seguridad de la información (8.3.1.3 SJTI-MN-01 Manual del SGSI versión 02).

8.1.3. La política y medidas de seguridad de la información son difundidos entre el personal mediante su oportuna puesta a disposición. Asimismo, se capacita al respecto al personal cuando se le contrata en la institución y cada vez que haya una modificación de dichas políticas y medidas de seguridad.

8.1.4. La política y medidas de seguridad son evaluados periódicamente por personal interno de la institución o terceros contratados al efecto.

8.2. Disposiciones generales

8.2.1. El TSC ejerce sus funciones de conformidad con lo dispuesto en el Reglamento de Organización y Funciones de SERVIR. En concordancia con tal marco normativo, presta apoyo técnico y administrativo a la Entidad, correspondiéndole entre otras funciones el custodiar las actas y archivos de las sesiones y tramitar la documentación generada y recibida.

8.2.2. La Oficina General de Administración y Finanzas, a través de la Subjefatura de Tecnologías de la Información, 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 del TSC bajo la supervisión del Supervisor.

8.2.3. 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).

8.2.4. 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.

8.2.5. 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.

8.3. Desarrollo e implementación del sistema de producción de microformas

8.3.1. 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.

8.3.2. El proceso de producción de microformas cuenta con los controles de calidad establecidos en el respectivo manual TSC-MN-01 Manual del Sistema de Producción de Microformas Digitales.

8.3.3. 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.

8.4. Mantenimiento y actualización del sistema de producción de microformas

8.4.1. 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).

8.5. Seguridad de la gestión del sistema de producción de microformas

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

8.5.2. El backup de la información del SPMD se realizará de manera diaria y estará a cargo de la Sub jefatura de Tecnologías de la Información según lo demanden las necesidades de la producción de microformas. (Procedimiento Backup y Protección de la Información (SJTI-PR-01)).

8.5.3. El SPMD deben 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.

8.5.4. Es de responsabilidad del soporte técnico de la Sub jefatura de Tecnologías de la Información mantener activos los archivos de actualización antivirus.

8.5.5. 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 establecidas en la DIRECTIVA Nº003-2011-SERVIR/OAF normas para el uso del correo electrónico en la Autoridad Nacional del Servicio Civil - Servir.

8.5.6. 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.

8.5.7. 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.

8.5.8. Es responsabilidad del usuario cumplir y acatar todas las normas descritas en este apartado Nº 8,5 referente a la Seguridad de la Gestión del Sistema de Producción de Microformas.

8.6. Recursos humanos

8.6.1. 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 8.6.2 a 8.6.5 del presente documento.

8.6.2. 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.

8.6.3. 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. El TSC dispone las coordinaciones y demás medidas necesarias para tal capacitación, la misma que incluye la capacitación correctiva luego de producida alguna contingencia.

8.6.4. 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.

8.6.5. 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.

8.7. Seguridad física y del entorno

8.7.1. 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.

8.7.2. La LPMD se encuentra ubicada en el segundo piso del inmueble ocupado por el TSC sito en Jr. Jirón Mariscal Miller N° 1153-1157, Jesús María, ciudad de Lima y su habitación está construida de material idóneo. El acceso al área está protegido. El acceso al inmueble está protegido con puerta externa, guardianía y puerta de acceso interna biométrica. El local cuenta con señalización y extintor contra incendios.

8.7.3. 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.

8.7.4. 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 Subjefatura 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.

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

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

8.8. Gestión de comunicaciones y operaciones

8.8.1. 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 8.8.4 del presente documento.

8.8.2. 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.

8.8.3. Para gestionar la seguridad de las redes, la Sub Jefatura de Tecnologías de la Información 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.

8.8.4. Para gestionar el correo electrónico, la Sub Jefatura de Tecnologías de la Información 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.

8.9. Control de accesos

8.9.1. La Sub Jefatura de Tecnologías de la Información 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.

8.9.2. 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 Sub Jefatura de Tecnologías de la Información.

8.10. Utilización de claves de acceso

8.10.1. 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 deberá 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.

8.10.2. 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.

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

8.10.3.1. 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.

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

8.10.3.3. 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, 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.

8.10.3.4. 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.

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

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

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

8.11. Directorios compartidos

8.11.1. 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.

8.11.2. 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.

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

8.12. Software utilizado

8.12.1. 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 autorizado por el Supervisor, es el único que puede instalar software de cualquier tipo en las computadoras: desktops, laptops, notebooks, servidor.

8.12.2. 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.

8.12.3. 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.

8.13. Actualización de equipos

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

8.13.2. La adquisición de repuestos o componentes necesarios para el proceso de actualización y reparación, requiere la autorización de la Secretaría Técnica del TSC.

8.13.3. 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.

8.14. Plan de contingencia

8.14.1. 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 con la política de seguridad de la entidad.

IX. ANEXOS

No aplica.

X. CUADRO DE CONTROL DE CAMBIOS

ITEM	TEXTO APROBADO EN LA VERSIÓN ANTERIOR	TEXTO ACTUALIZADO	VERSIÓN	FECHA	RESPONSABLE
01	Versión inicial	Elaboración inicial del documento.	01	-----	Tribunal del Servicio Civil
02	---------	Se agrega como numerales 4.4 y 4.5, las definiciones de SPMD y LPMD respectivamente. Se simplifica el manual eliminado textos que no corresponden y precisando las acciones de seguridad (8.2, 8.4, 8.5, 8.6, 8.7).	02	-----	Especialista en Gestión Documental y Archivo
03	---------	Se simplifica el manual, eliminando textos declarativos no relacionados directamente con el sistema de seguridad en la producción de microformas de la LPMD.	03	-----	Especialista en Gestión Documental y Archivo
04	---------	Se actualiza la aprobación del presente documento como referencia a la Norma Técnica N° 001-2018-SGP, Norma Técnica «Implementación de la Gestión por Procesos en las Entidades de la Administración pública», aprobada mediante la RSGP N° 006-2018-PCM-SGP y la Resolución 034-2020-SERVIR-PE, que aprueba la Directiva "Lineamientos para la formulación de documentos de gestión interna de SERVIR".	04	03/07/2020	Especialista en Gestión Documental y Archivo

Firmado digitalmente por ALARCON PAREDES Julio Cesar FAU 20477906461 soft
Motivo: Soy el autor del documento
Fecha: 2020/11/06 14:30:37-0500

Firmado digitalmente por DELGADO ALVA Luis Antonio FAU 20477906461 soft
Motivo: Soy el autor del documento
Fecha: 2020/11/16 13:36:57-0500

Firmado digitalmente por RISI QUIÑONES Ana Maria FAU 20477906461 hard
Motivo: Soy el autor del documento
Fecha: 2020/11/16 16:20:48-0500

Firmado digitalmente por FLORES LOAYZA Fidel FAU 20477906461 soft
Motivo: Soy el autor del documento
Fecha: 2020/11/11 14:42:15-0500

05	---------	En V Base normativa se agrega la referencia a las Resoluciones de Presidencia Ejecutiva 004-2018-SERVIR-PE, que autoriza la conversión de los documentos al sistema de microarchivos y 167-2019-SERVIR-PE que actualiza documentación del Sistema de Gestión de la Seguridad de la Información. En 8.1.2.1 se actualizó la referencia normativa a la versión vigente del Manual SJTI-MN-02 Lineamientos de Seguridad de la Información, versión 02. En 8.1.2.2. se actualizó la referencia normativa a la versión vigente del Manual SJTI-MN-01 Manual del Sistema de Seguridad de la Información, versión 02. En 8.6.4 y 8.6.5 se corrigió la numeración de los párrafos. En 8.7.2. se mejoró la redacción. En 8.8.1: se corrigió la referencia a los numerales del mismo documento. En 8.12.1 se mejoró la redacción.	05		Especialista en Gestión Documental y Archivo

Firmado digitalmente por ALARCON PAREDES Julio Cesar FAU 20477906461 soft
Motivo: Soy el autor del documento
Fecha: 2020/11/06 14:30:37-0500

Firmado digitalmente por DELGADO ALVA Luis Antonio FAU 20477906461 soft
Motivo: Soy el autor del documento
Fecha: 2020/11/16 13:36:57-0500

Firmado digitalmente por RISI QUIÑONES Ana Maria FAU 20477906461 hard
Motivo: Soy el autor del documento
Fecha: 2020/11/16 16:20:48-0500

Firmado digitalmente por FLORES LOAYZA Fidel FAU 20477906461 soft
Motivo: Soy el autor del documento
Fecha: 2020/11/11 14:42:15-0500